AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind propunerea Comisiei de regulament al Parlamentului European și al Consiliului privind cooperarea administrativă prin intermediul Sistemului de informare al pieței interne („IMI")

(2012/C 48/02)

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 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 [2],

având în vedere solicitarea unui aviz în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001,

ADOPTĂ PREZENTUL AVIZ:

1. INTRODUCERE

1.1. Consultarea AEPD

1. La 29 august 2011, Comisia a adoptat o propunere de regulament („propunerea" sau „regulamentul propus") al Parlamentului European și al Consiliului privind cooperarea administrativă prin intermediul Sistemului de informare al pieței interne („IMI") [3]. Propunerea a fost transmisă Autorității Europene pentru Protecția Datelor (AEPD) spre consultare în aceeași zi.

2. Înainte de adoptarea propunerii, Autorității Europene pentru Protecția Datelor i s-a dat posibilitatea de a formula observații neoficiale cu privire la propunere și, înainte de aceasta, cu privire la Comunicarea Comisiei „O mai bună guvernanță a pieței unice prin intensificarea cooperării administrative: o strategie pentru extinderea și dezvoltarea Sistemului de informare al pieței interne («IMI»)" („Comunicarea privind strategia IMI") [4], care a precedat propunerea. Multe dintre aceste observații au fost luate în considerare în cadrul propunerii și – în consecință – garanțiile privind protecția datelor existente în propunere au fost consolidate.

3. AEPD apreciază faptul că a fost consultată în mod oficial de către Comisie și că în preambulul propunerii a fost inclusă o trimitere la prezentul aviz.

1.2. Obiectivele și domeniul de aplicare al propunerii

4. Sistemul IMI este un instrument din domeniul tehnologiei informației care permite autorităților competente din statele membre să schimbe informații în cadrul procesului de aplicare a legislației care reglementează piața internă. IMI permite autorităților naționale, regionale și locale din statele membre ale UE să comunice rapid și ușor cu omologii lor din alte țări europene. Acest lucru implică și prelucrarea datelor cu caracter personal relevante, inclusiv a datelor sensibile.

5. Sistemul IMI a fost creat inițial ca un instrument de comunicare pentru schimburi de informații bilaterale realizate în conformitate cu Directiva privind calificările profesionale [5] și cu Directiva privind serviciile [6]. IMI îi ajută pe utilizatori să identifice autoritatea corespunzătoare din altă țară care trebuie contactată și să comunice cu aceasta prin utilizarea unor seturi de întrebări și răspunsuri standard deja traduse [7].

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2011) 522 final.
[4] COM(2011) 75.
[5] Directiva 2005/36/CE a Parlamentului European și a Consiliului din 7 septembrie 2005 privind recunoașterea calificărilor profesionale (JO L 255, 30.9.2005, p. 22).
[6] Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne (JO L 376, 27.12.2006, p. 36).
[7] Pentru exemplificare, o întrebare tipică privind date sensibile ar putea fi: „Documentul anexat justifică în mod legal absența suspendării sau a interzicerii exercitării activităților profesionale relevante în caz de eroare profesională gravă sau de infracțiune penală cu privire la (profesionistul migrant)?".

6. Cu toate acestea, IMI este conceput ca un sistem orizontal flexibil care să poată sprijini domenii multiple reglementate de legislația privind piața internă. Se preconizează că utilizarea sa va fi extinsă treptat pentru a sprijini în viitor domenii legislative suplimentare.

7. Se intenționează ca și funcționalitățile sistemului IMI să fie extinse. În plus față de schimburile de informații bilaterale, mai sunt prevăzute sau deja implementate și alte funcționalități, cum ar fi „proceduri de notificare, mecanisme de alertă, acorduri de asistență reciprocă și rezolvarea problemelor" ([8]), precum și „liste de informații consultabile ulterior ca referință de către actorii IMI" ([9]). Multe dintre aceste funcționalități, dar nu toate, pot presupune și prelucrări de date cu caracter personal.

8. Propunerea are ca scop asigurarea unui temei juridic clar pentru sistemul IMI și a unui cadru cuprinzător privind protecția datelor.

1.3. **Contextul propunerii: o abordare progresivă în vederea instituirii unui cadru cuprinzător privind protecția datelor pentru IMI**

9. În primăvara anului 2007, Comisia a solicitat ca avizul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal [Grupul de lucru instituit în temeiul articolului 29 („WP29")] să analizeze implicațiile sistemului IMI în ceea ce privește protecția datelor. WP29 a emis avizul la 20 septembrie 2007 ([10]). Avizul a recomandat Comisiei crearea unui temei juridic mai clar și a unor garanții specifice privind protecția datelor pentru schimbul de date din cadrul IMI. AEPD a participat în mod activ la lucrările subgrupului care s-a ocupat de IMI și a susținut concluziile avizului WP29.

10. Ulterior, AEPD a continuat să ofere orientare Comisiei în legătură cu felul în care se poate asigura, pas cu pas, un cadru mai cuprinzător al protecției datelor pentru IMI ([11]). În cadrul acestei cooperări și începând cu emiterea avizului său privind punerea în aplicare a IMI ([12]), la 22 februarie 2008, AEPD a susținut cu consecvență necesitatea adoptării unui nou instrument juridic prin procedura legislativă ordinară, pentru a se institui un cadru mai cuprinzător al protecției datelor pentru IMI și pentru a se asigura securitatea juridică. În prezent a fost înaintată propunerea privind un astfel de instrument juridic ([13]).

([8]) A se vedea considerentul 10.

([9]) A se vedea articolul 13 alineatul (2).

([10]) Avizul nr. 7/2007 al WP29 privind aspecte de protecție a datelor legate de Sistemul de informare al pieței interne (IMI), WP140. Disponibil la: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_en.pdf

([11]) Documentele-cheie referitoare la această cooperare sunt disponibile pe site-ul internet al Comisiei dedicat IMI, la: http://ec.europa.eu/internal_market/imi-net/data_protection_en.html, precum și pe site-ul internet al AEPD, la: http://www.edps.europa.eu

([12]) Avizul AEPD asupra Deciziei 2008/49/CE a Comisiei din 12 decembrie 2007 privind punerea în aplicare a Sistemului de informare al pieței interne (IMI) în ceea ce privește protecția datelor cu caracter personal (JO C 270, 25.10.2008, p. 1).

([13]) WP29 intenționează să prezinte și observații referitoare la această propunere. AEPD a urmărit acest evoluții din cadrul subgrupului relevant al WP29 și a contribuit cu observații.

2. **ANALIZA PROPUNERII**

2.1. **Opinii generale ale AEPD cu privire la propunere și la principalele provocări pe care le presupune reglementarea IMI**

11. Opiniile generale ale AEPD cu privire la IMI sunt favorabile. AEPD susține scopurile Comisiei de a crea un sistem electronic pentru schimbul de informații și de a reglementa aspectele privind protecția datelor din cadrul acestuia. Un asemenea sistem simplificat va îmbunătăți eficiența cooperării și va putea, de asemenea, să contribuie la asigurarea respectării legislației aplicabile privind protecția datelor. Sistemul poate face acestea prin oferirea unui cadru clar privind informațiile care pot fi schimbate, cu cine și în ce condiții.

12. AEPD salută, de asemenea, propunerea de către Comisie a unui instrument juridic orizontal pentru IMI sub formă de regulament al Consiliului și al Parlamentului. AEPD constată cu satisfacție faptul că propunerea evidențiază în mod cuprinzător cele mai relevante aspecte ale protecției datelor legate de IMI. Observațiile sale trebuie interpretate în acest context favorabil.

13. Cu toate acestea, AEPD avertizează că instituirea unui sistem electronic centralizat unic pentru domenii multiple ale cooperării administrative prezintă și anumite riscuri. Acestea includ, în primul rând, faptul că ar putea fi realizat schimbul de informații cu mai multe date și într-un domeniu mai larg decât este strict necesar în scopul unei cooperări eficiente și că aceste date, incluzând date potențial învechite și inexacte, ar putea rămâne în sistemul electronic mai mult decât este necesar. Securitatea acestui sistem de informare accesibil utilizatorilor din 27 de state membre este, de asemenea, o chestiune delicată, întrucât siguranța sistemului este determinată de cea mai slabă verigă a lanțului.

Principalele provocări

14. În ceea ce privește cadrul juridic al IMI care urmează să fie instituit prin regulamentul propus, AEPD atrage atenția asupra a două provocări principale:

— necesitatea asigurării consecvenței, respectând în același timp diversitatea; și

— necesitatea realizării unui echilibru între flexibilitate și securitate juridică.

15. Aceste provocări principale constituie puncte de referință importante și determină, în mare parte, abordarea adoptată de AEPD în prezentul aviz.

Consecvență, cu respectarea diversității

16. În primul rând, IMI este un sistem folosit în 27 de state membre. În stadiul actual al armonizării legislației europene, există diferențe considerabile între procedurile administrative naționale, precum și între legile naționale privind protecția datelor. IMI trebuie realizat astfel încât utilizatorii din fiecare dintre cele 27 de state membre să își poată respecta dreptul național, inclusiv legile naționale privind protecția datelor, atunci când fac schimb de date cu caracter personal prin intermediul sistemului IMI. În același timp, persoanele vizate trebuie să poată fi

asigurate de faptul că datele lor vor fi protejate cu consecvență, chiar dacă se efectuează un transfer de date prin intermediul sistemului IMI către un alt stat membru. Asigurarea consecvenței, respectând în același timp diversitatea, reprezintă o provocare importantă pentru realizarea atât a infrastructurii tehnice, cât și a celei juridice a sistemului IMI. Trebuie evitate excesele în ceea ce privește complexitatea și fragmentarea. Operațiunile de prelucrare de date care se efectuează în sistemul IMI trebuie să fie transparente, iar responsabilitățile pentru luarea deciziilor referitoare la conceperea, întreținerea și utilizarea zilnică a sistemului, precum și la supravegherea acestuia, trebuie să fie alocate în mod clar.

Realizarea unui echilibru între flexibilitate și securitate juridică

17. În al doilea rând, spre deosebire de alte sisteme informatice de mare anvergură, precum Sistemul de informații Schengen, Sistemul de informații privind vizele, Sistemul de informații al vămilor sau Eurodac, care vizează, toate, cooperarea în domenii specifice și clar definite, IMI este un instrument orizontal pentru schimbul de informații și poate fi folosit pentru facilitarea schimbului de informații în multe domenii de politică diferite. Se preconizează că domeniul de aplicare al sistemului IMI se va extinde treptat și la alte domenii de politică, iar funcționalitățile acestuia se pot modifica, de asemenea, pentru a include chiar și tipuri de cooperare administrativă nespecificate până în prezent. Aceste trăsături distinctive ale IMI fac mai dificilă definirea clară a funcționalităților sistemului și a schimburilor de date care pot avea loc în sistem. Prin urmare, este cu atât mai dificil să definești clar garanțiile corespunzătoare privind protecția datelor.

18. AEPD recunoaște faptul că este nevoie de flexibilitate și ia notă de dorința Comisiei ca regulamentul să „reziste probei timpului". Acest lucru nu trebuie să determine, totuși, o lipsă de claritate sau de securitate juridică din punctul de vedere al funcționalităților sistemului și al garanțiilor privind protecția datelor care trebuie să fie puse în aplicare. Din acest motiv, propunerea trebuie să cuprindă dispoziții cât mai explicite ori de câte ori este posibil și să facă mai mult decât să reitereze principalele principii de protecție a datelor prevăzute în Directiva 95/46/CE și în Regulamentul (CE) nr. 45/2001 ([14]).

2.2. **Domeniul de aplicare al IMI și extinderea preconizată a acestuia (articolele 3 și 4)**

2.2.1. *Introducere*

19. AEPD salută definirea clară în cadrul propunerii a domeniului de aplicare actual al sistemului IMI, în anexa I fiind enumerate actele relevante ale Uniunii pe baza cărora se poate face schimbul de informații. Acestea includ cooperarea în baza dispozițiilor specifice din Directiva privind calificările profesionale, Directiva privind serviciile și Directiva privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere ([15]).

20. Întrucât se preconizează că domeniul de aplicare al IMI se va extinde, domeniile potențiale de extindere sunt enumerate în anexa II. Elementele din anexa II pot fi transferate în anexa I printr-un act delegat care urmează să fie adoptat de Comisie în urma unei evaluări a impactului ([16]).

21. AEPD salută această metodă, întrucât: (i) delimitează clar domeniul de aplicare al IMI; (ii) asigură transparența; (iii) asigurând în același timp flexibilitatea pentru cazurile în care IMI va fi utilizat și pentru alte schimburi de informații în viitor. De asemenea, se previne astfel posibilitatea realizării vreunui schimb de informații prin intermediul IMI: (i) fără a dispune de un temei juridic adecvat în legislația specifică pieței interne care să permită sau să autorizeze schimbul de informații ([17]); și (ii) fără a include o trimitere la respectivul temei juridic în anexa I la regulament.

22. În plus, există încă incertitudini referitoare la domeniul de aplicare al sistemului IMI, cu privire la domeniile de politică în care poate fi extins și cu privire la funcționalitățile care sunt sau pot fi incluse în IMI.

23. În primul rând, nu se poate exclude posibilitatea ca domeniul de aplicare al IMI să se extindă și la alte domenii de politică decât cele enumerate în anexa I și anexa II. Acest lucru se poate produce dacă utilizarea sistemului IMI pentru anumite tipuri de schimburi de informații este prevăzută nu într-un act delegat al Comisiei, ci într-un act adoptat de Parlament și de Consiliu într-un caz în care acest lucru nu a fost preconizat în anexa II ([18]).

([14]) În această privință, a se vedea și observațiile noastre din secțiunea 2.2 cu privire la extinderea preconizată a sistemului IMI.

([15]) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

([16]) În textul proiectului de regulament în sine nu se menționează o evaluare a impactului. Cu toate acestea, la pagina 7 din expunerea de motive a propunerii se explică faptul că, prin adoptarea unui act delegat și „în urma unei evaluări a fezabilității tehnice, a raportului cost-eficiență, a ușurinței în utilizare și a impactului general al sistemului, precum și a rezultatelor unei posibile faze de testare", Comisia este împuternicită să transfere elemente din anexa II în anexa I.

([17]) Cu excepția SOLVIT (a se vedea anexa II punctul I subpunctul 1), unde nu este disponibil decât un instrument juridic neobligatoriu, o recomandare a Comisiei. Din punctul de vedere al protecției datelor, în opinia AEPD, temeiul juridic al prelucrării poate fi „acordul" persoanelor vizate, în cazul particular al SOLVIT.

([18]) Acest lucru se poate produce la inițiativa Comisiei, dar nu se poate exclude nici posibilitatea ca ideea de a utiliza IMI într-un anumit domeniu de politică să apară mai târziu în cadrul procesului legislativ, eventual la propunerea Parlamentului sau a Consiliului. Acest lucru s-a mai produs în trecut, în legătură cu Directiva privind drepturile pacienților în cadrul asistenței medicale transfrontaliere. Într-un astfel de caz este necesară mai multă claritate cu privire la „procedura" extinderii, care pare să vizeze doar situația extinderii prin intermediul actelor delegate (a se vedea dispozițiile referitoare la evaluarea impactului, acte delegate, actualizarea anexei I).

24. În al doilea rând, chiar dacă este posibil ca în unele cazuri extinderea domeniului de aplicare la noi domenii de politică să nu necesite schimbări sau să necesite numai modificări mărunte la nivelul funcționalităților existente ale sistemului ([19]), alte extinderi pot să necesite funcționalități noi sau diferite sau modificări importante ale funcționalităților existente:

— deși propunerea se referă la câteva funcționalități existente sau preconizate, adesea aceste trimiteri nu sunt suficient de clare sau suficient de detaliate. Acest lucru este valabil, într-o măsură mai mică sau mai mare, pentru trimiterile la alerte, actori externi, liste de informații, acorduri de asistență reciprocă și soluționarea problemelor ([20]). Spre exemplificare, termenul „alertă", care se referă la o funcționalitate existentă foarte importantă, este menționat o singură dată, la considerentul 10;

— conform regulamentului propus, este posibil să se adopte noi tipuri de funcționalități care nu sunt menționate deloc în propunere;

— sistemul IMI a fost descris până în prezent ca un instrument informatic destinat schimbului de informații: cu alte cuvinte, un instrument de comunicare (a se vedea, de exemplu, articolul 3 din propunere). Totuși, unele dintre funcționalitățile menționate în propunere, inclusiv funcția de „listă de informații", par să depășească acest rol. Propunerea de prelungire a perioadelor de păstrare la cinci ani sugerează, de asemenea, un pas către transformarea în „bază de date". Aceste evoluții ar schimba fundamental natura sistemului IMI ([21]).

2.2.2. *Recomandări*

25. În vederea eliminării acestor incertitudini, AEPD recomandă o abordare dublă. AEPD propune, în primul rând, ca funcționalitățile care sunt deja previzibile să fie clarificate și abordate într-un mod mai explicit, iar în al doilea rând, să se aplice garanții procedurale adecvate prin care să se garanteze că protecția datelor va fi analizată cu atenție și în cursul evoluției de viitor a IMI.

Clarificarea funcționalităților deja existente sau previzibile (de exemplu, schimburi bilaterale, alerte, liste de informații, rezolvarea problemelor și actorii externi)

26. AEPD recomandă ca regulamentul să fie mai explicit în privința funcționalităților, atunci când acestea sunt deja cunoscute, așa cum este cazul schimburilor de informații la care se referă anexele I și II.

27. De exemplu, ar putea fi prevăzute măsuri mai concrete și mai clare pentru integrarea SOLVIT ([22]) în IMI (prevederi privind „actorii externi" și „soluționarea problemelor") și pentru directoarele de profesioniști și furnizori de servicii (prevederi privind „listele de informații").

28. Ar trebui, de asemenea, aduse clarificări suplimentare cu privire la „alerte", care sunt deja folosite în temeiul Directivei privind serviciile și pot fi introduse și în domenii de politică suplimentare. În special „alerta" ca funcționalitate ar trebui definită clar la articolul 5 (împreună cu alte funcționalități, precum schimburile de informații bilaterale și listele de informații). De asemenea, trebuie clarificate și drepturile de acces și perioadele de păstrare ([23]).

Garanțiile procedurale (evaluarea impactului asupra protecției datelor și consultarea autorităților de protecție a datelor)

29. În cazul în care intenția este ca regulamentul să rămână „rezistent la proba timpului" din punctul de vedere al funcționalităților suplimentare ce pot deveni necesare pe termen mai lung, permițând astfel introducerea unor funcționalități suplimentare nedefinite încă în regulament, acest lucru trebuie să fie însoțit de garanții procedurale adecvate, care să asigure introducerea unor dispoziții corespunzătoare privind punerea în aplicare a garanțiilor necesare privind protecția datelor, înainte de exploatarea noii funcționalități. Același lucru trebuie să se aplice și pentru extinderile în noi domenii de politică, atunci când extinderea respectivă are un impact asupra protecției datelor.

30. AEPD recomandă un mecanism clar care să asigure realizarea unei analize atente a motivelor de îngrijorare legate de protecția datelor, înainte de fiecare extindere a funcționalităților sau extindere în noi domenii de politică și, dacă este necesar, punerea în aplicare a unor garanții suplimentare sau măsuri tehnice în arhitectura IMI. În special:

— evaluarea impactului menționată la pagina 7 din expunerea de motive ar trebui să fie solicitată în mod explicit chiar în regulament și ar trebui să cuprindă și o evaluare a impactului asupra protecției datelor, care să arate concret dacă și ce modificări sunt necesare privind modul în care este conceput IMI, astfel încât acesta să cuprindă în continuare garanții adecvate privind protecția datelor, care să includă și noile domenii de politică și/sau funcționalități;

— regulamentul ar trebui să prevadă explicit necesitatea consultării AEPD și a autorităților naționale de protecție a datelor înainte de fiecare extindere a IMI. Această consultare poate avea loc prin intermediul mecanismului prevăzut pentru supravegherea coordonată, la articolul 20.

([19]) De exemplu, schimburile de informații bilaterale care se efectuează în baza Directivei privind calificările profesionale și a Directivei privind drepturile pacienților în cadrul asistenței medicale transfrontaliere urmăresc în principal aceeași structură și pot fi abordate folosind funcționalități similare, sub rezerva unor garanții similare privind protecția datelor.

([20]) A se vedea considerentele 2, 10, 12, 13, 15 și articolul 5 literele (b) și (i), articolul 10 alineatul (7) și articolul 13 alineatul (2).

([21]) În legătură cu aceasta, dacă există intenția ca IMI să înlocuiască sau să completeze sistemele actuale de gestionare a dosarelor și de arhivare, și/sau de a folosi sistemul ca bază de date, acest lucru trebuie clarificat la articolul 3.

([22]) A se vedea anexa II punctul I subpunctul 1.

([23]) A se vedea secțiunile 2.4 și 2.5.5 de mai jos.

31. Aceste garanții procedurale (evaluarea impactului asupra protecției datelor și consultarea) trebuie aplicate atât unei extinderi printr-un act delegat al Comisiei (care transferă un element din anexa II în anexa I), cât și unei extinderi printr-un regulament al Parlamentului și al Consiliului care adaugă un element ce nu a fost enumerat în anexa II.

32. În cele din urmă, AEPD recomandă ca regulamentul să clarifice dacă domeniul de aplicare al actelor delegate pe care Comisia va fi împuternicită să le adopte în temeiul articolului 23 va include și alte aspecte decât transferarea unor elemente din anexa II în anexa I. Dacă este posibil, Comisia ar trebui să fie împuternicită prin regulament să adopte anumite acte de punere în aplicare sau delegate pentru a defini în continuare orice funcționalitate suplimentară a sistemului sau pentru a răspunde motivelor de îngrijorare legate de protecția datelor care ar putea apărea în viitor.

2.3. **Roluri, competențe și responsabilități (articolele 7-9)**

33. AEPD salută faptul că un capitol întreg (capitolul II) a fost dedicat clarificării funcțiilor și responsabilităților diferiților actori implicați în IMI. Dispozițiile respective ar putea fi consolidate și mai mult conform celor ce urmează.

34. Articolul 9 descrie responsabilitățile care decurg din rolul de controlor al Comisiei. AEPD recomandă în continuare includerea unei prevederi suplimentare referitoare la rolul Comisiei de a asigura conceperea sistemului cu aplicarea principiului „luării în considerare a vieții private începând cu momentul conceperii”, precum și la rolul acesteia de coordonare în ceea ce privește aspectele de protecție a datelor.

35. AEPD constată cu satisfacție faptul că sarcinile coordonatorilor IMI enumerate la articolul 7 cuprind acum în mod explicit sarcini de coordonare legate de protecția datelor, inclusiv rolul de punct de contact pentru Comisie. AEPD recomandă să se precizeze în mod suplimentar faptul că aceste sarcini de coordonare includ si menținerea contactului cu autoritățile naționale de protecție a datelor.

2.4. **Drepturi de acces (articolul 10)**

36. Articolul 10 prevede garanții cu privire la drepturile de acces. AEPD salută faptul că aceste dispoziții au fost consolidate în mod semnificativ ca urmare a observațiilor sale.

37. Având în vedere caracterul orizontal și extensibil al IMI, este important să se asigure garantarea de către sistem a aplicării „zidurilor chinezești”, care limitează informațiile prelucrate într-un anumit domeniu de politică exclusiv la domeniul de politică respectiv: utilizatorii IMI trebuie: (i) să acceseze informațiile numai din motive care țin de necesitatea de a cunoaște; și (ii) să se limiteze la un singur domeniu de politică.

38. Dacă este inevitabil ca un utilizator IMI să aibă drept de acces la mai multe domenii de politică (cum se întâmplă, de exemplu, în cazul unora dintre oficiile guvernamentale locale), ar trebui, cel puțin, ca sistemul să nu permită combinarea informațiilor provenite din domenii de politică diferite. Eventualele excepții, dacă sunt necesare, trebuie prevăzute în legislația de aplicare sau într-un act al Uniunii, cu respectarea strictă a principiului limitării scopului.

39. Aceste principii sunt prezentate acum în textul regulamentului, dar ar putea fi consolidate și operaționalizate în continuare.

40. În ceea ce privește drepturile de acces ale Comisiei, AEPD salută faptul că articolul 9 alineatele (2) și (4) și articolul 10 alineatul (6) din propunere, coroborate, precizează că Comisia nu are acces la datele cu caracter personal transmise între statele membre, cu excepția cazurilor în care Comisia este desemnată ca participant la o procedură de cooperare administrativă.

41. Drepturile de acces ale actorilor externi și drepturile de acces la alerte trebuie, de asemenea, explicitate mai bine ([24]). În ceea ce privește alertele, AEPD recomandă ca regulamentul să prevadă faptul că alertele nu trebuie trimise automat tuturor autorităților competente relevante din toate statele membre, ci doar celor vizate, pe baza necesității de a cunoaște. Acest lucru nu exclude trimiterea alertelor către toate statele membre în anumite cazuri sau în anumite domenii de politică, dacă sunt vizate toate. În mod similar, este necesară o analiză de la caz la caz pentru a stabili dacă Comisia trebuie să aibă acces la alerte.

2.5. **Păstrarea datelor cu caracter personal (articolele 13 și 14)**

2.5.1. *Introducere*

42. Articolul 13 din propunere prelungește durata stocării datelor în sistemul IMI de la perioada actuală de șase luni (calculată de la închiderea cazului) la cinci ani, cu o „blocare” a datelor după 18 luni. În cursul perioadei de „blocare”, datele sunt accesibile doar urmând o procedură specifică de extragere, care poate fi inițiată numai la cererea persoanei vizate sau în cazul în care datele sunt necesare „în scopul dovedirii faptului că a avut loc un schimb de informații prin intermediul sistemului IMI”.

43. În realitate, în acest mod, datele sunt stocate în sistemul IMI pe parcursul a trei perioade distincte:

— între momentul introducerii și momentul închiderii cazului;

— după închiderea cazului, pentru o perioadă de 18 luni ([25]);

— după expirarea perioadei de 18 luni, sub formă de date blocate pentru o perioadă suplimentară de trei ani și șase luni (cu alte cuvinte, până la expirarea a cinci ani de la închiderea cazului).

([24]) A se vedea și secțiunea 2.2.2.

([25]) Articolul 13 alineatul (1) sugerează că cele 18 luni reprezintă un termen „maxim”, aceasta însemnând că se poate stabili și o perioadă mai scurtă. Acest lucru nu ar influența, totuși, durata totală a păstrării, care s-ar întinde, în orice caz, până la expirarea a cinci ani de la închiderea cazului.

44. În plus față de aceste norme generale, articolul 13 alineatul (2) permite păstrarea datelor într-o „listă de informații" atât timp cât este necesar în acest scop, cu acordul persoanei vizate sau atunci când „acest lucru este necesar pentru conformitatea cu un act al Uniunii". În continuare, articolul 14 prevede un mecanism similar de blocare pentru păstrarea datelor cu caracter personal ale utilizatorilor IMI, pentru o perioadă de cinci ani de la data la care aceștia încetează a mai fi utilizatori IMI.

45. Nu există alte dispoziții specifice. Prin urmare, se intenționează, probabil, ca normele generale să se aplice nu doar schimburilor bilaterale, ci și alertelor, soluționării problemelor (ca și în SOLVIT ([26])) și tuturor celorlalte funcționalități care implică prelucrarea datelor cu caracter personal.

46. AEPD are mai multe motive de îngrijorare cu privire la perioadele de păstrare, prin prisma articolului 6 alineatul (1) litera (e) din Directiva 95/46/CE și a articolului 4 alineatul (1) litera (e) din Regulamentul (CE) nr. 45/2001, ambele impunând ca datele cu caracter personal să fie păstrate pentru o perioadă de timp care nu o depășește pe cea necesară scopurilor pentru care au fost colectate sau pentru care sunt ulterior prelucrate.

2.5.2. *De la introducere și până la închiderea cazului: necesitatea unei închideri în timp util a cazului*

47. În ceea ce privește prima perioadă, de la introducere și până la închiderea cazului, AEPD este preocupată de riscul ca unele cazuri să nu se închidă niciodată sau să se închidă numai după o perioadă disproporționat de lungă de timp. Acest lucru poate avea drept rezultat rămânerea unor date cu caracter personal în baza de date pentru o perioadă de timp mai lungă decât cea necesară, sau chiar pe termen nedefinit.

48. AEPD înțelege progresele înregistrate de Comisie, la nivel practic, în reducerea restanțelor din cadrul IMI și faptul că există un sistem care funcționează pentru schimburile bilaterale, monitorizând închiderea în timp util a cazurilor și semnalând periodic întârzierile. În plus, o nouă modificare introdusă în funcționalitățile sistemului, ca urmare a unei abordări conform principiului „luării în considerare a vieții private începând cu momentul conceperii", permite ca, printr-o singură apăsare de buton, să se accepte un răspuns și, în același timp, să se și închidă cazul. Înainte era nevoie de două acțiuni separate pentru acest lucru, iar aceasta ar putea explica unele dintre cazurile inactive rămase în sistem.

49. AEPD salută aceste eforturi depuse la nivel practic. Cu toate acestea, recomandă ca însuși textul regulamentului să prevadă garanții pentru închiderea în timp util a cazurilor în IMI și pentru ștergerea din baza de date a cazurilor inactive (cazuri fără activitate recentă).

([26]) A se vedea anexa II punctul I subpunctul 1.

2.5.3. *De la închiderea cazului și până la expirarea a 18 luni: este justificată prelungirea perioadei de șase luni?*

50. AEPD propune să se reanalizeze dacă există o justificare adecvată pentru prelungirea perioadei actuale de șase luni la 18 luni de la închiderea cazului și, în caz afirmativ, dacă aceasta se aplică numai schimburilor de informații bilaterale sau și altor tipuri de funcționalități. IMI există deja de mai mulți ani, iar experiența practică acumulată în această privință ar trebui valorificată.

51. Dacă IMI rămâne un instrument pentru schimbul de informații (spre deosebire de un sistem de gestionare a dosarelor, o bază de date sau un sistem de arhivare) și dacă autoritățile competente dispun de mijloace de extragere din sistem a informațiilor pe care le-au primit (fie în formă electronică, fie pe hârtie, dar în orice caz într-un mod în care informațiile extrase să poată fi utilizate ca dovezi ([27])), nu mai apare necesitatea ca datele să fie păstrate în IMI după închiderea cazului.

52. În schimburile de informații bilaterale, o perioadă de păstrare (rezonabil de scurtă) după închiderea cazului poate fi justificată de eventuala necesitate de a pune întrebări de monitorizare chiar și după ce a fost acceptat un răspuns și, astfel, s-a închis un caz. Perioada actuală de șase luni pare a fi, *prima facie*, suficient de generoasă în acest scop.

2.5.4. *De la 18 luni la cinci ani: date „blocate"*

53. AEPD consideră că nu au fost oferite justificări suficiente de către Comisie cu privire la necesitatea și proporționalitatea păstrării „datelor blocate" pentru o perioadă de până la cinci ani.

54. Expunerea de motive, de la pagina 8, face trimitere la hotărârea Curții de Justiție din cauza *Rijkeboer* ([28]). AEPD recomandă Comisiei să reanalizeze implicațiile acestei cauze asupra păstrării datelor în sistemul IMI. În opinia sa, *Rijkeboer* nu impune ca sistemul să fie configurat astfel încât să se păstreze date timp de cinci ani de la închiderea cazului.

55. AEPD nu consideră că trimiterea la hotărârea din cauza *Rijkeboer* sau la drepturile persoanelor vizate de a avea acces la datele proprii reprezintă o justificare suficientă și adecvată pentru păstrarea datelor în IMI pentru o perioadă de cinci ani de la închiderea cazului. Chiar și păstrarea „datelor de registru" (definite strict ca excluzând orice conținut, printre altele toate atașamentele sau datele sensibile) poate fi o opțiune mai puțin intruzivă, care ar merita o analiză suplimentară. Cu toate acestea, nici măcar legat de această opțiune, AEPD nu are convingerea, în acest moment, că ar fi necesară sau proporțională.

([27]) Înțelegem că s-au depus eforturi pentru a asigura acest lucru la nivel practic.

([28]) C-553/07, Rijkeboer, Rec., 2009, p. I-3889.

56. În plus, lipsa de claritate cu privire la cei care pot accesa „datele blocate" și în ce scop este, de asemenea, problematică. Simpla referire la utilizarea „în scopul dovedirii faptului că a avut loc un schimb de informații" [precum cea de la articolul 13 alineatul (3)] nu este suficientă. Dacă dispoziția referitoare la „blocare" se menține, ar trebui, în orice caz, să se precizeze mai exact cine poate solicita o dovadă a faptului că a avut loc un schimb de informații și în ce context. În plus față de persoana vizată, ar mai avea și alte persoane dreptul de a solicita accesul? Dacă da, acestea ar fi exclusiv autoritățile competente și exclusiv cu scopul de a dovedi faptul că un anumit schimb de informații, cu un anumit conținut, a avut loc (în cazul în care schimbul respectiv este contestat de către autoritățile competente care au trimis sau au primit mesajul)? Se mai anticipează și alte utilizări posibile „în scopul dovedirii faptului că a avut loc un schimb de informații" ([29])?

2.5.5. *Alertele*

57. AEPD recomandă o distincție mai clară între alerte și listele de informații. Trebuie făcută diferența între folosirea unei alerte ca instrument de comunicare pentru avertizarea autorităților competente în legătură cu un anumit delict sau o suspiciune și stocarea acestei alerte într-o bază de date pentru o perioadă de timp prelungită sau chiar nedefinită. Stocarea informațiilor referitoare la alertă ar da naștere unor motive de îngrijorare suplimentare și ar necesita norme specifice și garanții suplimentare privind protecția datelor.

58. Prin urmare, AEPD recomandă ca regulamentul să prevadă, ca normă implicită, ca: (i) – cu excepția cazului în care se prevedere altfel în legislația verticală și sub rezerva unor garanții suplimentare adecvate – alertelor să li se aplice o perioadă de păstrare de șase luni; și, mai important, ca (ii) această perioadă să fie calculată începând cu momentul trimiterii alertei.

59. În mod alternativ, AEPD recomandă ca în regulamentul propus să se stabilească explicit garanții detaliate cu privire la alerte. AEPD este pregătită să ajute în continuare Comisia și legiuitorii cu recomandări în această privință, în cazul în care se adoptă această a doua abordare.

2.6. **Categorii speciale de date (articolul 15)**

60. AEPD salută diferențierea între datele cu caracter personal menționate la articolul 8 alineatul (1) din Directiva 95/46/CE, pe de o parte, și datele cu caracter personal menționate la articolul 8 alineatul (5), pe de altă parte. De asemenea, AEPD salută faptul că regulamentul precizează clar categoriile speciale de date care pot fi prelucrate numai pe baza unui motiv specific menționat la articolul 8 din Directiva 95/46/CE.

61. În această privință, interpretarea AEPD este aceea că IMI va prelucra un volum semnificativ de date sensibile care intră sub incidența articolului 8 alineatul (2) din Directiva 95/46/CE. Într-adevăr, încă de la început, când a fost exploatat în scopul sprijinirii cooperării administrative în temeiul Directivei privind serviciile și al Directivei privind calificările profesionale, IMI a fost conceput pentru a prelucra astfel de date, în special date referitoare la evidențele infracțiunilor și contravențiilor care pot avea consecințe asupra dreptului profesionistului sau al furnizorului de servicii de a presta activitatea/serviciile respective într-un alt stat membru.

62. În plus, este posibil ca în sistemul IMI să se prelucreze și o cantitate semnificativă de date sensibile conform articolului 8 alineatul (1) (în principal date din domeniul sănătății), după ce IMI se va extinde pentru a include un modul pentru SOLVIT ([30]). În cele din urmă, nu se poate exclude posibilitatea ca, în viitor, prin IMI să se colecteze și alte date sensibile, *ad hoc* sau în mod sistematic.

2.7. **Securitatea (articolul 16 și considerentul 16)**

63. AEPD constată cu satisfacție faptul că articolul 16 se referă în mod explicit la obligația Comisiei de a-și respecta propriile norme interne adoptate conform articolului 22 din Regulamentul (CE) nr. 45/2001 și de a adopta și actualiza în permanență un plan de securitate pentru IMI.

64. Pentru a consolida și mai mult aceste dispoziții, AEPD recomandă ca regulamentul să impună o evaluare a riscului și o analiză a planului de securitate înainte de orice extindere a IMI într-un domeniu de politică nou sau înainte de adăugarea unei noi funcționalități cu impact asupra datelor cu caracter personal ([31]).

65. În plus, AEPD constată și faptul că articolul 16 și considerentul 16 se referă numai la obligațiile Comisiei și la rolul de supraveghere al AEPD. Această mențiune poate induce în eroare. Deși Comisia este, într-adevăr, operatorul sistemului și în această calitate răspunde de o parte predominantă din activitățile de menținere a securității IMI, obligații mai au și autoritățile competente care, la rândul lor, sunt supravegheate de autoritățile naționale de protecție a datelor. Prin urmare, articolul 16 și considerentul 16 ar trebui să se refere și la obligațiile privind securitatea aplicabile celorlalți actori IMI în temeiul Directivei 95/46/CE și la competențele de supraveghere care revin autorităților naționale de protecție a datelor.

2.8. **Informațiile furnizate persoanelor vizate și transparența (articolul 17)**

2.8.1. *Informații furnizate în statele membre*

66. În ceea ce privește articolul 17 alineatul (1), AEPD recomandă ca regulamentul să conțină mai multe dispoziții specifice care să asigure informarea deplină a persoanelor vizate cu privire la prelucrarea datelor lor în cadrul IMI. Având în vedere faptul că sistemul IMI este folosit de numeroase autorități competente, printre care multe oficii guvernamentale locale, se recomandă insistent ca transmiterea notificărilor să fie coordonată la nivel național.

([29]) Deși păstrarea datelor cu caracter personal prezintă comparativ mai puține riscuri pentru viața privată, AEPD consideră, totuși, că nici păstrarea datelor cu caracter personal ale utilizatorilor IMI pentru o perioadă de cinci ani după ce aceștia nu mai au acces la IMI nu a fost justificată suficient.

([30]) A se vedea anexa II punctul I subpunctul 1.

([31]) A se vedea și secțiunea 12 privind recomandările referitoare la audituri.

2.8.2. *Informații furnizate de către Comisie*

67. Articolul 17 alineatul (2) litera (a) impune Comisiei să transmită o notificare privind confidențialitatea referitoare la activitățile de prelucrare a datelor proprii, în conformitate cu articolele 10 și 11 din Regulamentul (CE) nr. 45/2001. În plus, articolul 17 alineatul (2) litera (b) impune Comisiei să furnizeze, de asemenea, informații privind „aspectele legate de protecția datelor în cadrul procedurilor de cooperare administrativă în IMI menționate la articolul 12". În sfârșit, articolul 17 alineatul (2) litera (c) impune Comisiei să furnizeze informații cu privire la „excepții sau limitări ale drepturilor persoanelor vizate menționate la articolul 19".

68. AEPD constată cu satisfacție introducerea acestor dispoziții, care contribuie la asigurarea transparenței operațiunilor de prelucrare a datelor în cadrul IMI. Conform observațiilor din secțiunea 2.1 de mai sus, în cazul unui sistem informatic folosit în 27 de state membre este crucial să se asigure consecvența în ceea ce privește operarea sistemului, garanțiile privind protecția datelor aplicate și informațiile furnizate persoanelor vizate ([32]).

69. În plus, dispozițiile articolului 17 alineatul (2) ar trebui să fie consolidate și mai mult. Comisia, în calitate de operator al sistemului, este cea mai potrivită pentru a prelua un rol proactiv în asigurarea unui prim „nivel" de notificare privind protecția datelor și în furnizarea altor informații relevante pentru persoanele vizate, pe site-ul său internet multilingv, precum și „în numele" autorităților competente, adică incluzând informațiile necesare în conformitate cu articolul 10 sau 11 din Directiva 95/46/CE. În acest caz, de cele mai multe ori ar fi suficient ca notificările transmise de autoritățile competente din statele membre să facă doar o trimitere la notificarea Comisiei, completând-o, după caz, cu orice informație suplimentară specifică impusă de dreptul național.

70. În plus, articolul 17 alineatul (2) litera (b) ar trebui să clarifice faptul că informațiile furnizate de către Comisie se vor referi în mod complet la toate domeniile de politică, la toate tipurile de proceduri de cooperare administrativă și la toate funcționalitățile din cadrul IMI și, de asemenea, vor include în mod explicit categoriile de date care pot fi prelucrate. Aceasta trebuie să includă publicarea pe site-ul internet al IMI a seturilor de întrebări folosite în cooperarea bilaterală, astfel cum se procedează în practică în prezent.

2.9. **Drepturile de acces, rectificare și anulare (articolul 18)**

71. AEPD dorește să se refere încă o dată, după cum s-a menționat în secțiunea 2.1 de mai sus, la faptul că este crucial să se asigure consecvența în ceea ce privește operarea sistemului și garanțiile care se aplică privind protecția datelor. Din acest motiv, AEPD ar explicita și mai mult dispozițiile referitoare la drepturile de acces, de corectare și de ștergere.

72. Articolul 18 ar trebui să precizeze cui trebuie să se adreseze persoanele vizate pentru a depune o cerere de acces. Acest lucru ar trebui să fie clar în privința accesului la date pe parcursul unor perioade de timp diferite:

— înainte de închiderea cazului;

— după închiderea cazului, dar înainte de expirarea perioadei de păstrare de 18 luni;

— și, în cele din urmă, în cursul perioadei în care datele sunt „blocate".

73. Regulamentul ar trebui, de asemenea, să impună autorităților competente să coopereze în privința cererilor de acces, dacă este necesar. Corectarea și ștergerea ar trebui să se efectueze „cât mai curând, dar în termen de cel mult 60 de zile" mai degrabă decât „în termen de 60 de zile". Ar trebui, de asemenea, să se facă trimiteri la posibilitatea creării unui modul de protecție a datelor și la posibilitatea adoptării soluțiilor de „luare în considerare a vieții private începând cu momentul conceperii" în ceea ce privește cooperarea între autorități cu privire la drepturile de acces, precum și „împuternicirea persoanelor vizate", de exemplu, acordându-le acces direct la datele lor, atunci când acest lucru este relevant și fezabil.

2.10. **Supravegherea (articolul 20)**

74. În ultimii ani a fost elaborat modelul „supravegherii coordonate". Acest model de supraveghere, astfel cum funcționează în prezent în Eurodac și în anumite părți ale Sistemului de informații al vămilor, a fost adoptat și pentru Sistemul de informații privind vizele (VIS) și pentru Sistemul de informații Schengen de a doua generație (SIS II).

75. Acest model are trei niveluri:

— supravegherea la nivel național este asigurată de autoritățile naționale de protecție a datelor;

— supravegherea la nivelul UE este asigurată de AEPD;

— coordonarea este asigurată prin reuniuni periodice și alte activități coordonate, sprijinite de AEPD prin îndeplinirea rolului de secretariat pentru acest mecanism de coordonare.

76. Acest model care s-a bucurat de succes și s-a dovedit a fi eficient ar trebui luat în considerare în viitor pentru alte sisteme de informații.

77. AEPD salută faptul că articolul 20 din propunere prevede în mod explicit supravegherea coordonată între autoritățile naționale de protecție a datelor și AEPD urmând – în linii mari – modelul stabilit în regulamentele VIS și SIS II ([33]).

([32]) Această abordare de asigurare a consecvenței trebuie, desigur, să țină seama de orice divergență națională, atunci când acest lucru este necesar și justificat.

([33]) A se vedea Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (SIS II) (JO L 381, 28.12.2006, p. 4) și Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS) (JO L 218, 13.8.2008, p. 60).

78. AEPD ar dori o consolidare a dispozițiilor privind supravegherea coordonată, în anumite privințe și, în acest scop, se pronunță pentru introducerea unor dispoziții similare celor existente, de exemplu, în contextul Sistemului de informații privind vizele (articolele 41-43 din Regulamentul VIS) și al Schengen II (articolele 44-46 din Regulamentul SIS II) și preconizate pentru Eurodac ([34]). În special, ar fi util ca regulamentul:

— la articolul 20 alineatele (1) și (2), să stabilească și să împartă mai clar sarcinile de supraveghere ale autorităților naționale de protecție a datelor și respectiv ale AEPD ([35]);

— la articolul 20 alineatul (3), să precizeze faptul că autoritățile naționale de protecție a datelor și AEPD, acționând fiecare în conformitate cu propriile competențe, „cooperează activ" și „asigură o supraveghere coordonată a IMI" (mai degrabă decât să se refere doar la supravegherea coordonată, fără a menționa cooperarea activă) ([36]); și

— să precizeze mai în detaliu ce poate cuprinde cooperarea, de exemplu impunând autorităților naționale de protecție a datelor și AEPD, „acționând fiecare în conformitate cu propriile competențe, să facă schimb de informații relevante, să se asiste reciproc în realizarea activităților de audit și a inspecțiilor, să examineze dificultățile legate de interpretarea sau punerea în aplicare a Regulamentului IMI, să analizeze problemele care pot apărea în ceea ce privește exercitarea supravegherii independente sau a drepturilor persoanelor vizate, să formuleze propuneri armonizate în vederea găsirii unor soluții comune la eventualele probleme și să asigure sensibilizarea în privința drepturilor în materie de protecție a datelor, dacă este necesar" ([37]).

79. Acestea fiind spuse, AEPD este conștientă de dimensiunea actuală mai redusă, de natura diferită a datelor prelucrate, precum și de caracterul evolutiv al sistemului IMI. Prin urmare, AEPD recunoaște faptul că, în privința frecvenței reuniunilor și a auditurilor, ar fi recomandabilă mai multă flexibilitate. Pe scurt, AEPD recomandă ca regulamentul să prevadă normele minime necesare pentru asigurarea unei cooperări eficiente, dar fără să creeze sarcini administrative inutile.

80. Articolul 20 alineatul (3) din propunere nu impune reuniuni periodice, ci prevede doar că AEPD poate „invita autoritățile naționale de supraveghere să se reunească […] dacă acest lucru este necesar". AEPD salută faptul că aceste dispoziții lasă la latitudinea părților implicate să decidă cu privire la frecvența și modalitățile în care să aibă loc reuniunile, precum și alte detalii procedurale ale cooperării lor. Acestea pot fi convenite în cadrul normelor de procedură, care sunt deja menționate în propunere.

81. În ceea ce privește auditurile periodice, de asemenea poate fi mai eficient ca autoritățile care cooperează să aibă dreptul de a stabili, în normele lor de procedură, când și cu ce frecvență să aibă loc auditurile. Aceste lucruri pot să depindă de o serie de factori și pot să sufere modificări în timp. Prin urmare, AEPD sprijină abordarea Comisiei, care și în această privință permite mai multă flexibilitate.

2.11. **Utilizarea IMI la nivel național**

82. AEPD salută faptul că propunerea prevede un temei juridic clar pentru utilizarea IMI la nivel național și că această utilizare este supusă mai multor condiții, inclusiv aceea că autoritatea națională de protecție a datelor trebuie consultată și că utilizarea respectivă trebuie să fie în conformitate cu dreptul național.

2.12. **Schimbul de informații cu țări terțe (articolul 22)**

83. AEPD salută cerințele stabilite la articolul 22 alineatul (1) pentru schimburile de informații, precum și faptul că articolul 22 alineatul (3) asigură transparența procesului de extindere prin publicarea în Jurnalul Oficial a unei liste actualizate a țărilor terțe care utilizează sistemul IMI [articolul 22 alineatul (3)].

84. În plus, AEPD recomandă Comisiei să limiteze trimiterea la derogările în temeiul articolului 26 din Directiva 95/46/CE astfel încât să includă numai articolul 26 alineatul (2). Cu alte cuvinte: autoritățile competente sau alți actori externi dintr-o țară terță care nu își poate permite o protecție adecvată nu ar trebui să aibă acces direct la IMI decât în cazul în care există clauze contractuale corespunzătoare în vigoare. Aceste clauze ar trebui negociate la nivelul Uniunii Europene.

85. AEPD subliniază faptul că nu ar trebui folosite alte derogări, precum aceea ca „transferul să fie necesar sau impus prin lege pentru apărarea unui interes public important, sau pentru constatarea, exercitarea sau apărarea unui drept în justiție", pentru a justifica transferuri de date către țări terțe care folosesc accesul direct la IMI ([38]).

2.13. **Responsabilitatea (articolul 26)**

86. În concordanță cu consolidarea preconizată a acordurilor pentru creșterea responsabilității în cadrul analizei cadrului de protecție a datelor la nivelul UE ([39]), AEPD recomandă ca regulamentul să stabilească un cadru clar pentru instituirea unor mecanisme de control intern adecvate, care să asigure respectarea protecției datelor și să furnizeze dovezi în acest sens, și care să conțină cel puțin elementele menționate în cele ce urmează.

([34]) Regulamentul (CE) nr. 2725/2000 al Consiliului din 11 decembrie 2000 privind instituirea sistemului „Eurodac" pentru compararea amprentelor digitale în scopul aplicării eficiente a Convenției de la Dublin (JO L 316, 15.12.2000, p. 1), în prezent în curs de revizuire. În acest context, sunt luate în considerare dispoziții similare celor din regulamentele VIS și SIS II.

([35]) A se vedea, de exemplu, articolele 41 și 42 din Regulamentul VIS.

([36]) A se vedea, de exemplu, articolul 43 alineatul (1) din Regulamentul VIS.

([37]) A se vedea, de exemplu, articolul 43 alineatul (2) din Regulamentul VIS.

([38]) O abordare similară a fost adoptată la articolul 22 alineatul (2) pentru situația Comisiei în calitate de actor IMI.

([39]) A se vedea secțiunea 2.2.4 din Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor – „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană", COM(2010) 609 final. A se vedea și secțiunea 7 din avizul emis de AEPD cu privire la această comunicare a Comisiei la 14 ianuarie 2011.

87. În acest context, AEPD salută cerința de la articolul 26 alineatul (2) din regulament, conform căreia o dată la trei ani Comisia trebuie să prezinte AEPD un raport privind aspectele referitoare la protecția datelor, inclusiv la securitate. Ar fi recomandabil ca regulamentul să clarifice faptul că AEPD, la rândul său, ar fi obligată să transmită raportul Comisiei la autoritățile naționale de protecție a datelor, în cadrul supravegherii coordonate menționate la articolul 20. De asemenea, ar fi util să se clarifice faptul că raportul trebuie să se refere, cu privire la fiecare domeniu de politică și la fiecare funcționalitate, la felul cum au fost abordate în practică cele mai importante principii și motive de îngrijorare privind protecția datelor (de exemplu, informațiile destinate persoanelor vizate, drepturile de acces, securitatea).

88. În plus, regulamentul ar trebui să clarifice și necesitatea ca structura-cadru pentru mecanismele de control intern să includă și declarații de confidențialitate (incluzând și o analiză de risc privind securitatea), o politică de protecție a datelor (incluzând un plan de securitate) adoptată pe baza rezultatelor acestora, precum și verificări și audituri periodice.

2.14. **Luarea în considerare a vieții private începând cu momentul conceperii**

89. AEPD salută trimiterea la acest principiu care se face la considerentul 6 din regulament ([40]). AEPD recomandă ca, în afară de această trimitere, regulamentul să mai introducă și garanții specifice pentru luarea în considerare a vieții private începând cu momentul conceperii, precum:

— un modul de protecție a datelor care să permită persoanelor vizate să își exercite drepturile mai eficient ([41]);

— o linie de demarcație clară între diferitele domenii de politică incluse în IMI („zidurile chinezești") ([42]);

— soluții tehnice specifice care să limiteze capacitățile de căutare în directoare, informațiile referitoare la alerte și alte aspecte, pentru a asigura limitarea scopului;

— măsuri specifice prin care să se asigure închiderea cazurilor fără activitate ([43]);

— garanții procedurale adecvate în contextul evoluțiilor viitoare ([44]).

3. **CONCLUZII**

90. Opiniile generale ale AEPD cu privire la IMI sunt favorabile. AEPD susține scopurile Comisiei de a crea un sistem electronic pentru schimbul de informații și de a reglementa aspectele privind protecția datelor ale acestuia. De asemenea, AEPD salută propunerea de către Comisie a unui instrument juridic orizontal pentru IMI sub formă de regulament al Parlamentului și al Consiliului. AEPD constată cu satisfacție faptul că propunerea evidențiază în mod cuprinzător cele mai relevante aspecte ale protecției datelor legate de IMI.

91. În ceea ce privește cadrul juridic al IMI care urmează să fie instituit prin regulamentul propus, AEPD atrage atenția asupra a două provocări majore:

— necesitatea asigurării consecvenței, respectând în același timp diversitatea; și

— necesitatea realizării unui echilibru între flexibilitate și securitate juridică.

92. Funcționalitățile IMI care sunt deja previzibile ar trebui să fie clarificate și abordate într-un mod mai explicit.

93. Ar trebui să se aplice garanții procedurale adecvate, prin care să se asigure luarea atentă în considerare a protecției datelor în cursul dezvoltării viitoare a IMI. Printre acestea trebuie să se numere o evaluare a impactului și consultarea AEPD și a autorităților naționale de protecție a datelor înainte de fiecare extindere a domeniului de aplicare al IMI cu un domeniu de politică nou și/sau cu funcționalități noi.

94. Drepturile de acces ale actorilor externi și drepturile de acces la alerte ar trebui să fie mai bine explicitate.

95. În ceea ce privește perioadele de păstrare:

— regulamentul ar trebui să prevadă garanții privind închiderea în timp util a cazurilor în cadrul IMI și ștergerea din baza de date a cazurilor inactive (cazuri fără activitate recentă);

— ar trebui să se reanalizeze dacă există o justificare adecvată pentru prelungirea perioadei actuale de șase luni la 18 luni de la închiderea cazului;

— Comisia nu a oferit suficiente justificări cu privire la necesitatea și proporționalitatea păstrării „datelor blocate" pentru o perioadă de până la cinci ani și, prin urmare, această propunere ar trebui reanalizată;

— ar trebui să se facă o distincție mai clară între alerte și listele de informații. Regulamentul ar trebui să prevadă, ca normă implicită, ca: (i) – cu excepția cazului în care se prevedere altfel în legislația verticală și sub rezerva unor garanții suplimentare adecvate – alertelor să li se aplice o perioadă de păstrare de șase luni; și ca (ii) această perioadă să fie calculată de la momentul trimiterii alertei.

96. Regulamentul ar trebui să impună o evaluare a riscului și o revizuire a planului de securitate înainte de orice extindere a IMI într-un domeniu de politică nou sau înainte de adăugarea unei noi funcționalități cu impact asupra datelor cu caracter personal.

97. Dispozițiile referitoare la informarea persoanelor vizate și la drepturile de acces ar trebui consolidate și ar trebui să încurajeze o abordare mai consecventă.

([40]) Idem.
([41]) A se vedea secțiunea 2.9 de mai sus.
([42]) A se vedea secțiunea 2.4 de mai sus.
([43]) A se vedea secțiunea 2.5.2 de mai sus.
([44]) A se vedea secțiunea 2.2.2 de mai sus.

98. AEPD ar dori o consolidare a dispozițiilor privind supravegherea coordonată în anumite privințe și, în acest scop, susține introducerea unor dispoziții similare celor existente, de exemplu, în contextul Sistemului de informații privind vizele și al Sistemului Schengen II și preconizate pentru Eurodac. În ceea ce privește frecvența reuniunilor și a auditurilor, AEPD susține abordarea flexibilă a propunerii, menită să asigure stabilirea de către regulament a normelor minime necesare pentru asigurarea unei cooperări eficiente, dar fără crearea unor sarcini administrative inutile.

99. Regulamentul ar trebui să prevadă că autoritățile competente sau alți actori externi dintr-o țară terță care nu permite o protecție adecvată pot avea acces direct la IMI numai în cazul în care există clauze contractuale corespunzătoare. Aceste clauze ar trebui negociate la nivelul Uniunii Europene.

100. Regulamentul ar trebui să stabilească un cadru clar pentru instituirea unor mecanisme de control intern adecvate, care să asigure respectarea protecției datelor și să furnizeze dovezi în acest sens, inclusiv declarații de confidențialitate (incluzând și o analiză de risc privind securitatea), o politică de protecție a datelor (incluzând un plan de securitate) adoptată pe baza rezultatelor acestora, precum și verificări și audituri periodice.

101. Regulamentul ar trebui să mai introducă și garanții specifice pentru luarea în considerare a vieții private începând cu momentul conceperii.

Adoptat la Bruxelles, 22 noiembrie 2011.

Giovanni BUTTARELLI

Adjunctul Autorității Europene pentru Protecția Datelor