Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei către Parlamentul European și Consiliu „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor”

(2009/C 276/02)

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,

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

1. La 10 iunie 2009, Comisia a adoptat comunicarea sa către Parlamentul European și Consiliu intitulată „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor” ([1]). În conformitate cu articolul 41 din Regulamentul (CE) nr. 45/2001, AEPD își prezintă avizul.

2. Înainte de adoptarea comunicării, Comisia a consultat în mod informal AEPD cu privire la aceasta, prin intermediul scrisorii din 19 mai 2009. Ca răspuns la această consultare, la 20 mai 2009, AEPD a trimis observații informale menite să aducă alte îmbunătățiri textului comunicării. În plus, AEPD a contribuit în mod activ la scrisoarea din 14 ianuarie 2009 a Grupului de lucru pentru poliție și justiție cu privire la Programul multianual privind spațiul de libertate, securitate și justiție ([2]).

3. Comunicarea (punctul 1) subliniază faptul că Uniunea „trebuie să se doteze cu un nou program multianual care, plecând de la progresele înregistrate și trăgând învățăminte din slăbiciunile actuale, să se proiecteze cu îndrăzneală către viitor. Acest nou program ar trebui să definească priorități pentru următorii cinci ani”. Respectivul program multianual (cunoscut deja sub denumirea de „Programul de la Stockholm”) va continua programele de la Tampere și de la Haga, care au constituit un impuls politic important pentru spațiul de libertate, securitate și justiție.

4. Comunicarea este menită să fie baza acestui nou program multianual. În acest context, AEPD constată că, deși programele multianuale în sine nu sunt instrumente cu un caracter obligatoriu, acestea au un impact considerabil asupra politicii pe care o vor dezvolta instituțiile în zona în cauză, întrucât multe dintre acțiunile concrete, cu și fără caracter legislativ, vor decurge din program.

5. Comunicarea în sine trebuie privită din această perspectivă. Este următorul pas într-o dezbatere care a început, mai mult sau mai puțin, cu două rapoarte prezentate în iunie 2008 de așa-zisele „grupuri privind viitorul” înființate de Președinția Consiliului pentru a furniza idei: „Libertate, securitate, viață privată – Afaceri interne europene într-o lume deschisă” ([3]) și „Soluții propuse pentru Programul Uniunii Europene privind viitorul justiției” ([4]).

II. IDEILE PRINCIPALE ALE AVIZULUI

6. Prezentul aviz reprezintă nu numai o reacție la comunicare, ci și o contribuție a AEPD la dezbaterea mai generală cu privire la viitorul spațiului de libertate, securitate și justiție, care trebuie să ducă la elaborarea unui nou program de lucru strategic (Programul de la Stockholm), după cum a anunțat președinția suedeză a UE ([5]). De asemenea, prezentul aviz va analiza unele consecințe ale posibilei intrări în vigoare a Tratatului de la Lisabona.

7. După ce partea III descrie perspectivele principale ale avizului, partea IV reprezintă o evaluare generală a comunicării.

8. Partea V analizează chestiunea răspunsului la necesitatea respectării în continuare a protecției vieții private și a datelor cu caracter personal într-un context de schimburi tot mai intense de date cu caracter personal. Se va pune accentul pe punctul 2.3 al comunicării cu privire la protecția datelor cu caracter personal și a vieții private și, într-un mod mai general, pe necesitatea unor acțiuni suplimentare, cu și fără caracter legislativ, în vederea îmbunătățirii cadrului pentru protecția datelor.

([1]) COM(2009) 262 final („comunicarea”)

([2]) Nepublicat. Grupul de lucru pentru poliție și justiție (*Working Party on Police and Justice* — WPPJ) a fost instituit în cadrul Conferinței europene a comisarilor pentru protecția datelor pentru a pregăti pozițiile acesteia în domeniul aplicării legii și pentru a acționa în numele acesteia în cazuri de urgență.

([3]) Documentul nr. 11657/08 al Consiliului. Denumit în continuare „raportul privind afacerile interne”.

([4]) Documentul nr. 11549/08 al Consiliului („raportul privind justiția”).

([5]) Programul de lucru al UE prezentat de guverne, http://www.regeringen.se

9. Partea VI discută nevoile și posibilitățile de stocare, acces și schimb de informații ca instrumente de aplicare a legii sau pentru „o Europă care protejează", după cum se precizează în comunicare. Punctul 4 al comunicării cuprinde un număr de obiective privind fluxul de informații și instrumentele tehnologice, în special la punctele 4.1.2 (Controlul fluxului de informații), 4.1.3 (Mobilizarea instrumentelor tehnologice necesare) și 4.2.3.2 (Sistemele de informații). Elaborarea unui model european de informare (punctul 4.1.2), poate fi considerată a fi cea mai provocatoare propunere în acest context. Avizul AEPD examinează această propunere în profunzime.

10. Partea VII abordează pe scurt un subiect specific din domeniile libertății, securității și justiției cu relevanță pentru protecția datelor, și anume accesul la justiție și e-justiție.

III. **PERSPECTIVELE AVIZULUI**

11. Prezentul aviz va analiza comunicarea și, într-un mod mai general, viitorul spațiului de libertate, securitate și justiție, astfel cum a fost conturat de noul program multianual, concentrându-se în mod special pe necesitatea protejării drepturilor fundamentale. În plus, acesta se va baza pe contribuțiile AEPD, în principal în rolul său consultativ, la dezvoltarea politicii UE în domeniu. Până în prezent, AEPD a adoptat peste treizeci de avize și observații cu privire la inițiativele care decurg din Programul de la Haga, care pot fi consultate în totalitate pe site-ul AEPD.

12. În evaluarea comunicării, AEPD va lua în considerare, în special, următoarele patru perspective care sunt relevante pentru viitorul spațiului de libertate, securitate și justiție. Toate aceste perspective joacă un rol-cheie și în comunicare.

13. Prima perspectivă este reprezentată de creșterea exponențială a informațiilor digitale cu privire la cetățeni, ca urmare a evoluției tehnologiilor informației și comunicațiilor ([6]). Societatea se îndreaptă spre ceea ce este adesea numit o „societate de supraveghere", în care fiecare tranzacție și aproape fiecare mișcare a cetățenilor sunt de natură să creeze o înregistrare digitală. Așa-numitele „internet al obiectelor" și „inteligență ambiantă" cunosc deja o evoluție rapidă, prin utilizarea de etichete IDFR. Caracteristicile „digitalizate" ale corpului uman (biometrie) sunt folosite din ce în ce mai mult. Acest lucru duce la o lume tot mai conectată, în care organizațiile de securitate publică pot avea acces la cantități uriașe de informații potențial utile, care pot afecta în mod direct viața persoanelor în cauză.

14. Cea de a doua perspectivă este internaționalizarea. Pe de o parte, în era digitală, schimbul de date nu este limitat de frontierele externe ale Uniunii Europene, în timp ce, pe de altă parte, sporește necesitatea cooperării internaționale în întreaga gamă de activități ale UE în spațiul de libertate, securitate și justiție: lupta împotriva terorismului, cooperarea polițienească și judiciară, justiția civilă și controlul la frontieră sunt doar câteva exemple.

15. Cea de a treia perspectivă se referă la utilizarea datelor în scopul aplicării legii: amenințări recente la adresa societății, în legătură sau nu cu terorismul, au condus la (cereri pentru) mai multe posibilități ale organelor de aplicare a legii de a colecta, stoca și schimba date cu caracter personal. În multe cazuri sunt implicate activ părți private, după cum reiese, printre altele, din directiva privind păstrarea datelor ([7]) și din diversele instrumente referitoare la PNR ([8]).

16. Cea de a patra perspectivă se referă la libera circulație. Pentru dezvoltarea treptată a unui spațiu de libertate, securitate și justiție, este necesar ca frontierele interne și obstacolele posibile în calea liberei circulații în interiorul spațiului să fie eliminate în continuare. În orice caz, noile instrumente în acest domeniu ar trebui să nu restabilească bariere. În contextul actual, libera circulație cuprinde, pe de o parte, libera circulație a persoanelor și, pe de altă parte, libera circulație a datelor (cu caracter personal).

17. Aceste patru perspective demonstrează că informațiile sunt utilizate într-un context care se schimbă rapid. Într-un astfel de context, nu poate exista niciun dubiu cu privire la importanța unui mecanism puternic de protecție a drepturilor fundamentale ale cetățeanului și, în special, a vieții private și a datelor. Tocmai din aceste motive, AEPD își concentrează analiza pe necesitatea protecției, astfel cum se menționează la punctul 11.

([6]) În acest context, raportul privind afacerile interne se referă chiar la un „tsunami digital".

([7]) 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, JO L 105, 13.4.2006, p. 54.

([8]) A se vedea, de exemplu, Acordul între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor din registrul cu numele pasagerilor (PNR), de către transportatorii aerieni, către Departamentul pentru Securitate Internă al Statelor Unite (DHS) (Acordul PNR 2007), JO L 204, 4.8.2007, p. 18 și Propunerea de decizie-cadru a Consiliului privind utilizarea registrului cu numele pasagerilor (PNR) în scopul aplicării legii, COM(2007) 654 final.

IV. EVALUARE GENERALĂ

18. Comunicarea și Programul de la Stockholm urmăresc să specifice intențiile UE pentru următorii cinci ani, cu eventuale efecte pe un termen chiar mai lung. AEPD constată că modul în care a fost redactată comunicarea poate fi caracterizat drept „neutru față de Lisabona". AEPD înțelege pe deplin de ce Comisia a preferat această abordare, dar, în același timp, regretă că această comunicare nu a putut profita la maxim de posibilitățile suplimentare oferite de Tratatul de la Lisabona. Prezentul aviz se va concentra mai mult pe perspectiva Tratatului de la Lisabona.

19. Comunicarea se bazează pe rezultatele acțiunilor pe care UE le-a întreprins în ultimii ani în spațiul de libertate, securitate și justiție. Se poate afirma că aceste rezultate au fost influențate de evenimente, în special în ceea ce privește măsurile de extindere a competențelor de care dispun autoritățile de aplicare a legii, care sunt intruzive pentru cetățean. Acest lucru se întâmplă cu siguranță în domeniile în care datele cu caracter personal se utilizează și se schimbă intensiv și care sunt, în consecință, de o importanță vitală pentru protecția datelor. Rezultatele sunt influențate de evenimente din momentul în care evenimente externe, precum cele din 11 septembrie și atentatele cu bombă de la Madrid și Londra, au impulsionat puternic activitățile legislative. De exemplu, transferul de date privind pasagerii către Statele Unite poate fi considerat o consecință a evenimentelor din 11 septembrie ([9]), în timp ce atentatele cu bombă de la Londra au dus la adoptarea Directivei 2006/24/CE privind păstrarea datelor ([10]). Se punea accentul pe măsuri mai intruzive, întrucât legislatorul UE s-a axat pe măsuri care să faciliteze utilizarea și schimbul de date, în timp ce discutarea măsurilor menite să garanteze protecția datelor cu caracter personal a devenit mai puțin urgentă. Principala măsură de protecție adoptată este Decizia-cadru 2008/977/JAI a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală ([11]), în urma unor dezbateri care au durat trei ani în cadrul Consiliului. Rezultatul a fost o decizie-cadru a Consiliului care nu este pe deplin satisfăcătoare (a se vedea punctele 29-30).

20. Experiența din ultimii ani demonstrează că, înainte de adoptarea unor noi instrumente, este necesar să se reflecteze la consecințele asupra autorităților de aplicare a legii și asupra cetățenilor europeni. 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 revizuiri periodice. De asemenea, această reflecție este esențială înainte ca un nou program multianual să stabilească principalele inițiative pentru viitorul apropiat.

21. AEPD își exprimă satisfacția pentru faptul că protecția drepturilor fundamentale, în special protecția datelor cu caracter personal, este recunoscută în comunicare drept unul dintre aspectele-cheie ale viitorul spațiului de libertate, securitate și justiție. Punctul 2 din comunicare descrie UE ca spațiu unic de protecție a drepturilor fundamentale pe baza unor valori comune. De asemenea, este de apreciat faptul că aderarea la Convenția Europeană a Drepturilor Omului este menționată ca prioritate – chiar constituie prima prioritate în comunicare. Aderarea reprezintă un pas important înainte în asigurarea unui sistem armonios și coerent de protecție a drepturilor fundamentale. În sfârșit, dar nu în ultimul rând, protecției datelor i s-a acordat un loc de frunte în comunicare.

22. Ideile subliniate în comunicare demonstrează intenția fermă de a asigura protecția drepturilor cetățeanului și – prin aceasta – de a avea o abordare mai echilibrată. 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. Pentru a fi în serviciul cetățenilor ([12]), Uniunea Europeană trebuie să protejeze acest echilibru.

23. În opinia AEPD, comunicarea ia foarte bine în considerare necesitatea acestui echilibru, inclusiv necesitatea protecției datelor cu caracter personal. Aceasta recunoaște faptul că este necesar să se pună accentul pe alte aspecte. Acest lucru este important, întrucât politicile referitoare la spațiul de libertate, securitate și justiție nu ar trebui să favorizeze trecerea treptată spre o societate de supraveghere. AEPD se așteaptă ca Consiliul să aibă aceeași abordare în Programul de la Stockholm, inclusiv prin recunoașterea orientărilor enunțate la punctul 25 de mai jos.

24. Acest lucru este cu atât mai important cu cât spațiul de libertate, securitate și justiție este unul care „determină împrejurările vieții cetățenilor, în special spațiul privat al propriei responsabilități și al securității personale și sociale, care este protejat de drepturile fundamentale", după cum a subliniat foarte recent Curtea Constituțională germană în hotărârea din 30 iunie 2009 cu privire la Tratatul de la Lisabona ([13]).

([9]) Acordul PNR 2007, menționat în nota de subsol precedentă, precum și cele care i-au precedat.

([10]) 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, JO L 105, 13.4.2006, p. 54. Deși articolul 95 din TCE constituie temeiul juridic al directivei, aceasta a reprezentat o reacție imediată la atentatele cu bombă de la Londra.

([11]) Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, JO L 350, 30.12.2008, p. 60.

([12]) A se vedea titlul comunicării.

([13]) Comunicat de presă nr. 72/2009 din 30 iunie 2009 al Curții Constituționale Federale a Germaniei, punctul 2 c).

25. AEPD subliniază faptul că, într-un astfel de spațiu:

— Autoritățile din statele membre, inclusiv, după caz, organismele sau bazele de date europene, ar trebui să facă schimb de informații pe baza unor mecanisme adecvate și eficiente, care să respecte pe deplin drepturile fundamentale ale cetățeanului și să asigure încrederea reciprocă.

— Acest lucru necesită nu numai disponibilitatea informațiilor, împreună cu recunoașterea reciprocă a sistemelor juridice ale statelor membre (și al UE), ci și, de asemenea, o armonizare a standardelor de protecție a informațiilor, de exemplu, dar nu numai prin intermediul unui cadru comun de protecție a datelor.

— Aceste standarde comune nu ar trebui să fie aplicabile numai în situații cu dimensiuni transfrontaliere. Încrederea reciprocă poate exista numai în cazul în care standardele sunt solide și sunt întotdeauna respectate, fără a exista riscul ca acestea să nu se aplice în momentul în care dimensiunea transfrontalieră nu este sau nu mai este evidentă. În afara de aceasta, mai ales atunci când este vorba despre utilizarea informațiilor, diferențele dintre datele „interne" și cele „transfrontaliere" nu pot exista în practică ([14]).

V. INSTRUMENTE DE PROTECȚIE A DATELOR

V.1. Către un regim complet de protecție a datelor

26. AEPD susține abordarea strategică conform căreia protecția datelor ocupă un loc important în comunicare. Într-adevăr, multe inițiative cu privire la spațiul de libertate, securitate și justiție se bazează pe utilizarea datelor cu caracter personal, iar protecția corespunzătoare a datelor este crucială pentru succesul acestora. Respectarea vieții private și protecția datelor nu reprezintă numai o obligație legală din ce în ce mai recunoscută la nivelul UE, ci și un aspect de o importanță vitală pentru cetățenii europeni, după cum arată rezultatele Eurobarometrului ([15]). Mai mult, restricționarea accesului la datele cu caracter personal este, de asemenea, esențială pentru asigurarea încrederii de către agențiile de aplicare a legii.

27. Punctul 2.3 din comunicare prevede că este necesar un regim complet de protecție a datelor care să acopere toate domeniile de competență a UE ([16]). AEPD sprijină pe deplin acest obiectiv, indiferent de intrarea în vigoare a Tratatului de la Lisabona. Autoritatea ia act, de asemenea, de faptul că un astfel de regim nu înseamnă neapărat că va exista un cadru juridic unic aplicabil tuturor prelucrărilor. Conform tratatelor actuale, posibilitățile de adoptare a unui cadru juridic cuprinzător care să se aplice tuturor operațiilor de prelucrare a datelor sunt limitate din cauza structurii pe piloni și a faptului că – cel puțin în primul pilon – protecția datelor prelucrate de către instituțiile europene are un temei juridic separat (articolul 286 din TCE). Cu toate acestea, AEPD subliniază că pot fi aduse unele îmbunătățiri prin exploatarea deplină a posibilităților oferite de tratatele în vigoare, după cum a subliniat deja Comisia în comunicarea sa privind „Punerea în aplicare a Programului de la Haga - calea de urmat" ([17]). După intrarea în vigoare a Tratatului de la Lisabona, articolul 16 din TFUE va furniza temeiul juridic necesar pentru un cadru juridic cuprinzător, care să se aplice tuturor prelucrărilor.

28. AEPD constată că este esențial - în orice caz - să se asigure coerența cadrului juridic în ceea ce privește protecția datelor, acolo unde este necesar prin armonizarea și consolidarea diferitelor instrumente juridice aplicabile în spațiul de libertate, securitate și justiție.

În temeiul tratatelor actuale

29. Recent, s-a făcut un prim pas prin adoptarea Deciziei-cadru 2008/977/JAI a Consiliului ([18]). Totuși, acest instrument juridic nu poate fi considerat drept un cadru cuprinzător, în principal deoarece dispozițiile sale nu au aplicabilitate generală. Acestea nu se aplică situațiilor interne, în care datele cu caracter personal provin de la statul membru care le utilizează. O astfel de limitare nu poate decât să diminueze valoarea adăugată a deciziei-cadru a Consiliului, cu excepția cazului în care toate statele membre ar decide să includă situațiile interne în legislația națională de punere în aplicare, ceea ce este improbabil.

30. Un al doilea motiv pentru care AEPD consideră că, pe termen lung, Decizia-cadru 2008/977/JAI a Consiliului nu cuprinde un cadru satisfăcător de protecție a datelor într-un spațiu de libertate, securitate și justiție este acela că mai multe dispoziții esențiale nu sunt conforme cu Directiva 95/46/CE. Conform tratatelor actuale, s-ar putea face un al doilea pas prin extinderea domeniului de aplicare și alinierea deciziei-cadru a Consiliului la Directiva 95/46/CE.

31. Stabilirea unei viziuni clare și pe termen lung ar putea da un nou impuls instituirii unui regim complet de protecție a datelor. Această viziune ar putea să cuprindă o abordare globală și coerentă pentru a defini colectarea și schimburile

([14]) AEPD a elaborat acest ultim punct în Avizul din 19 decembrie 2005 privind propunerea de Decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală [COM(2005) 475 final], JO C 47, 25.2.2006, p. 27, punctele 30-32.

([15]) Protecția datelor în Uniunea Europeană – Percepțiile cetățenilor – Raport analitic, Eurobarometrul Flash Seria 225, ian. 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) A se vedea subiectele prioritare ale comunicării.

([17]) COM(2006) 331 final, 28.6.2006.

([18]) A se vedea nota de subsol nr. 11.

de date – precum și exploatarea bazelor de date existente - și, în același timp, garanțiile de protecție a datelor. Viziunea ar trebui să prevină suprapunerile și duplicările inutile ale instrumentelor (și, astfel, ale prelucrării datelor cu caracter personal). Ar trebui să promoveze, de asemenea, coerența politicilor UE în acest domeniu, precum și încrederea cu privire la modul în care autoritățile publice administrează datele referitoare la cetățeni. AEPD recomandă Consiliului să comunice necesitatea unei viziuni clare și pe termen lung în Programul de la Stockholm.

32. O altă recomandare a AEPD este ca măsurile care au fost deja adoptate în acest domeniu, punerea lor în practică și eficacitatea lor să fie evaluate și plasate în perspectivă. Această evaluare ar trebui să țină seama în mod corespunzător de costurile pentru protecția vieții private și de eficiența aplicării legii. În cazul în care, în urma acestor evaluări, se constată că anumite măsuri nu dau rezultatele scontate sau nu sunt proporționale cu scopurile urmărite, ar trebui să fie luate în considerare următoarele etape:

— Într-o primă etapă, modificarea sau abrogarea măsurilor, în măsura în care acestea nu par a fi suficient de justificate în ceea ce privește generarea de valoare adăugată concretă pentru autoritățile de aplicare a legii și pentru cetățenii europeni;

— În a doua etapă, evaluarea posibilităților de îmbunătățire a aplicării măsurilor existente;

— Abia în a treia etapă, propunerea de noi măsuri legislative, în cazul în care este probabil ca aceste măsuri să fie necesare în scopurile avute în vedere. Ar trebui adoptate noi instrumente numai dacă acestea au o valoare adăugată clară și concretă pentru autoritățile de aplicare a legii și pentru cetățenii europeni.

AEPD recomandă ca Programul de la Stockholm să facă trimitere la un sistem de evaluare a măsurilor existente.

33. Nu în ultimul rând, ar trebui să se pună un accent deosebit pe o mai bună aplicare a măsurilor de siguranță existente, conform comunicării Comisiei cu privire la continuarea Programului de lucru pentru o mai bună punere în aplicare a Directivei privind protecția datelor ([19]) și pe propunerile cuprinse în avizul AEPD cu privire la respectiva comunicare ([20]). Din păcate, în ceea ce privește al treilea pilon, Comisia nu are posibilitatea de a iniția procedurile pentru situațiile de încălcare a dreptului comunitar.

În temeiul Tratatului de la Lisabona

34. Tratatul de la Lisabona oferă posibilitatea unui cadru autentic și cuprinzător de protecție a datelor. În conformitate cu articolul 16.2 din Tratatul privind funcționarea Uniunii Europene, Consiliul și Parlamentul European trebuie să stabilească normele referitoare la protecția datelor de către instituțiile, organismele, birourile și agențiile Uniunii, de către statele membre în exercitarea activităților care intră în domeniul de aplicare a dreptului comunitar, precum și de către părți private.

35. AEPD interpretează faptul că în comunicare se pune accentul pe un regim complet de protecție a datelor ca pe o ambiție a Comisiei de a propune un cadru juridic aplicabil tuturor activităților de prelucrare. AEPD susține în totalitate această ambiție, care sporește coerența sistemului, asigură securitatea juridică și, prin aceasta, îmbunătățește protecția. În special, acest lucru ar evita, în viitor, dificultățile în identificarea unei linii de demarcație între piloni în situațiile în care datele colectate în sectorul privat în scopuri comerciale sunt ulterior utilizate în scopuri de aplicare a legii. Această linie de demarcație între piloni nu reflectă pe deplin realitatea, după cum o demonstrează hotărârile importante ale Curții de Justiție în ceea ce privește PNR ([21]) și păstrarea datelor ([22]).

36. AEPD propune ca Programul de la Stockholm să sublinieze logica unui regim complet de protecție a datelor. Acest lucru arată că un astfel de sistem nu este doar o simplă preferință, ci o necesitate, având în vedere practicile în schimbare în ceea ce privește utilizarea datelor. AEPD recomandă includerea ca prioritate în Programul de la Stockholm a necesității unui nou cadru legislativ care, printre altele, să înlocuiască Decizia-cadru 2008/977/JAI a Consiliului.

37. AEPD subliniază faptul că noțiunea de regim complet de protecție a datelor bazat pe un cadru juridic general nu exclude adoptarea de norme suplimentare în materie de protecție a datelor pentru poliție și sectorul judiciar. Aceste norme suplimentare ar putea lua în considerare nevoile specifice în materie de aplicare a legii, astfel cum se prevede în Declarația 21, anexată la Tratatul de la Lisabona ([23]).

V.2. **Redefinirea principiilor de protecție a datelor**

38. Comunicarea face referire la schimbările tehnologice care transformă modalitățile de comunicare între persoanele fizice și organizațiile publice și private. Potrivit Comisiei, acest lucru necesită redefinirea unui număr de principii de bază referitoare la protecția datelor.

([19]) COM(2007) 87 final, 7 martie 2007

([20]) Avizul din 25 iulie 2007, JO C 255, 27.10.2007, p. 1, în special punctul 30.

([21]) Hotărârea Curții din 30 mai 2006, Parlamentul European/Consiliul Uniunii Europene (C-317/04) și Comisia Comunităților Europene (C-318/04), cauzele conexate C-317/04 și C-318/04, Rec.[2006], p. I-4721.

([22]) Hotărârea Curții din 10 februarie 2009, Irlanda/Parlamentul European și Consiliul Uniunii Europene, cauza C-301/06, nepublicată încă în Repertoriu.

([23]) A se vedea Declarația 21 cu privire la protecția datelor cu caracter personal în domeniul cooperării judiciare în materie penală și al cooperării polițienești, anexată la actul final al conferinței intergovernamentale în cadrul căreia s-a adoptat Tratatul de la Lisabona, JO C 115, 9.5.2008, p. 345.

39. AEPD salută aceste intenții ale comunicării. O evaluare a eficienței acestor principii în perspectiva schimbărilor tehnologice este extrem de utilă. În primul rând, este important de menționat că redefinirea și reafirmarea principiilor de protecție a datelor nu trebuie să aibă întotdeauna o legătură directă cu evoluțiile tehnologice. Evaluarea ar putea fi necesară, de asemenea, în lumina altor perspective, menționate anterior în partea III, precum internaționalizarea, utilizarea tot mai intensă a datelor în scopul aplicării legii și libera circulație.

40. Mai mult, din punctul de vedere al AEPD, această evaluare poate fi unul dintre subiectele consultării publice anunțate de către Comisie, în cadrul Conferinței „Datele cu caracter personal – utilizare mai intensă, o mai bună protecție?" din 19-20 mai 2009. Această consultare publică ar putea furniza idei valoroase ([24]). AEPD propune ca, în textul Programului de la Stockholm elaborat de Consiliu și în declarațiile publice privind consultarea ale Comisiei, să se sublinieze legătura dintre intențiile exprimate în comunicare la punctul 2.3 și consultarea publică privind viitorul protecției datelor.

41. Ca o ilustrare a aspectelor pe care le-ar putea acoperi evaluarea, sunt menționate următoarele:

— Datele cu caracter personal din domeniul libertății, securității și justiției sunt susceptibile de a fi deosebit de sensibile, precum datele referitoare la condamnările penale, datele deținute de poliție și datele biometrice, cum ar fi amprentele digitale si profilurile ADN.

— Prelucrarea acestora ar putea avea consecințe negative asupra persoanelor vizate, în special dacă se iau în considerare competențele coercitive ale autorităților de aplicare a legii. Mai mult, monitorizarea și analiza datelor sunt din ce în ce mai automatizate, destul de des fără intervenție umană. Tehnologia permite utilizarea de baze de date cu date cu caracter personal pentru căutările generale (extragerea datelor, crearea de profiluri etc.). Obligațiile legale care stau la baza prelucrării datelor ar trebui stabilite în mod clar.

— O piatră de temelie a legislației privind protecția datelor este aceea că datele cu caracter personal se colectează în scopuri determinate și nu sunt utilizate într-un mod incompatibil cu aceste scopuri. Utilizarea în scopuri incompatibile ar trebui să fie permisă numai în măsura în care este prevăzută de lege și necesară pentru urmărirea unor interese publice specifice, precum cele prevăzute la articolul 8.2 din CEDO.

— Necesitatea de a respecta principiul limitării scopului ar putea avea consecințe asupra tendințelor actuale în utilizarea datelor. Autoritățile de aplicare a legii utilizează date colectate în scopuri comerciale de către companii private din domenii de activitate precum telecomunicațiile, transportul și sectorul financiar. În plus, sunt elaborate sisteme de informații de mari dimensiuni, de exemplu, în domeniul imigrației și al controlului la frontiere. Mai mult, sunt permise interconexiuni și accesul la bazele de date, scopurile pentru care datele cu caracter personal au fost colectate inițial fiind astfel extinse. Este necesar să se reflecteze asupra acestor tendințe actuale, inclusiv asupra oricăror posibile adaptări și/sau măsuri de siguranță suplimentare, acolo unde este cazul.

— Pe lângă principiile de protecție a datelor menționate în comunicare, evaluarea ar trebui să acorde atenție nevoii de transparență a prelucrării, care să permită ca persoana vizată să își exercite drepturile. Transparența reprezintă o chestiune deosebit de dificilă în domeniul aplicării legii, în special pentru că transparența trebuie să fie pusă în balanță cu riscurile la adresa anchetelor.

— Ar trebui identificate soluții pentru schimburile cu țări terțe.

42. În plus, această evaluare ar trebui să se concentreze pe posibilitățile de îmbunătățire a eficienței în ceea ce privește aplicarea principiilor de protecție a datelor. În acest context, ar putea fi util să se axeze pe instrumentele care pot consolida responsabilitățile operatorilor de date. Conform acestor instrumente, operatorii de date trebuie să aibă răspundere deplină pentru gestionarea datelor. Noțiunea de „guvernanță a datelor" (*data governance*) este utilă în acest context. Aceasta acoperă toate mijloacele juridice, tehnice și organizaționale prin care organizațiile asigură deplina răspundere asupra modului în care sunt prelucrate datele, precum planificarea și controlul, utilizarea tehnologiei sunetului, formarea adecvată a personalului, auditurile de conformitate, etc.

V.3. **Tehnologiile „care respectă viața privată"**

43. AEPD își exprimă satisfacția pentru faptul că punctul 2.3 din comunicare menționează certificarea care să asigure respectarea vieții private. În plus, s-ar putea face referire la „respectarea vieții private din concepție" (*privacy by design*) și la necesitatea de a identifica „cele mai bune tehnici disponibile" care să respecte cadrul UE de protecție a datelor.

44. În opinia AEPD, „respectarea vieții private din concepție" și tehnologiile care respectă viața privată ar putea constitui instrumente utile pentru o mai bună protecție, dar și pentru o utilizare mai eficace a informațiilor. AEPD sugerează două căi de urmat care nu se exclud reciproc:

— Un sistem de certificare care să asigure respectarea vieții private și protecția datelor ([25]) , ca opțiune pentru proiectanții și utilizatorii de sisteme de informații, care să beneficieze sau nu de sprijin din fonduri europene sau prin legislația UE.

([24]) Grupul de lucru al articolului 29 privind protecția datelor, din care face parte și AEPD, a hotărât să își pregătească intensiv contribuția la această consultare publică.

([25]) Un exemplu de asemenea sistem este marca europeană de protecție a vieții private (*EuroPriSe — European Privacy Seal*).

— O obligație legală pentru proiectanții și utilizatorii de sisteme de informații de a utiliza sisteme conforme cu principiul respectării vieții private din concepție. Acest lucru ar putea necesita extinderea domeniului actual de aplicare a legislației privind protecția datelor pentru ca proiectanții să devină responsabili pentru sistemele de informațiile pe care le dezvoltă ([26]).

AEPD propune să se menționeze aceste posibile căi de urmat în Programul de la Stockholm.

V.4. **Aspecte externe**

45. Un alt subiect menționat în comunicare este elaborarea și promovarea de standarde internaționale pentru protecția datelor. In prezent se desfășoară multe activități menite să stabilească standarde fezabile aplicabile la nivel mondial, precum, de exemplu, Conferința internațională a comisarilor pentru protecția datelor și viață privată. În viitorul apropiat, acest lucru ar putea duce la un acord internațional. AEPD propune ca Programul de la Stockholm să sprijine aceste activități.

46. Comunicarea menționează, de asemenea, încheierea de acorduri bilaterale, având în vedere progresele deja înregistrate cu Statele Unite ale Americii. AEPD resimte, de asemenea, necesitatea unui cadru juridic clar pentru transferul de date către țări terțe, motiv pentru care a salutat lucrările desfășurate în comun de către UE și autoritățile SUA în cadrul Grupului de contact la nivel înalt privind un posibil instrument transatlantic de protecție a datelor, făcând în același timp un apel la mai multă claritate și atenție la chestiuni specifice ([27]). Din această perspectivă este, de asemenea, interesant să se menționeze ideile incluse în Raportul privind afacerile interne pentru un spațiu euroatlantic de cooperare în domeniul libertății, securității și justiției asupra căruia, potrivit acestui raport, UE ar trebui să se decidă până în 2014. Un astfel de spațiu nu ar fi posibil fără garanții adecvate privind protecția datelor.

47. Potrivit AEPD, standardele europene pentru protecția datelor, bazate pe Convenția 108 a Consiliului Europei pentru protejarea persoanelor fizice față de prelucrarea automatizată a datelor cu caracter personal ([28]) și pe jurisprudența Curții Europene de Justiție și a Curții Europene pentru Drepturile Omului, ar trebui să stabilească nivelul de protecție într-un acord general cu Statele Unite privind protecția datelor și schimbul de date. Un astfel de acord general ar putea constitui baza unor dispoziții specifice pentru schimbul de date cu caracter personal. Acest lucru este cu atât mai important având în vedere intenția formulată la punctul 4.2.1 din comunicare conform căreia Uniunea Europeană trebuie să încheie acorduri de cooperare polițienească ori de câte ori este necesar.

48. AEPD înțelege pe deplin nevoia de consolidare a cooperării internaționale, în unele cazuri inclusiv cu țările care nu protejează drepturile fundamentale. Cu toate acestea ([29]), este esențial să se ia în considerare faptul că această cooperare internațională este susceptibilă să genereze o creștere importantă a colectării și a transferului internațional de date. În consecință, este esențial ca principiile de prelucrare corectă și legală – precum și principiile privind un proces echitabil în general – să se aplice colectării și transferului de date cu caracter personal în afara granițelor Uniunii și este, de asemenea, esențial ca datele cu caracter personal să fie transferate către țări terțe sau organizații internaționale numai în cazul în care părțile terțe în cauză garantează un nivel corespunzător de protecție sau alte măsuri de siguranță adecvate.

49. Pentru a încheia, AEPD recomandă ca Programul de la Stockholm să sublinieze importanța acordurilor generale cu Statele Unite și cu alte țări terțe privind protecția datelor și schimbul de date, bazate pe nivelul de protecție garantat pe teritoriul UE. Într-un context mai general, AEPD subliniază importanța promovării active a respectării drepturilor fundamentale și, în special, a drepturilor privind protecția datelor, în raport cu țările terțe și cu organizațiile internaționale ([30]). Mai mult, Programul de la Stockholm ar putea menționa noțiunea generală conform căreia schimbul de date cu caracter personal cu țări terțe necesită un nivel adecvat de protecție sau alte măsuri de siguranță corespunzătoare în aceste țări terțe.

VI. **UTILIZAREA INFORMAțIILOR**

VI.1. **Către un model european de informare**

50. Un mai bun schimb de informații este un obiectiv esențial de politică pentru Uniunea Europeană în spațiul de libertate, securitate și justiție. Punctul 4.1.2 din comunicare subliniază faptul că securitatea în Uniunea Europeană se bazează pe mecanisme performante de schimb de informații între autoritățile naționale și alți actori europeni. Acest accent pe schimbul de informații este logic, în lipsa unei forțe de poliție europene, a unui sistem european de justiție penală și a unui control european la frontiere. Măsurile referitoare la informații

([26]) Utilizatorii de informații, precum și operatorii care monitorizează sau procesează datele, fac obiectul legii privind protecția datelor.

([27]) A se vedea Avizul Autorității Europene pentru Protecția Datelor din 11 noiembrie 2008 privind Raportul final al Grupului de contact la nivel înalt UE-SUA privind schimbul de informații și protecția vieții private și a datelor cu caracter personal, J.O. C 128, 6.6.2009, p. 1.

([28]) ETS nr. 108, 28.1.1981.

([29]) A se vedea scrisoarea AEPD din 28 noiembrie 2005 privind comunicarea Comisiei cu privire la dimensiunea externă a spațiului de libertate, securitate și justiție, disponibilă pe site-ul AEPD.

([30]) Jurisprudența recentă cu privire la listele cuprinzând nume de teroriști confirmă faptul că sunt necesare garanții – inclusiv în relațiile cu Organizația Națiunilor Unite – care să asigure că măsurile antiteroriste sunt conforme cu standardele UE privind drepturile fundamentale (Cauzele conexate C-402/05 P și C-415/05, Kadi și Al Barakaat Foundation/Consiliul, hotărârea din 3 septembrie 2008, nepublicată încă în Repertoriu.).

sunt, prin urmare, contribuții esențiale ale Uniunii Europene care permit autorităților din statele membre să abordeze criminalitatea transfrontalieră într-un mod eficient și să protejeze efectiv frontierele externe. Cu toate acestea, ele nu contribuie numai la securitatea cetățenilor, ci și la libertatea acestora – libera circulație a persoanelor a fost menționată anterior ca o perspectivă a prezentului aviz - și la justiție.

51. Tocmai din aceste motive a fost introdus principiul disponibilității în Programul de la Haga. Acesta presupune faptul că informațiile necesare în lupta împotriva criminalității trebuie să traverseze frontierele interne ale UE fără obstacole. Din experiențele recente reiese că a fost dificil ca acest principiu să fie transpus în măsuri legislative. Propunerea Comisiei de decizie-cadru a Consiliului privind schimbul de informații în temeiul principiului disponibilității din 12 octombrie 2005 ([31]) nu a fost acceptată de către Consiliu. Statele membre nu au fost pregătite să accepte toate consecințele principiului disponibilității. S-au adoptat în schimb instrumente mai limitate ([32]) , precum Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (Decizia de la Prüm) ([33]).

52. În timp ce principiul disponibilității a reprezentat ideea principală a Programului de la Haga, Comisia pare să aibă acum o abordare mai modestă. Aceasta preconizează stimularea în continuare a schimbului de informații între autoritățile din statele membre prin introducerea modelului european de informare. Președinția suedeză a UE are o abordare similară ([34]). Aceasta va prezenta o propunere de strategie pentru schimbul de informații. Consiliul a început deja lucrările la acest proiect ambițios de strategie a Uniunii Europene de gestionare a informațiilor, care este strâns legat de modelul european de informare. AEPD ia act de aceste evoluții cu mare interes și subliniază atenția care ar trebui acordată elementelor de protecție a datelor în cadrul acestor proiecte.

Un model european de informare și de protecție a datelor

53. Ca punct de plecare, ar trebui subliniat faptul că viitorul spațiului de libertate, securitate și justiție nu ar trebui să fie „bazat pe tehnologie", în sensul că ar trebui verificată întotdeauna compatibilitatea oportunităților aproape nelimitate oferite de noile tehnologii cu principiile relevante privind protecția datelor, iar aceste oportunități ar trebui utilizate numai în măsura în care sunt conforme cu aceste principii.

54. AEPD constată că în comunicare se prezintă modelul de informare nu numai ca un model tehnic: o mare capacitate de analiză strategică și o mai bună colectare și tratament al informațiilor operaționale. De asemenea, recunoaște faptul că aspectele legate de politici – precum criteriile privind colectarea, partajarea și prelucrarea informațiilor – ar trebui luate în considerare cu respectarea principiilor de protecție a datelor.

55. Atât tehnologia informației, cât și condițiile legale sunt – și vor continua să fie – esențiale. AEPD salută faptul că comunicarea pornește de la ipoteza că un model european de informare nu poate fi înțeles plecând de la considerente tehnice. Este esențial ca informațiile să fie colectate, partajate și prelucrate numai în funcție de necesitățile concrete în materie de securitate și ținând seama de principiile de protecție a datelor. De asemenea, AEPD subscrie în totalitate necesității de a defini un mecanism de monitorizare care să evalueze modul în care se efectuează schimbul de informații. AEPD propune Consiliului să elaboreze în continuare aceste elemente în Programul de la Stockholm.

56. În acest context, AEPD subliniază faptul că protecția datelor în scopul protejării cetățenilor nu ar trebui considerată un aspect care împiedică gestionarea eficientă a datelor. Aceasta furnizează instrumente importante pentru îmbunătățirea stocării și a schimbului de informații, precum și a accesului la acestea. Drepturile persoanei vizate de a fi informată cu privire la informațiile care o privesc și care sunt prelucrate, precum și de a rectifica informațiile incorecte pot spori, de asemenea, acuratețea datelor în sistemele de gestionare a datelor.

57. Legislația privind protecția datelor are, în esență, următoarele consecințe: în cazul în care datele sunt necesare pentru un scop specific și legitim, acestea pot fi utilizate; în cazul în care datele cu caracter personal nu sunt necesare pentru un scop bine definit, acestea nu trebuie utilizate. În primul caz, pot fi necesare măsuri suplimentare care să furnizeze garanțiile corespunzătoare.

58. Cu toate acestea, AEPD are o atitudine critică în ceea ce privește măsura în care comunicarea menționează „identificarea nevoilor viitoare" ca parte a modelului de informare. AEPD subliniază faptul că și în viitor, principiul limitării scopului ar trebui să fie la baza conceperii sistemelor de informații ([35]). Este una dintre garanțiile esențiale pe care sistemul de protecție a datelor le furnizează cetățeanului: acesta trebuie să fie în măsură să știe dinainte pentru ce scop sunt colectate datele care îl privesc, precum și că acestea vor fi utilizate numai în acest scop, în special în viitor. Această garanție este chiar consfințită la articolul 8 din Carta drepturilor fundamentale a Uniunii. Principiul limitării scopului permite excepții – care sunt relevante în special în spațiul de libertate, securitate și justiție –, dar aceste excepții nu ar trebui să determine construirea unui sistem.

([31]) COM(2005) 490 final.

([32]) Din perspectiva disponibilității; Decizia de la Prüm cuprinde dispoziții de o importanță considerabilă pentru utilizarea datelor biometrice (ADN și amprente digitale).

([33]) JO L 210, 6.8.2008, p. 1.

([34]) A se vedea Programul de lucru al UE prezentat de guverne, citat în nota de subsol 5, p. 23.

([35]) A se vedea punctul 41 de mai sus.

Alegerea arhitecturii corespunzătoare

59. Totul începe cu alegerea arhitecturii corespunzătoare pentru schimbul de informații. Importanța unor arhitecturi adecvate ale sistemelor de informații este recunoscută în comunicare (punctul 4.1.3), dar din păcate numai în legătură cu interoperabilitatea.

60. AEPD subliniază un alt aspect: în cadrul modelului european de informare, cerințele de protecție a datelor ar trebui să fie parte integrantă a dezvoltării întregului sistem și nu ar trebui considerată a fi doar o condiție necesară pentru legalitatea unui sistem ([36]). Ar trebui să se utilizeze conceptele de „respectare a vieții private din concepție" și de necesitate a identificării „celor mai bune tehnici disponibile" ([37]), după cum s-a menționat anterior la punctul 43. Modelul european de informare ar trebui să se bazeze pe aceste concepte. Mai concret, aceasta înseamnă că sistemele de informații concepute în scopul siguranței publice trebuie să fie elaborate întotdeauna în conformitate cu principiul „respectării vieții private din concepție". AEPD recomandă Consiliului să includă aceste elemente în Programul de la Stockholm.

Interoperabilitatea sistemelor

61. AEPD subliniază faptul că interoperabilitatea nu este o chestiune de natură pur tehnică, ci că aceasta are consecințe inclusiv asupra protecției cetățeanului, în special asupra protecției datelor. Din punctul de vedere al protecției datelor, dacă este bine realizată, interoperabilitatea sistemelor prezintă avantaje clare în ceea ce privește evitarea stocării duble. Cu toate acestea, este de asemenea evident că a face accesul la date sau schimbul de date posibil din punct de vedere tehnic devine, în multe cazuri, un motiv puternic pentru a accesa sau schimba „de facto" aceste date. Cu alte cuvinte, interoperabilitatea prezintă riscuri specifice de interconectare între baze de date care au scopuri diferite ([38]). Ea poate afecta limitele stricte cu privire la scopul bazelor de date.

62. Pe scurt, simplul fapt că tehnic este posibil să se facă schimb de informații digitale între baze de date interoperabile sau să se fuzioneze aceste baze de date nu justifică o excepție de la principiul limitării scopului. În situații concrete, interoperabilitatea ar trebui să se bazeze pe opțiuni de politică clare și bine gândite. AEPD propune să se menționeze această noțiune în Programul de la Stockholm.

VI.2. **Utilizarea de informații colectate în alte scopuri**

63. Comunicarea nu se referă în mod explicit la una dintre tendințele cele mai importante din ultimii ani, și anume utilizarea în scopuri de aplicare a legii a datelor colectate în sectorul privat în scopuri comerciale. Această tendință nu se referă numai la datele de transfer specifice comunicațiior electronice și la datele privind pasagerii care călătoresc cu avionul în (anumite) țări terțe ([39]), ci se axează și pe sectorul financiar. Un exemplu în acest sens este Directiva 2005/60/CE a Parlamentului European și a Consiliului din 26 octombrie 2005 privind prevenirea utilizării sistemului financiar în scopul spălării banilor și finanțării terorismului ([40]). Un alt exemplu binecunoscut și foarte dezbătut se referă la prelucrarea datelor cu caracter personal, necesare în scopurile Programului de urmărire a finanțărilor în scopuri teroriste al Departamentului de Trezorerie al SUA, de către *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) ([41]).

64. AEPD consideră că aceste tendințe necesită o atenție deosebită în cadrul Programului de la Stockholm. Ele pot fi considerate a fi derogări de la principiul limitării scopului și sunt adesea foarte intruzive la adresa vieții private, deoarece utilizarea acestor date poate dezvălui multe despre comportamentul persoanelor. În fiecare caz în care sunt propuse asemenea măsuri, trebuie să existe dovezi foarte clare că o astfel de măsură intruzivă este necesară. În cazul în care se furnizează această dovadă, trebuie să se asigure faptul că drepturile persoanelor sunt pe deplin protejate.

65. Potrivit AEPD, utilizarea în scopul aplicării legii a datelor cu caracter personal colectate în scopuri comerciale ar trebui să fie permisă numai în condiții stricte, cum ar fi:

— Datele sunt utilizate numai pentru scopuri definite în mod expres, precum lupta împotriva terorismului și a formelor grave de criminalitate, care urmează să fie stabilite de la caz la caz.

— Datele sunt transferate mai degrabă printr-un sistem de tip „înaintare", decât de tip „retragere" ([42]).

([36]) A se vedea „Orientări și criterii pentru dezvoltarea, implementarea și utilizarea tehnologiilor din domeniul securității pentru consolidarea protecției vieții private" elaborate în cadrul proiectului PRISE (http://www.prise.oeaw.ac.at).

([37]) „Cele mai bune tehnici disponibile" desemnează stadiul cel mai eficient și avansat al dezvoltării activităților și metodelor de funcționare a acestora, care indică faptul că anumite tehnici sunt corespunzătoare în practică pentru a constitui, în principiu, o bază pentru ca aplicațiile și sistemele ITS să respecte cerințele cadrului de reglementare al UE în ceea ce privește viața privată, protecția datelor și securitatea.

([38]) A se vedea, de asemenea, observațiile AEPD cu privire la Comunicarea Comisiei privind interoperabilitatea bazelor de date europene, 10 martie 2006, disponibile la http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) A se vedea punctul 15 de mai sus.

([40]) JO L 309, 25.11.2005, p. 15.

([41]) A se vedea Avizul 10/2006 al Grupului de lucru al articolului 29 privind prelucrarea datelor cu caracter personal de către *Society for Worldwide Interbank Financial Telecommunication* (SWIFT).

([42]) În cadrul unui sistem de tip „înaintare" (*„push"-system*), operatorul de date trimite datele la cerere (le „înaintează") agenției de aplicare a legii. În cadrul unui sistem de tip „retragere" (*„pull"-system*), agenția de aplicare a legii are acces la baza de date a operatorului și extrage („retrage") informații din această bază de date. În cazul sistemului de tip „retragere", este mai dificil ca operatorul să preia răspunderea.

— Solicitările de date ar trebui să fie proporționale, strict direcționate și, în principiu, bazate pe suspiciuni cu privire la persoane specifice.

— Căutările de rutină, extragerea datelor (*data mining*) și crearea de profiluri (*profiling*) ar trebui evitate.

— Ar trebui să se țină evidența fiecărei utilizări a datelor în scopul aplicării legii, pentru a permite controlul efectiv asupra acestei utilizări, de către persoana vizată care își exercită drepturile, de către autoritățile de protecție a datelor și de către autoritățile judiciare.

VI.3. **Sistemele de informații și organismele UE**

Sistemele de informații cu sau fără stocare centralizată ([43])

66. In ultimii ani, numărul sistemelor de informații bazate pe legislația UE a crescut semnificativ în spațiul de libertate, securitate și justiție. Uneori se iau decizii pentru a se institui un sistem care presupune stocarea centralizată a datelor la nivel european, iar în alte cazuri, legea prevede numai schimbul de informații între bazele de date naționale. Sistemul de Informații Schengen este, probabil, cel mai bun exemplu de sistem cu stocare centralizată. Decizia 2008/615/JAI a Consiliului (Decizia de la Prüm) ([44]) este, din punctul de vedere al protecției datelor, exemplul cel mai semnificativ de sistem fără stocare centralizată, întrucât prevede un schimb masiv de date biometrice între autoritățile din statele membre.

67. Comunicarea ilustrează faptul că această tendință de creare de noi sisteme va continua. Un prim exemplu, menționat la punctul 4.2.2, se referă la un sistem de informații care extinde Sistemul european de informații cu privire la cazierele judiciare (ECRIS) pentru a include și resortisanți din țări care nu sunt membre ale UE. Comisia a comandat deja un studiu privind indicele european de resortisanți condamnați din țări terțe (EICTCN), care ar putea duce la crearea unei baze de date centralizate. Un al doilea exemplu este schimbul de informații privind persoanele consemnate în registrele de insolvabilitate din alte state membre, in cadrul e-justiției (punctul 3.4.1 din comunicare), fără stocare centralizată.

68. Un sistem descentralizat ar prezenta anumite avantaje din punctul de vedere al protecției datelor. Acesta evită dubla stocare a datelor de către autoritatea statului membru și de către sistemul centralizat, responsabilitatea pentru date este clară întrucât autoritatea din statul membru va fi operatorul datelor, iar controlul de către sistemul judiciar și de către autoritățile de protecție a datelor se poate exercita la nivelul statelor membre. Dar acest sistem are și deficiențe în cazul în care se face schimb de date cu alte jurisdicții, de exemplu în ceea ce privește asigurarea faptului că informațiile sunt actualizate atât în țara de origine, cât și în țara de destinație și în ceea ce privește asigurarea unui control efectiv de către ambele părți. Este chiar mai complicat să se asigure responsabilitatea pentru sistemul tehnic în cazul unui schimb. Aceste deficiențe pot fi depășite dacă se optează pentru un sistem centralizat, în cadrul căruia responsabilitatea le revine organismelor europene cel puțin pentru anumite părți ale sistemului (cum ar fi infrastructura tehnică).

69. În acest context, ar fi util să se dezvolte criterii de fond pentru alegerea între sistemele centralizate și cele descentralizate, care să asigure opțiuni de politică clare și bine gândite în cazuri concrete. Aceste criterii pot contribui la funcționarea sistemelor în sine, precum și la protecția datelor cu privire la cetățeni. AEPD propune să se includă intenția de a elabora astfel de criterii în Programul de la Stockholm.

Sisteme de informații de mari dimensiuni

70. Punctul 4.2.3.2 din comunicare prezintă pe scurt viitorul sistemelor de informații de mari dimensiuni, punând accentul pe Sistemul de Informații Schengen (SIS) și pe Sistemul de Informații privind Vizele (VIS).

71. De asemenea, punctul 4.2.3.2 menționează instituirea unui sistem de înregistrare electronică a intrărilor și ieșirilor de pe teritoriul statelor membre care să funcționeze în paralel cu programele privind călătorii înregistrați. Acest sistem a fost anunțat anterior de către Comisie ca parte a „pachetului privind frontierele", la inițiativa vicepreședintelui Frattini ([45]). În observațiile sale preliminare ([46]), AEPD a avut o atitudine destul de critică în privința acestei propuneri, deoarece necesitatea unui astfel de sistem intruziv, pe lângă sistemele de mari dimensiuni deja existente, nu a fost demonstrată suficient. AEPD constată că nu există nicio dovadă suplimentară cu privire la necesitatea unui astfel de sistem și, prin urmare, propune Consiliului să nu mai menționeze această idee în Programul de la Stockholm.

72. În acest context, AEPD dorește să facă trimitere la avizele sale privind diverse inițiative în domeniul schimbului de informații la nivelul UE ([47]) în care a făcut numeroase sugestii și observații cu privire la implicațiile asupra protecției datelor ale utilizării bazelor de date de mari dimensiuni la nivelul UE. Printre alte chestiuni, a acordat

([43]) În acest context, stocarea centralizată înseamnă stocarea la un nivel european central, în timp ce stocarea descentralizată înseamnă stocarea la nivelul statelor membre.

([44]) A se vedea nota de subsol nr. 33.

([45]) Comunicarea Comisiei „Pregătirea următoarelor etape ale gestionării frontierelor în Uniunea Europeană", 13.2.2008, COM(2008) 69.

([46]) Observații preliminare ale AEPD cu privire la trei comunicări ale Comisiei privind gestiunea frontierelor [COM(2008) 69, COM(2008) 68 și COM(2008) 67], 3 martie 2008. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/_Interoperability_EN.pdf

([47]) În special: Avizul din 23 martie 2005 privind propunerea de regulament al Parlamentului European și al Consiliului privind Sistemul de Informații privind Vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere, JO C 181, 23.7.2005, p. 13 și 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.

o atenție deosebită necesității unor măsuri de siguranță stricte și adaptate care ar trebui puse în aplicare, precum și proporționalității și necesității evaluărilor de impact înainte de propunerea sau adoptarea oricăror măsuri în acest domeniu. AEPD a susținut întotdeauna un echilibru corect și conform normelor de protecție a datelor între cerințele de securitate, pe de o parte, și protecția vieții private a persoanelor care fac obiectul sistemelor, pe de altă parte. A avut aceeași poziție în momentul în care i-a revenit sarcina de a supraveghea părțile centrale ale sistemelor.

73. În plus, AEPD profită de ocazie pentru a sublinia necesitatea unei abordări coerente a schimbului de informații în ansamblu la nivelul UE, în ceea ce privește coerența juridică, tehnică și în materie de supraveghere dintre sistemele deja existente și cele în curs de dezvoltare. Într-adevăr, în prezent mai mult decât anterior, este evidentă necesitatea unei viziuni curajoase și cuprinzătoare asupra modului în care ar trebui să fie schimbul de informații la nivelul UE și viitorul sistemelor de informații de mari dimensiuni. Numai pe baza unei astfel de viziuni ar putea fi reanalizată ideea unui sistem de înregistrare electronică a intrărilor și ieșirilor de pe teritoriul statelor membre.

74. AEPD propune ca în Programul de la Stockholm să se facă trimitere la intenția de a concepe o astfel de viziune, care ar trebui să includă o reflecție asupra posibilei intrări în vigoare a Tratatului de la Lisabona și asupra implicațiilor acestuia asupra sistemelor al căror temei juridic este cuprins în primul și în al treilea pilon.

75. În sfârșit, comunicarea menționează instituirea unei noi agenții care, conform comunicării, ar trebui să aibă, de asemenea, competențe în ceea ce privește sistemul de înregistrare electronică a intrărilor și ieșirilor. Între timp, Comisia a adoptat o propunere pentru instituirea unei astfel de agenții ([48]). AEPD susține respectiva propunere, în principiu, întrucât poate eficientiza funcționarea acestor sisteme, inclusiv privind protecția datelor. La momentul oportun va prezenta un aviz cu privire la această propunere.

Europol și Eurojust

76. Rolul Europol este menționat în repetate rânduri în comunicare, care subliniază ca o chestiune prioritară faptul că Europol trebuie să joace un rol central în coordonarea, schimbul de informații și formarea profesioniștilor. De asemenea, punctul 4.2.2 din comunicare se referă la recentele schimbări ale cadrului juridic de cooperare dintre Eurojust și Europol și precizează că va fi continuată consolidarea Eurojust, în special în ceea ce privește anchetele în domeniile criminalității organizate transfrontaliere. AEPD sprijină pe deplin aceste obiective, cu condiția ca garanțiile de protecție a datelor să fie respectate în mod corespunzător.

77. În acest context, AEPD salută noul proiect de acord convenit recent între Europol și Eurojust ([49]), care are ca scop îmbunătățirea și consolidarea cooperării reciproce între cele două organisme și care prevede schimbul eficient de informații între ele. În acest domeniu de activitate, protecția eficientă și reală a datelor joacă un rol-cheie.

VI.4. **Utilizarea datelor biometrice**

78. AEPD constată că în comunicare nu se abordează problema utilizării tot mai intensive a datelor biometrice în diferite instrumente juridice ale Uniunii Europene cu privire la utilizarea schimburilor de informații, inclusiv instrumentele de instituire a sistemelor de informații de mari dimensiuni. Acest lucru este regretabil, dat fiind faptul că este vorba despre o chestiune deosebit de importantă și de sensibilă din punctul de vedere al protecției datelor și a vieții private.

79. Deși recunoaște avantajele generale ale utilizării datelor biometrice, AEPD a subliniat în mod constant impactul major al utilizării unor astfel de date asupra drepturilor persoanelor și a propus introducerea unor măsuri de siguranță stricte pentru utilizarea datelor biometrice în cadrul fiecărui sistem în parte. Hotărârea recentă a Curții Europene a Drepturilor Omului în cauza *S. și Marper/Regatul Unit* ([50]) furnizează indicații utile în acest context, în special cu privire la justificarea și limitele utilizării datelor biometrice. În special, utilizarea informațiilor ADN poate să dezvăluie informații sensibile despre persoanele în cauză, având în vedere, de asemenea, că posibilitățile tehnice de a extrage informații din ADN sunt din ce în ce mai numeroase. În cazul utilizării pe scară largă a datelor biometrice în sistemele de informații există, de asemenea, o problemă generată de inexactitățile inerente în colectarea și compararea datelor biometrice. Din aceste motive, legislatorul UE ar trebui să dea dovadă de reținere în ceea ce privește utilizarea acestor date.

80. Un alt subiect recurent în ultimii ani a fost utilizarea amprentelor digitale ale copiilor și ale persoanelor în vârstă, din cauza imperfecțiunilor inerente ale sistemelor de date biometrice pentru aceste grupe de vârstă. AEPD a solicitat realizarea unui studiu aprofundat menit să identifice în mod corespunzător acuratețea sistemelor ([51]). Aceasta a propus o limită de vârstă de 14 ani pentru copii, cu excepția cazului în care concluziile studiului susmenționat vor fi contrare. AEPD propune să se menționeze acest lucru în Programul de la Stockholm.

([48]) Propunerea Comisiei din 24 iunie 2009 de regulament al Parlamentului European și al Consiliului de instituire a Agenției pentru gestionarea operațională a Sistemului de Informații Schengen (SIS II), a Sistemului de Informații privind Vizele (VIS), a EURODAC și a altor sisteme informatice de mari dimensiuni, în spațiul de libertate, securitate și justiție [COM(2009) 293/2].

([49]) Proiect de acord aprobat de Consiliu, dar care trebuie încă semnat de ambele părți. A se vedea registrul Consiliului: http://register.consilium.europa.eu/pdf/ro/09/st10/st10126.ro07.pdf http://register.consilium.europa.eu/pdf/ro/09/st10/st10126.ro07.pdf

([50]) Cereri conexate 30562/04 și 30566/04, S. și Marper/Regatul Unit, hotărârea din 4 decembrie 2008, CEDO încă nepublicate.

([51]) Avizul din 26 martie 2008 privind propunerea de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (CE) nr. 2252/2004 al Consiliului de modificare a Regulamentului (CE) nr. 2252/2004 al Consiliului privind standardele pentru elementele de securitate și elementele biometrice integrate în pașapoarte și în documente de călătorie emise de statele membre, JO C 200, 6.8.2008, p. 1.

81. Acestea fiind spuse, AEPD sugerează că ar fi util să se elaboreze criterii de fond privind utilizarea datelor biometrice. Aceste criterii ar trebui să asigure faptul că datele sunt folosite numai atunci când sunt necesare, adecvate și proporționale și atunci când legiuitorul a demonstrat existența unui scop explicit, specific și legitim. Mai precis, datele biometrice și, în special, datele ADN nu ar trebui utilizate în cazul în care se poate obține același efect prin utilizarea altor informații mai puțin sensibile.

VII. **ACCESUL LA JUSTIȚIE ȘI E-JUSTIȚIE**

82. Tehnologia va fi, de asemenea, utilizată ca un instrument pentru o mai bună cooperare judiciară. Punctul 3.4.1 din comunicare prezintă e-justiția ca o oportunitate pentru cetățeni de a avea acces mai ușor la justiție. E-justiția este un portal cu informații și videoconferințe, ca parte a procedurii judiciare. Mai mult, acesta permite desfășurarea de proceduri juridice on-line și prevede interconectarea registrelor naționale, precum registrele de insolvabilitate. AEPD constată că comunicarea nu menționează noi inițiative despre e-justiție, dar consolidează acțiunile deja în curs de desfășurare. AEPD este implicată în unele dintre aceste acțiuni, ca urmare a avizului pe care l-a emis la 19 decembrie 2008 privind Comunicarea Comisiei „Către o strategie europeană în domeniul e-justiției” ([52]).

83. E-justiție este un proiect ambițios care are nevoie de sprijin deplin. Acesta poate îmbunătăți efectiv sistemul judiciar în Europa și protecția judiciară a cetățeanului. Reprezintă un pas important în direcția unui spațiu european de justiție. Luând în considerare această apreciere pozitivă, se pot formula câteva observații:

— Sistemele tehnologice pentru e-justiție ar trebui să fie construite în conformitate cu principiul „respectării vieții private din concepție”. După cum s-a menționat anterior cu privire la modelul european de informare, totul începe cu alegerea arhitecturii corespunzătoare.

— Interconectarea și interoperabilitatea sistemelor ar trebui să respecte principiul limitării scopului.

— Responsabilitățile diferiților actori ar trebui să fie clar definite.

— Consecințele asupra persoanelor ale interconectării registrelor naționale cu date sensibile cu caracter personal, precum registrele de insolvabilitate, ar trebui analizate dinainte.

VIII. **CONCLUZII**

84. AEPD aprobă faptul că protecția drepturilor fundamentale, în special protecția datelor cu caracter personal, este recunoscută în comunicare drept unul dintre aspectele-cheie ale viitorul spațiului de libertate, securitate și justiție. În opinia AEPD, comunicarea promovează, pe bună dreptate, un echilibru între necesitatea unor instrumente adecvate menite să garanteze securitatea cetățenilor și protecția drepturilor fundamentale ale acestora. AEPD recunoaște că ar trebui să se pună mai mult accentul pe protecția datelor cu caracter personal.

85. AEPD sprijină pe deplin punctul 2.3 din comunicare, care îndeamnă la un regim complet de protecție a datelor care să acopere toate domeniile de competență ale UE, indiferent de intrarea în vigoare a Tratatului de la Lisabona. În acest context, recomandă:

— să se comunice necesitatea unei viziuni clare și pe termen lung asupra unui astfel de regim în Programul de la Stockholm;

— să se evalueze măsurile care au fost adoptate în acest domeniu, punerea lor în aplicare concretă și eficiența acestora, luându-se în considerare costurile pentru protecția vieții private și eficiența aplicării legii;

— să se includă ca prioritate în Programul de la Stockholm necesitatea unui nou cadru legislativ care, printre altele, să înlocuiască Decizia-cadru 2008/977/JAI a Consiliului.

86. AEPD salută intenția Comisiei de a reafirma principiile de protecție a datelor, care trebuie să facă obiectul consultării publice anunțate de Comisie, în cadrul Conferinței „Datele cu caracter personal – utilizare mai intensă, o mai bună protecție?” din 19-20 mai 2009. Pe fond, AEPD subliniază importanța principiului limitării scopului ca piatră de temelie a legislației privind protecția datelor, precum și a concentrării pe posibilitățile de îmbunătățire a eficienței aplicării principiilor de protecție a datelor, prin intermediul unor instrumente care pot consolida responsabilitățile operatorilor de date.

87. Principiul „respectării vieții private din concepție” și tehnologiile care respectă viața privată ar putea fi promovate prin

— Un sistem de certificare privind viața privată și protecția datelor, ca opțiune pentru proiectanții și utilizatorii de sisteme de informații;

— O obligație legală pentru proiectanții și utilizatorii de sisteme de informații de a utiliza sisteme conforme cu principiul respectării vieții private din concepție.

88. În ceea ce privește aspectele externe ale protecției datelor, AEPD recomandă:

— să se sublinieze, în Programul de la Stockholm, importanța acordurilor generale cu Statele Unite și cu alte țări terțe privind protecția datelor și schimbul de date;

([52]) Avizul din 19 decembrie 2008 privind Comunicarea Comisiei „Către o strategie europeană în domeniul e-justiției”, JO C 128, 6.6.2009, p. 13.

— să se promoveze activ respectarea drepturilor fundamentale și, în special, a drepturilor privind protecția datelor, în raport cu țările terțe și cu organizațiile internaționale;

— să se menționeze, în Programul de la Stockholm, faptul că schimbul de date cu caracter personal cu țări terțe necesită un nivel adecvat de protecție sau alte măsuri de siguranță corespunzătoare în aceste țări terțe.

89. AEPD constată cu mare interes progresele realizate către o strategie a Uniunii Europene de gestionare a informațiilor și un model european de informare și subliniază atenția care ar trebui acordată în aceste proiecte elementelor de protecție a datelor, pentru a fi elaborate în continuare în cadrul Programului de la Stockholm. Arhitectura pentru schimbul de informații ar trebui să se bazeze pe principiul „respectării vieții private din concepție” și pe „cele mai bune tehnici disponibile”.

90. Simplul fapt că tehnic este posibil să se facă schimb de informații digitale între baze de date interoperabile sau să se fuzioneze aceste baze de date nu justifică o excepție de la principiul limitării scopului. În situații concrete, interoperabilitatea ar trebui să se bazeze pe opțiuni de politică clare și bine gândite. AEPD propune să se menționeze acest lucru în Programul de la Stockholm.

91. Potrivit AEPD, utilizarea în scopul aplicării legii a datelor cu caracter personal colectate în scopuri comerciale ar trebui să fie permisă numai în condiții stricte, enumerate la punctul 65 din prezentul aviz.

92. Alte propuneri referitoare la utilizarea informațiilor cu caracter personal includ următoarele:

— Să se elaboreze criterii de fond pentru alegerea între sistemele centralizate și cele descentralizate și să se includă intenția de a elabora astfel de criterii în Programul de la Stockholm.

— În Programul de la Stockholm nu ar trebui menționată instituirea unui sistem de înregistrare electronică a intrărilor și ieșirilor de pe teritoriul statelor membre care să funcționeze în paralel cu programele privind călătorii înregistrați.

— Sprijinul pentru consolidarea Europol și Eurojust și pentru noul acord elaborat recent între Europol și Eurojust.

— Să se elaboreze criterii de fond privind utilizarea datelor biometrice, care să asigure faptul că datele sunt folosite numai atunci când sunt necesare, adecvate și proporționale și atunci când legiuitorul a demonstrat existența unui scop explicit, specific și legitim. Datele ADN nu ar trebui utilizate în cazul în care se poate obține același efect prin utilizarea altor informații mai puțin sensibile.

93. AEPD sprijină e-justiția și a formulat câteva observații în vederea îmbunătățirii proiectului (a se vedea punctul 83).

Adoptat la Bruxelles, 10 iulie 2009

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor