I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind propunerea de decizie a Consiliului de instituire a sistemului european de informații cu privire la cazierele judiciare (ECRIS) și de punere în aplicare a articolului 11 din Decizia-cadru 2008/…/JAI

(2009/C 42/01)

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,

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, în special articolul 41,

având în vedere solicitarea de aviz conform articolului 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 trimisă către AEPD la 27 mai 2008,

ADOPTĂ PREZENTUL AVIZ:

I. OBSERVAȚII INTRODUCTIVE

1. La 27 mai 2008, Comisia a adoptat o propunere de decizie a Consiliului de instituire a sistemului european de informații cu privire la cazierele judiciare (ECRIS) și de punere în aplicare a articolului 11 din Decizia-cadru 2008/…/JAI (denumită în continuare: „propunerea") ([1]). Propunerea a fost transmisă de Comisie către AEPD pentru consultare, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001.

2. Propunerea vizează punerea în aplicare a articolului 11 din decizia-cadru a Consiliului privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre ([2]) (denumită în continuare: decizia-cadru a Consiliului) pentru a construi și dezvolta un sistem informatizat de schimb de informații între statele membre ([3]). Astfel cum este prevăzut la articolul 1, aceasta instituie sistemul european de informații cu privire la cazierele judiciare (ECRIS) și stabilește, de asemenea, elementele unui format standardizat pentru schimbul electronic de informații, precum și alte aspecte generale și tehnice de punere în aplicare pentru a organiza și a facilita schimburile de informații.

3. AEPD salută faptul că este consultată și recomandă menționarea acestei consultări în considerentele propunerii, într-un mod similar celui din cadrul altor texte legislative asupra cărora a fost consultată AEPD, în conformitate cu Regulamentul (CE) nr. 45/2001.

II. CADRU ȘI CONTEXT

4. AEPD reamintește că a emis un aviz privind decizia-cadru a Consiliului la 29 mai 2006. Câteva elemente ale acestui aviz care merită reamintite sunt:

— sublinierea importanței unui format standardizat ca mijloc de a înlătura ambiguitatea cu privire la conținutul informațiilor din cazierul judiciar,

([1]) Documentul COM(2008) 332 final.

([2]) Neadoptată încă; ultimul text al propunerii, astfel cum a fost reformulat de Consiliu, este disponibil în registrul public al Consiliului (documentul 5968/08).

([3]) Considerentul 6 al propunerii.

— susținerea alegerilor făcute în cadrul deciziei-cadru a Consiliului de a nu prevedea o bază de date europeană centralizată și de a nu permite accesul direct la bazele de date care ar fi dificil de monitorizat,

— aplicarea Deciziei-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală cu privire la informații extrase din cazierele judiciare, de asemenea în legătură cu transferurile de date cu caracter personal către țările terțe,

— eficiența schimbului de informații în contextul diferențelor semnificative dintre legislațiile naționale privind cazierele judiciare, care necesită dispoziții suplimentare pentru a face ca acesta să funcționeze,

— împărțirea responsabilităților între statele membre și dificultățile care apar în urma acestei împărțiri pentru o monitorizare adecvată. Desemnarea unei autorități centrale la nivel național a fost considerată pozitivă,

— domeniul larg de aplicare a deciziei-cadru a Consiliului care se aplică tuturor condamnărilor care sunt consemnate în cazierul judiciar.

5. Aceste elemente ale avizului din 2006 sunt încă ilustrative pentru contextul în care va fi analizată prezenta propunere. În special, divergența legislațiilor naționale privind cazierele judiciare este determinantă pentru context. Această divergență necesită măsuri suplimentare pentru a face ca sistemul de schimb să funcționeze. În acest sens, propunerea privind ECRIS reprezintă o măsură suplimentară. Cu toate acestea, contextul evoluează de asemenea.

6. În primul rând, decizia-cadru a Consiliului și punerea sa în aplicare în propunerea privind ECRIS constituie un set dintr-o serie de instrumente juridice noi vizând facilitarea schimbului de informații dintre statele membre ale Uniunii Europene în scopul aplicării legii. Toate acestea concretizează principiul disponibilității, astfel cum a fost introdus prin Programul de la Haga din 2004 ([1]). În timp ce majoritatea acestor instrumente se axează pe cooperarea polițienească, acest instrument reprezintă un mijloc de cooperare judiciară în materie penală în sensul articolului 31 din TUE ([2]). Totuși, acesta are același obiectiv: facilitarea schimbului de informații în scopul aplicării legii. În multe cazuri, astfel de instrumente includ sau sunt susținute de sisteme informatizate și/sau de standardizarea practicilor de schimb. În acest sens, propunerea privind ECRIS nu este unică. În evaluarea prezentei propuneri, AEPD beneficiază de experiența din trecut cu instrumente comparabile.

7. În al doilea rând, cadrul juridic al UE pentru protecția datelor evoluează. Adoptarea Deciziei-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală („FDDP"), menționată în considerentul 14 drept cadrul general care se aplică în contextul schimbului informatizat de informații extrase din cazierele judiciare, ar trebui să se facă până la sfârșitul anului 2008. Decizia-cadru a Consiliului va prevede garanții minime pentru protecția datelor, în cazul în care date cu caracter personal sunt sau au fost transmise sau puse la dispoziție între statele membre ([3]). Aceasta va duce la o mai mare convergență a legislațiilor naționale privind condițiile de utilizare a datelor cu caracter personal (în sensul articolului 9 din Decizia-cadru a Consiliului *privind schimbul de informații extrase din cazierele judiciare*).

8. În acest context, ar trebui subliniat faptul că negocierile privind FDDP au dus la anumite modificări, dintre care unele vor afecta în mod specific cadrul juridic în care are loc schimbul de informații extrase din cazierele judiciare:

— limitarea domeniului de aplicare, care se referă în prezent numai la schimbul de date cu caracter personal cu alte state membre și nu se mai aplică datelor prelucrate numai la nivel intern în cadrul unui stat membru,

— nu sunt furnizate niciun fel de mecanisme de coordonare eficientă între autoritățile pentru protecția datelor.

9. În acest context, articolul 9 din Decizia-cadru privind schimbul de informații extrase din cazierele judiciare — care stabilește anumite „condiții de utilizare a datelor cu caracter personal" — trebuie considerat drept *lex specialis* privind protecția datelor, care oferă garanții suplimentare față de cele prevăzute în *lex generalis*, FDDP. Articolul respectiv — în special alineatele (2) și (4) — precizează principiul limitării scopului în ceea ce privește schimbul de informații extrase din cazierele judiciare. Acesta permite excepții de la acest principiu numai în situațiile menționate în mod explicit în acele dispoziții.

10. În al treilea rând, strâns legată de prezenta propunere, Comisia a prezentat o Comunicare privind o strategie europeană în domeniul e-justiției ([4]). Prin această comunicare, Comisia Europeană intenționează să contribuie la consolidarea și dezvoltarea instrumentelor în domeniul e-justiției la nivel european. Comunicarea cuprinde o serie de inițiative cu impact semnificativ asupra protecției datelor cu caracter personal, precum, de exemplu, crearea unei rețele de schimburi securizate pentru schimbul de informații între autoritățile judiciare și crearea unei baze de date europene a traducătorilor și interpreților în domeniul juridic. AEPD intenționează să ofere un răspuns la această comunicare într-un document distinct.

([1]) JO C 53, 3.3.2005, p. 1.

([2]) Schimbul de informații prin intermediul Eurojust reprezintă un alt exemplu. Cadrul juridic pentru acest schimb va fi modificat, după adoptarea unei decizii a Consiliului privind consolidarea Eurojust și de modificare a Deciziei 2002/187/JAI (a se vedea inițiativa publicată în JO C 54, 27.2.2008, p. 4).

([3]) A se vedea articolul 1 din propunerea respectivă de decizie-cadru a Consiliului (ultimul text disponibil în registrul Consiliului, 24 iunie 2008, documentul 9260/08).

([4]) Comunicarea Comisiei către Consiliu, Parlamentul European și Comitetul Economic și Social European — Către o strategie europeană în domeniul e-justiției, documentul COM(2008) 329 final.

III. **SCHIMBUL DE INFORMAȚII PREVĂZUT ÎN DECIZIA-CADRU A CONSILIULUI**

11. Articolul 11 din decizia-cadru a Consiliului descrie ce informații trebuie sau pot fi transmise [la alineatul (1) al acestuia]; acesta prevede, de asemenea, la alineatul (3), temeiul juridic al prezentei propuneri. Anexa II din decizia-cadru a Consiliului prevede un formular care trebuie utilizat pentru schimburi. Acesta include informații care trebuie furnizate de statul membru solicitant și informații care trebuie furnizate ca răspuns la solicitare. Formularul poate fi modificat printr-o decizie a Consiliului, astfel cum propune în prezent Comisia.

12. Articolul 11 alineatul (1) face distincția între informațiile obligatorii, informațiile opționale, informațiile suplimentare și orice alte informații. Formularul din anexa II nu reflectă această distincție. De exemplu, informațiile privind numele părinților persoanei condamnate sunt considerate la articolul 11 drept informații opționale care trebuie transmise numai dacă sunt consemnate în cazierele judiciare. Anexa II nu reflectă caracterul opțional al acestei transmiteri.

13. AEPD propune folosirea acestei ocazii pentru a restructura integral formularul în conformitate cu articolul 11. Aceasta va restrânge transmiterea datelor cu caracter personal la cele care sunt cu adevărat necesare pentru scopul schimbului. În exemplul menționat mai sus, nu pare să fie necesară transmiterea automată a numelor părinților persoanelor condamnate. Transmiterea acestora ar putea aduce, în mod inutil, prejudicii persoanelor în cauză, în special părinților.

IV. **SISTEMUL ECRIS**

Observații generale

14. Articolul 3 constituie partea principală a propunerii. Acesta instituie ECRIS bazat pe o structură descentralizată a tehnologiei informației și care cuprinde trei elemente: baze de date ale cazierelor judiciare din statele membre, o infrastructură comună de comunicații și o aplicație software de interconectare.

15. AEPD susține prezenta propunere de instituire a ECRIS, cu condiția ca observațiile formulate în prezentul aviz să fie luate în considerare.

16. În acest context, AEPD subliniază că, pe de o parte, nicio bază de date centrală europeană nu este stabilită și niciun fel de acces direct la bazele de date ale cazierelor judiciare ale altor state membre nu este prevăzut, în timp ce, pe de altă parte, la nivel național responsabilitățile sunt centralizate pe lângă autoritățile centrale ale statelor membre, desemnate în temeiul articolului 3 din decizia-cadru a Consiliului. Acest mecanism restrânge la maxim stocarea și schimbul datelor cu caracter personal, stabilind în același timp în mod clar responsabilitățile autorităților centrale. În cadrul acestei mecanism, statele membre sunt responsabile de funcționarea bazelor de date naționale ale cazierelor judiciare și de eficiența schimburilor. De asemenea, acestea sunt responsabile de aplicația software de interconectare [articolul 3 alineatul (2) din propunere].

17. Va exista o infrastructură comună. Inițial, aceasta va fi rețeaua S-TESTA ([1]), care poate fi înlocuită cu altă rețea securizată gestionată de Comisie [articolul 3 alineatul (4) din propunere]. AEPD consideră că Comisia este responsabilă de infrastructura comună, deși acest lucru nu este precizat la articolul 3. AEPD propune clarificarea acestei responsabilități în cadrul textului, din motive de siguranță juridică.

Primul element: baze de date ale cazierelor judiciare din statele membre

18. În avizul său din 29 mai 2006, AEPD și-a exprimat sprijinul pentru o structură descentralizată. Printre altele, aceasta evită duplicarea suplimentară a datelor cu caracter personal într-o bază de date centrală. Alegerea unei astfel de structuri descentralizate presupune în mod automat că statele membre sunt responsabile de bazele de date ale cazierelor judiciare și de prelucrarea datelor cu caracter personal în cadrul acestor baze de date. Mai precis, autoritățile centrale ale statelor membre sunt inspectorii acelor baze de date. Acestea sunt, în calitate de inspectori, responsabile de bazele de date și de conținutul schimbului de informații. Decizia-cadru a Consiliului stabilește obligațiile statului membru de condamnare și ale statului membru de cetățenie.

19. În acest cadru, ECRIS reprezintă o rețea de entități omoloage (peer-to-peer) pentru schimbul de informații între aceste baze de date naționale. O rețea de entități omoloage (peer-to-peer) precum ECRIS prezintă anumite riscuri care trebuie abordate.

— în practică, împărțirea responsabilităților între autoritățile centrale ale statelor membre nu funcționează de la sine. Sunt necesare măsuri suplimentare, de exemplu pentru a asigura faptul că informațiile deținute de statul membru expeditor și de statul membru destinatar (statul de condamnare și, respectiv, statul de cetățenie) sunt actualizate și identice,

— această structură implică o mare diversitate în privința modului în care este aplicată de diferitele state membre, care este și mai vizibilă în contextul diferențelor semnificative dintre legislațiile naționale (de exemplu, privind cazierele judiciare).

20. Armonizarea utilizării rețelei și a procedurilor legate de această utilizare este, prin urmare, esențială. AEPD remarcă în mod deosebit importanța utilizării armonizate a rețelei, la înalte standarde de protecție a datelor. Măsurile de punere în aplicare care se adoptă în temeiul articolului 6 din propunere sunt, prin urmare, de o deosebită importanță. AEPD recomandă ca la articolul 6 să se menționeze un înalt nivel de protecție a datelor, ca o condiție prealabilă pentru toate măsurile de punere în aplicare care urmează a fi adoptate.

([1]) Servicii transeuropene de telematică între administrații.

21. Autoritățile naționale de protecție a datelor ar putea juca un rol în acest context, cu condiția ca acestea să își desfășoare activitatea armonizat. AEPD propune includerea unui considerent care să sublinieze rolul autorităților de protecție a datelor, similar modului în care considerentul 11 și articolul 3 alineatul (5) precizează că Comisia asistă statele membre. Noul considerent ar trebui, de asemenea, să încurajeze cooperarea autorităților de protecție a datelor.

22. În cele din urmă, AEPD salută includerea dispoziției de la articolul 3 alineatul (3) prin care este promovată utilizarea celor mai bune tehnici disponibile pentru a asigura confidențialitatea și integritatea datelor din cazierele judiciare transmise altor state membre. Cu toate acestea, ar fi de dorit ca autoritățile competente de protecție a datelor să fie, de asemenea, implicate — împreună cu (autoritățile centrale ale) statelor membre și Comisia — în identificarea acestor tehnici.

Al doilea element: infrastructura comună de comunicații

23. Responsabilitatea Comisiei pentru infrastructura comună de comunicații presupune că aceasta ar trebui văzută ca furnizor al rețelei. În scopul protecției datelor, Comisia poate fi considerată drept inspector în sensul articolului 2 litera (i) din decizia-cadru a Consiliului privind protecția datelor cu caracter personal, deși are competențe limitate: pune la dispoziție rețeaua și asigură securitatea acesteia. În cazul în care datele cu caracter personal sunt prelucrate în contextul punerii la dispoziție a rețelei sau dacă apar probleme de protecția datelor în legătură cu securitatea rețelei, Comisia va răspunde în calitate de inspector. Acest rol al Comisiei este comparabil cu rolul pe care îl are în cadrul sistemelor SIS, VIS și Eurodac, și anume cel al responsabilului de gestionare operațională (și nu de conținut al datelor cu caracter personal). Acest rol a fost calificat drept unul de „inspector *sui generis*" ([1]).

24. Infrastructura comună de comunicații va fi bazată pe S-TESTA, cel puțin pe termen scurt. S-TESTA urmărește interconectarea organismelor UE cu autoritățile naționale, cum ar fi administrații și agenții aflate pe tot cuprinsul Europei. Este o rețea de comunicații dedicată. Centrul serviciului operațional este situat în Bratislava. Acesta reprezintă, de asemenea, baza unor alte sisteme de informații din spațiul de libertate, securitate și justiție, precum Sistemul de informații Schengen. AEPD sprijină opțiunea pentru S-TESTA, care s-a dovedit a fi un sistem fiabil pentru schimburi.

25. Responsabilitatea Comisiei în calitate de inspector „*sui generis*" are, de asemenea, consecințe asupra legii aplicabile în domeniul protecției datelor și asupra supravegherii. Articolul 3 din Regulamentul (CE) nr. 45/2001 dispune că acest regulament „se aplică prelucrării de date cu caracter personal din cadrul tuturor instituțiilor și organelor comunitare în măsura în care această prelucrare este efectuată prin desfășurarea tuturor sau a unei părți a activităților care intră sub incidența dreptului comunitar".

26. Dacă activitățile de prelucrare ale Comisiei ar intra, în totalitate sau în parte, în domeniul de aplicare al dreptului comunitar, nu ar fi niciun dubiu cu privire la aplicabilitatea Regulamentului (CE) nr. 45/2001. În special, articolul 1 al acestui regulament prevede că instituțiile și organismele comunitare protejează drepturile și libertățile fundamentale ale persoanelor fizice, în special dreptul acestora la viață privată în ce privește prelucrarea datelor cu caracter personal. În conformitate cu articolul 22 al acestui regulament, Comisia „pune în aplicare măsurile organizaționale și tehnice adecvate pentru a asigura un nivel de securitate în concordanță cu riscurile reprezentate de către prelucrarea și tipul datelor cu caracter personal care trebuie protejate". Aceste activități se desfășoară sub supravegherea AEPD.

27. Cu toate acestea, până în prezent și contrar Sistemului de informații Schengen ([2]), trebuie să se observe faptul că temeiul juridic al activităților de prelucrare se află în titlul IV al Tratatului UE (al treilea pilon). Aceasta înseamnă că Regulamentul (CE) nr. 45/2001 nu se aplică în mod automat și nici un alt cadru juridic privind protecția datelor și supravegherea nu se aplică activităților de prelucrare ale Comisiei. Această situație este regretabilă pentru motivul evident al lipsei protecției pentru persoana vizată, în special având în vedere caracterul sensibil al prelucrării datelor cu caracter personal referitoare la condamnări penale, astfel cum se menționează la articolul 10 alineatul (5) din Regulamentul (CE) nr. 45/2001 care definește prelucrarea referitoare la condamnări penale ca fiind operații de prelucrare care pot prezenta riscuri specifice. Este cu atât mai regretabil cu cât AEPD este — în temeiul altor instrumente juridice — implicată în supravegherea S-TESTA. Pentru acest motiv, AEPD propune introducerea unei dispoziții în decizie ([3]), care să precizeze că Regulamentul (CE) nr. 45/2001 se aplică prelucrării datelor cu caracter personal sub responsabilitatea Comisiei.

Al treilea element: aplicații software de interconectare

28. Propunerea face distincție între infrastructura tehnică comună pentru conectarea bazelor de date și aplicațiile software de interconectare. După cum s-a menționat, statele membre sunt responsabile de aplicațiile software de interconectare. În conformitate cu considerentul 11, Comisia poate asigura aplicațiile software, dar statele membre par a fi libere să utilizeze sau nu aceste aplicații software în locul propriilor aplicații software de interconectare.

([1]) A se vedea avizul din 19 octombrie 2005 privind trei propuneri referitoare la Sistemul de informații Schengen de a doua generație (SIS II) (JO C 91, 19.4.2006, p. 38, punctul 5.1).

([2]) Și contrar VIS și Eurodac, acestea fiind sisteme ce intră în totalitate în cadrul domeniului de aplicare al dreptului comunitar.

([3]) A se vedea, în acest sens, în cadrul celui de-al treilea pilon, articolul 39 alineatul (6) din Decizia Consiliului privind înființarea Oficiului European de Poliție (Europol), ce prevede aplicarea Regulamentului (CE) nr. 45/2001 în cazul prelucrării datelor cu caracter personal referitoare la personalul Europol (textul din 24 iunie 2008, documentul 8706/08 al Consiliului).

29. Apare întrebarea referitoare la motivele pentru care trebuie să se facă distincție între responsabilitățile pentru infrastructura tehnică și pentru conectarea aplicațiilor software și cele pentru care Comisia ar trebui să aibă una dintre aceste responsabilități sau pe amândouă. Într-adevăr, ambele cazuri implică rețeaua între autoritățile centrale ale statelor membre (punctele naționale de acces la rețea) și nu schimbul de informații în cadrul statelor membre.

30. Acordarea acestei responsabilități suplimentare Comisiei nu ar afecta caracterul descentralizat al arhitecturii tehnologiei informaționale, în timp ce, pe de altă parte, eficiența schimbului ar trebui să fie optimă. Îmbunătățirea eficienței este importantă din perspectiva protecției datelor pentru motive referitoare la calitatea datelor: doar datele esențiale trebuie să fie transmise și nu este nevoie de informații suplimentare din cauza imperfecțiunilor sistemului. Mai mult, s-ar permite o mai bună supraveghere a sistemului dacă responsabilitățile pentru infrastructura comună de comunicații și aplicațiile software de interconectare aparțin aceluiași factor de decizie.

31. Aceasta este și mai importantă având în vedere funcția aplicației software de instrument pentru schimb. Printre caracteristicile importante ale aplicației software de conectare trebuie să fie cea care permite identificarea expeditorului, precum și compatibilitatea și integritatea solicitărilor și, în consecință, permiterea validării solicitărilor. Interoperabilitatea aplicațiilor software utilizate de statele membre este, astfel, o condiție prealabilă. Nu toate statele membre trebuie să utilizeze, în mod obligatoriu, aceeași aplicație software (deși opțiunea aceasta ar fi cea mai practică), dar aplicațiile software trebuie să fie deplin interoperabile.

32. Propunerea recunoaște necesitatea armonizării aspectelor referitoare la aplicațiile software de interconectare. Măsurile de punere în aplicare menționate la articolul 6 — care trebuie adoptate prin procedura de comitologie — includ, de exemplu, „proceduri de verificare a conformității aplicațiilor de software cu specificațiile tehnice". Articolul 6 menționează, de asemenea, un set comun de protocoale. Cu toate acestea, un astfel de set comun de protocoale nu este prevăzut în cazul aplicațiilor software de interconectare. Articolul 6 nu prevede nici identificarea unui sistem software.

33. Având în vedere motivele menționate, pentru a îmbunătăți eficiența și securitatea schimburilor, AEPD recomandă, după cum urmează:

— la un nivel minim, măsurile de punere în aplicare trebuie să fie adoptate cu asigurarea interoperabilității aplicațiilor software,

— ca opțiune preferată, texul ar trebui să oblige Comisia și statele membre — probabil prin procedura de comitologie — să elaboreze sau să identifice un sistem software care să respecte toate cerințele menționate anterior,

— textul ar trebui să menționeze faptul că Comisia răspunde de aplicațiile software de interconectare.

V. ALTE ASPECTE

Manualul

34. Articolul 6 litera (b) precizează că un manual care va fi adoptat prin procedura de comitologie va cuprinde procedura pentru schimbul de informații, „abordând în special modalitățile de identificare a autorilor infracțiunilor". AEPD se întreabă ce va conține, cu exactitate, acest manual și dacă, de exemplu, prevede identificarea prin mijloace biometrice.

35. AEPD subliniază faptul că identificarea autorilor infracțiunilor nu ar trebui să conducă la schimburi de date cu caracter personal care nu sunt prevăzute în mod explicit în decizia-cadru. În plus, manualul ar trebui să prevadă garanții corespunzătoare pentru prelucrarea și transmiterea unor categorii speciale de date, cum sunt datele biometrice.

Colectarea datelor statistice

36. Articolul 6 litera (c) și articolul 8 menționează colectarea datelor statistice, care reprezintă un element-cheie nu numai în ce privește evaluarea eficienței sistemului de schimburi de date, ci și în ce privește supravegherea respectării garanțiilor privind protecția datelor. Pe acest fundal, AEPD recomandă, în conformitate cu alte instrumente juridice privind schimbul de date cu caracter personal ([1]), ca elementele statistice care trebuie colectate să fie definite cu un plus de detaliu și luând în mod corespunzător în considerare necesitatea de a asigura supravegherea protecției datelor. De exemplu, datele statistice ar putea include, în mod explicit, elemente cum ar fi numărul de cereri de acces sau rectificare a datelor cu caracter personal, durata și finalizarea procesului de actualizare, calitatea persoanelor care au acces la aceste date, precum și cazurile de încălcări ale normelor de securitate. Mai mult, datele statistice și rapoartele bazate pe acestea ar trebui să fie puse în întregime la dispoziția autorităților competente de protecție a datelor.

Coordonarea supravegherii prelucrării datelor

37. AEPD a evidențiat deja, în avizul său din 29 mai 2006 privind decizia-cadru privind schimbul de informații extrase din cazierele judiciare, faptul că propunerea nu ar trebui să abordeze doar cooperarea între autoritățile centrale, ci și cooperarea între diferitele autorități competente de protecție a datelor. Această necesitate a devenit și mai importantă din momentul în care negocierile privind FDDP au dus la eliminarea dispoziției care stabilea crearea unui grup de lucru ce reunea autorități de protecție a datelor din UE și coordona activitățile acestora cu privire la prelucrarea datelor în cadrul cooperării polițienești și judiciare în materie penală.

([1]) A se vedea, de exemplu, articolul 3 alineatele (3) și (4) 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.

38. Prin urmare, în vederea asigurării unei supravegheri atât eficiente cât și de bună calitate a circulației transfrontaliere a datelor extrase din cazierele judiciare, ar fi necesară elaborarea unor mecanisme adecvate de coordonare între autoritățile competente de protecție a datelor. Aceste mecanisme ar trebui să ia în considerare, de asemenea, atribuțiile în materie de supraveghere ale AEPD cu privire la infrastructura S-TESTA. Aceste mecanisme ar putea fi incluse fie într-o dispoziție specifică, fie adăugate la măsurile de punere în aplicare care vor fi adoptate în temeiul articolului 6 din propunere.

Traduceri

39. Considerentele 6 și 8, precum și expunerea de motive a Comisiei, menționează utilizarea pe scară largă a traducerii automate. Deși AEPD salută orice măsură menită să îmbunătățească înțelegerea reciprocă a informațiilor transmise, aceasta subliniază, de asemenea, că este important să se definească și să se încadreze în mod clar utilizarea traducerii automate. În fapt, în măsura în care se face o pre-traducere corespunzătoare a categoriilor de infracțiuni menționate în anexa deciziei, utilizarea codurilor comune va permite autorităților naționale să citească traducerea automată a acestor categorii în propria lor limbă. Utilizarea traducerii automate reprezintă un instrument util și acesta poate favoriza înțelegerea reciprocă a încălcărilor cu caracter penal în cauză.

40. Cu toate acestea, utilizarea traducerii automate pentru transmiterea informațiilor care nu au fost pre-traduse în mod corespunzător, cum ar fi observațiile suplimentare sau specificările adăugate în fiecare caz în parte, poate afecta calitatea informațiilor transmise — și, astfel, pe cea a deciziei luate în temeiul acestora — și ar trebui să fie, în principiu, exclusă. AEPD recomandă menționarea acestui aspect în considerentele deciziei Consiliului.

VI. **CONCLUZII**

41. AEPD recomandă menționarea prezentei consultări în considerentele propunerii.

42. Se propune ca această ocazie să fie utilizată pentru restructurarea integrală a formularului în conformitate cu articolul 11 din decizia-cadru a Consiliului privind cazierele judiciare, care face distincție între informațiile obligatorii, informațiile opționale, informațiile suplimentare și orice alt tip de informații.

43. AEPD susține prezenta propunere de instituire a ECRIS, cu condiția ca observațiile formulate în prezentul aviz să fie luate în considerare, inclusiv:

— responsabilitatea Comisiei pentru infrastructura comună de comunicații ar trebui să fie clarificată în text pentru motive de siguranță juridică,

— ar trebui adăugată o dispoziție în decizie care să precizeze că Regulamentul (CE) nr. 45/2001 se aplică prelucrării datelor cu caracter personal sub responsabilitatea Comisiei,

— la articolul 6, ar trebui să se facă o trimitere la un înalt nivel de protecție a datelor, ca o condiție prealabilă pentru toate măsurile de punere în aplicare care urmează a fi adoptate,

— un considerent ar trebui să sublinieze rolul autorităților de protecție a datelor în legătură cu măsurile de punere în aplicare și ar trebui să încurajeze, de asemenea, cooperarea între autoritățile de protecție a datelor,

— măsurile de punere în aplicare trebuie să fie adoptate cu asigurarea interoperabilității aplicațiilor software,

— comisia și statele membre ar trebui să fie obligate — probabil prin procedura de comitologie — să elaboreze sau să identifice un sistem software care să respecte toate cerințele,

— ar trebui să se menționeze în text faptul că Comisia răspunde de aplicațiile software de interconectare.

44. Elementele statistice care urmează a fi colectate ar trebui să fie definite cu un plus de detaliu și luând în mod corespunzător în considerare necesitatea de a asigura supravegherea protecției datelor.

45. Ar trebui elaborate mecanisme corespunzătoare de coordonare între autoritățile competente de protecție a datelor, luând în considerare atribuțiile în materie de supraveghere ale AEPD cu privire la infrastructura S-TESTA.

46. Ar trebui să se specifice în considerentele deciziei Consiliului faptul că utilizarea traducerii automate nu ar trebui să se extindă la transmiterea informațiilor care nu au fost pre-traduse în mod corespunzător.

Adoptat la Bruxelles, 16 septembrie 2008.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor