Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei către Parlamentul European și Consiliu – „Strategia de securitate internă a UE în acțiune: cinci pași către o Europă mai sigură”

(2011/C 101/02)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16,

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 8,

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

având în vedere solicitarea unui aviz, formulată în conformitate cu Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date [2], în special articolul 41,

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

1. La 22 noiembrie 2010, Comisia a adoptat o Comunicare intitulată „Strategia de securitate internă a UE în acțiune: cinci pași către o Europă mai sigură” (denumită în continuare „Comunicarea”) [3], care a fost trimisă spre consultare Autorității Europene pentru Protecția Datelor (AEPD).

2. AEPD salută faptul că a fost consultată de către Comisie. AEPD furnizase anterior adoptării Comunicării observații informale cu privire la proiectul de text, unele dintre acestea fiind luate în considerare în versiunea finală a Comunicării.

Contextul Comunicării

3. Strategia de securitate internă a UE (denumită în continuare SSI), abordată în cadrul Comunicării, a fost adoptată la 23 februarie 2010, în cursul președinției spaniole [4]. Strategia instituie un model european de securitate care include, printre altele, măsuri privind aplicarea legii și cooperarea judiciară, gestionarea frontierelor și protecția civilă, acordând atenția cuvenită valorilor europene comune, precum drepturile fundamentale. Principalele sale obiective sunt următoarele:

— informarea publicului cu privire la instrumentele existente ale UE care contribuie deja la garantarea securității și libertății cetățenilor UE și a valorii adăugate pe care acțiunea UE o realizează în acest domeniu;

— dezvoltarea suplimentară a instrumentelor și politicilor comune, utilizând o abordare mai integrată a cauzelor insecurității și nu doar a efectelor acesteia;

— consolidarea aplicării legii și a cooperării judiciare, gestionarea frontierelor, protecția civilă și gestionarea dezastrelor.

4. SSI vizează cele mai urgente amenințări și provocări pentru securitatea UE, cum ar fi infracțiunile grave și criminalitatea organizată, terorismul și criminalitatea cibernetică, gestionarea frontierelor externe ale UE și dezvoltarea unei capacități de reziliență în caz de dezastre naturale sau provocate de om. Strategia prevede orientări generale, principii și instrucțiuni cu privire la modul în care UE ar trebui să reacționeze la aceste probleme și invită Comisia să propună măsuri oportune de aplicare a strategiei.

5. Mai mult decât atât, este important să se menționeze, în acest context, concluziile recente ale Consiliului Justiție și Afaceri Interne privind crearea și punerea în aplicare a unui ciclu de politică al UE pentru combaterea crimei organizate și a infracțiunilor grave internaționale, adoptate la 8-9 noiembrie 2010 [5] (denumite în continuare „Concluziile din noiembrie 2010”). Acest document este ulterior Concluziei din 2006 a Consiliului privind arhitectura securității interne [6] și invită Consiliul și Comisia să definească o strategie de securitate internă cuprinzătoare, bazată pe valorile și principiile comune ale UE, astfel cum au fost reafirmate în Carta drepturilor fundamentale a UE [7].

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2010) 673 final.
[4] Doc. 5842/2/10.
[5] A 3043-a reuniune a Consiliului Justiție și Afaceri Interne, 8-10 noiembrie 2010, Bruxelles.
[6] Doc. 7039/2/06 JAI 86 CATS 34.
[7] Ciclul de politică al UE pentru combaterea crimei organizate și a infracțiunilor grave internaționale, prezentat în Concluziile din noiembrie 2010, cuprinde patru etape: 1) evoluții ale politicilor pe baza unei evaluări a amenințărilor pe care le reprezintă infracțiunile grave și criminalitatea organizată în Uniunea Europeană (EU SOCTA), 2) elaborarea politicilor și luarea deciziilor prin identificarea de către Consiliu a unui număr limitat de priorități, 3) punerea în aplicare și monitorizarea Planului de acțiune operațional anual (OAP) și 4) la sfârșitul ciclului de politică, o evaluare aprofundată care va servi, de asemenea, drept bază pentru viitorul ciclu de politică.

6. Printre instrucțiunile și obiectivele care ar trebui să orienteze punerea în aplicare a SSI, Concluziile din noiembrie 2010 fac referire la reflectarea unei abordări proactive și bazate pe informații, la cooperarea strânsă între agențiile UE, inclusiv îmbunătățirea în continuare a schimbului lor de informații, și la scopul de a-i face pe cetățeni conștienți de importanța acțiunilor Uniunii în vederea protejării acestora. De asemenea, aceste concluzii invită Comisia să elaboreze, împreună cu experții agențiilor competente și ai statelor membre, un plan strategic multianual (denumit în continuare PSM) pentru fiecare prioritate, care să definească strategia cea mai adecvată de soluționare a problemei. De asemenea, Comisia este invitată să elaboreze, prin consultări cu experți ai statelor membre și ai agențiilor UE, un mecanism independent de evaluare a punerii în aplicare a PSM. AEPD va reveni la aceste aspecte în continuarea prezentului aviz, deoarece sunt strâns legate sau au un impact considerabil asupra protecției datelor cu caracter personal, a vieții private și a altor drepturi și libertăți fundamentale.

Conținutul și obiectivul Comunicării

7. Comunicarea propune cinci obiective strategice, toate având legătură cu protecția vieții private și a datelor:

   — destrămarea rețelelor infracționale internaționale,

   — prevenirea terorismului și combaterea radicalizării și a recrutării,

   — creșterea nivelului de securitate pentru cetățeni și întreprinderi în spațiul cibernetic,

   — consolidarea securității prin gestionarea frontierelor și

   — creșterea capacității de reziliență a Europei în caz de crize și de dezastre.

8. „Strategia de securitate internă în acțiune” propusă în cadrul Comunicării prezintă un program comun pentru statele membre, Parlamentul European, Comisie, Consiliu, agenții și alți actori, inclusiv societatea civilă și autoritățile locale, și sugerează modul în care toți aceștia ar trebui să colaboreze în următorii patru ani pentru a atinge obiectivele SSI.

9. Comunicarea se întemeiază pe Tratatul de la Lisabona și confirmă orientările prevăzute în Programul de la Stockholm (și planul său de acțiune) care subliniază, la capitolul 4.1, necesitatea unei strategii de securitate internă exhaustive, bazate pe respectarea drepturilor fundamentale, protecția internațională și statul de drept. De asemenea, conform Programului de la Stockholm, elaborarea, monitorizarea și punerea în aplicare a strategiei de securitate internă ar trebui să devină una dintre atribuțiile prioritare ale Comitetului pentru securitate internă (COSI) instituit în temeiul articolului 71 din TFUE. Pentru a se asigura punerea în aplicare efectivă a strategiei de securitate internă, aceasta trebuie să acopere, de asemenea, aspecte de securitate ale unei gestionări integrate a frontierelor și, după caz, cooperarea judiciară în materie penală relevantă pentru cooperarea operațională în domeniul securității interne. De asemenea, este important de menționat, în acest context, că programul de la Stockholm invită la o abordare integrată a SSI, care ar trebui să țină seama și de strategia de securitate externă elaborată de UE, precum și alte politici ale UE, în special cele privind piața internă.

Scopul avizului

10. Comunicarea se referă la diferite domenii de politică incluse sau având un impact asupra conceptului de „securitate internă”, în sens larg, în Uniunea Europeană.

11. Scopul prezentului aviz nu constă într-o analiză a tuturor domeniilor de politică și a subiectelor specifice la care face referire Comunicarea, ci în:

   — prezentarea obiectivelor propriu-zise ale SSI propuse în Comunicare din perspectiva specifică a protecției vieții private și a datelor și sublinierea, din acest punct de vedere, a legăturilor necesare cu alte strategii care se discută și se adoptă la nivelul Uniunii Europene;

   — definirea mai multor noțiuni și concepte privind protecția datelor care ar trebui luate în considerare în elaborarea, dezvoltarea și punerea în aplicare a SSI la nivelul UE;

   — prezentarea, atunci când este util și relevant, a unor sugestii cu privire la modul în care problemele legate de protecția datelor pot fi cel mai bine luate în considerare în cadrul punerii în aplicare a acțiunilor propuse în Comunicare.

12. AEPD va realiza aceasta punând un accent deosebit pe legăturile dintre strategia de securitate internă și strategia de gestionare a informațiilor și activitatea legată de cadrul complet privind protecția datelor. De asemenea, AEPD va face referire la concepte precum cele mai bune tehnici existente și „luarea în considerare a vieții private începând cu momentul conceperii”, evaluarea impactului asupra protecției datelor și a vieții private și drepturile persoanelor vizate, concepte care au efecte directe asupra elaborării și punerii în aplicare a SSI. De asemenea, avizul prezintă observații asupra mai multor domenii de politică selectate, precum gestionarea integrată a frontierelor, inclusiv EUROSUR, și prelucrarea datelor cu caracter personal de către FRONTEX, precum și asupra altor domenii, de exemplu, spațiul cibernetic și TFTP.

II. OBSERVAȚII GENERALE

Necesitatea unei abordări mai inteligente, cuprinzătoare și „strategice” a strategiilor UE legate de SSI

13. În prezent, la nivelul UE se discută și se propun diverse strategii europene bazate pe Tratatul de la Lisabona și Programul de la Stockholm, care au un impact direct sau indirect asupra protecției datelor. Strategia de securitate internă este una dintre acestea și este strâns legată de alte strategii (fie abordate în Comunicările recente ale Comisiei, fie prevăzute pentru viitorul apropiat), cum ar fi Strategia de gestionare a informațiilor și Modelul european de schimb de informații, strategia privind punerea în aplicare efectivă a Cartei drepturilor fundamentale a Uniunii Europene, strategia globală privind protecția datelor și politica UE de combatere a terorismului. În prezentul aviz, AEPD acordă o atenție deosebită Strategiei de gestionare a informațiilor și cadrului general privind protecția datelor în temeiul articolului 16 din TFUE, care au legături politice evidente cu SSI din perspectiva protecției datelor.

14. Toate aceste strategii constituie un ansamblu disparat și complex de orientări politice, programe și planuri de acțiuni interdependente care necesită o abordare globală și integrată la nivelul Uniunii Europene.

15. În termeni mai generali, această abordare a „asocierii strategiilor”, dacă ar fi luată în considerare în acțiunile viitoare, ar demonstra că există o viziune europeană a *strategiilor UE* și că aceste strategii și comunicările recent adoptate care le dezvoltă sunt strâns legate, după cum este și cazul, Programul de la Stockholm reprezentând punctul lor de referință comun. De asemenea, abordarea respectivă ar avea drept rezultat sinergii pozitive între diferitele politici din cadrul spațiului de libertate, securitate și justiție și ar evita orice posibilă dublare a activității și eforturilor în acest domeniu. Nu mai puțin important, această abordare ar duce și la aplicarea mai eficientă și mai coerentă a normelor de protecție a datelor în contextul tuturor strategiilor interrelaționate.

16. AEPD subliniază că gestionarea eficientă a informațiilor în Uniunea Europeană reprezintă unul dintre pilonii SSI; aceasta ar trebui să se bazeze pe principiile necesității și proporționalității pentru a justifica nevoia schimbului de informații.

17. De asemenea, după cum se menționează în avizul AEPD referitor la Comunicarea privind modul de gestionare a informațiilor ([8]), AEPD subliniază că toate măsurile legislative noi care ar facilita stocarea și schimbul de date cu caracter personal ar trebui să fie propuse doar dacă se bazează pe dovezi concrete privind necesitatea acestora ([9]). Această cerință juridică ar trebui transformată într-o abordare politică proactivă în momentul punerii în aplicare a SSI. De asemenea, necesitatea unei abordări exhaustive a SSI duce în mod inevitabil la necesitatea evaluării tuturor instrumentelor și mecanismelor deja existente în domeniul securității interne înainte de a propune altele noi.

18. În acest context, AEPD propune, de asemenea, utilizarea mai frecventă a clauzelor care prevăd evaluarea periodică a instrumentelor existente, cum ar fi cele incluse în Directiva privind păstrarea datelor, în prezent, în curs de evaluare ([10]).

Protecția datelor ca obiectiv al SSI

19. Comunicarea face referire la protecția datelor cu caracter personal la alineatul „Politicile de securitate bazate pe valori comune”, în care se menționează că instrumentele și acțiunile care trebuie utilizate pentru punerea în aplicare a SSI trebuie să se bazeze pe valori comune, inclusiv pe statul de drept și pe respectarea drepturilor fundamentale, astfel cum se prevede în Carta drepturilor fundamentale a UE. În acest context, aceasta stipulează că „Atunci când aplicarea eficientă a legii în UE este facilitată prin schimbul de informații, trebuie să protejăm, de asemenea, viața privată a persoanelor și dreptul fundamental al acestora la protecția datelor cu caracter personal.”

20. Această declarație este salutată, însă nu poate fi considerată, în sine, o abordare suficientă a problemei protecției datelor în cadrul SSI. Comunicarea nu dezvoltă subiectul protecției datelor ([11]) și nici nu explică modul în care respectarea vieții private și protecția datelor cu caracter personal vor fi asigurate în practică de măsurile de aplicare a SSI.

([8]) Avizul din 30 septembrie 2010 privind Comunicarea Comisiei către Parlamentul European și Consiliu – „Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție”.

([9]) Aceasta este o cerință juridică; a se vedea, în special, Hotărârea CEJ în Cauzele conexe C-92/09 și C-93/09 din 2 noiembrie 2010. În contexte mai specifice, AEPD a promovat această abordare și în alte avize privind propuneri legislative legate de spațiul de libertate, securitate și justiție, de exemplu, în avizul din 19 octombrie 2005 referitor la trei propuneri privind Sistemul de Informații Schengen din a doua generație (SIS II); avizul din 20 decembrie 2007 referitor la propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii; avizul din 18 februarie 2009 referitor la propunerea de regulament privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. [.../...][de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid]; avizul din 18 februarie 2009 privind propunerea de regulament de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau un apatrid și avizul din 7 octombrie 2009 referitor la propunerile legate de accesul la EURODAC oferit autorităților de aplicare a legii.

([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, OJ L 105, 13.4.2006, p. 54.

([11]) Protecția datelor este menționată mai precis doar în contextul prelucrării datelor cu caracter personal de către FRONTEX.

21. Potrivit AEPD, *Strategia de securitate în acțiune* ar trebui să aibă ca obiectiv *protecția* în sens larg, care să asigure echilibrul *perfect* între protecția cetățenilor împotriva amenințărilor existente, pe de o parte, și protecția vieții lor private și dreptul la protecția datelor cu caracter personal, pe de altă parte. Cu alte cuvinte, problemele în materie de securitate și viață privată trebuie luate la fel de serios în considerare în elaborarea SSI, ceea ce ar fi în conformitate cu Programul de la Stockholm și cu Concluziile Consiliului.

22. Pe scurt, asigurarea securității cu respectarea deplină a vieții private și a protecției datelor ar trebui menționată ca obiectiv propriu-zis al strategiei de securitate internă a UE. Acest obiectiv ar trebui să se reflecte în toate măsurile luate de statele membre și de instituțiile europene pentru punerea în aplicare a strategiei.

23. În acest context, AEPD face trimitere la Comunicarea (2010) 609 privind abordarea globală a protecției datelor cu caracter personal în Uniunea Europeană ([12]). AEPD va emite în curând un aviz referitor la această Comunicare, dar subliniază în prezentul aviz că o strategie eficientă de securitate internă nu poate fi instituită fără sprijinul unui sistem solid de protecție a datelor care să o completeze și să asigure încredere reciprocă și o mai mare eficacitate.

III. NOȚIUNI ȘI CONCEPTE APLICABILE CONCEPERII ȘI PUNERII ÎN APLICARE A SSI

24. Este evident că unele dintre acțiunile care decurg din obiectivele SSI pot determina creșterea riscurilor pentru viața privată a persoanelor fizice și protecția datelor. Pentru a contracara aceste riscuri, AEPD ar dori să atragă atenția, în mod special, asupra unor concepte precum „luarea în considerare a vieții private începând cu momentul conceperii", evaluarea impactului asupra protecției datelor și a vieții private, drepturile persoanelor vizate și cele mai bune tehnici existente..Toate acestea ar trebui luate în considerare pentru implementarea SSI și pot contribui în mod util la politicile orientate într-o mai mare măsură spre viața privată și protecția datelor din acest domeniu.

Luarea în considerare a vieții private începând cu momentul conceperii

25. AEPD a susținut în mai multe rânduri și în diverse avize conceptul de viață privată „integrată" (prin „luarea în considerare a vieții private începând cu momentul conceperii" sau prin „confidențialitatea prestabilită"). Acest concept este, în prezent, dezvoltat atât pentru sectorul privat, cât și pentru sectorul public și, prin urmare, trebuie, de asemenea, să joace un rol important în contextul securității interne a UE și în domeniul poliției și justiției ([13]).

26. Comunicarea nu menționează acest concept. AEPD propune să se facă trimitere la acest concept în acțiunile vizate ce urmează a fi propuse și întreprinse pentru punerea în aplicare a SSI, în special în contextul obiectivului 4, „consolidarea securității prin gestionarea frontierelor", unde se menționează în mod clar utilizarea într-o mai mare măsură a noilor tehnologii pentru controalele la frontieră și supravegherea frontierelor.

Evaluarea impactului asupra protecției datelor și a vieții private

27. AEPD încurajează Comisia să reflecteze, ca parte a activității viitoare în ceea ce privește elaborarea și punerea în aplicare a SSI pe baza Comunicării, asupra a ceea ce ar trebui să se înțeleagă printr-o „evaluare efectivă a impactului asupra protecției datelor și a vieții private" (Privacy Impact Assessment – PIA) în spațiul de libertate, securitate și justiție, în special în strategia de securitate internă.

28. Comunicarea face referire la evaluarea amenințării și la evaluarea riscurilor, această referire fiind binevenită. Comunicarea nu menționează însă la niciun punct evaluarea impactului asupra protecției datelor și a vieții private. AEPD consideră că lucrările la punerea în aplicare a Comunicării privind SSI oferă o bună ocazie de a dezvolta asemenea evaluări ale impactului asupra protecției datelor și a vieții private în contextul securității interne. AEPD ia notă de faptul că nici orientările din Comunicare, nici Orientările Comisiei privind evaluarea impactului ([14]) nu specifică acest aspect și nu îl dezvoltă într-o cerință de politică.

29. Prin urmare, AEPD recomandă ca, la punerea în aplicare a instrumentelor viitoare, să se realizeze o evaluare mai specifică și mai riguroasă a impactului asupra protecției datelor și a vieții private, fie ca evaluare separată, fie ca parte a evaluării impactului asupra drepturilor fundamentale generale efectuate de Comisie. Această evaluare a impactului nu ar trebui să afirme doar principiile generale sau să analizeze opțiunile politice, așa cum se întâmplă în prezent, ci să recomande, de asemenea, garanții specific și concrete.

30. În consecință, ar trebui să se elaboreze indicatori și funcții specifice pentru a garanta că fiecare propunere care exercită un impact asupra protecției datelor și a vieții private în domeniul securității interne a UE face obiectul unei examinări atente, incluzând aspecte precum proporționalitatea, necesitatea și principiul limitării scopului.

31. În plus, ar putea fi util să se facă trimitere în acest context la articolul 4 din Recomandarea privind dispozitivele de identificare prin radiofrecvență (RFID) ([15]) în care Comisia a făcut un apel la statele membre să asigure faptul că industria, în colaborare cu părțile interesate relevante ale societății civile, elaborează un cadru pentru evaluările

([12]) Comunicarea Comisiei către Parlamentul European, Consiliu și Comitetul Economic și Social European și Comitetul Regiunilor privind abordarea exhaustivă a protecției datelor în Uniunea Europeană, COM(2010) 609.

([13]) În avizul referitor la Comunicarea Comisiei privind Programul de la Stockholm, AEPD a recomandat introducerea unei obligații legale pentru proiectanții și utilizatorii de sisteme de informații de a utiliza sisteme conforme cu principiul „luării în considerare a vieții private începând cu momentul conceperii".

([14]) SEC(2009) 92, 15.1.2009.

([15]) C(2009) 3200 final, 12.5.2009.

impactului asupra protecției datelor și a vieții private. De asemenea, Rezoluția de la Madrid, adoptată în noiembrie 2009 în cadrul Conferinței Internaționale a Comisarilor pentru Protecția Datelor și Viața Privată, a încurajat aplicarea PIA înainte de aplicarea noilor sisteme și tehnologii de informații în vederea prelucrării datelor cu caracter personal sau a unor modificări substanțiale ale prelucrărilor existente.

Drepturile persoanelor vizate

32. AEPD ia notă de faptul că această Comunicare nu vizează în mod specific problema drepturilor persoanelor vizate care constituie un element esențial al protecției datelor și ar trebui să aibă impact asupra conceperii SSI. Este esențial să se asigure că în toate sistemele și instrumentele diferite care au legătură cu securitatea internă a UE, persoanele vizate beneficiază de drepturi similare în ceea ce privește modalitatea de prelucrare a datele lor cu caracter personal.

33. Multe dintre sistemele la care se face referire în Comunicare stabilesc norme specifice privind drepturile persoanelor vizate (vizând, de asemenea, categorii de persoane cum ar fi victimele, infractorii suspectați sau migranții), însă există foarte multe diferențe între sisteme și instrumente, fără o justificare corespunzătoare.

34. Prin urmare, AEPD invită Comisia să examineze mai atent aspectul alinierii drepturilor persoanelor vizate din UE în contextul strategiei de securitate internă și al strategiei de gestionare a informațiilor în viitorul apropiat.

35. O atenție deosebită ar trebui acordată mecanismelor de recurs. Strategia de securitate internă ar trebui să garanteze faptul că, ori de câte ori drepturile persoanelor fizice nu sunt pe deplin respectate, controlorii de date ar trebui să prevadă proceduri de contestare ușor disponibile, eficiente și acceptabile.

Cele mai bune tehnici existente

36. Punerea în aplicare a SSI se va baza, în mod inevitabil, pe utilizarea unei infrastructuri IT care va sprijini acțiunile prevăzute în Comunicare. Cele mai bune tehnici existente pot fi privite ca factori ce asigură atingerea echilibrului perfect între realizarea obiectivelor strategiei de securitate internă și respectarea drepturilor persoanelor fizice. În contextul de față, AEPD ar dori să reitereze recomandarea formulată în avizele precedente ([16]) referitoare la necesitatea definirii și promovării de către Comisie împreună cu părțile interesate din industrie a unor măsuri concrete privind aplicarea celor mai bune tehnici existente. Aplicarea acestora înseamnă stadiul cel mai eficient și mai avansat în desfășurarea activităților și îmbunătățirea metodelor lor de exploatare, care indică adecvarea din punct de vedere practic a anumitor tehnici pentru a oferi rezultatele previzionate în mod eficient și conform cu cadrul UE de protecție a datelor și a vieții private. Această abordare este în deplină concordanță cu abordarea menționată anterior, respectiv „luarea în considerare a vieții private începând cu momentul conceperii".

37. Atunci când este relevant și posibil, ar trebui elaborate documente de referință cu privire la cele mai bune tehnici existente pentru a oferi orientări și un grad mai ridicat de securitate juridică în ceea ce privește aplicarea concretă a măsurilor încadrate de SSI. De asemenea, strategia ar putea promova armonizarea acestor măsuri la nivelul diferitelor state membre. Nu în ultimul rând, definirea celor mai bune tehnici existente care facilitează protecția datelor și a vieții private va contribui la îndeplinirea rolului de supraveghere al autorităților pentru protecția datelor, prin furnizarea acestora de referințe tehnice conforme privind protecția datelor și a vieții private, adoptate de controlorii de date.

38. De asemenea, AEPD remarcă importanța unei alinieri adecvate a SSI la activitățile desfășurate deja în cadrul celui de-al șaptelea Program-cadru de cercetare și dezvoltare tehnologică și în cadrul Programului-cadru „Securitate și protecția libertăților". O viziune comună care vizează să asigure cele mai bune tehnici existente va facilita inovarea cunoștințelor și capacităților necesare pentru protejarea cetățenilor, respectând, totodată, drepturile fundamentale.

39. În final, AEPD subliniază rolul pe care îl joacă Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) în elaborarea orientărilor și în evaluarea capacităților de securitate necesare pentru asigurarea integrității și disponibilității sistemelor informatice, precum și în promovarea celor mai bune tehnici existente. Având în vedere acest aspect, AEPD salută includerea agenției ca actor central în procesul de îmbunătățire a capacităților de combatere a atacurilor cibernetice și de luptă împotriva criminalității cibernetice ([17]).

Clarificări în ceea ce privește actorii și rolurile lor

40. În acest context, sunt necesare mai multe clarificări în privința actorilor care fac parte din sau contribuie la arhitectura SSI. Comunicarea face referire la diferiți actori și părți interesate precum cetățeni, organe judiciare, agenții

([16]) Avizul AEPD privind sistemele de transport inteligente din iulie 2009 și avizul AEPD privind Comunicarea referitoare la RFID din decembrie 2007; a se vedea, de asemenea, Raportul anual 2006 al AEPD, p.48-49.

([17]) AEPD intenționează să adopte un aviz privind cadrul juridic al ENISA tot în luna decembrie 2010.

europene, autorități naționale, poliție și întreprinderi. Rolurile și competențele specifice ale acestor actori ar trebui mai bine abordate în acțiunile specifice care urmează a fi propuse pentru punerea în aplicare a SSI.

IV. OBSERVAȚII SPECIFICE PRIVIND DOMENIILE DE POLITICĂ LEGATE DE SSI

Gestionarea integrată a frontierelor (GIF)

41. Comunicarea face trimitere la faptul că, odată cu intrarea în vigoare a Tratatului de la Lisabona, UE poate să utilizeze mai bine sinergiile dintre politicile de gestionare a frontierelor în materie de persoane și mărfuri. În ceea ce privește circulația persoanelor, Comunicarea menționează că „UE poate aborda gestionarea migrației și combaterea criminalității ca pe un dublu obiectiv al strategiei privind gestionarea integrată a frontierelor". Documentul percepe gestionarea frontierelor ca pe un puternic mijloc posibil de destrămare a infracțiunilor grave și a criminalității organizate ([18]).

42. De asemenea, AEPD observă că în Comunicare sunt identificate trei aspecte strategice: 1) o utilizare mai intensă a noilor tehnologii pentru verificările la frontiere (SIS II, VIS, sistemul de intrare/ieșire și programul de înregistrare a călătorilor); 2) o utilizare mai intensă a noilor tehnologii pentru supravegherea frontierelor (Sistemul European de supraveghere a frontierelor, EUROSUR) și 3) o coordonare mai bună între statele membre, prin intermediul FRONTEX.

43. AEPD dorește să profite de ocazia oferită de prezentul aviz pentru a aminti solicitările formulate într-o serie de avize precedente legate de instituirea, la nivelul UE, a unei politici clare în domeniul gestionării frontierelor, care să respecte pe deplin normele privind protecția datelor. AEPD consideră că lucrările actuale privind SSI și gestionarea informațiilor reprezintă ocazii excelente pentru a lua măsuri mai concrete în direcția unei abordări politice coerente în aceste domenii.

44. AEPD ia notă de faptul că această Comunicare nu se referă exclusiv la sistemele de mari dimensiuni deja existente și la cele care ar putea puse în funcțiune în viitorul apropiat (cum ar fi SIS, SIS II și VIS), ci, în aceeași abordare, și la sistemele care ar putea fi propuse de Comisie în viitor, însă în legătură cu care nu a fost încă adoptată o decizie [de exemplu, Programul privind călătorii înregistrați (*Registered Travellers Programme* – RTP) și sistemul de intrare/ieșire]. În acest context, ar trebui amintit că este încă necesar ca obiectivele și legitimitatea introducerii acestor sisteme să fie clarificate și demonstrate, de asemenea, în lumina rezultatelor evaluărilor de impact specifice efectuate de Comisie. În caz contrar, Comunicarea poate fi privită ca o anticipare a procesului decizional și, în consecință, neluând în considerare faptul că nu a fost încă adoptată o decizie finală cu privire la introducerea în Uniunea Europeană a RTP și a sistemului de intrare/ieșire.

45. Prin urmare, AEPD propune ca asemenea anticipări să fie evitate în activitatea viitoare privind punerea în aplicare a SSI. Astfel cum s-a menționat anterior, orice decizie privind introducerea unor noi sisteme de mari dimensiuni intruzive asupra vieții private ar trebui luată numai în urma unei evaluări adecvate a tuturor sistemelor existente, ținând seama de necesitate și proporționalitate.

EUROSUR

46. Comunicarea menționează că, în 2011, Comisia va prezenta o propunere legislativă de înființare a EUROSUR pentru a contribui la securitatea internă și la combaterea criminalității. De asemenea, se menționează că EUROSUR va utiliza noi tehnologii dezvoltate prin proiecte de cercetare și activități finanțate de UE, cum ar fi imagistica prin satelit pentru detectarea și urmărirea țintelor la frontierele maritime, de exemplu, urmărirea ambarcațiunilor de viteză care transportă droguri spre UE.

47. În acest context, AEPD remarcă faptul că nu este clar dacă și în ce măsură propunerea legislativă privind EUROSUR, pe care Comisia urmează să o prezinte în 2011, prevede și prelucrarea datelor cu caracter personal în contextul EUROSUR. Comisia nu a adoptat încă o poziție clară în acest sens în Comunicare. Acest aspect este cu atât mai relevant cu cât Comunicarea stabilește legături clare între EUROSUR și FRONTEX la nivel tactic, operațional și strategic (a se vedea observațiile de mai jos cu privire la FRONTEX) și solicită o cooperare strânsă între acestea.

Prelucrarea datelor cu caracter personal de către FRONTEX

48. La 17 mai 2010, AEPD a emis un aviz privind revizuirea Regulamentului FRONTEX ([19]), în cadrul căruia invită la o adevărată dezbatere și la o reflecție aprofundată asupra problemei protecției datelor în contextul consolidării sarcinilor existente ale FRONTEX și al atribuirii de noi responsabilități.

49. Comunicarea se referă la necesitatea consolidării contribuției FRONTEX la frontierele externe în cadrul obiectivului 4 *Consolidarea securității prin gestionarea frontierelor*. În acest context, Comunicarea menționează că, pe baza experienței dobândite și în contextul abordării globale a UE în materie de gestionare a informațiilor, Comisia consideră că posibilitatea pentru FRONTEX de a prelucra și utiliza aceste

([18]) Comunicat de presă – „Strategia de securitate internă a UE în acțiune – cinci pași către o Europă mai sigură", Memo 10/598.

([19]) Avizul AEPD din 17 mai 2010 privind propunerea de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (CE) nr. 2007/2004 al Consiliului de instituire a Agenției Europene pentru Gestionarea Cooperării Operative la Frontierele Externe ale Statelor Membre ale Uniunii Europene (FRONTEX).

informații, într-un scop limitat și în conformitate cu norme clar definite de gestionare a datelor cu caracter personal, va contribui în mod semnificativ la dezmembrarea organizațiilor infracționale. Aceasta reprezintă o abordare nouă față de propunerea Comisiei privind revizuirea Regulamentului FRONTEX care nu menționează absolut nimic despre prelucrarea datelor cu caracter personal, revizuire care face în prezent obiectul discuțiilor în Parlamentul European și Consiliu.

50. În acest context, AEPD salută faptul că această Comunicare oferă o serie de indicii legate de situațiile în care prelucrarea datelor cu caracter personal s-ar putea dovedi necesară (de exemplu, analiza riscurilor, îmbunătățirea operațiunilor comune sau schimbul de informații cu Europol). Mai exact, Comunicarea explică faptul că, în prezent, informațiile pe care le obține FRONTEX cu privire la infractorii implicați în rețelele de trafic nu pot fi utilizate în continuare pentru analiza riscurilor sau pentru a viza mai bine obiectivele viitoarelor operațiuni comune. De asemenea, datele relevante privind infractorii suspectați nu ajung la autoritățile naționale competente sau la Europol în vederea efectuării unor anchete suplimentare.

51. Cu toate acestea, AEPD notează că această Comunicare nu se referă la discuțiile aflate în desfășurare cu privire la revizuirea cadrului juridic al FRONTEX care, după cum s-a menționat anterior, abordează problema în vederea identificării unor soluții legislative. În plus, se poate considera că textul Comunicării, care subliniază rolul FRONTEX în contextul obiectivului de dezmembrare a organizațiilor infracționale, extinde mandatul FRONTEX. AEPD propune ca acest punct să fie avut în vedere atât în revizuirea Regulamentului FRONTEX, cât și în punerea în aplicare a SSI.

52. De asemenea, AEPD atrage atenția asupra necesității de a se asigura că între Europol și FRONTEX nu există nicio suprapunere de sarcini. În acest context, AEPD salută faptul că în Comunicare se prevede că suprapunere sarcinilor FRONTEX și Europol ar trebui evitată. Acest aspect ar trebui însă abordat cu mai multă claritate atât în Regulamentul FRONTEX revizuit, cât și în acțiunile de punere în aplicare a strategiei de securitate internă, care prevăd o cooperare strânsă între FRONTEX și EUROPOL. Această cooperare este deosebit de importantă din punct de vedere al principiilor limitării scopului și al calității datelor. Această observație este valabilă și în cazul viitoarei cooperări cu agenții cum ar fi Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) sau Biroul European de Sprijin pentru Azil.

Utilizarea biometriei

53. Comunicarea nu vizează în mod specific fenomenul actual al utilizării mai frecvente a datelor biometrice în spațiul de libertate, securitate și justiție, inclusiv a sistemelor informatice la scară largă ale UE și a altor instrumente de gestionare a frontierelor.

54. Prin urmare, AEPD profită de ocazie pentru a aminti propunerea sa ([20]) potrivit căreia acest aspect foarte sensibil din perspectiva protecției datelor să fie luat serios în considerare în punerea în aplicare a SSI, în special în contextul gestionării frontierelor.

55. De asemenea, AEPD recomandă elaborarea unei politici clare și stricte privind utilizarea biometriei în spațiul de libertate, securitate și justiție, bazată pe o evaluare riguroasă și pe o analiză de la caz la caz a necesității utilizării biometriei în contextul SSI, cu respectarea deplină a principiilor fundamentale privind protecția datelor, precum proporționalitatea, necesitatea și limitarea scopului.

TFTP

56. Comunicarea anunță că, în 2011, Comisia va dezvolta o politică pentru ca UE să extragă și să analizeze datele de mesagerie financiară deținute pe teritoriul său. În acest context, AEPD face referire la avizul său din 22 iunie 2010 privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste (TFTP II) ([21]). Toate observațiile critice exprimate în avizul respectiv sunt în mod egal valabile și aplicabile în contextul lucrărilor prevăzute la stabilirea unui cadru european privind datele de mesagerie financiară. Prin urmare, aceste observații ar trebui luate în considerare în discuțiile pe această temă. Ar trebui acordată o atenție deosebită proporționalității extragerii și prelucrării unor cantități mari de date privind persoane care nu sunt suspecte, precum și problemei supravegherii eficiente de către autorități independente și organe judiciare.

Securitatea pentru cetățeni și întreprinderi în spațiul cibernetic

57. AEPD salută importanța pe care Comunicarea o arată măsurilor preventive la nivelul UE și consideră consolidarea securității în rețelele informatice ca fiind un factor esențial ce contribuie la buna funcționare a societății informaționale. De asemenea, AEPD sprijină activitățile specifice de îmbunătățire a capacităților de combatere a atacurilor cibernetice, de dezvoltare a capacităților în domeniul aplicării legii și în cadrul sistemului judiciar, precum și de creare de parteneriate cu sectorul industrial în vederea punerii la dispoziția cetățenilor și întreprinderilor a unor mijloace de acțiune. De asemenea, rolul ENISA de promotor a multor acțiuni, prevăzut la acest obiectiv, este binevenit.

([20]) A se vedea, în special, avizul AEPD referitor la Comunicarea „Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție", menționat la nota de subsol 8.

([21]) Avizul AEPD din 22 iunie 2010 privind propunerea de decizie a Consiliului privind încheierea Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste (TFTP II).

58. Cu toate acestea, *Strategia de securitate internă în acțiune* nu dezvoltă măsurile de aplicare a legii prevăzute în spațiul cibernetic, modul în care aceste activități ar putea pune în pericol drepturile persoanelor fizice și garanțiile necesare care ar trebui să existe. AEPD solicită o abordare mai ambițioasă a garanțiilor corespunzătoare; această abordare ar trebui stabilită pentru a proteja drepturile fundamentale ale tuturor persoanelor fizice, inclusiv a celor care pot fi afectate de acțiuni menite să contracareze orice activitate infracțională posibilă în acest domeniu.

V. **CONCLUZII ȘI RECOMANDĂRI**

59. AEPD solicită asocierea mai multor strategii și Comunicări ale UE în cursul implementării SSI. Această abordare ar trebui urmată de un plan de acțiune concret, sprijinit printr-o evaluare efectivă a necesităților, al cărui rezultat să se concretizeze într-o politică europeană cuprinzătoare, integrată și bine structurată privind strategia de securitate internă.

60. De asemenea, AEPD profită de acest prilej pentru a sublinia importanța cerinței juridice privind evaluarea efectivă a tuturor instrumentelor existente ce urmează a fi utilizate în contextul SSI și a schimbului de informații înainte de a propune noi instrumente. În acest context, se recomandă insistent includerea unor dispoziții privind evaluarea periodică a eficacității instrumentelor relevante.

61. În pregătirea Planului strategic multianual solicitat în cadrul Concluziilor Consiliului din noiembrie 2010, AEPD propune să se țină seama de lucrările în curs la cadrul global de protecție a datelor în temeiul articolului 16 din TFUE, în special al Comunicării (2009) 609.

62. AEPD prezintă o serie de propuneri privind noțiunile și conceptele relevante din punct de vedere al protecției datelor care ar trebui luate în considerare în domeniul SSI, de exemplu, luarea în considerare a vieții private începând cu momentul conceperii, evaluarea impactului asupra protecției datelor și a vieții private, cele mai bune tehnici existente.

63. AEPD recomandă ca, la punerea în aplicare a viitoarelor instrumente, să se realizeze o evaluare a impactului asupra protecției datelor și a vieții private, fie ca evaluare separată, fie ca parte din evaluarea impactului asupra drepturilor fundamentale generale efectuată de Comisie.

64. De asemenea, AEPD invită Comisia să elaboreze o politică mai coerentă și mai consecventă cu privire la condițiile prealabile pentru utilizarea biometriei în domeniul SSI, precum și pentru o mai bună aliniere la nivelul UE din punct de vedere al drepturilor persoanelor vizate.

65. În final, AEPD prezintă o serie de observații cu privire la prelucrarea datelor cu caracter personal în contextul gestionării frontierelor, în special de către FRONTEX, și, posibil, în contextul EUROSUR.

Adoptat la Bruxelles, 17 decembrie 2010.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor