Avizul Comitetului Economic și Social European privind Propunerea de regulament al Parlamentului European și al Consiliului privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE (în materie de frontiere și vize) și de modificare a Deciziei 2004/512/CE a Consiliului, a Regulamentului (CE) nr. 767/2008, a Deciziei 2008/633/JAI a Consiliului, a Regulamentului (UE) 2016/399 și a Regulamentului (UE) 2017/2226

[COM(2017) 793 final – 2017/0351 (COD)]

și privind Propunerea de regulament al Parlamentului European și al Consiliului privind instituirea unui cadru de interoperabilitate între sistemele de informații ale UE (cooperare polițienească și judiciară, azil și migrație)

[COM(2017) 794 final – 2017/0352 (COD)]

(2018/C 283/07)

Raportor: **Laure BATUT**

Sesizare	Comisia Europeană, 18.1.2018
	Parlamentul European, 28.2.2018
Temei juridic	Articolul 304 din Tratatul privind funcționarea Uniunii Europene
Secțiunea competentă	Secțiunea pentru ocuparea forței de muncă, afaceri sociale și cetățenie
Data adoptării în secțiune	25.4.2018
Data adoptării în sesiunea plenară	23.5.2018
Sesiunea plenară nr.	535
Rezultatul votului	160/3/2
(voturi pentru/voturi împotrivă/ abțineri)	

1. **Concluzii și recomandări**

1.1. CESE consideră utilă și pozitivă propunerea Comisiei Europene care vizează îmbunătățirea interoperabilității sistemelor de informații ale UE privind frontierele și vizele, cooperarea polițienească și judiciară, azilul și migrația.

1.2. CESE consideră că interoperabilitatea trebuie să fie un obiectiv strategic al UE pentru ca aceasta să rămână un spațiu deschis, garant al drepturilor fundamentale și al mobilității. UE și statele membre au obligația de a proteja viața și siguranța tuturor ființelor umane; principiul nereturnării trebuie respectat pe deplin.

1.3. Măsurile în materie de interoperabilitate vor fi cu atât mai bine înțelese cu cât:

— garantează, în cadrul strategiei UE în domeniul migrației, condițiile de echilibru între libertate și securitate, asigurând respectarea separării puterilor;

— garantează respectarea drepturilor fundamentale ale persoanelor vizate, în special protejarea datelor cu caracter personal și a vieții lor private, dreptul de acces la propriile date, de rectificare sau de ștergere a lor într-un termen rezonabil, prin proceduri accesibile;

— reafirmă, inclusiv în toate textele de punere în aplicare, cerința de integrare a principiilor protecției datelor încă din faza de proiect (*privacy by design*);

— nu crează noi obstacole în calea circulației normale a pasagerilor și a mărfurilor.

1.4. CESE solicită proceduri și garanții pentru utilizarea datelor în scopul asigurării respectării legii, care:

— să prevadă aplicarea în acest domeniu a legislației europene cu cel mai ridicat grad de protecție (Regulamentul general privind protecția datelor);

— să permită accelerarea stabilirii statului membru responsabil cu examinarea cererilor de protecție internațională;

— să garanteze, pentru persoanele vizate, dreptul la două grade de jurisdicție;

— să garanteze, pentru minori, în special pentru cei neînsoțiți, indiferent dacă se află în situație neregulamentară, de persecuție sau infracțională, dreptul de a obține viză, de a fi protejați și integrați și „dreptul de a fi uitați" într-un termen mai scurt decât cel aplicat persoanelor majore.

1.5. CESE consideră că actualul temei juridic al sistemelor de informații ar trebui să fie îmbunătățit și să țină seama de evoluția sistemelor de colectare a datelor. El solicită:

— consolidarea securității bazelor de date existente și a canalelor de comunicare a lor;

— evaluarea impactului intensificării controlului a priori asupra gestionării riscurilor;

— controlul și evaluarea permanentă a arhitecturii sistemului de către autoritățile responsabile pentru protecția datelor (AEPD); solicită responsabililor să transmită anual autorităților de decizie și Comisiei rapoarte anuale privind securitatea elementelor de interoperabilitate și rapoarte bienale privind impactul măsurilor asupra drepturilor fundamentale.

1.6. CESE consideră că proiectul ar trebui să dispună de un personal competent și solicită:

— programe consistente de formare pentru autoritățile implicate și pentru agenții eu-LISA;

— un control strict al competențelor agenților și candidaților la posturi în această agenție.

1.7. CESE își exprimă îngrijorarea cu privire la finanțarea noului sistem. Monitorizarea planificării va fi esențială pentru a evita abaterile în materie de buget și a permite proiectului să fie finalizat până în 2029.

1.8. CESE recomandă ca cetățenii să fie informați cu privire la evoluția proiectului până la finalizarea acestuia, iar persoanele care sunt supuse controalelor să beneficieze de o informare instructivă. Consideră că trebuie prevăzută posibilitatea stopării întregului proces în cazul în care libertatea și drepturile fundamentale sunt amenințate de utilizarea abuzivă a sistemului.

2. **Introducere**

2.1. În contextul internațional al anului 2017, considerat instabil atât în plan geopolitic, cât și în ceea ce privește securitatea internă a statelor membre, Consiliul a solicitat în repetate rânduri Comisiei să pună în aplicare mijloace de localizare a persoanelor considerate „cu risc", care fuseseră deja luate în evidență ca atare într-un stat membru. Reperarea trecerilor frontierelor, a deplasărilor și a itinerariilor urmate de aceste persoane în Europa ar putea fi esențială pentru securitatea în Uniune.

2.2. În rezoluția sa din 6 iulie 2016, Parlamentul European a invitat Comisia să furnizeze garanțiile necesare pentru protecția datelor.

2.3. Textele supuse examinării se înscriu în obiectivul de „menținere și consolidare a spațiului Schengen" ([1]). Uniunea s-a dotat deja cu numeroase reglementări și servicii digitale de informații în domeniile legate de controlul persoanelor și mărfurilor la trecerea frontierei.

2.4. Notă:

— **SIS: Sistemul de informații Schengen**, unul dintre cele mai vechi mecanisme, revizuit, gestionează o gamă largă de alerte privind persoanele și bunurile;

([1]) COM(2017) 570 final.

— **Eurodac: sistemul european pentru compararea datelor dactiloscopice** ale solicitanților de azil și ale resortisanților țărilor terțe aflați într-o situație neregulamentară la frontiere și pe teritoriul statelor membre și determinarea statului membru responsabil cu examinarea cererilor (CESE 2016-02981, raportor: Moreno Díaz) ([2]);

— **VIS: Sistemul de Informații privind vizele** (Codul de vize), care gestionează vizele pentru ședere de scurtă durată (CESE 2014-02932, raportor: Pezzini-Pariza Castaños) ([3]);

— **EES: Sistemul de intrare/ieșire**, aflat în prezent în așteptarea unei decizii, ar urma să gestioneze electronic datele din pașapoarte și datele de intrare/ieșire ale resortisanților țărilor terțe care vizitează spațiul Schengen (CESE 2016-03098 SOC/544, raportor: Pîrvulescu) ([4]);

— **ETIAS: Sistemul european de informații și de autorizare privind călătoriile**, aflat în prezent în așteptarea unei decizii, ar urma să constituie un vast sistem automatizat de stocare și de verificare *ex ante* a datelor resortisanților țărilor terțe scutiți de obligativitatea vizei de tranzit pentru spațiul Schengen (CESE 2016-06889 SOC/556, raportor: Simons) ([5]);

— **ECRIS-TCN: Sistemul european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe**, propus în prezent de Comisie, un sistem electronic de schimb de informații privind hotărârile judecătorești pronunțate deja de instanțele naționale.

2.5. Putem face analogia între mijloacele utilizate în prezent de o autoritate abilitată și un *smartphone* cu diferite aplicații, funcționând fiecare separat și oferind *propriile* informații.

2.6. Cu excepția SIS, aceste sisteme sunt axate pe gestionarea resortisanților țărilor terțe. Există șase sisteme, complementare și descentralizate. Suma informațiilor căutate este constituită din diversele răspunsuri pe care serviciile de anchetă le obțin din diferite baze de date, în funcție de autorizațiile lor de acces.

2.7. Comisia își propune să dea răspunsuri cu privire la următoarea chestiune:

— prin ce metodă, fără a modifica structurile deja dobândite și menținând complementaritatea lor, pot fi aliniate simultan toate bazele de date astfel încât, la un punct de intrare pe teritoriul UE și printr-o singură consultare a sistemului, toate informațiile deja colectate în bazele existente să conveargă către autoritatea de control autorizată, respectându-se, în același timp, normele privind protecția datelor și drepturile fundamentale.

2.8. În propunerile examinate, Comisia Europeană:

2.8.1. dorește să adauge posibilitățile suplimentare pe care le-ar oferi un acces la bazele de date ale Europol și Interpol, instituții care colaborează deja cu autoritățile de control europene;

2.8.2. dorește să *sincronizeze* căutările de informații, pentru a reduce timpii de răspuns în ceea ce privește dosarul migranților și pentru a accelera reacția de asigurare a securității în caz de necesitate. În acest scop, ea propune crearea unor noi entități, care ar permite funcționarea în simbioză a bazelor de date existente.

2.9. **Obiectivele sale sunt: acoperirea pe cât posibil a lacunelor din diferitele sisteme, îmbunătățirea** gestionării frontierelor externe ale spațiului Schengen, contribuția la securitatea internă a Uniunii, gestionarea cazurilor de fraudă de identitate și soluționarea cazurilor de identități multiple, localizarea persoanelor suspectate sau deja condamnate și verificarea identității acestora în spațiul Schengen.

2.10. Pentru a relua comparația cu *smartphone*-ul, autoritatea abilitată ar avea la dispoziție nu doar numeroase aplicații, ci ar putea de asemenea să obțină simultan și în cadrul aceleiași căutări, prin utilizarea codurilor sale de acces, datele stocate pe toate suporturile sale: computere, dispozitive mobile, telefoane, tablete, laptopuri etc.

([2]) JO C 34, 2.2. 2017, p. 144.
([3]) JO C 458, 19.12.2014, p. 36.
([4]) JO C 487, 28.12. 2016, p. 66.
([5]) JO C 246, 28.7. 2017, p. 28.

3. **Funcționarea sistemului**

3.1. Comisia a organizat consultări și a reunit un grup de experți la nivel înalt ([6]) în domeniul sistemelor de informații și al interoperabilității, numiți de statele membre, de țările din Grupul Schengen și de agenții europene precum eu-LISA2 ([7]) și FRA ([8]), sub coordonarea DG Migrație și Afaceri Interne.

Metoda: interconectivitate sau interoperabilitate?

3.1.1. **Interconectivitatea** sistemelor informatice se referă la posibilitatea de a le conecta între ele în așa fel încât datele conținute într-unul dintre ele să poată fi consultate automat de un altul.

3.1.2. **Interoperabilitatea** ([9]) se referă la capacitatea diferitelor sisteme de a comunica, de a face schimb de informații și de a utiliza aceste informații comunicate, cu respectarea autorizațiilor de acces la sisteme.

3.2. *Opțiunea interoperabilității*

3.2.1. Comisia consideră că această opțiune nu va afecta negativ realizările structurilor și competențelor actuale și că datele vor rămâne stocate în memorii compartimentate. Deși comunicarea ar fi sporită, acest fapt ar prezenta un avantaj de securitate pentru sisteme și date, niciunele dintre acestea nefiind, în mod evident, accesibile prin internet. Textele supuse avizării prezintă asemănări importante:

— unul dintre acestea [COM(2017) 793] se referă la interoperabilitatea sistemelor de informații privind frontierele și vizele;

— iar celălalt [COM(2017) 794] se referă la cooperarea polițienească și judiciară, la azil și la migrație.

3.3. *Noile instrumente*

3.3.1. Pentru a funcționa în regim de interoperabilitate, o nouă arhitectură formată din patru noi instrumente va trebui să completeze cele șase baze de date astfel încât să se lucreze rapid, printr-o singură interogare a sistemului, căutările urmând să fie lansate întotdeauna de la persoanele autorizate.

3.4. *Portalul european de căutare (ESP)*

3.4.1. Autoritatea de control abilitată (utilizatorul final) ar trebui să dispună de un acces unic la întregul sistem. În loc să efectueze șase căutări, ar urma să lanseze una singură (poliție, vamă etc.), prin care ar căuta datele necesare în mod simultan mai multe baze de date, fără a le stoca. Dacă datele respective există, sistemul le va găsi. În cazul identificării unui suspect sau a unei activități teroriste, chiar dacă primul nivel de căutare a persoanei care face obiectul verificării nu ar da rezultate („not-hit"), dacă datele sale sunt asociate cu o a doua informație („hit") existentă în bazele de date precum SIS, EES, ETIAS, acest fapt ar putea conduce la investigații suplimentare ale rezultatelor căutării și la o anchetă.

3.5. *Serviciul comun de comparare a datelor biometrice* (shared biometric matching service)

3.5.1. Această platformă partajată de armonizare va permite căutarea și compararea simultană a datelor matematizate, biometrice, a amprentelor digitale și a fotografiilor de identitate în diverse baze de date precum SIS, Eurodac, VIS, *EES* ([10]), *ECRIS*, dar nu în *ETIAS*; prin urmare, datele din aceste baze trebuie să fie compatibile.

3.5.2. Astfel, datele matematizate nu vor fi păstrate în forma lor originală.

3.6. *Registrul comun de date de identitate – CIR (Common Identity Repository)*

3.6.1. Un „registru comun de date de identitate" va reuni datele referitoare la identitatea biografică și biometrică a persoanelor din țărilor terțe care fac obiectul verificării, indiferent dacă se află la frontieră sau pe teritoriul statelor membre (din spațiul Schengen). Un indicator de concordanță a informațiilor din diferitele baze de date va accelera căutările. Sub responsabilitatea și cu ajutorul mijloacelor de securitate ale Agenției eu-LISA, aceste date vor fi stocate în așa fel încât nimeni să nu poată avea acces la mai mult de un rând alfanumeric odată. Întrucât este dezvoltat pe baza EES și ETIAS, CIR nu ar trebui să ajungă să dubleze datele. Registrul va putea fi folosit, de asemenea, pentru căutări din domeniul civil.

([6]) DG Migrație și Afaceri Interne, unitatea B/3; Decizia C/2016/3780 a Comisiei din 17 iunie 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=RO.

([7]) Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă, în Spațiul de Libertate, Securitate și Justiție.

([8]) FRA: Agenția UE pentru Drepturi Fundamentale.

([9]) Comunicarea Comisiei COM(2016) 205 final, intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate".

([10]) Caracterele cursive reamintesc că textele privind aceste organe nu au fost încă adoptate.

3.7. *Detectorul de identități multiple – MID (Multiple-Identity Detector)*

3.7.1. Acesta va avea rolul de a confirma identitatea persoanelor de bună-credință și de a combate fraudele de identitate, printr-o căutare simultană în toate bazele de date. Nicio administrație nu a utilizat încă acest instrument, care ar trebui să contribuie la prevenirea furtului de identitate.

3.8. *Rolul Agenției eu-LISA* ([11])

3.8.1. Agenția, creată în 2011, are ca misiune să faciliteze politicile UE în domeniile justiției, securității și libertății. Având sediul la Tallin, în Estonia, ea asigură deja schimbul de informații între diferitele autorități de aplicare a legii din statele membre, asigurând funcționarea fără întreruperi a sistemelor informatice la scară largă și libertatea de mișcare a persoanelor în spațiul Schengen.

3.8.2. Eu-LISA lucrează la proiectul „Frontiere inteligente" și va avea, în cadrul noii arhitecturi de schimb de date, un rol de conservare a elementelor referitoare la persoane, autorități, anchete și anchetatori. Agenția va verifica autorizațiile solicitanților și va asigura securitatea datelor, inclusiv în caz „de incident" [articolul 44, propunerile (2017) 793 și 794)].

3.8.3. **Utilizarea formatului universal pentru mesaje – UMF** (*Universal Message Format*), care urmează să fie creat, ar trebui să faciliteze lucrul cu noile sisteme, care ar fi obligatorii, impunând crearea de interfețe în statele membre în care acestea lipsesc și un sistem de traducere provizorie dintr-un limbaj în altul.

3.9. *Protecția datelor cu caracter personal* (articolele 7 și 8 din Cartă)

3.9.1. Propunerea de regulament recunoaște posibilitatea producerii unor accidente de securitate. Statele membre și sistemele lor de date trebuie să fie primele care să respecte principiile de protecție a datelor prevăzute de texte, de tratat, de Carta drepturilor fundamentale și de RGPD ([12]), care va intra în vigoare la 25 mai 2018.

4. **Dezbatere**

4.1. *Valoarea adăugată a interoperabilității în democrație*

4.1.1. UE are nevoie de reglementare și de mijloace de investigare care să o protejeze împotriva criminalității. Interoperabilitatea sistemelor de informații este o ocazie de a face să prevaleze statul de drept și protecția drepturilor omului.

4.1.2. Sistemele EES și ETIAS, conectate cu BMS și CIR, vor permite controlarea trecerilor la frontieră pentru persoanele suspecte, precum și păstrarea datelor acestora. Totuși, posibilitatea ca „serviciile de aplicare a legii să aibă acces prin BMS la sistemele de informații care nu intră în sfera asigurării respectării legii la nivelul UE" [articolul 17/CIR, propunerile (2017) 794 și 793], nu poate fi compatibilă cu scopurile enunțate drept temeiuri ale propunerilor supuse examinării. Comitetul [conform articolului 300 alineatul (4) din TFUE] se consideră dator să invoce la acest punct principiul proporționalității și solicită Comisiei să evite orice sistem de tip „Big Brother" ([13]) și să nu creeze obstacole în calea libertății de circulație a cetățenilor europeni (articolul 3 din TUE).

4.1.3. Modelul propus pentru colectarea și utilizarea datelor cu caracter personal obținute la frontieră și pe teritoriul Uniunii în timpul controalelor deplasărilor persoanelor și ale documentelor deținute de acestea este prezentat ca fiind etanș, accesibil doar persoanelor autorizate și numai în scopuri de securitate și de gestionare și va asigura o fluiditate sporită a procedurilor.

4.1.4. Comitetul exprimă îndoieli cu privire la această etanșeitate: vor rămâne anumite lacune, construcția repartizată pe nouă ani sprijinindu-se pe „temelii" care încă nu există, precum bazele EES sau ETIAS sau interfețele naționale. Contextul tehnologic este în evoluție constantă, or proiectul se bazează în mod necesar pe starea actuală a tehnologiei și nu prevede resurse bugetare pentru gestionarea obsolescenței care ar apărea în anumite sectoare digitale.

([11]) Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție.

([12]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). Avizul CESE: JO C 229, 31.7.2012, p. 90 și JO C 345, 13.10.2017, p. 138.

([13]) Din cartea *1984*, de George Orwell.

4.1.5. Pe de altă parte, dezvoltarea rapidă a utilizării așa-numiților algoritmi de inteligență artificială (IA) ar fi putut să fie luată în considerare în cadrul proiectului, atât ca instrument de control al sistemelor, cât și ca o cheie de securitate care să fie pusă la dispoziția autorităților de decizie, cu scopul de a garanta utilizarea democratică a arhitecturii.

4.1.6. Propunerea dezvoltă un sistem pentru protagoniști de bună-credință, care respectă legile. Faptul că sistemul ar fi administrat de persoane este liniștitor, dar persoanele pot să constituie de asemenea o vulnerabilitate. Comitetul sugerează adăugarea unui articol care să prevadă „disjunctoare diferențiale" pentru cazurile de criză politică și/sau de „management", întrucât orice problemă dintr-o bază de date ar putea constitui un risc pentru întreaga arhitectură ([14]). Utilizarea UMF pe scară largă ar putea determina utilizarea datelor la nivel global, ceea ce constituie un aspect pozitiv, dar totodată foarte riscant din perspectiva protecției datelor. Autoritățile abilitate își asumă o mare responsabilitate. Aceste aspecte nu sunt luate în considerare în textele în discuție.

4.2. *Protecția drepturilor fundamentale*

4.2.1. Drepturile fundamentale sunt absolute; ele nu pot fi afectate nici măcar în măsură limitată, cu excepția cazului în care acest lucru este necesar și răspunde efectiv obiectivelor de interes general recunoscute de Uniune și dacă conținutul lor esențial este respectat [articolul 8 și articolul 52 alineatul (1) din Carta Drepturilor Fundamentale]. Comitetul se întreabă cum poate fi evaluată proporționalitatea măsurilor de control, în cazul migranților care fug din calea persecuțiilor și care solicită azil în zonele de coastă ale Uniunii [COM(2017) 794 final – Expunere de motive – Drepturi fundamentale]. Căutarea suspecților cu scopul de a preveni infracțiunile, în special actele de terorism, **nu trebuie să introducă în democrațiile noastre conceptul de „infracțiune cu anticipare"**; trebuie să se păstreze o diferență între „fapte" care tulbură ordinea publică și „opinii".

4.2.2. Respectarea, pentru orice persoană, a drepturilor enunțate în Cartă trebuie să asigure echilibrul între securitate și libertate, fără de care democrația nu poate supraviețui. Comitetul consideră că acest echilibru este esențial și trebuie să constituie un obiectiv permanent al tuturor autorităților, inclusiv al celor de control, atât la nivel național, cât și la nivel european.

4.2.3. Lanțul autorităților asociate într-o căutare, precum și metadatele aferente acesteia vor fi păstrate în sistem. Trebuie să se respecte de asemenea, în ceea ce privește datele generate, drepturile fundamentale ale acestor autorități abilitate, în special în privința securității și a vieții private, în cazul în care se produce o intruziune rău intenționată în structura și în utilizarea necorespunzătoare a datelor între momentul introducerii și cel al ștergerii lor.

4.3. *Protecția datelor*

4.3.1. Propunerile recunosc principiul protecției datelor cu caracter personal începând cu momentul conceperii și în mod implicit, deși expunerea de motive reamintește că, potrivit Curții de Justiție a Uniunii Europene (CJUE), nu este vorba despre o prerogativă absolută. Comitetul recunoaște avantajele măsurilor preventive care garantează securitatea, ale combaterii identităților false și ale garantării dreptului la azil. Totuși, Comitetul ține să sublinieze limitele matematizării și ale anonimizării datelor: persoanele vizate ar putea avea nevoie ulterior de datele lor.

4.3.2. Comitetul subliniază, de asemenea, că tipul de date stocate, biometrice și biologice, prezintă un interes deosebit pentru anumite întreprinderi și pentru mediul infracțional. Din acest punct de vedere, securitatea cibernetică este la fel de importantă ca securitatea fizică, or textul propunerilor o menționează într-o măsură insuficientă. Datele păstrate vor fi stocate într-un singur loc fizic; chiar dacă se garantează securitatea acestuia, el poate totuși să fie expus.

4.3.3. CESE reamintește că, în ceea ce privește protecția datelor și dreptul la ștergerea acestora (dreptul de a fi uitat), instituțiile și organismele Uniunii au obligația de a respecta Regulamentul nr. 45/2001, care oferă un grad mai redus de protecție față de RGPD ([15]) din 2016 (care urmează să intre în vigoare în mai 2018) și trebuie să fie respectat de către statele membre. Comitetul subliniază complexitatea punerii în aplicare a acestui drept și își exprimă îngrijorarea că migranții, călătorii și solicitanții de azil nu vor fi capabili să asigure respectarea sa:

1. protecția datelor cu caracter personal trebuie să fie validată pentru toate bazele de date existente, naționale și europene, astfel încât ansamblul să fie protejat;

2. această protecție este fundamentală dacă se dorește ca cetățenii să accepte să devină subiecții unei rețele de supraveghere de o asemenea anvergură.

4.3.4. Durata păstrării datelor colectate de autoritățile abilitate nu este clar precizată în propuneri. Textele menționează procedura dreptului la rectificarea și/sau la ștergerea datelor, ea fiind asigurată fie de statul membru căruia i s-a adresat cererea, fie de statul membru responsabil, însă nu stabilește termene pentru păstrarea datelor (articolul 47 din propuneri). Comitetul propune stabilirea unui astfel de termen, care trebuie să fie mai scurt în cazul minorilor (articolul 24 din Cartă), cu excepția cazurilor de terorism, astfel încât aceștia să beneficieze de posibilități de integrare.

([14]) AEPD, anexă, raportul final întocmit de grupul de experți la nivel înalt, publicat în mai 2017.
([15]) RGPD, Regulamentul general privind protecția datelor [Regulamentul (UE) 2016/679].

4.4. *Guvernanța și asumarea răspunderii*

4.4.1. Bazele de date internaționale nu sunt supuse aceloraşi reguli ca sistemele informatice europene. Instituirea unui format universal de acces, cu posibilă vocație de a deveni internațional, nu va fi decât un element tehnic incapabil să unifice reglementările, chiar dacă este adevărat că Interpol trebuie să respecte articolul 17 din pactul ONU ([16]). Pe de altă parte, autorizările vor rămâne în domeniul de competență al statelor membre. CESE consideră că acest aspect ar trebui să fie abordat în propuneri.

4.4.2. Se va lansa o singură interogare, iar simbioza dintre bazele de date europene va răspunde la aceasta. CESE subliniază că birocrația generată va fi mai mult decât proporțională cu viteza câştigată. Guvernanța va fi asigurată de Comisie în colaborare cu statele membre, în cadrul unei proceduri de control. Pivotul va fi reprezentat de Agenția eu-LISA, însărcinată în mod special cu punerea în aplicare a procedurilor de colectare a informațiilor privind funcționarea interoperabilității; ea va primi informațiile de la statele membre și de la Europol și va prezenta Consiliului, Parlamentului European și Comisiei, din patru în patru ani, un raport de evaluare tehnică, urmând ca Comisia să pregătească la rândul său, un an mai târziu, un raport global (articolul 68 din propuneri). În opinia Comitetului, aceste secvențe sunt mult prea lungi. Evaluarea securității elementelor de interoperabilitate [articolul 68 alineatul (5) litera (d)] ar trebui să aibă loc cel puțin anual, iar evaluarea impactului asupra drepturilor fundamentale, cel puțin o dată la doi ani [același articol litera (b)].

4.4.3. Comitetul regretă că problematici atât de importante cum sunt cele abordate de aceste propuneri vor fi gestionate de agenții europene ale căror procese de recrutare a personalului și funcționare sunt neclare pentru mulți cetățeni. Comitetul consideră că este necesar să se pună în comun bunele practici și să se asocieze procesului de avizare toate autoritățile independente din domeniul controlului utilizării datelor (AEPD), precum și alte agenții precum FRA și ENISA.

4.4.4. Punerea în aplicare a tuturor acestor noi structuri și proceduri se va realiza prin acte delegate și acte de punere în aplicare adoptate de Comisie. Comitetul ar dori ca obiectivul respectării drepturilor fundamentale și al protecției datelor cu caracter personal să rămână înscris în toate aceste acte de-a lungul timpului, în vederea unei primiri mai bune a persoanelor la frontiere. CESE recomandă ca cetățenii europeni să fie informați cu privire la evoluția proiectului până la finalizarea acestuia, iar persoanele care sunt supuse controalelor să beneficieze de o informare instructivă.

5. **Formarea necesară a autorităților de control din întreaga Uniune**

5.1. Comitetul consideră că vor fi necesare numeroase stagii de formare în prima perioadă (după 2021), contrar celor susținute de Comisie în rezumatul evaluării impactului (C). Comisia menționează cifra de 76 de milioane EUR pe an. Trecerea la noi proceduri necesită întotdeauna un proces de modernizare. În acest caz este vorba de toate frontierele Uniunii și de sistemele naționale. Anumite state membre nu dispun încă de sisteme compatibile și vor trebui să depună un efort considerabil și să creeze interfețe care să le confere capacitatea de a participa. Pentru ca interoperabilitatea să funcționeze, ar trebui eliminate disparitățile dintre statele membre.

5.2. Formarea în domeniul utilizării datelor de calitate și a UMF va fi esențială. Comitetul recomandă organizarea unui pol de formări comune pentru autoritățile abilitate – inclusiv eu-LISA, în cazul căreia va trebui să se verifice cu strictețe competențele membrilor – în colaborare cu CEPOL ([17]), Frontex, Europol etc.

5.3. Nu există nicăieri altundeva un instrument precum MID. În caz de reuşită, acest instrument va fi puternic. Noua arhitectură va necesita cel mai înalt nivel de calitate a datelor. Pentru ca întregul sistem să se ridice la înălțimea așteptărilor proiectului, toate statele membre trebuie să participe în egală măsură, în caz contrar lacunele vor deveni mai grave decât înainte. Într-o astfel de situație, dreptul la azil și dreptul de acces la protecție internațională ar fi slăbite (articolele 18 și 19 din cartă).

6. **Finanțarea**

6.1. Ansamblul arhitecturii propuse se sprijină pe câteva ipoteze: adoptarea de către autoritățile de decizie a sistemelor *EES*, *ETIAS*, *UMF*, buna funcționare a *MID* și securizarea *CIR*. Cele două organe – AEPD și Agenția eu-LISA – și eventual Agenția ENISA vor dispune oare de resurse umane și financiare suficiente? Comisia propune o cofinanțare UE-statele membre. Comitetul observă că gestionarea „Semestrului" se face încă din bugete de austeritate și că, pe de altă parte, utilizarea actuală a bazelor existente (SIS, VIS, Prüm, EES) trebuie să fie optimizată în continuare, cu respectarea cerințelor legale (raportul grupului de experți).

([16]) Pactul internațional ONU cu privire la drepturile civile și politice – „Articolul 17: (1) Nimeni nu va putea fi supus vreunor imixtiuni arbitrare sau ilegale în viața particulară, în familia, domiciliul sau corespondența sa, nici la atingeri ilegale aduse onoarei și reputației sale. (2) Orice persoană are drept la protecția legii împotriva unor asemenea imixtiuni sau atingeri."

([17]) CEPOL, Agenția Uniunii Europene pentru Formare în Materie de Aplicare a Legii (Budapesta, Ungaria).

6.2. CESE își pune întrebări cu privire la consecințele bugetare ale Brexitului, deși Regatul Unit nu face parte din sistemul Schengen, și – pe un plan mai general – la posibilitatea ca gestionarea interoperabilității în țările europene care nu sunt membre ale SIS, dar participă la alte sisteme (cum ar fi Eurodac), să devină mai complexă.

6.3. Fondul prevăzut este FSI (Fondul pentru securitate internă). Momentul punerii în funcțiune este prevăzut pentru 2023. Comitetul se întreabă dacă vor fi suficienți cinci ani pentru reducerea disparităților de la nivel european și pentru asigurarea condițiilor necesare reușitei. Bugetul prevăzut este de 424,7 milioane EUR pentru nouă ani (2019-2027). Uniunea Europeană (FSI) și statele membre vor trebui să asigure acest buget. Statele membre trebuie să ajungă în situația în care sistemele lor actuale să funcționeze corect cu noua arhitectură informatică. Comitetul apreciază că reluarea creșterii economice va putea sprijini realizarea acestor investiții.

Bruxelles, 23 mai 2018.

Președintele
Comitetului Economic și Social European
Luca JAHIER