COMISIA
EUROPEANĂ

Bruxelles, 6.4.2016
COM(2016) 205 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate

1. INTRODUCERE

Europa este o societate mobilă. Milioane de cetățeni ai UE și de resortisanți ai țărilor terțe trec zilnic frontierele interne și externe. În 2015, peste 50 de milioane de resortisanți ai țărilor terțe au vizitat UE, reprezentând peste 200 de milioane de treceri ale frontierelor externe ale spațiului Schengen.

Dincolo de aceste fluxuri de călătorie regulamentare, conflictul din Siria și crizele din alte zone au antrenat, doar în anul 2015, 1,8 milioane de cazuri de trecere neregulamentară a frontierelor externe ale Europei. Cetățenii UE se așteaptă ca la frontierele externe controalele asupra persoanelor să fie eficiente, pentru a permite gestionarea eficace a migrației și pentru a contribui la securitatea internă. Atacurile teroriste de la Paris din 2015 și cele de la Bruxelles din martie 2016 au demonstrat cu vehemență amenințarea continuă la adresa securității interne a Europei.

Ambele aspecte au adus în prim plan necesitatea de a ne uni și de a consolida într-o manieră cuprinzătoare cadrele de cooperare ale UE privind gestionarea frontierelor, migrația și securitatea, precum și instrumentele de informare. Gestionarea frontierelor, asigurarea respectării legii și controlul migrației sunt interconectate în mod dinamic. Se cunoaște faptul că există cetățeni ai UE care au trecut frontiera externă pentru a călători în zone de conflict în scopuri teroriste și că aceștia prezintă un risc la întoarcere. Există dovezi cu privire la faptul că teroriștii au utilizat rute de migrație neregulamentară pentru a intra pe teritoriul UE, iar apoi s-au deplasat în spațiul Schengen fără a fi detectați.

Agendele europene privind securitatea și migrația au stabilit calea de urmat pentru elaborarea și punerea în aplicare a politicii UE, astfel încât să se răspundă provocărilor paralele reprezentate de gestionarea migrației și combaterea terorismului și a criminalității organizate. Prezenta comunicare se bazează pe sinergiile dintre aceste două agende și este concepută ca un punct de plecare pentru o dezbatere cu privire la modul în care sistemele de informații existente și viitoare ar putea consolida atât gestionarea frontierelor externe, cât și securitatea internă în UE. Aceasta completează propunerea din decembrie 2015 privind crearea unei Paze europene de frontieră și de coastă și îmbunătățirea prevenirii crizelor și a intervenției la frontierele externe.

La nivelul UE, există o serie de sisteme de informații care le oferă polițiștilor de frontieră și agenților de poliție informații relevante privind persoanele, însă arhitectura UE a gestionării datelor nu este perfectă. Prezenta comunicare stabilește câteva opțiuni posibile pentru valorificarea la maximum a avantajelor oferite de sistemele de informații existente și, dacă este necesar, pentru elaborarea unor acțiuni noi și complementare menite să remedieze lacunele. Comunicarea subliniază, de asemenea, necesitatea de a îmbunătăți interoperabilitatea sistemelor de informații, acesta fiind un obiectiv pe termen lung, astfel cum a fost identificat și de Consiliul European și de Consiliu[1], și prezintă idei referitoare la modul în care sistemele de informații pot fi dezvoltate în viitor pentru a se asigura că polițiștii de frontieră, autoritățile vamale, agenții de poliție și autoritățile judiciare dispun de informațiile necesare.

Orice inițiativă viitoare va fi elaborată pe baza principiilor privind o mai bună reglementare, cu o consultare publică și o evaluare a impactului, inclusiv în ceea ce

[1] Concluziile reuniunii Consiliului European din 17 și 18 decembrie 2015; Declarație comună a miniștrilor UE responsabili de justiție și afaceri interne și a reprezentanților instituțiilor UE cu privire la atacurile teroriste din 22 martie 2016 de la Bruxelles (24 martie 2016); Concluziile Consiliului UE și ale statelor membre reunite în cadrul Consiliului privind combaterea terorismului (20 noiembrie 2015).

privește drepturile fundamentale și, în special, dreptul la protecția datelor cu caracter personal.

2. PROVOCĂRILE CARE TREBUIE ABORDATE

Absența frontierelor interne în spațiul Schengen necesită o gestionare solidă și fiabilă a circulației persoanelor la frontierele externe. Aceasta este o condiție prealabilă pentru a asigura un nivel înalt de securitate internă și libera circulație a persoanelor în spațiul respectiv. În același timp, absența frontierelor interne înseamnă că autoritățile de asigurare a respectării legii din statele membre au, de asemenea, acces la datele relevante referitoare la persoane. La nivelul UE există o serie de sisteme de informații și baze de date care le oferă polițiștilor de frontieră, agenților de poliție și altor autorități informații relevante privind persoanele, în conformitate cu scopurile lor[2].

Cu toate acestea, există, de asemenea, deficiențe legate de sistemele de informații care împiedică activitatea acestor autorități naționale. Prin urmare, s-a evidențiat faptul că un schimb mai bun de informații reprezintă o prioritate esențială în cadrul Agendei europene privind securitatea. Printre principalele deficiențe se numără: (a) funcționalitățile sub nivelul optim ale sistemelor de informații existente, (b) lacunele din cadrul arhitecturii UE a gestionării datelor, (c) un mediu complex de sisteme de informații reglementate în mod diferit și (d) o arhitectură fragmentată a gestionării datelor pentru controlul și securitatea frontierelor.

Sistemele de informații existente în UE pentru gestionarea frontierelor și securitate internă acoperă o gamă largă de funcționalități. Cu toate acestea, există în continuare **deficiențe în ceea ce privește funcționalitățile sistemelor existente**. Analizând procedurile de control la frontieră aplicabile diferitelor categorii de călători, devine evident că există deficiențe în cadrul unora dintre aceste proceduri, precum și între respectivele sisteme de informații utilizate pentru controale la frontieră. În mod similar, trebuie optimizată performanța instrumentelor existente pentru asigurarea respectării legii. Prin urmare, este necesar să se aibă în vedere măsuri de îmbunătățire a sistemelor de informații existente (secțiunea 5).

În plus, există **lacune în ceea ce privește arhitectura UE a gestionării datelor**. Există în continuare probleme legate de controalele la frontieră ale anumitor categorii de călători, cum ar fi resortisanții țărilor terțe care dețin o viză de ședere pe termen lung. De asemenea, există un deficit de informații înainte de sosirea la frontieră în ceea ce privește resortisanții țărilor terțe care sunt scutiți de obligația de a deține viză. Ar trebui să se analizeze dacă este necesar ca aceste lacune să fie remediate prin dezvoltarea unor sisteme de informații suplimentare, după caz (secțiunea 6).

Polițiștii de frontieră și, în special, agenții de poliție se confruntă cu un **mediu complex de sisteme de informații reglementate în mod diferit** la nivelul UE. Această complexitate generează dificultăți practice, mai ales în ceea ce privește bazele de date care ar trebui consultate într-o anumită situație. În plus, nu toate statele membre ale UE sunt conectate la toate sistemele existente[3]. Actuala complexitate legată de accesarea sistemelor

[2] A se vedea secțiunea 4 pentru o imagine de ansamblu asupra sistemelor de informații în materie de frontiere și securitate, iar anexa 2 pentru un inventar mai detaliat.

[3] Sub rezerva condițiilor specifice ale Protocolului 22 în ceea ce privește Danemarca și ale Protocoalelor 21 și 36 în ceea ce privește Regatul Unit și Irlanda, precum și ale actelor de aderare respective.

de informații la nivelul UE ar putea fi redusă prin crearea unei interfețe de căutare unice la nivel național care să respecte scopurile diferite de acces (secțiunea 7.1).

Arhitectura actuală a UE a gestionării datelor pentru controlul și securitatea frontierelor se caracterizează prin **fragmentare**. Acest lucru se datorează diverselor contexte instituționale, juridice și politice în care au fost dezvoltate sistemele. Informațiile sunt stocate separat în diverse sisteme care sunt rareori interconectate. Există neconcordanțe între bazele de date, precum și practici divergente în ceea ce privește accesul la date al autorităților competente. Astfel pot rezulta „unghiuri moarte", în special pentru autoritățile de asigurare a respectării legii, întrucât poate fi foarte dificil să se recunoască conexiunile dintre fragmentele de date. Prin urmare, este necesar și urgent să se depună eforturi în vederea găsirii unor soluții integrate care să permită o mai bună accesibilitate a datelor în scopul gestionării și al securității frontierelor, cu respectarea deplină a drepturilor fundamentale. Din acest motiv, este necesar să se inițieze un proces prin care să se realizeze interoperabilitatea sistemelor de informații existente (secțiunea 7).

3. DREPTURI FUNDAMENTALE

Respectarea deplină a drepturilor fundamentale și a normelor de protecție a datelor reprezintă o condiție prealabilă esențială pentru soluționarea oricăreia dintre provocările menționate anterior.

Respectarea drepturilor fundamentale necesită sisteme tehnologice și de informații bine concepute și corect utilizate. Sistemele tehnologice și de informații pot ajuta autoritățile publice să protejeze drepturile fundamentale ale cetățenilor. Tehnologia biometrică poate reduce riscul de erori de identitate, de discriminare și de profiluri bazate pe criterii rasiale. Aceasta poate contribui, de asemenea, la contracararea riscurilor în materie de protecție pentru copii, cum ar fi copiii dispăruți sau cei care devin victime ale traficului, cu condiția corelării acestei tehnologii cu garanțiile oferite de drepturile fundamentale și cu măsuri de protecție. Această tehnologie poate reduce riscul reținerii și arestării greșite a unor persoane și, de asemenea, poate contribui la sporirea securității cetățenilor care locuiesc în spațiul Schengen, întrucât va contribui la combaterea terorismului și a formelor grave de criminalitate.

Existența unor sisteme de informații la scară largă implică și potențiale riscuri la adresa vieții private, care trebuie anticipate și contracarate în mod corespunzător. Colectarea și utilizarea datelor cu caracter personal din aceste sisteme au un impact asupra dreptului la viață privată și la protecția datelor cu caracter personal, consacrat în Carta drepturilor fundamentale a Uniunii Europene. Toate sistemele trebuie să respecte principiile de protecție a datelor și cerințele privind necesitatea, proporționalitatea, limitarea scopului și calitatea datelor. Trebuie instituite garanții care să asigure drepturile persoanelor vizate în ceea ce privește protecția vieții private și a datelor lor cu caracter personal. Datele ar trebui păstrate doar atât timp cât sunt necesare în scopul pentru care au fost colectate. Trebuie prevăzute mecanisme care să asigure o gestionare corectă a riscurilor și o protecție eficace a drepturilor persoanelor vizate.

În decembrie 2015, colegiuitorii au ajuns la un acord politic referitor la reforma privind protecția datelor. Odată adoptate, noul Regulament general privind protecția datelor și Directiva privind protecția datelor care se adresează autorităților polițienești și judiciare[4] vor deveni aplicabile în 2018 și vor asigura un cadru armonizat pentru prelucrarea datelor cu caracter personal.

[4] A se vedea http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

Limitarea scopului este un principiu-cheie al protecţiei datelor, astfel cum este consacrat în Carta drepturilor fundamentale. Ca urmare a diferitelor contexte instituţionale, juridice şi politice în care au fost elaborate sistemele de informaţii de la nivelul UE, principiul limitării scopului a fost pus în aplicare prin intermediul unei structuri compartimentate a gestionării informaţiilor[5]. Acesta este unul dintre motivele fragmentării actuale a arhitecturii UE a gestionării datelor pentru controlul frontierelor şi securitatea internă. Odată cu aplicarea în UE a noului cadru cuprinzător pentru protecţia datelor cu caracter personal şi ca urmare a evoluţiilor semnificative în materie de tehnologie şi securitate informatică, principiul limitării scopului poate fi pus în aplicare mai uşor la nivel de acces şi de utilizare a datelor stocate, cu respectarea deplină a Cartei drepturilor fundamentale şi a jurisprudenţei recente a Curţii Europene de Justiţie. Ar trebui ca garanţiile, cum ar fi compartimentarea datelor în cadrul unui singur sistem şi normele specifice de acces şi de utilizare a datelor pentru fiecare categorie de date şi de utilizatori, să asigure limitarea necesară a scopului la soluţiile integrate pentru gestionarea datelor. Astfel se deschide o cale către interoperabilitatea sistemelor de informaţii, însoţită de normele stricte de acces şi de utilizare necesare fără ca acest lucru să aibă repercusiuni asupra limitării existente a scopului.

„Protecţia datelor începând cu momentul conceperii” şi „protecţia implicită a datelor” sunt acum principii integrate în normele UE de protecţie a datelor. La elaborarea de noi instrumente care se bazează pe utilizarea tehnologiei informaţiei, Comisia se va strădui să urmeze această abordare. Aceasta presupune includerea protecţiei datelor cu caracter personal în baza tehnologică a unui instrument propus, limitând prelucrarea datelor la cele necesare pentru un anumit scop şi acordând accesul la date numai acelor entităţi care „trebuie să le cunoască”[6].

Cerinţele Cartei drepturilor fundamentale şi, în special, noile instrumente de reformare a protecţiei datelor vor orienta Comisia în ceea ce priveşte soluţionarea actualelor lacune şi deficienţe din cadrul arhitecturii UE a gestionării datelor pentru controlul şi securitatea frontierelor. Acest lucru va garanta faptul că dezvoltarea în continuare a sistemelor de informaţii în aceste domenii va fi în conformitate cu cele mai înalte standarde în materie de protecţie a datelor şi că acestea vor respecta drepturile fundamentale, astfel cum sunt garantate de Carta drepturilor fundamentale, şi vor contribui la acestea.

4. PREZENTARE GENERALĂ A SISTEMELOR DE INFORMAŢII ÎN MATERIE DE FRONTIERE ŞI SECURITATE[7]

Sistemele de informaţii existente în UE pentru gestionarea frontierelor şi securitatea internă au propriile lor obiective, scopuri, temeiuri juridice[8], grupuri de utilizatori şi propriul context instituţional. Împreună, ele constituie un model complex de baze de date relevante.

Principalele trei **sisteme centralizate de informaţii** elaborate de UE sunt (i) Sistemul de informaţii Schengen (SIS) cu un spectru larg de alerte referitoare la persoane şi obiecte,

---

5 COM(2010) 385 final.

6 Pentru o descriere cuprinzătoare a sintagmei „luarea în considerare a vieţii private începând cu momentul conceperii”, a se vedea Avizul Autorităţii Europene pentru Protecţia Datelor privind promovarea încrederii în societatea informaţională prin încurajarea protecţiei datelor şi a confidenţialităţii, Autoritatea Europeană pentru Protecţia Datelor, 18.3.2010.

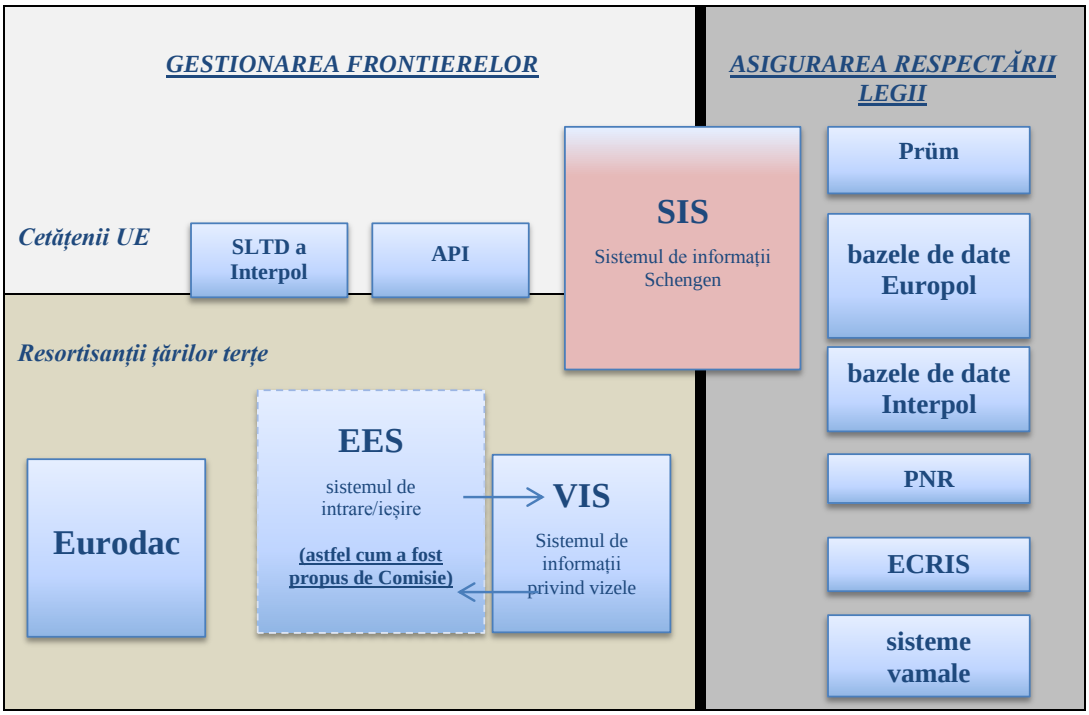
7 A se vedea anexa 2 pentru un inventar al sistemelor de informaţii utilizate în prezent pentru gestionarea frontierelor şi asigurarea respectării legii.

8 Sub rezerva condiţiilor specifice ale Protocolului 22 în ceea ce priveşte Danemarca şi ale Protocoalelor 21 şi 36 în ceea ce priveşte Regatul Unit şi Irlanda.

(ii) Sistemul de informații privind vizele (VIS) cu date privind vizele de scurtă ședere și (iii) sistemul Eurodac cu date dactiloscopice ale solicitanților de azil și ale resortisanților din țări terțe care au trecut neregulamentar frontierele externe. Aceste trei sisteme sunt complementare și – cu excepția SIS – sunt destinate, în principal, resortisanților țărilor terțe. Sistemele sprijină, de asemenea, autoritățile naționale în lupta împotriva criminalității și a terorismului[9]. Acest lucru este valabil în special în ceea ce privește SIS, instrumentul de schimb de informații utilizat pe scara cea mai largă în prezent. Schimbul de informații între aceste sisteme se efectuează într-o infrastructură de comunicații specializată și securizată, numită sTESTA[10].

În plus față de aceste sisteme existente, Comisia propune instituirea unui al patrulea sistem centralizat de gestionare a frontierelor, **sistemul de intrare/ieșire** (EES)[11], care ar trebui să fie pus în aplicare până în 2020 și care se adresează tot resortisanților țărilor terțe.

Figura 1 *Prezentare schematică a principalelor sisteme de informații pentru gestionarea frontierelor și asigurarea respectării legii:*



Printre celelalte instrumente la care se recurge pentru gestionarea frontierelor se numără baza de date a Interpol privind documentele de călătorie furate și pierdute (SLTD), precum și informațiile prealabile referitoare la pasageri (API) care colectează date cu privire la pasageri înaintea zborurilor cu destinația UE. Aceste instrumente sunt relevante atât pentru cetățenii UE, cât și pentru resortisanții țărilor terțe.

---

[9] Accesul la VIS și Eurodac în scopul asigurării respectării legii poate fi exercitat în anumite condiții, dat fiind că asigurarea respectării legii este un obiectiv auxiliar al acestor sisteme. În ceea ce privește VIS, statele membre au obligația de a desemna o autoritate competentă pentru a controla accesul în scopul asigurării respectării legii, iar poliția trebuie să furnizeze dovezi cu privire la faptul că accesul agenților săi este necesar în scopul unor anchete penale. În ceea ce privește Eurodac, autoritatea responsabilă de efectuarea unei anchete trebuie să caute în sistemul automat de identificare a amprentelor digitale (AFIS) existent la nivel național, în Prüm și VIS înainte de a i se permite accesul la Eurodac.

[10] Aceasta urmează să fie înlocuită în curând cu TESTA-NG.

[11] COM(2016) 194 final.

UE a elaborat **instrumente descentralizate pentru schimbul de informații**, destinate în special asigurării respectării legii, anchetelor penale și cooperării judiciare, și anume (i) cadrul Prüm pentru schimbul de date referitoare la ADN, amprente digitale și datele privind înmatricularea vehiculelor, precum și (ii) Sistemul european de informații cu privire la cazierele judiciare (ECRIS) pentru schimbul de informații referitoare la cazierele judiciare naționale. ECRIS permite schimbul de informații, prin intermediul unei rețele securizate, cu privire la condamnările anterioare pronunțate împotriva unei anumite persoane de către instanțele penale din Uniunea Europeană. Cererile se bazează în principal pe informațiile de identificare alfanumerice, deși este posibil schimbul de date biometrice.

Europol, centrul de informare al UE privind criminalitatea, sprijină schimbul de informații între organele naționale de poliție. Sistemul informațional Europol (EIS) constituie o bază de date centralizată a informațiilor în materie penală care permite statelor membre să stocheze date privind formele grave de criminalitate și terorismul și să efectueze căutări în această bază de date. Punctele de contact din cadrul Europol oferă fișiere de lucru pentru analiză, care sunt dedicate câte unui subiect și conțin informații privind operațiunile aflate în derulare în statele membre. Aplicația de rețea a Europol pentru schimbul securizat de informații (SIENA) permite statelor membre să facă schimb de informații rapid, sigur și ușor, între ele, cu Europol sau cu părți terțe care au încheiat un acord de cooperare cu Europol. În același timp, SIENA pune un accent deosebit pe interoperabilitatea cu alte sisteme din cadrul Europol, de exemplu în vederea schimbului direct de date cu punctele de contact. Această aplicație prevede posibilitatea introducerii în bazele de date ale Europol a unor informații rezultate în urma schimbului dintre statele membre. SIENA ar trebui, prin urmare, să devină prima alegere a statelor membre pentru canalizarea schimbului de informații în scopul asigurării respectării legii la nivelul UE.

O serie de alte sisteme de prelucrare a datelor cu caracter personal care vor fi elaborate în toate statele membre se referă la **registrele cu numele pasagerilor** (PNR)[12]. Datele PNR constau în informațiile furnizate în momentul rezervării și al înregistrării.

În cele din urmă, **autoritățile vamale** reprezintă, de asemenea, un actor esențial în ceea ce privește cooperarea între agenții, la frontierele externe. Acestea dispun de diferite sisteme[13] și baze de date care conțin date privind circulația mărfurilor, identificarea operatorilor economici și informații referitoare la riscuri, care pot fi utilizate pentru consolidarea securității interne. Aceste sisteme au propria infrastructură controlată, restricționată și securizată (rețeaua comună de comunicații), care și-a dovedit viabilitatea. Ar trebui explorate în continuare sinergiile și convergențele între sistemele de informații și infrastructurile lor corespunzătoare utilizate pentru gestionarea frontierelor UE și pentru operațiunile vamale.

5. ÎMBUNĂTĂȚIREA SISTEMELOR DE INFORMAȚII EXISTENTE

Sistemele de informații existente în UE pentru gestionarea frontierelor și securitate internă acoperă o gamă largă de funcționalități. Totuși, există încă **deficiențe** în cadrul acestor sisteme care trebuie remediate pentru a îmbunătăți performanța acestora.

[12] A se vedea secțiunea 6.2.

[13] Sistemele de informații ale vămilor cuprind toate sistemele create în temeiul Codului Vamal Comunitar (Regulamentul 2913/92) și al viitorului Cod vamal al Uniunii (Regulamentul 952/2013), al Deciziei privind crearea unui mediu informatizat pentru vamă și comerț (Decizia 70/2008/CE) și al Sistemului de informații al vămilor care a fost instituit prin Convenția SIV din 1995. Scopul acestor sisteme este de a contribui la combaterea criminalității legate de domeniul vamal, prin facilitarea cooperării între autoritățile vamale europene.

Sistemul de informații Schengen (SIS)

Verificările la frontieră în cadrul **Sistemului de informații Schengen** (SIS) se desfășoară în prezent pe baza căutărilor alfanumerice (de exemplu, nume și data nașterii). Amprentele digitale pot fi utilizate numai pentru a verifica și a confirma identitatea unei persoane care a fost deja identificată pe baza numelui. Această lacună în materie de securitate le permite persoanelor care fac obiectul unei alerte să utilizeze documente falsificate pentru a scăpa de o corespondență perfectă în SIS.

Această deficiență fundamentală va fi remediată prin adăugarea în SIS a unei funcții de căutare a amprentelor digitale printr-un **sistem automat de identificare a amprentelor digitale (AFIS)**, astfel cum prevede cadrul juridic existent[14]. AFIS ar trebui să fie operațional de la jumătatea anului 2017[15]. Odată elaborat, AFIS va putea fi accesat de către Europol și, prin urmare, va completa sistemele Europol privind anchetele penale și lupta împotriva terorismului, precum și schimburile de amprente digitale efectuate în cadrul Prüm. Comisia și eu-LISA vor examina posibilitatea unei utilizări mai extinse a viitorului sistem AFIS.

Pe baza unei evaluări permanente și a unui studiu tehnic, Comisia examinează în prezent **posibilitatea de a adăuga anumite funcționalități ale SIS** în vederea prezentării de propuneri de revizuire a temeiului juridic al sistemului. Printre aspectele luate în considerare se numără:

- crearea de alerte SIS privind migranții în situație neregulamentară care fac obiectul deciziilor de returnare;
- utilizarea imaginilor faciale pentru identificarea biometrică, pe lângă amprentele digitale;
- transmiterea automatizată de informații privind obținerea unui rezultat pozitiv în urma unei verificări;
- stocarea în sistemul central al SIS a informațiilor privind rezultatele pozitive referitoare la verificarea alertelor discrete și specifice;
- crearea unei noi categorii de alerte privind persoanele necunoscute căutate pentru care în bazele de date naționale pot exista date criminalistice (de exemplu, o amprentă latentă lăsată la locul infracțiunii)[16].

Comisia va continua să sprijine cu finanțare din partea UE punerea în aplicare a proiectelor care permit efectuarea unor căutări simultane în SIS și în bazele de date ale Interpol privind documentele de călătorie furate și pierdute (SLTD), precum și privind infractori dați în urmărire, vehicule sau arme de foc (iARMS), care sunt complementare cu sistemele de informații de la nivelul UE[17].

---

[14] Articolul 22 litera (c) din 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) și Decizia 533/2007/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II) (JO L 381, 28.12.2006, p. 4 și JO L 205, 7.8.2007 p. 63).

[15] În martie 2016, Comisia a prezentat Parlamentului European și Consiliului un raport privind disponibilitatea și gradul de adecvare al tehnologiei pentru identificarea unei persoane pe baza amprentelor digitale deținute în Sistemul de informații Schengen de a doua generație (SIS II)..

[16] Crearea acestei noi alerte va fi evaluată în vederea asigurării complementarității și a evitării suprapunerii cu actualul cadru Prüm pentru căutarea amprentelor digitale în diferitele baze de date naționale din statele membre ale UE.

[17] Instrumentele de căutare de informații elaborate de Interpol, cum ar fi baza de date a Interpol în rețea fixă (FIND) și baza de date a Interpol în rețea mobilă (MIND), au ca obiectiv să faciliteze căutările simultane în sistemele Interpol și SIS.

Baza de date a Interpol privind documentele de călătorie furate și pierdute (SLTD)

Pentru a asigura o gestionare eficace a frontierelor, este esențial ca documentele de călătorie ale tuturor resortisanților țărilor terțe și ale cetățenilor UE să fie verificate cu ajutorul **bazei de date SLTD**. Autoritățile de asigurare a respectării legii ar trebui să utilizeze baza de date SLTD și pentru căutările din spațiul Schengen. În urma atacurilor teroriste din 13 noiembrie 2015 de la Paris, Consiliul a solicitat ca, până în martie 2016, să se realizeze conexiuni electronice la bazele de date relevante ale Interpol la toate punctele de trecere a frontierelor externe și verificarea automată a documentelor de călătorie[18]. Toate statele membre ar trebui să stabilească conexiunile electronice relevante și să instituie sisteme care să permită actualizarea automată a datelor privind documentele de călătorie furate sau pierdute în baza de date SLTD.

Informații prealabile referitoare la pasageri (API)

În conformitate cu cele mai bune practici existente, statele membre ar trebui, de asemenea, să sporească valoarea adăugată a datelor din **sistemul de informații prealabile referitoare la pasageri** (API) prin stabilirea unei verificări încrucișate automate a acestor date în SIS și în baza de date SLTD a Interpol. Comisia va evalua necesitatea revizuirii temeiului juridic referitor la prelucrarea datelor API, pentru a se asigura punerea în aplicare pe scară mai largă și pentru a include o obligație pentru statele membre de a solicita și utiliza datele API pentru toate zborurile dus și întors. Acest lucru este deosebit de relevant în contextul punerii în aplicare a viitoarei directive privind registrul cu numele pasagerilor, întrucât o utilizare combinată a datelor PNR și API sporește și mai mult eficacitatea datelor PNR în combaterea terorismului și a formelor grave de criminalitate[19].

Sistemul de informații privind vizele (VIS)

De asemenea, Comisia este în curs de a efectua o evaluare generală a **Sistemului de informații privind vizele** (VIS), care urmează să se încheie în 2016. Evaluarea analizează, printre altele, modul în care VIS este utilizat pentru verificările la frontierele externe și în interiorul statelor membre, precum și modul în care acesta contribuie la lupta împotriva fraudării identității și a vizelor. Pe această bază, Comisia va examina ulterior posibilitățile de consolidare a funcționalităților VIS, inclusiv prin:

- îmbunătățirea calității imaginii faciale pentru a permite corespondențe biometrice;
- utilizarea datelor biometrice ale solicitanților de vize pentru a căuta în viitorul sistem automat de identificare a amprentelor digitale care urmează să fie dezvoltat pentru SIS;
- reducerea limitei de vârstă pentru colectarea amprentelor digitale ale copiilor cu vârsta cuprinsă între 6 și 12 ani, oferind, în același timp, garanții solide privind drepturile fundamentale și măsuri de protecție[20];
- facilitarea verificării în baza de date SLTD a Interpol în timpul unei proceduri privind cererea de acordare a vizei.

În ceea ce privește posibilitățile oferite de cadrul juridic existent pentru accesul la datele VIS în scopul **asigurării respectării legii**, statele membre aplică aceste posibilități într-un mod inegal. În acest context, statele membre au semnalat existența unor probleme practice în procedurile pentru accesarea VIS de către autoritățile de asigurare a

[18] Concluziile Consiliului UE și ale statelor membre reunite în cadrul Consiliului privind combaterea terorismului, 20 noiembrie 2015.

[19] A se vedea secțiunea 6.2 referitoare la propunerea de directivă privind registrul cu numele pasagerilor.

[20] Astfel cum este indicat ca posibil din punct de vedere tehnic în studiul JRC „Recunoașterea amprentelor digitale pentru copii"; EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013.

respectării legii. De asemenea, punerea în aplicare a accesului la Eurodac în scopul asigurării respectării legii este, în continuare, foarte limitată. Comisia va analiza dacă este necesară revizuirea cadrului juridic privind accesul la VIS și Eurodac în scopul asigurării respectării legii.

Eurodac

Astfel cum se prevede în Comunicarea intitulată „Posibilități de reformare a sistemului european comun de azil și de îmbunătățire a căilor legale de migrație”[21], Comisia va prezenta o propunere de reformare a **Eurodac**, menită să consolideze funcționalitățile acestui sistem în ceea ce privește migrația neregulamentară și returnarea. Astfel se va aborda lacuna actuală în ceea ce privește posibilitatea de a repera deplasările secundare ale migranților în situație neregulamentară între statele membre. În plus, propunerea va urmări sporirea eficacității procedurilor de returnare și readmisie prin furnizarea de mijloace pentru identificarea și furnizarea de noi documente de identitate migranților în situație neregulamentară în scopul returnării. În acest context, propunerea va acoperi și schimbul cu țările terțe de informații conținute în Eurodac, ținând seama de garanțiile necesare în materie de protecție a datelor.

Europol

UE a acordat **Europol** accesul la principalele baze de date centrale, dar agenția încă nu a făcut uz din plin de această oportunitate. Europol are dreptul de a accesa și de a căuta direct datele introduse în SIS cu privire la arestări, verificări discrete și specifice și obiecte căutate care fac obiectul unui sechestru. Europol a efectuat până în prezent doar un număr relativ limitat de căutări în SIS. Accesul la VIS pentru consultare a fost posibil din punct de vedere juridic pentru Europol începând din septembrie 2013. Din iulie 2015, temeiul juridic al Eurodac permite accesul de către Europol. Agenția ar trebui să accelereze lucrările în desfășurare în vederea stabilirii conexiunii cu VIS și Eurodac. La un nivel mai general, Comisia va evalua dacă este necesar să li se ofere acces suplimentar la sistemele de informații și altor agenții ale UE din domeniul afacerilor interne, în special viitoarei Paze europene de frontieră și de coastă.

Cadrul Prüm

În prezent, **cadrul Prum** nu își valorifică întregul său potențial, din cauza faptului că nu toate statele membre și-au pus în aplicare obligațiile juridice în ceea ce privește integrarea rețelei cu propriile lor sisteme. Statele membre au beneficiat de sprijin financiar și tehnic semnificativ pentru această punere în aplicare și, în prezent, ar trebui să pună în aplicare pe deplin cadrul Prüm. Comisia face uz de competențele care îi sunt conferite pentru a asigura punerea deplină în aplicare a obligațiilor juridice ale statelor membre, iar în ianuarie 2016 a inițiat un dialog structurat (EU Pilot) cu statele membre interesate. În cazul în care răspunsurile statelor membre se dovedesc a fi nesatisfăcătoare, Comisia nu va ezita să lanseze proceduri de constatare a neîndeplinirii obligațiilor.

Sistemul european de informații cu privire la cazierele judiciare (ECRIS)

Sistemul european de informații cu privire la cazierele judiciare, **ECRIS**, permite schimbul de informații privind condamnările referitoare la resortisanții țărilor terțe și la apatrizi, însă nu există nicio procedură care să permită realizarea acestui demers într-un mod eficient. În ianuarie 2016, Comisia a adoptat o propunere legislativă pentru a remedia această lacună[22]. În acest context, Comisia a propus să li se permită autorităților naționale să caute resortisanții țărilor terțe pe baza amprentelor digitale în vederea unei identificări

[21] COM(2016) 197 final.
[22] COM(2016) 7 final, 19.1.2016.

mai sigure. Parlamentul European și Consiliul ar trebui să adopte textul legislativ în 2016.

Aspecte orizontale

O preocupare generală în ceea ce privește sistemele de informații vizează **nivelul de punere în aplicare** de către statele membre. Punerea în aplicare neuniformă a cadrului Prüm și lipsa conexiunilor electronice la baza de date SLTD sunt exemple frapante în acest sens. Pentru a spori nivelul de punere în aplicare în ceea ce privește sistemele de informații, Comisia va monitoriza îndeaproape performanța fiecărui stat membru[23]. Monitorizarea va examina nu numai dacă statele membre își îndeplinesc obligațiile juridice în domeniul sistemelor de informații, ci și modul în care acestea utilizează instrumentele existente și măsura în care urmează cele mai bune practici. Comisia va utiliza diverse surse pentru monitorizarea și promovarea nivelului de punere în aplicare, inclusiv notificările transmise de statele membre și vizitele efectuate în cadrul mecanismului de evaluare și monitorizare Schengen.

O altă preocupare generală în ceea ce privește sistemele de informații este reprezentată de **calitatea datelor introduse**. În cazul în care statele membre nu respectă cerințele minime de calitate, fiabilitatea și valoarea datelor stocate devin foarte limitate, iar riscul unor neconcordanțe și al unor rezultate negative subminează valoarea sistemelor în sine. Pentru a îmbunătăți calitatea datelor introduse, eu-LISA va dezvolta un **mecanism central de monitorizare a calității datelor** pentru toate sistemele care țin de competența sa.

Majoritatea sistemelor de informații din domeniul controalelor la frontiere și al securității administrează date de identificare provenind din documente de călătorie și de identitate. Pentru a se consolida frontierele și securitatea, este necesar ca, pe lângă existența unor sisteme performante, documentele de călătorie și de identitate să fie autentificate cu ușurință și în siguranță. În acest scop, Comisia va prezenta măsuri menite să sporească **securitatea documentelor** electronice și gestionarea documentelor de identitate și să intensifice lupta împotriva fraudării documentelor. Nivelurile interoperabile de identificare securizată, care pot fi atinse cu ajutorul Regulamentului eIDAS[24], ar putea oferi un mijloc pentru a realiza acest lucru.

<u>Acțiuni în vederea îmbunătățirii sistemelor de informații existente</u>

Sistemul de informații Schengen (SIS)

- Comisia și eu-LISA trebuie să elaboreze și să pună în aplicare, până la jumătatea anului 2017, o funcționalitate în cadrul SIS bazată pe un sistem automat de identificare a amprentelor digitale (AFIS).
- Comisia trebuie să prezinte, până la sfârșitul anului 2016, propuneri în vederea revizuirii temeiului juridic al SIS pentru a consolida în continuare funcționalitatea acestuia.
- Statele membre trebuie să maximizeze utilizarea SIS, atât prin introducerea tuturor informațiilor relevante, cât și prin consultarea sistemului ori de câte ori este necesar.

[23] Sub rezerva condițiilor specifice ale Protocolului 22 în ceea ce privește Danemarca și ale Protocoalelor 21 și 36 în ceea ce privește Regatul Unit și Irlanda.

[24] Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

Baza de date a Interpol privind documentele de călătorie furate și pierdute (SLTD)

- Statele membre trebuie să stabilească conexiuni electronice cu instrumentele Interpol la toate punctele de trecere a frontierelor externe.
- Statele membre trebuie să își respecte obligația de a introduce și de a consulta datele privind documentele de călătorie furate sau pierdute, simultan în SIS și în baza de date SLTD.

Informații prealabile referitoare la pasageri (API)

- Statele membre trebuie să automatizeze utilizarea datelor API în vederea efectuării de verificări în SIS și în baza de date a Interpol privind documentele de călătorie furate și pierdute (SLTD), în concordanță cu cele mai bune practici existente.
- Comisia trebuie să evalueze necesitatea revizuirii temeiului juridic pentru prelucrarea de date API.

Sistemul de informații privind vizele (VIS)

- Comisia trebuie să aibă în vedere și alte îmbunătățiri ale VIS înainte de sfârșitul anului 2016.

Eurodac

- Comisia trebuie să prezinte o propunere de revizuire a temeiului juridic al Eurodac, în vederea consolidării funcționalităților acestui sistem în ceea ce privește migrația neregulamentară și returnarea.

Europol

- Europol trebuie să facă uz pe deplin de drepturile sale de acces existente pentru consultarea SIS, VIS și Eurodac.
- Comisia și Europol trebuie să examineze și să promoveze sinergii între sistemul informațional Europol (EIS) și alte sisteme, în special SIS.
- Comisia și eu-LISA trebuie să examineze dacă sistemul automat de identificare a amprentelor digitale (AFIS) care urmează să fie elaborat pentru SIS poate completa sistemele Europol în scopul anchetelor penale și al combaterii terorismului.

Cadrul Prüm

- Statele membre trebuie să pună pe deplin în aplicare și să utilizeze cadrul Prüm.
- Dacă este necesar, Comisia va iniția acțiuni în constatarea neîndeplinirii obligațiilor împotriva statelor membre care nu s-au conectat la cadrul Prüm.
- Comisia și eu-LISA trebuie să examineze dacă sistemul automat de identificare a amprentelor digitale (AFIS) care urmează să fie elaborat pentru SIS poate completa schimburile de date privind amprentele digitale efectuate în cadrul Prüm.

Sistemul european de informații cu privire la cazierele judiciare (ECRIS)

- Parlamentul European și Consiliul ar trebui să adopte în 2016 propunerea legislativă care permite autorităților naționale să caute în ECRIS resortisanți ai țărilor terțe pe baza amprentelor digitale.

Aspecte orizontale

- Comisia trebuie **să monitorizeze și să promoveze nivelul de punere în aplicare** în ceea ce privește sistemele de informații.
- eu-LISA trebuie să dezvolte un **mecanism central de monitorizare a calității datelor** pentru toate sistemele care țin de competența sa.

- Comisia trebuie să prezinte măsuri menite să sporească **securitatea documentelor** electronice **și gestionarea documentelor de identitate** și să intensifice lupta împotriva fraudării documentelor.
- Comisia trebuie să exploreze sinergiile și convergențele dintre sistemele de informații și infrastructurile corespunzătoare pentru gestionarea frontierelor UE și pentru **operațiunile vamale**.

6. DEZVOLTAREA DE SISTEME DE INFORMAȚII SUPLIMENTARE ȘI REMEDIEREA LACUNELOR

Deși sistemele de informații existente acoperă un spectru foarte larg de date care sunt necesare în cadrul gestionării frontierelor și al asigurării respectării legii, există și lacune importante. Unele dintre aceste lacune au fost remediate de către Comisie prin propuneri legislative, și anume propunerile privind un sistem de intrare/ieșire și privind registrul UE cu numele pasagerilor (PNR). În ceea ce privește celelalte lacune care au fost identificate, este oportun să se evalueze cu atenție dacă sunt necesare instrumente suplimentare ale UE.

1. Sistemul de intrare/ieșire

Comisia a prezentat propunerile legislative revizuite pentru instituirea unui sistem de intrare/ieșire (EES), în paralel cu prezenta comunicare. După adoptarea acestora de către colegiuitori, va fi necesar ca eu-LISA să dezvolte și să pună în aplicare sistemul, în cooperare cu statele membre ale spațiului Schengen.

EES va înregistra punctele de trecere a frontierei (intrare și ieșire) pentru toți resortisanții țărilor terțe care vizitează spațiul Schengen pentru o ședere de scurtă durată (maximum 90 de zile pe parcursul unei perioade de 180 de zile), atât pentru călătorii supuși obligației de a deține viză, cât și pentru cei scutiți de obligația de a deține viză, sau pentru șederi efectuate pe baza noii vize de circuit (până la un an). Obiectivele EES sunt: (a) îmbunătățirea gestionării frontierelor externe, (b) reducerea migrației neregulamentare prin abordarea fenomenului de depășire a perioadei permise de ședere și (c) sprijinirea luptei împotriva terorismului și a formelor grave de criminalitate, contribuind astfel la asigurarea unui nivel ridicat de securitate internă.

EES va înregistra identitatea resortisanților țărilor terțe (date alfanumerice, patru amprente digitale și o imagine facială), precum și detalii privind documentele lor de călătorie și va stabili o legătură între aceste informații și datele electronice înregistrate privind intrarea și ieșirea. Practica actuală de ștampilare a documentelor de călătorie va fi eliminată. EES va permite gestionarea eficace a șederilor de scurtă durată autorizate, un grad sporit de automatizare în ceea ce privește controalele la frontieră și îmbunătățirea detectării fraudării de documente și de identitate. Înregistrarea centrală va permite detectarea persoanelor care depășesc perioada permisă de ședere și identificarea persoanelor fără forme legale în spațiul Schengen. EES propus remediază, prin urmare, o lacună importantă în contextul sistemelor de informații existente.

2. Registrul cu numele pasagerilor

Datele din registrul cu numele pasagerilor (PNR) constau în confirmarea rezervării, cu date de contact, informații complete privind cursa și rezervarea, observații speciale, informații privind locul și bagajele, precum și mijloacele de plată. Datele PNR s-au dovedit utile și necesare în eforturile de identificare a călătorilor cu un grad de risc ridicat, în contextul combaterii terorismului, a traficului de droguri, a traficului de persoane, a exploatării sexuale a copiilor și a altor infracțiuni grave. Propunerea de

directivă privind PNR va asigura o cooperare mai bună între sistemele naționale și va reduce lacunele în materie de securitate între statele membre. Prin urmare, această propunere abordează o lacună importantă în ceea ce privește disponibilitatea datelor care sunt necesare pentru combaterea formelor grave de criminalitate și a terorismului. **Directiva privind PNR ar trebui adoptată și pusă în aplicare în regim de urgență.**

Viitoarea directivă va prevedea că statele membre trebuie să instituie unități de informații despre pasageri (UIP), care vor primi date PNR de la transportatori. Aceasta nu va presupune crearea unui sistem central sau a unei baze de date centrale, dar va beneficia de un anumit grad de standardizare a soluțiilor și a procedurilor tehnice naționale. Aceasta va facilita schimbul de date PNR între UIP-uri, astfel cum se prevede în propunerea de directivă. În acest scop, Comisia va sprijini statele membre să analizeze diferite scenarii pentru interconectivitatea dintre UIP-uri, în vederea oferirii unor soluții și a unor proceduri standardizate. Odată ce directiva va fi adoptată, Comisia va accelera lucrările cu privire la protocoalele comune și la formatele de date compatibile pentru transferul de date PNR de către transportatorii aerieni către UIP-uri. Comisia va pregăti un proiect de act de punere în aplicare în termen de trei luni de la adoptarea directivei.

3. Deficit de informații înainte de sosirea resortisanților țărilor terțe scutiți de obligația de a deține viză

Deși identitatea, contactele și informațiile de context ale titularilor de vize sunt înregistrate în VIS, singurele informații disponibile privind persoanele scutite de obligația de a deține viză provin din documentul lor de călătorie. Pentru călătorii care sosesc pe calea aerului sau pe mare, acestea pot fi completate înainte de sosire cu date API. În conformitate cu propunerea de directivă privind PNR, datele PNR vor fi colectate și în cazul în care călătorii ajung în UE pe calea aerului. Pentru persoanele care intră în UE pe la punctele terestre de trecere a frontierei, nu este disponibilă nicio informație înainte de sosirea acestora la frontiera externă a UE.

Deși autoritățile de asigurare a respectării legii pot obține informații privind titularii de vize din VIS, dacă acest lucru este necesar pentru combaterea formelor grave de criminalitate și a terorismului, nu sunt disponibile date comparabile privind persoanele scutite de obligația de a deține viză. Această lipsă de informații este deosebit de problematică pentru gestionarea frontierelor terestre ale UE, în cazul în care un număr substanțial de călători scutiți de obligația de a deține viză sosesc cu autoturismul, autobuzul sau trenul. Mai multe țări învecinate ale UE sunt deja scutite de obligația de a deține viză, iar dialogurile privind liberalizarea vizelor dintre UE și alte țări învecinate sunt în curs. Acest lucru va putea antrena o creștere semnificativă în viitorul apropiat a numărului de călători scutiți de obligația de a deține viză.

Comisia va evalua dacă un nou instrument al UE menit să soluționeze această problemă este necesar, fezabil și proporțional. O opțiune care ar putea fi luată în considerare este un **sistem al UE de informații și autorizare a călătoriilor** (ETIAS), în care călătorii scutiți de obligația de a deține viză ar înregistra informații relevante privind călătoria planificată. Prelucrarea automată a acestor informații i-ar putea ajuta pe polițiștii de frontieră în evaluările lor privind vizitatorii care sosesc din țări terțe pentru o ședere de scurtă durată. Țări precum SUA, Canada și Australia au pus deja în aplicare sisteme similare, inclusiv pentru cetățenii UE.

Sistemele de autorizare a călătoriilor se bazează pe cereri online în care solicitantul furnizează, înainte de plecare, detalii cu privire la identitatea sa, date de contact, scopul călătoriei, itinerariul etc. După obținerea autorizației, procedurile la frontieră devin mai rapide și mai ușoare la sosire. Dincolo de beneficiile în materie de securitate și de

gestionare a frontierelor, precum și de relevanța sa potențială în contextul reciprocității vizelor, un sistem precum ETIAS ar servi, așadar, drept instrument de facilitare a călătoriilor.

4. Sistemul european de inventariere a evidențelor poliției (EPRIS)

Astfel cum se menționează în Agenda europeană privind securitatea, disponibilitatea în timp real a datelor deținute de poliție existente la nivelul statelor membre va face obiectul unor lucrări viitoare privind schimbul de informații. Comisia va evalua necesitatea, fezabilitatea tehnică și proporționalitatea unui sistem european de inventariere a evidențelor poliției (EPRIS) pentru a facilita accesul transfrontalier la informațiile deținute în bazele de date ale autorităților naționale însărcinate cu asigurarea respectării legii. În acest context, Comisia sprijină cu fonduri ale UE implementarea unui proiect-pilot de către un grup de cinci state membre vizând instituirea unui mecanism de căutare transfrontalieră automatizată în registrele naționale pe baza unui sistem de tip „rezultat/niciun rezultat”[25].Comisia va ține seama de rezultatele proiectului în evaluarea sa.

<u>Acțiuni pentru elaborarea unor sisteme de informații suplimentare și pentru remedierea lacunelor în materie de informații</u>

Sistemul de intrare/ieșire (EES)

- Parlamentul European și Consiliul ar trebui să trateze propunerile legislative privind EES drept o prioritate absolută, în vederea adoptării acestor propuneri până la sfârșitul anului 2016.

Registrele cu numele pasagerilor (PNR)

- Parlamentul European și Consiliul ar trebui să adopte Directiva privind PNR până în aprilie 2016.
- Statele membre ar trebui să pună în aplicare în regim de urgență Directiva privind PNR, de îndată ce aceasta va fi adoptată.
- Comisia ar trebui să sprijine schimbul de date între unitățile de informații despre pasageri prin soluții și proceduri standardizate.
- Comisia ar trebui să pregătească un proiect de decizie de punere în aplicare a protocoalelor comune și a formatelor de date compatibile pentru transferul de date PNR de către transportatorii aerieni către UIP-uri, în termen de trei luni de la adoptarea Directivei privind PNR.

Deficit de informații înainte de sosirea resortisanților țărilor terțe scutiți de obligația de a deține viză

- În 2016, Comisia ar trebui să evalueze necesitatea, fezabilitatea tehnică și proporționalitatea creării unui nou instrument al UE, cum ar fi un sistem al UE de informații și autorizare a călătoriilor.

[25] Proiectul-pilot privind procedura referitoare la schimbul automatizat de date (ADEP) vizează crearea unui sistem tehnic care să permită, prin intermediul unui indice, să se afle dacă în evidențele poliției din unul sau mai multe state membre există un cazier judiciar referitor la o persoană fizică sau o anchetă penală a poliției. Răspunsul automatizat la o căutare în cadrul indicelui ar indica doar dacă datele sunt disponibile sau nu; un așa-numit răspuns de tip „rezultat” sau „niciun rezultat”. În cazul unui răspuns de tip „rezultat”, într-o a doua etapă ar trebui solicitate date cu caracter personal suplimentare, prin intermediul canalelor obișnuite de cooperare polițienească.

Sistemul european de inventariere a evidențelor poliției (EPRIS)

- În 2016, Comisia ar trebui să evalueze necesitatea, fezabilitatea tehnică și proporționalitatea instituirii EPRIS.

7. CĂTRE INTEROPERABILITATEA SISTEMELOR DE INFORMAȚII

Interoperabilitatea reprezintă capacitatea sistemelor de informații de a face schimb de date și de a permite schimbul de informații. Se pot distinge **patru dimensiuni ale interoperabilității**, fiecare prezentând probleme juridice[26], tehnice și operaționale, inclusiv în ceea ce privește protecția datelor:

- o interfață de căutare unică pentru a interoga simultan mai multe sisteme de informații și pentru a produce rezultate combinate pe un singur ecran;
- interconectivitatea sistemelor de informații atunci când datele înregistrate într-un sistem vor fi consultate în mod automat de un alt sistem;
- instituirea unui serviciu comun de corespondențe biometrice în sprijinul diferitelor sisteme de informații;
- un depozit comun de date pentru diferite sisteme de informații (modulul de bază).

În vederea inițierii unui proces vizând obținerea interoperabilității sistemelor de informații la nivelul UE, Comisia va institui, împreună cu agențiile UE, experții naționali și părțile interesate instituționale relevante, un **grup de experți** la nivel înalt **privind sistemele de informații și interoperabilitatea**. Grupul de experți va avea sarcina de a aborda aspectele juridice, tehnice și operaționale ale diferitelor opțiuni pentru realizarea interoperabilității sistemelor de informații, inclusiv necesitatea, fezabilitatea tehnică și proporționalitatea opțiunilor disponibile, precum și implicațiile acestora în materie de protecție a datelor. Acest grup ar trebui să remedieze deficiențele și lacunele actuale în materie de cunoștințe care sunt cauzate de complexitatea și de fragmentarea sistemelor de informații la nivel european. Grupul de experți va avea o perspectivă amplă și cuprinzătoare asupra gestionării frontierelor și a asigurării respectării legii, ținând seama totodată de rolurile, responsabilitățile și sistemele utilizate de autoritățile vamale în acest sens. Metoda de lucru a grupului va urmări crearea unei sinergii între toate experiențele relevante care, în trecut, au fost, prea adesea, compartimentate.

Obiectivul acestui proces este acela de a oferi o viziune strategică generală asupra arhitecturii UE a gestionării datelor pentru controlul și securitatea frontierelor, precum și acela de a oferi soluții pentru punerea în aplicare a acestei viziuni.

Acest proces de consultare va **avea următoarele obiective**:

- Sistemele de informații ar trebui să fie complementare. Ar trebui evitate suprapunerile, iar redundanțele existente ar trebui eliminate. Lacunele trebuie să fie abordate în mod adecvat.
- Ar trebui să se urmărească o abordare modulară, valorificând pe deplin progresele tehnologice și bazându-se pe principiul protecției vieții private începând cu momentul conceperii.
- Respectarea deplină a tuturor drepturilor fundamentale atât ale cetățenilor UE, cât și ale resortisanților țărilor terțe ar trebui asigurată încă de la început, în conformitate cu Carta drepturilor fundamentale.

[26] Sub rezerva condițiilor specifice ale Protocolului 22 în ceea ce privește Danemarca și ale Protocoalelor 21 și 36 în ceea ce privește Regatul Unit și Irlanda.

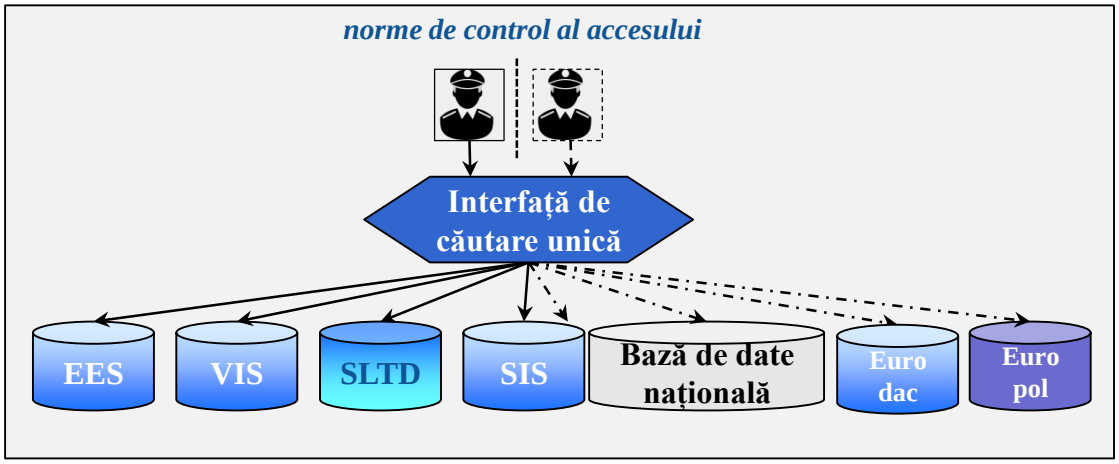
- Atunci când este necesar și fezabil, sistemele de informații ar trebui să fie interconectate și interoperabile. Căutările simultane în cadrul sistemelor ar trebui facilitate pentru a se asigura că toate informațiile relevante sunt puse la dispoziția polițiștilor de frontieră sau a agenților de poliție atunci când și în cazul în care acest lucru este necesar pentru sarcinile lor, fără a modifica drepturile de acces existente.

1. Interfață de căutare unică

Prima dimensiune a interoperabilității este **capacitatea**, oferită polițiștilor de frontieră și agenților de poliție, **de a interoga simultan mai multe sisteme de informații și de a produce rezultate combinate pe un singur ecran**, cu respectarea deplină a drepturilor de acces ale acestora, în conformitate cu respectivele scopuri. Aceasta necesită platforme cu o interfață de căutare unică susceptibile de a consulta simultan diferite sisteme de informații printr-o singură interogare. De exemplu, prin citirea cipului unui document de călătorie sau prin utilizarea datelor biometrice, această platformă ar putea interoga în același timp mai multe baze de date diferite. Abordarea bazată pe căutarea unică se aplică tuturor autorităților care au nevoie să acceseze și să utilizeze datele (adică, polițiștii de frontieră, autoritățile de asigurare a respectării legii, serviciile de azil), în conformitate cu limitarea scopului și cu normele stricte de control al accesului. De asemenea, aceasta poate fi folosită cu echipamente mobile. Instituirea unei interfețe de căutare unică reduce complexitatea sistemelor de informații la nivel european, întrucât le permite polițiștilor de frontieră și agenților de poliție să interogheze simultan mai multe sisteme de informații prin intermediul unei singure proceduri, în conformitate cu drepturile lor de acces.

Mai multe state membre au instalat deja astfel de platforme cu o interfață de căutare unică. Pe baza celor mai bune practici existente, Comisia, împreună cu eu-LISA, se va strădui să identifice o soluție standardizată pentru o interfață de căutare unică. Statele membre ar trebui să utilizeze finanțarea din partea UE în temeiul programelor lor naționale din cadrul Fondului pentru securitate internă în vederea finanțării instalării unei astfel de funcționalități. Comisia va monitoriza îndeaproape modul în care statele membre utilizează funcționalitatea unei interfețe de căutare unică la nivel național.

Figura 2 *Interfață de căutare unică*



Căutarea în cadrul mai multor sisteme centralizate sau naționale (conform descrierii) este mai ușor de realizat decât căutarea în cadrul unor sisteme descentralizate. Comisia și eu-LISA vor analiza dacă o interfață de căutare unică poate fi, de asemenea, utilizată pentru a efectua, în cadrul unui ghișeu unic, căutări simultane în sisteme descentralizate precum Prüm și ECRIS. Comisia și eu-LISA vor efectua această analiză, împreună cu Grupul de

experți privind sistemele de informații și interoperabilitatea, fără a modifica drepturile de acces existente.

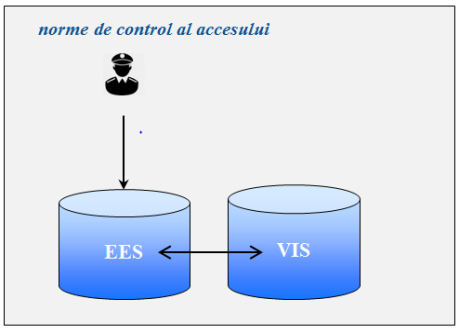
2. Interconectivitatea sistemelor de informații

O a doua dimensiune a interoperabilității este interconectivitatea sistemelor de informații. Aceasta înseamnă că diferitele sisteme sau baze de date sunt în măsură să „comunice unele cu altele” din punct de vedere tehnic. **Datele înregistrate într-un sistem ar putea fi consultate automat, la nivel central, de un alt sistem**. Acest lucru necesită o compatibilitate tehnică între sisteme, iar elementele de date stocate în aceste sisteme (de exemplu, amprentele digitale) trebuie să fie interoperabile. Interconectivitatea poate reduce cantitatea de date care circulă în rețelele de comunicații și tranzitează sistemele naționale.

Interconectivitatea necesită garanții corespunzătoare de protecție a datelor și norme stricte de control al accesului. Acordul politic la care au ajuns colegiuitorii în decembrie 2015 cu privire la reforma în materie de protecție a datelor va institui un cadru modern privind protecția datelor la nivelul UE care va furniza aceste garanții. Este important ca colegiuitorii să adopte, fără întârziere, Regulamentul general privind protecția datelor și Directiva privind protecția datelor.

Conceptul de interconectivitate este inclus în viitorul sistem de intrare/ieșire (EES). Viitorul EES va fi în măsură să comunice direct cu VIS la nivel central și viceversa. Aceasta este o etapă importantă în ceea ce privește remedierea fragmentării actuale a arhitecturii UE a gestionării datelor pentru controlul și securitatea frontierelor, precum și a problemelor conexe. Efectuarea de verificări încrucișate automate va scuti statele membre de necesitatea de a interoga VIS cu ocazia verificărilor la frontieră, va reduce cerințele de întreținere și va îmbunătăți performanța sistemului.

Figura 3 *Interconectivitatea sistemelor: exemplul EES/VIS*



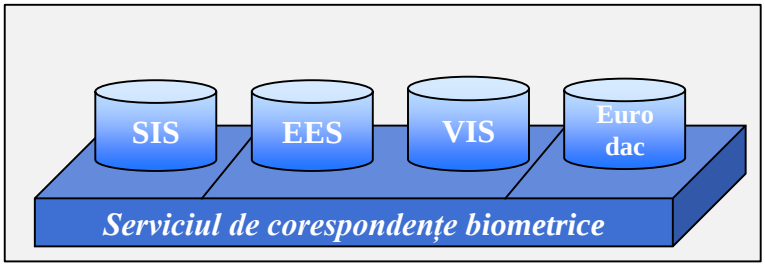
Ca o etapă următoare, Comisia și eu-LISA vor analiza dacă interconectivitatea la nivel central între viitorul EES și VIS poate fi extinsă la SIS și dacă se poate stabili o interconectivitate între Eurodac și SIS. Comisia și eu-LISA vor efectua această analiză împreună cu Grupul de experți privind sistemele de informații și interoperabilitatea.

3. Serviciul comun de corespondențe biometrice

O a treia dimensiune a interoperabilității este domeniul elementelor biometrice de identificare. De exemplu, în cazul în care sunt colectate amprente digitale la un consulat al unui stat membru cu echipamente specifice, este esențial ca aceste amprente să poată fi corelate prin intermediul VIS la un punct de control la frontieră dintr-un alt stat membru, utilizând echipamente de alt tip. Aceeași cerință se aplică și interogărilor de amprente digitale din alte sisteme: eșantioanele biometrice trebuie să respecte cerințele minime de calitate și format pentru a asigura, fără dificultate, acest tip de interoperabilitate.

La nivelul sistemului, interoperabilitatea elementelor biometrice de identificare permite utilizarea unui serviciu comun de corespondențe biometrice pentru mai multe sisteme de informații, respectând normele privind protecția datelor cu caracter personal prin compartimentarea datelor, cu norme separate de control al accesului pentru fiecare categorie de date[27]. Aceste servicii comune generează importante beneficii financiare, de întreținere și operaționale.

Figura 4 *Serviciul comun de corespondențe biometrice*



Comisia și eu-LISA vor analiza dacă instituirea unui serviciu comun de corespondențe biometrice pentru toate sistemele de informații relevante este necesară și fezabilă din punct de vedere tehnic. Comisia și eu-LISA vor efectua această analiză împreună cu Grupul de experți privind sistemele de informații și interoperabilitatea.

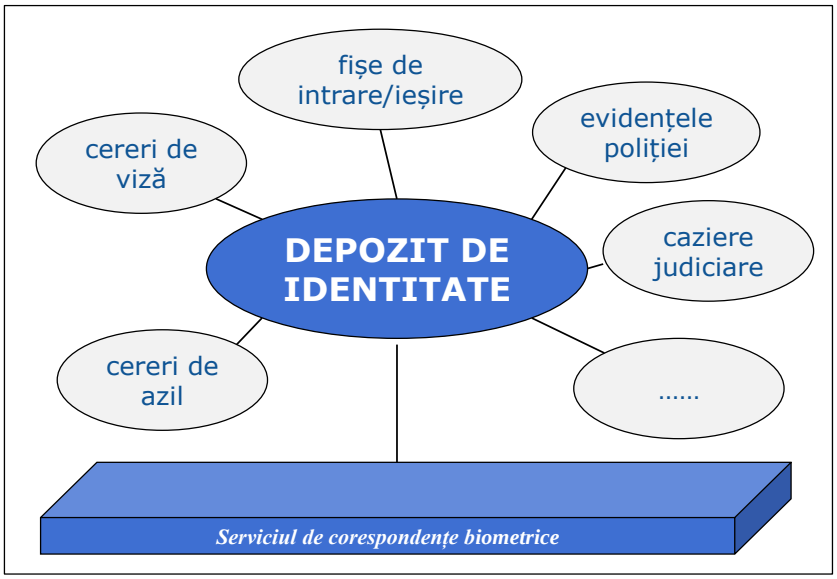
4. Depozitul comun de date

Cea mai ambițioasă abordare pe termen lung în materie de interoperabilitate ar fi un **depozit comun de date la nivelul UE pentru diferite sisteme de informații.** Depozitul comun ar constitui un modul de bază, care conține datele fundamentale (date alfanumerice și biometrice), în timp ce alte elemente de date și caracteristicile specifice ale diverselor sisteme de informații (de exemplu, date privind vizele) ar fi stocate în module specifice. Modulul de bază și modulele specifice ar fi conectate între ele pentru a face legătura între seturile de date respective. Astfel s-ar crea o **gestionare modulară și integrată a identității în materie de frontiere și securitate.** Respectarea normelor de protecție a datelor ar trebui să fie asigurată, de exemplu prin compartimentarea datelor, recurgându-se la norme separate de control al accesului pentru fiecare categorie de date.

Instituirea unui depozit comun de date ar permite depășirea fragmentării actuale a arhitecturii UE a gestionării datelor pentru controlul și securitatea frontierelor. Această fragmentare este contrară principiului minimizării datelor, întrucât rezultă în stocarea de mai multe ori a aceloraşi date. În cazul în care este necesar, depozitul comun ar permite recunoașterea conexiunilor și ar oferi o imagine generală prin combinarea unor elemente de date individuale stocate în diferite sisteme de informații. Astfel, ar fi remediate lacunele actuale în materie de cunoaștere și s-ar face lumină în „unghiurile moarte” pentru polițiștii de frontieră și agenții de poliție.

[27] Comparabil cu partajarea unui server de fișiere fizice cu o multitudine de utilizatori, fiecare având drepturi de acces specifice doar pentru anumite dosare.

Figura 5 *Depozitul comun de date*



Opțiunea de a institui un depozit comun de date la nivelul UE ridică întrebări importante de definire a scopului, a necesității, a fezabilității tehnice și a proporționalității prelucrării datelor în cauză. Ar fi necesară o revizuire completă a cadrului juridic de instituire a diferitelor sisteme de informații, și anume un obiectiv care nu ar putea fi atins decât pe termen lung. Grupul de experți privind sistemele de informații și interoperabilitatea va aborda chestiunile juridice, tehnice și operaționale legate de un depozit comun de date, inclusiv aspectele referitoare la protecția datelor.

Pentru toate cele patru dimensiuni ale interoperabilității menționate mai sus (interfața de căutare unică, interconectivitatea sistemelor, serviciul unic de corespondențe biometrice și depozitul comun de date), este necesar ca datele stocate în diferite sisteme de informații sau module să fie compatibile. Pentru a realiza acest lucru, este important să se continue activitatea privind un **format uniform al mesajelor** (*Uniform Message Format* – UMF), în vederea creării unui standard comun pentru toate sistemele de informații relevante[28].

<u>Acțiuni în vederea interoperabilității sistemelor de informații</u>

- Comisia trebuie să instituie, împreună cu agențiile UE, cu statele membre și cu părțile interesate relevante, un **grup de experți privind sistemele de informații și interoperabilitatea** pentru a examina aspectele juridice, tehnice și operaționale legate de consolidarea interoperabilității sistemelor de informații, inclusiv de necesitatea, fezabilitatea tehnică și proporționalitatea opțiunilor disponibile și implicațiile lor în materie de protecție a datelor.

[28] Comisia a sprijinit dezvoltarea în continuare a UMF în Comunicarea din 2012 privind modelul european de schimb de informații (EIXM) și, în prezent, finanțează cel de al treilea proiect-pilot privind UMF, cu scopul de a crea un standard comun pentru toate bazele de date relevante, care să fie utilizat la nivel național (la nivelul statelor membre), la nivelul UE (pentru sistemele centrale și de către agenții) și la nivel internațional (Interpol).

Interfață de căutare unică

- Comisia și eu-LISA trebuie să sprijine statele membre la instalarea unei interfețe de căutare unice pentru a interoga sistemele centrale.
- Comisia și eu-LISA trebuie să examineze, împreună cu grupul de experți, dacă interfața de căutare unică ar putea fi utilizată pentru a efectua, în cadrul unui ghișeu unic, căutări simultane în toate sistemele relevante, fără a modifica drepturile de acces existente.

Interconectivitatea sistemelor de informații

- Comisia și eu-LISA trebuie să analizeze, împreună cu grupul de experți, dacă interconectivitatea între sistemele de informații centralizate ar putea fi promovată mai mult, dincolo de interconectivitatea deja propusă între sistemul de intrare/ieșire și Sistemul de informații privind vizele.

Serviciul de corespondențe biometrice

- Comisia și eu-LISA trebuie să analizeze, împreună cu grupul de experți, necesitatea și fezabilitatea tehnică a creării unui serviciu comun de corespondențe biometrice pentru toate sistemele de informații relevante.

Depozitul comun de date (modulul de bază)

- Comisia și eu-LISA trebuie să examineze, împreună cu grupul de experți, implicațiile juridice, tehnice, operaționale și financiare ale elaborării pe termen mai lung a unui depozit comun de date.
- Comisia și eu-LISA trebuie să participe la lucrările în curs vizând crearea unui format uniform al mesajelor pentru toate sistemele de informații relevante.

8. CONCLUZII

Prezenta comunicare propune o reflecție asupra modului în care sistemele de informații din UE pot consolida într-un mod mai eficient gestionarea frontierelor și securitatea internă, bazându-se pe sinergiile importante dintre agendele europene privind securitatea și migrația. O serie de sisteme de informații le oferă deja polițiștilor de frontieră și agenților de poliție informații relevante, însă aceste sisteme nu sunt perfecte. UE se confruntă cu provocarea reprezentată de crearea unei arhitecturi mai solide și mai inteligente a gestionării datelor, cu respectarea deplină a drepturilor fundamentale, în special a protecției datelor cu caracter personal și a principiului aferent de limitare a scopului.

Lacunele existente în ceea ce privește arhitectura UE a gestionării datelor trebuie remediate. Împreună cu prezenta comunicare, Comisia a prezentat o propunere privind un sistem de intrare/ieșire, care ar trebui adoptată în regim de urgență. Directiva privind registrul cu numele pasagerilor trebuie, de asemenea, să fie adoptată în săptămânile următoare. Propunerea privind Paza europeană de frontieră și de coastă ar trebui adoptată până în vara acestui an. În paralel, Comisia va continua să depună eforturi în vederea consolidării și, dacă este necesar, a simplificării sistemelor existente, cum ar fi dezvoltarea unei funcționalități a sistemului automat de identificare a amprentelor digitale pentru Sistemul de informații Schengen.

Statele membre trebuie să utilizeze pe deplin sistemele de informații existente și să stabilească, în conformitate cu obligațiile lor legale, conexiunile tehnice necesare pentru toate sistemele de informații și bazele de date. Deficiențele existente, în special în cadrul Prüm, trebuie remediate fără întârziere. Deși prezenta comunicare inițiază o dezbatere și

începe un proces vizând remedierea lacunelor și a deficiențelor sistemice, este responsabilitatea statelor membre să remedieze de urgență deficiențele persistente în ceea ce privește introducerea de informații în bazele de date ale UE și schimbul de informații în întreaga Uniune.

Pentru a îmbunătăți din punct de vedere structural arhitectura UE a gestionării datelor pentru controlul și securitatea frontierelor, prezenta comunicare inițiază un proces ce vizează realizarea interoperabilității sistemelor de informații. Comisia va institui un grup de experți privind sistemele de informații și interoperabilitatea pentru a aborda modalitățile juridice, tehnice și operaționale ale diferitelor opțiuni menite să realizeze interoperabilitatea sistemelor de informații și să remedieze deficiențele și lacunele. În urma constatărilor grupului de experți, Comisia Europeană va prezenta alte propuneri concrete Parlamentului European și Consiliului ca bază pentru o discuție comună privind calea de urmat. Comisia va solicita, de asemenea, contribuția Autorității Europene pentru Protecția Datelor și a autorităților naționale de protecție a datelor care se reunesc în cadrul Grupului de lucru „Articolul 29”.

Obiectivul ar trebui să fie elaborarea unei strategii comune pentru ca gestionarea datelor în UE să fie mai eficace și mai eficientă, cu respectarea deplină a cerințelor privind protecția datelor, pentru a proteja mai bine frontierele externe ale UE și pentru a consolida securitatea internă a acesteia, în beneficiul tuturor cetățenilor.

ANEXA 1: ABREVIERI

API	Informații prealabile referitoare la pasageri
AFIS	Sistemul automat de identificare a amprentelor digitale: sistemul care permite captarea, stocarea, compararea și verificarea amprentelor digitale.
SIV	Sistemul de informații al vămilor
ECRIS	Sistemul european de informații cu privire la cazierele judiciare
EES	Sistemul de intrare/ieșire (propus)
EIXM	Modelul european de schimb de informații
EIS	Sistemul informațional Europol
EPRIS	Sistemul european de inventariere a evidențelor poliției
Eurodac	Sistemul dactiloscopic european
Europol	Oficiul European de Poliție (Agenția Uniunii Europene în materie de aplicare a legii)
ETIAS	Sistemul UE de informații și autorizare a călătoriilor (posibil)
eu-LISA	Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție.
FIND	Baza de date a Interpol în rețea fixă
Frontex	Agenția Europeană pentru Gestionarea Cooperării Operative la Frontierele Externe ale Statelor Membre ale Uniunii Europene
iARMS	Sistemul (Interpol) de înregistrare și de gestionare a urmăririi armelor ilicite
Interpol	Organizația Internațională de Poliție Criminală
MIND	Baza de date a Interpol în rețea mobilă
UIP	Unitate de informații despre pasageri: unitate care trebuie instituită în fiecare stat membru pentru a primi date PNR de la transportatori
PNR	Registru cu numele pasagerilor
Prüm	Mecanismul de cooperare polițienească pentru schimbul de informații referitoare la ADN, amprente digitale și date privind înmatricularea vehiculelor
SafeSeaNet	Platforma europeană pentru schimbul de date din domeniul maritim între autoritățile maritime din statele membre
SBC	Codul frontierelor Schengen
SIENA	Aplicație de rețea pentru schimbul securizat de informații
SIS	Sistemul de informații Schengen (denumit uneori și de a doua generație – SIS II)
SLTD	Baza de date (a Interpol) privind documentele de călătorie furate și pierdute
sTESTA	Servicii transeuropene securizate de telematică între administrații [care vor face obiectul unei modernizări, trecându-se la TESTA-NG (generația următoare)]
UMF	Format uniform pentru mesaje: formatul mesajelor care permite compatibilitatea între sistemele de informații

VIS	Sistemul de informații privind vizele
VRD	Date privind înmatricularea vehiculelor

ANEXA 2: INVENTARUL SISTEMELOR DE INFORMAȚII EXISTENTE PENTRU GESTIONAREA FRONTIERELOR ȘI ASIGURAREA RESPECTĂRII LEGII

1. Sistemul de informații Schengen (SIS)

SIS este cea mai mare și mai utilizată platformă pentru schimbul de informații privind imigrația și asigurarea respectării legii. Acesta este un sistem centralizat, utilizat de 25 de state membre ale UE[29] și patru țări asociate spațiului Schengen[30], care cuprinde în prezent 63 de milioane de alerte. Acestea sunt înregistrate și consultate de autoritățile competente precum poliția, autoritățile de control la frontiere și serviciile de imigrație. Acest sistem conține înregistrări privind resortisanții țărilor terțe cărora li se interzice intrarea sau șederea în spațiul Schengen, precum și privind cetățenii UE și resortisanții țărilor terțe care sunt dați în urmărire sau dispăruți (inclusiv copii) și privind obiecte căutate (arme de foc, vehicule, documente de identitate, echipamente industriale etc.). Caracteristica distinctivă a SIS în comparație cu alte instrumente în materie de schimb de informații este aceea că informațiile din cadrul său sunt completate de o instrucțiune vizând măsuri concrete care urmează să fie luate de către agenții de pe teren, cum ar fi arestarea sau sechestrarea.

Verificările SIS sunt obligatorii pentru prelucrarea vizelor de scurtă ședere, pentru controalele la frontieră în cazul resortisanților țărilor terțe și, într-un mod nesistematic[31], pentru cetățenii UE și alte persoane care beneficiază de dreptul la liberă circulație. În plus, fiecare verificare a poliției de pe teritoriul unui stat ar trebui să includă o verificare automată în SIS.

2. Sistemul de informații privind vizele (VIS)

VIS este un sistem centralizat pentru schimbul de date privind vizele de scurtă ședere între statele membre. Acesta prelucrează datele și deciziile referitoare la cererile de vize de scurtă ședere pentru a vizita sau a tranzita spațiul Schengen. Toate consulatele statelor din spațiul Schengen (aproximativ 2 000) și toate punctele lor de trecere a frontierelor externe (aproximativ 1 800 în total) au fost racordate la sistem.

VIS conține date privind cererile de viză și deciziile aferente, specificând, de asemenea, dacă vizele eliberate sunt revocate, anulate sau prelungite. Sistemul conține în prezent date referitoare la 20 de milioane de cereri de viză, iar, în perioadele de vârf, gestionează peste 50 000 de operațiuni pe oră. Fiecare solicitant de viză furnizează informații biografice detaliate, o fotografie digitală și zece amprente digitale. Astfel, VIS reprezintă un mijloc sigur pentru a verifica identitatea solicitanților de viză, a evalua posibilele cazuri de migrație neregulamentară și riscurile potențiale la adresa securității, precum și pentru a preveni fenomenul de „visa shopping”.

La punctele de trecere a frontierei sau pe teritoriul statelor membre, VIS este utilizat pentru a verifica identitatea titularilor de viză prin compararea amprentelor digitale ale acestora cu amprentele digitale stocate în VIS. Această procedură garantează că persoana care a depus cererea de viză este aceeași persoană cu cea care trece frontiera. O căutare a amprentelor digitale în VIS permite, de asemenea, identificarea unei persoane care a depus o cerere de viză în ultimii cinci ani și care poate nu este în posesia unor documente de identitate.

---

[29] Toate, cu excepția Irlandei, Ciprului, Croației.

[30] Elveția, Liechtenstein, Norvegia și Islanda.

[31] Această regulă poate face obiectul unor modificări, astfel cum se prevede în propunerea Comisiei COM/2015/0670 privind modificarea Codului frontierelor Schengen.

3. Eurodac

Eurodac (sistemul dactiloscopic european) conține amprentele digitale ale solicitanților de azil și ale resortisanților țărilor terțe care trec în mod neregulamentar frontierele externe ale spațiului Schengen. În prezent, scopul său principal este de a stabili ce țară a UE este responsabilă de prelucrarea unei cereri de azil, în conformitate cu Regulamentul Dublin. Acesta este disponibil la punctele de trecere a frontierei, dar, spre deosebire de SIS și VIS, nu este un sistem de gestionare a frontierelor.

Amprentele digitale ale migranților în situație neregulamentară care intră în UE în mod ilegal sunt prelevate la punctele de trecere a frontierei. Acestea sunt stocate în Eurodac pentru a verifica identitatea persoanei vizate în cazul unei viitoare cereri de azil. Autoritățile de imigrare și organele de poliție pot, de asemenea, să compare datele dactiloscopice ale migranților în situație neregulamentară din statele membre ale UE, pentru a verifica dacă aceștia au solicitat azil într-un alt stat membru. Autoritățile de asigurare a respectării legii și Europol au, de asemenea, dreptul să efectueze căutări în cadrul Eurodac pentru a preveni, a detecta sau a investiga infracțiuni grave sau infracțiuni de terorism.

Înregistrarea amprentelor digitale ale solicitanților de azil sau ale migranților aflați în situație neregulamentară într-un sistem centralizat permite identificarea și monitorizarea deplasărilor lor secundare[32] în interiorul UE, până când se depune o cerere de protecție internațională sau se emite o decizie de returnare (în viitor, cu o alertă corespunzătoare în SIS). Pe plan mai general, identificarea și monitorizarea migranților în situație neregulamentară sunt necesare pentru a asigura furnizarea de noi documente de identitate de către autoritățile din țările lor de origine și pentru a facilita astfel returnarea acestora.

4. Baza de date privind documentele de călătorie furate și pierdute (SLTD)

Baza de date a Interpol privind documentele de călătorie furate și pierdute (SLTD) este o bază de date centrală pentru pașapoarte și alte documente de călătorie pe care autoritățile emitente le-au declarat către Interpol ca fiind furate sau pierdute. Aceasta include informații despre blanchetele de pașapoarte furate. Documentele de călătorie declarate ca fiind pierdute sau furate autorităților din țările participante la SIS sunt introduse atât în SLTD, cât și în SIS. De asemenea, SLTD conține informații privind documentele de călătorie introduse de către țările care nu participă la SIS (Irlanda, Croația, Cipru și țări terțe).

Astfel cum se arată în concluziile Consiliului din 9 și 20 noiembrie 2015, precum și în Propunerea Comisiei din 15 decembrie 2015 de regulament privind o modificare punctuală a Codului frontierelor Schengen[33], documentele de călătorie ale tuturor resortisanților țărilor terțe și ale persoanelor care beneficiază de dreptul la liberă circulație ar trebui să fie verificate în raport cu SLTD. Toate posturile de inspecție la frontieră trebuie să fie conectate la SLTD. În plus, căutările în SLTD în scopul asigurării respectării legii ar avea efecte pozitive suplimentare în ceea ce privește securitatea.

---

[32] De exemplu, refugiații ajunși în Grecia fără intenția de a depune o cerere de azil în Grecia, ci de a-și continua călătoria în alte state membre pe cale terestră.

[33] COM(2015) 670 final, Propunere de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (CE) nr. 562/2006 în ceea ce privește consolidarea controalelor prin consultarea bazelor de date relevante la frontierele externe.

5. Informații prealabile referitoare la pasageri (API)

Obiectivul API este de a colecta informații cu privire la identitatea unei persoane înainte de îmbarcarea pentru zborurile cu destinația UE, precum și de a identifica migranții în situație neregulamentară la sosire. Datele API sunt informațiile care figurează într-un document de călătorie și se referă la numele complet, data nașterii, naționalitatea, numărul și tipul documentului de călătorie al unui călător, precum și informații privind punctul de trecere a frontierei de plecare și de intrare, cât și detalii despre transport. Datele API privind pasagerii sunt colectate, de obicei, la momentul înregistrării.

În cazul transportului pe mare, informațiile prealabile sosirii trebuie să fie transmise, în temeiul Convenției privind facilitarea traficului maritim internațional, cu 24 de ore înaintea sosirii navei. Directiva 2010/65/UE[34] prevede transmiterea de date în format electronic, printr-o interfață unică, ce conectează SafeSeaNet, e-Customs și alte sisteme electronice.

Nu există niciun sistem central al UE pentru a înregistra datele API.

6. Sistemul informațional Europol

Sistemul informațional Europol (EIS) este o bază de date centralizată a informațiilor în materie penală în scopuri investigative. Acesta poate fi utilizat de statele membre și de Europol pentru a stoca și a efectua căutări de date privind infracțiunile grave și terorismul. Informațiile stocate în EIS se referă la persoane, documente de identitate, automobile, arme de foc, numere de telefon, adrese de e-mail, amprente digitale, ADN și informații legate de criminalitatea cibernetică, ce pot fi corelate în diferite moduri, pentru a crea o imagine mai detaliată și structurată a unui caz de criminalitate. EIS sprijină cooperarea în domeniul asigurării respectării legii și nu este disponibil pentru autoritățile de control la frontieră.

Schimbul de informații se efectuează prin intermediul platformei SIENA[35], care este o rețea de comunicații electronice securizată între Europol, birourile de legătură, unitățile naționale ale Europol, autoritățile competente desemnate (cum ar fi autoritățile vamale, birourile de recuperare a activelor etc.) și părțile terțe conexe.

În mai 2017 va intra în vigoare un nou cadru juridic pentru Europol. Acest cadru va permite consolidarea capacității operaționale a Europol de a efectua analize și de a identifica mai bine legăturile dintre informațiile disponibile.

7. Cadrul Prüm

Cadrul Prüm are la bază un acord multilateral[36] între statele membre care permite schimbul de informații referitoare la ADN, amprente digitale și date privind înmatricularea vehiculelor (VRD). Conceptul se bazează pe interconectarea unui sistem național la sistemele naționale din toate celelalte state membre ale UE, astfel încât să se permită căutări încrucișate la distanță. În cazul în care o căutare generează un rezultat pozitiv în baza de date a altor state membre, se face schimb de detalii cu privire la rezultatul pozitiv prin intermediul mecanismelor de schimburi bilaterale.

---

[34] Directiva 2010/65/UE a Parlamentului European și a Consiliului din 20 octombrie 2010 privind formalitățile de raportare aplicabile navelor la sosirea în și/sau la plecarea din porturile statelor membre și de abrogare a Directivei 2002/6/CE.

[35] *Secure Information Exchange Network Application* (Aplicație de rețea pentru schimbul securizat de informații).

[36] Tratatul de la Prüm din 2005. Tratatul a fost integrat în legislația UE în 2008 prin Decizia 2008/615/JAI a Consiliului.

8. Sistemul european de informații cu privire la cazierele judiciare (ECRIS)

ECRIS este un sistem electronic care permite schimbul de informații privind condamnările anterioare pronunțate împotriva unei anumite persoane de instanțele penale din UE în scopul unui proces penal împotriva acelei persoane și, în cazul în care acest lucru este permis de legislația națională, în alte scopuri. Statele membre de condamnare trebuie să notifice condamnările pronunțate împotriva unui resortisant al unui alt stat membru statului membru al cărui resortisant este cetățeanul respectiv. Statul membru de cetățenie trebuie să stocheze aceste informații și, prin urmare, poate să furnizeze, la cerere, informații la zi cu privire la cazierele judiciare ale resortisanților săi, indiferent de statul membru al UE în care au fost pronunțate condamnările.

ECRIS permite, de asemenea, schimbul de informații privind condamnările unor resortisanți ai țărilor terțe sau ale unor apatrizi. Autoritățile centrale desemnate din fiecare stat membru sunt punctele de contact în cadrul rețelei ECRIS și îndeplinesc toate atribuțiile, cum ar fi notificarea, stocarea, solicitarea și furnizarea de informații privind cazierele judiciare.