COMISIA EUROPEANĂ

Bruxelles, 20.7.2010

COM(2010)385 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CĂTRE CONSILIU

Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție

1. INTRODUCERE

Uniunea Europeană a cunoscut importante transformări din momentul în care liderii a cinci țări europene au decis la Schengen, în 1985, să elimine controalele la frontierele lor comune. Acordul acestora a condus la încheierea, în 1990, a Convenției Schengen, care conținea premisele pentru multe din politicile actuale de gestionare a informației. Eliminarea controalelor la frontierele interne a stimulat dezvoltarea unei întregi serii de măsuri la frontierele externe, în principal cu privire la eliberarea vizelor, coordonarea politicilor în materie de azil și imigrare, consolidarea cooperării polițienești, judiciare și vamale în lupta împotriva criminalității transfrontaliere. Nici spațiul Schengen, nici piața internă a UE nu ar putea funcționa astăzi în absența schimbului transfrontalier de date.

Atacurile teroriste din Statele Unite ale Americii din 2001, precum și atentatele cu bombă din Madrid și Londra din 2004 și respectiv 2005, au insuflat o altă dinamică în dezvoltarea politicilor Europei în materie de gestionare a informațiilor. Consiliul și Parlamentul European au adoptat, în 2006, Directiva privind păstrarea datelor, cu scopul de a permite autorităților naționale să combată criminalitatea gravă prin păstrarea datelor de trafic și localizare ale telecomunicațiilor[1]. Ulterior, Consiliul a adoptat inițiativa suedeză de simplificare a schimbului transfrontalier de informații în anchetele penale și operațiunile de culegere a datelor operative. În 2008, a aprobat Decizia Prüm pentru accelerarea schimbului de date cu privire la profilurile ADN, amprente digitale și înmatricularea autovehiculelor în lupta împotriva terorismului și a altor forme de criminalitate. Cooperarea transfrontalieră între unitățile de informații financiare, oficiile de recuperare a creanțelor și platformele de luptă împotriva criminalității informatice, precum și recursul statelor membre la Europol și Eurojust constituite instrumente suplimentare în lupta împotriva criminalității grave în spațiul Schengen.

În urma atacurilor teroriste din 11 septembrie 2001, Guvernul SUA a instituit programul de urmărire a finanțărilor în scopuri teroriste (*Terrorist Finance Tracking Program-TFTP*) pentru a contracara comploturile similare prin monitorizarea tranzacțiilor financiare suspecte. Parlamentul European a aprobat încheierea Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din

[1] În prezent, nu există o definiție armonizată a noțiunii de „criminalitate gravă”. De exemplu, decizia Consiliului care împuternicește Europol să consulte VIS (Decizia Consiliului 2008/633/JAI, JO L 218, 13.8.2008, p. 129) definește „infracțiunile grave” prin referire la lista infracțiunilor prezentată în decizia privind mandatul european de arestare (Decizia 2002/584/JAI a Consiliului, JO L 190, 18.7.2002, p. 1). Directiva privind păstrarea datelor (Directiva 2002/58/CE, JO L 105, 13.4.2006, p. 54) lasă la latitudinea statelor membre să definească „criminalitatea gravă”. Decizia privind Europol (Decizia 2009/371/JAI a Consiliului, JO L 121, 15.5.2009, p. 37) cuprinde o altă listă a infracțiunilor definite drept „criminalitate gravă”, care este foarte similară, însă nu identică cu lista cuprinsă în Decizia privind mandatul european de arestare.

Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste (Acordul UE-SUA privind TFTP)[2]. Schimbul cu țările terțe a registrelor cu numele pasagerilor (date PNR) a permis, de asemenea, UE să combată terorismul și alte forme de criminalitate gravă[3]. Încheind acorduri PNR cu SUA, Australia și Canada, Comisia a revenit recent asupra fazei de elaborare pentru a-și reevalua abordarea în ceea ce privește instituirea unui sistem PNR în UE și împărtășirea acestor date cu țările terțe.

Măsurile prezentate anterior au permis libera circulație în spațiul Schengen, au contribuit la prevenirea și combaterea atacurilor teroriste și a altor forme de criminalitate gravă și au consolidat dezvoltarea unei politici comune în materie de vize și azil.

Această comunicare oferă, pentru prima dată, o prezentare generală completă a măsurilor instituite la nivelul UE, în vigoare sau în curs de examinare, care reglementează aspectele legate de colectarea, stocarea sau schimbul transfrontalier de informații cu caracter personal în scopul aplicării legislației sau al gestionării migrației. Cetățenii au dreptul să fie informați despre datele cu caracter personal care îi privesc și care sunt prelucrate și care fac obiectul schimbului, de către cine și în ce scop. Documentul de față oferă un răspuns transparent la aceste întrebări, clarifică scopul principal al acestor instrumente, structura acestora, tipurile de date cu caracter personal la care se referă, lista autorităților care au acces la astfel de date și dispozițiile care reglementează protecția și păstrarea datelor. De asemenea, cuprinde un număr limitat de exemple care ilustrează modul în care aceste instrumente funcționează în practică (a se vedea anexa I). În fine, comunicarea prezintă principiile de bază pe care ar trebui să se fundamenteze elaborarea și evaluarea instrumentelor de gestionare a informațiilor în spațiul de libertate, securitate și justiție.

Prin prezentarea generală a măsurilor la nivelul UE de reglementare a gestionării informațiilor cu caracter personal și prin propunerea unui set de principii pentru dezvoltarea și evaluarea măsurilor de acest tip, prezenta comunicare contribuie la un dialog politic documentat cu toate părțile interesate. În același timp, oferă un prim răspuns la invitația statelor membre de a dezvolta o abordare mai „coerentă” a schimbului de informații cu caracter personal în scopul asigurării aplicării legii, subiect care a fost tratat recent în Strategia UE de gestionare a informațiilor[4], și oferă posibilitatea de a reflecta asupra eventualei necesități de dezvoltare a unui model european de schimb de informații bazat pe evaluarea măsurilor curente în această materie[5].

Limitarea scopului este un aspect esențial pentru majoritatea instrumentelor care fac obiectul acestei comunicări. Un sistem de informații al UE, unic și general, cu scopuri multiple ar duce la cel mai ridicat grad de partajare a informațiilor. Cu toate acestea, crearea unui astfel de sistem ar constitui o îngrădire importantă și nelegitimă a dreptului persoanei la viață privată și

---

2 Rezoluția Parlamentului European, P7_TA-PROV(2010)0279, 8.7.2010.

3 Spre deosebire de criminalitatea gravă, „infracțiunile de terorism” sunt definite în mod clar în Decizia-cadru a Consiliului privind combaterea terorismului (Decizia-cadru 2002/475/JAI a Consiliului, JO L 164, 22.6.2002, p. 3; modificată prin Decizia-cadru 2008/919/JAI a Consiliului, JO L 330, 9.12.2008, p. 21).

4 Concluziile Consiliului privind o strategie de gestionare a informațiilor pentru securitatea internă a UE, Consiliul Justiție și Afaceri Interne, 30.11.2009 (Strategia UE de gestionare a informațiilor); Libertate, securitate, viață privată — Afaceri interne europene într-o lume deschisă, Raportul Grupului consultativ informal la nivel înalt privind viitorul politicii europene în domeniul afacerilor interne, („Grupul viitorului”), iunie 2008.

5 Programul de la Stockholm — O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora, Documentul Consiliului 5731/10, 3.3.2010, secțiunea 4.2.2.

la protecția datelor și ar crea importante provocări în ceea ce privește dezvoltarea și funcționarea sa. În practică, politicile în domeniul libertății, securității și justiției au fost dezvoltate progresiv, având ca rezultat o serie de instrumente și sisteme de informații, diferite din punct de vedere al dimensiunii, sferei de aplicare și scopului. Structura compartimentată a gestionării informației care a apărut în ultimele decenii favorizează garantarea dreptului cetățenilor la viață privată mai mult decât orice altă opțiune alternativă centralizată.

Această comunicare nu tratează măsurile care presupun schimbul de date fără caracter personal în scopuri strategice, ca de exemplu analize generale de risc sau evaluări ale amenințărilor; și nici nu analizează în detaliu dispozițiile privind protecția datelor aferente instrumentelor în discuție, întrucât, în prezent, Comisia efectuează în baza articolului 16 din Tratatul privind funcționarea Uniunii Europene, un exercițiu distinct privind un nou cadru general pentru protecția datelor cu caracter personal în UE. Consiliul examinează în prezent propunerile de directive de negociere pentru un acord UE-SUA privind protecția datelor cu caracter personal în momentul transferării și prelucrării în scopul prevenirii, anchetării, identificării sau urmării penale a infracțiunilor, inclusiv infracțiunea de terorism, în cadrul cooperării polițienești și a cooperării judiciare în materie penală. Întrucât se estimează că aceste negocieri vor determina modalitățile în care cele două părți pot asigura un nivel ridicat de protecție a drepturilor și libertăților fundamentale în momentul transferării sau prelucrării datelor cu caracter personal și nu fondul efectiv al transferurilor sau prelucrării unor astfel de date, prezenta comunicare nu acoperă această inițiativă[6].

2. INSTRUMENTE UE DE REGLEMENTARE A COLECTĂRII, STOCĂRII SAU SCHIMBULUI DE DATE CU CARACTER PERSONAL PENTRU APLICAREA LEGII SAU ÎN SCOPUL MIGRAȚIEI

Această secțiune oferă o prezentare generală a instrumentelor Uniunii Europene care reglementează colectarea, stocarea sau schimbul transfrontalier de date cu caracter personal în scopul punerii în aplicare a legii sau a gestionării migrației. Secțiunea 2.1 pune accent pe măsurile în vigoare în prezent, în curs de aplicare sau de examinare; secțiunea 2.2 tratează inițiativele prevăzute în Planul de acțiune privind Programul de la Stockholm[7]. Această secțiune oferă informații cu privire la următoarele aspecte ale fiecărui instrument:

– context (dacă măsura a fost propusă de statele membre sau de către Comisie);[8]

– scopul (scopurile) pentru care datele sunt colectate, stocate sau fac obiectul schimbului;

– structură (sistem de informații centralizat sau schimb descentralizat de date);

– sfera datelor cu caracter personal;

---

6 COM(2010)252, 26.5.2010.

7 COM(2010)171, 20.4.2010 (Planul de acțiune privind Programul de la Stockholm).

8 În fosta structură cu trei piloni a Uniunii Europene privind cooperarea polițienească și judiciară în materie penală, statele membre și Comisia împărțeau dreptul de inițiativă. Tratatul de la Amsterdam a integrat domeniile privind controlul la frontierele externe, vize, azil și imigrație în (primul) pilon al Comunității, în cadrul căruia Comisia beneficia de drept exclusiv de inițiativă. Tratatul de la Lisabona a eliminat structura cu piloni a Uniunii, reafirmând dreptul de inițiativă al Comisiei. Cu toate acestea, în domeniile care țin de cooperarea polițienească și judiciară în materie penală (inclusiv cooperarea administrativă) legislația poate fi propusă în continuare la inițiativa unui sfert din statele membre.

– autoritățile care au acces la date;

– dispoziții privind protecția datelor;

– norme privind păstrarea datelor;

– stadiul punerii în aplicare;

– mecanismul de revizuire.

2.1. Instrumente operaționale, în curs de aplicare sau în curs de examinare

Instrumente UE al căror scop este consolidarea funcționării spațiului Schengen și a uniunii vamale

Sistemul de Informații Schengen (SIS) s-a concretizat ca urmare a dorinței statelor membre de a crea un spațiu fără controale la frontierele interne, facilitând în același timp circulația persoanelor în afara frontierelor externe[9]. Operațional din 1995, sistemul urmărește menținerea securității publice, inclusiv a securității naționale, în spațiul Schengen și facilitarea circulației persoanelor care utilizează informațiile comunicate prin acest sistem. SIS este un sistem centralizat de informații care cuprinde o parte națională în fiecare stat participant și o funcție de suport tehnic în Franța. Statele membre pot emite semnalări pentru personale căutate pentru a fi arestate în vederea extrădării; pentru resortisanții țărilor terțe în vederea refuzării intrării; pentru personale dispărute; pentru martori sau pentru personale citate să compară în fața unei instanțe; pentru persoane și vehicule care fac obiectul monitorizării excepționale ca urmare a amenințării pe care o reprezintă la adresa securității publice sau naționale; pentru vehicule, documente și arme de foc pierdute sau furate; precum și pentru bancnote suspecte. Printre datele introduse în SIS se numără numele și pseudonimele, trăsăturile fizice, locul și data nașterii, naționalitatea și mențiunea dacă persoana este înarmată și violentă. Poliția, autoritățile de frontieră, autoritățile vamale și judiciare pot avea acces la aceste date în cadrul procedurilor de urmărire penală, conform competențelor judiciare respective. Autoritățile de imigrație și oficiile consulare au acces la datele referitoare la resortisanții țărilor terțe înscriși pe lista persoanelor cu interdicție de intrare și la semnalările cu privire la documentele pierdute și furate. Europol poate avea acces la unele categorii de date SIS, inclusiv semnalările privind persoanele căutate pentru arestare în vederea extrădării, și la cele privind persoanele care fac obiectul monitorizării excepționale deoarece reprezintă o amenințare la securitatea publică sau națională. Eurojust poate accesa semnalările privind persoanele căutate pentru arestare în vederea extrădării și pe cele privind martorii sau persoanele convocate să compară în fața unei instanțe. Datele cu caracter personal pot fi folosite exclusiv în scopul semnalării specifice pentru care au fost furnizate. Datele cu caracter personal introduse în Sistemul de Informații Schengen în scopul localizării persoanelor urmărite pot fi păstrate numai atâta timp cât este necesar pentru atingerea scopului pentru care au fost furnizate, și cel mult trei ani de la data la care au fost introduse. Datele cu privire la persoanele care fac obiectul monitorizării excepționale ca urmare a riscului pe care îl reprezintă pentru securitatea națională sau publică trebuie șterse după un an. Statele membre trebuie să adopte norme naționale prin care să prevadă un nivel al protecției datelor cel puțin egal cu cel care rezultă din Convenția Consiliului Europei din 1981 pentru

[9] Convenția de punere în aplicare a Acordului Schengen din 14 iunie 1985 între guvernele statelor din Uniunea Economică Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune, JO L 239, 22.9.2000, p. 19.

protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și din Recomandarea din 1987 a Comitetului de Miniștri a Consiliului Europei ce reglementează utilizarea datelor personale în sectorul polițienesc[10]. Deși Convenția Schengen nu prevede un mecanism de revizuire, semnatarii pot propune modificări la aceasta, în urma cărora textul modificat trebuie aprobat prin unanimitate și ratificat de parlamentele naționale. SIS se aplică integral în 22 de state membre, precum și în Elveția, Norvegia și Islanda. Regatul Unit și Irlanda participă la aspectele ce țin de cooperarea polițienească în temeiul Convenției Schengen și SIS, cu excepția semnalărilor legate de resortisanții țărilor terțe aflați pe lista persoanelor cu interdicție de intrare. Cipru a semnat Convenția Schengen, însă nu a pus-o în aplicare deocamdată. Liechtenstein urmează să o pună în aplicare în 2010; se estimează că Bulgaria și România vor aplica convenția în 2011. Căutarea în SIS duce la un rezultat atunci când informațiile cu privire la o persoană sau un obiect căutat corespund celor unei semnalări existente. Odată ce au obținut un rezultat, autoritățile de aplicare a legii pot solicita, prin intermediul rețelei de birouri SIRENE, informații suplimentare cu privire la subiectul unei semnalări[11].

Pe măsură ce noi state membre au intrat în spațiul Schengen, baza de data SIS a crescut în egală măsură: în perioada cuprinsă între ianuarie 2008 și 2010, numărul total de semnalări SIS a crescut de la 22,9 la 31,6 milioane[12]. Anticipând această creștere a volumului de date și modificările în nevoile utilizatorilor, statele membre au decis în 2001 să dezvolte **Sistemul de informații Schengen din a doua generație** (SIS II), încredințând această sarcină Comisiei[13]. În curs de dezvoltare în prezent, SIS II are ca scop asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție prin consolidarea funcțiilor sistemului de primă generație și prin facilitarea circulației persoanelor, utilizând informațiile comunicate prin intermediul acestui sistem. Pe lângă categoriile de date originale care au făcut obiectul sistemului de primă generație, SIS II va putea trata amprente digitale, fotografii, copii ale mandatului european de arestare, dispoziții de protejare a intereselor persoanelor a căror identitate este uzurpată și legăturile între diferitele semnalări. De exemplu, SIS II va permite corelarea semnalărilor referitoare la o persoană căutată pentru răpire, persoana răpită și vehiculul folosit în comiterea acestei infracțiuni. Normele privind drepturile de acces și păstrarea datelor sunt identice cu cele aferente sistemului de primă generație. Datele cu caracter personal pot fi folosite exclusiv în scopul semnalării specifice pentru care au fost furnizate. Datele cu caracter personal introduse în SIS II trebuie prelucrate în conformitate cu dispozițiile specifice ale actelor normative de bază care reglementează acest sistem [Regulamentul (CE) nr. 1987/2006 și Decizia 2007/533/JAI a Consiliului) și care clarifică principiile Directivei 95/46/CE, precum și în conformitate cu Regulamentul (CE) nr. 45/2001, Convenția 108 a Consiliului Europei și Recomandarea privind sectorul polițienesc[14]. SIS II va

---

10 Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

11 SIRENE este acronimul pentru „Supplementary Information Request at the National Entry" (solicitări suplimentare de informații la intrarea pe teritoriul național).

12 Documentul Consiliului 5441/08, 30.1.2008; Documentul Consiliului 6162/10, 5.2.2010.

13 Regulamentul (CE) nr. 1986/2006, JO L 381, 28.12.2006, p. 1; Regulamentul (CE) nr. 1987/2006, JO L 381, 28.12.2006, p. 4; Decizia 2007/533/JAI, JO L 205, 7.8.2007, p. 63.

14 Regulamentul (CE) nr. 1987/2006, JO L 381, 28.12.2006, p. 4; Decizia 2007/533/JAI, JO L 205, 7.8.2007, p. 63; Directiva 95/46/CE, JO L 281, 23.11.1995, p. 31; Regulamentul (CE) nr. 45/2001, JO L 8, 12.1.2001, p.1. Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei);

utiliza s-TESTA, rețeaua Comisiei de comunicare securizată a datelor[15]. De îndată ce va fi operațional, acest sistem se va aplica în toate statele membre, Elveția, Liechtenstein, Norvegia și Islanda[16]. Comisia trebuie să trimită Parlamentului European și Consiliului un raport bianual privind progresele înregistrate cu privire la dezvoltarea SIS II și posibila migrare de la sistemul de primă generație[17].

Dezvoltarea **EURODAC** își are originea în eliminarea frontierelor interne, ceea ce a dus la necesitatea de a stabili norme clare privind prelucrarea cererilor de azil. EURODAC este un sistem automat și centralizat de identificare a amprentelor digitale care conține datele cu privire la amprentele digitale ale anumitor resortisanți ai țărilor terțe. Funcțional din ianuarie 2003, scopul acestui sistem este de a oferi asistență în vederea stabilirii statului membru care ar trebui să fie responsabil, în temeiul Regulamentului Dublin, de examinarea unei anumite cereri de azil[18]. Persoanelor în vârstă de 14 ani sau peste 14 ani care solicită azil într-un stat membru li se iau automat amprentele digitale, ca și resortisanților țărilor terțe care au fost reținuți pentru trecerea ilegală a frontierei externe. Prin compararea amprentelor digitale ale acestor persoane cu evidențele EURODAC, autoritățile naționale doresc să stabilească locul în care respectiva persoană a depus o cerere de azil sau a intrat pentru prima dată în Uniunea Europeană. De asemenea, autoritățile pot compara cu evidențele EURODAC amprentele digitale ale resortisanților țărilor terțe în situație de ședere ilegală pe teritoriul lor. Statele membre trebuie să indice lista autorităților care au acces la această bază de date, care de obicei cuprinde autoritățile cu responsabilități în domeniul azilului și migrației, grănicerii și poliția. Statele membre încarcă datele relevante în baza de date centrală prin intermediul punctelor naționale de acces. Datele cu caracter personal din EURODAC nu pot fi folosite decât în scopul facilitării aplicării Regulamentului Dublin; utilizarea în alt scop face obiectul sancțiunilor. Amprentele digitale ale solicitanților de azil se arhivează pentru 10 ani; cele ale migranților ilegali, pentru doi ani. Evidențele cu privire la solicitanții de azil se șterg de îndată ce dobândesc cetățenia unui stat membru; cele ale migranților ilegali se șterg de îndată ce obțin un permis de ședere sau cetățenia, sau în cazul în care părăsesc teritoriul statelor membre. Directiva 95/46/CE se aplică prelucrării datelor cu caracter personal în temeiul prezentului instrument[19]. EURODAC funcționează pe rețeaua s-TESTA a Comisiei și se aplică în fiecare stat membru, precum și în Norvegia, Islanda și Elveția. Este în curs de încheiere un acord care să permită conectarea Principatului Liechtenstein la rețea. Comisia trebuie să prezinte Parlamentului European și Consiliului rapoarte anuale privind funcționarea unității centrale a EURODAC.

Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

15 S-TESTA, abrevierea pentru *Secure Trans-European Services for Telematics between Administrations* (Servicii transeuropene securizate de telematică între administrații) este o rețea de comunicare a datelor finanțată de Comisie care permite schimbul securizat și criptat de informații între administrațiile naționale și instituțiile, agențiile și organismele UE.

16 Regatul Unit și Irlanda vor participa la SIS II cu excepția semnalărilor legate de resortisanții țărilor terțe incluși pe lista persoanelor cu interdicție de intrare.

17 Regulamentul (CE) nr. 1104/2008 al Consiliului, JO L 299, 8.11.2008, p. 1; Decizia 2008/839/JAI a Consiliului, JO L 299, 8.11.2008, p. 43.

18 Regulamentul (CE) nr. 343/2003 al Consiliului, JO L 50, 25.2.2003, p. 1 (Regulamentul Dublin), Regulamentul (CE) 2725/2000 al Consiliului, JO L 316, 15.12.2000, p. 1 (Regulamentul EURODAC). Aceste instrumente sunt fundamentate pe convenția de la Dublin din 1990 (JO C 254, 19.8.1997, p. 1), prin care se urmărea stabilirea statului membru care trebuie să examineze cererile de azil. Sistemul de evaluare a cererilor de azil este cunoscut sub denumirea „sistemul Dublin”.

19 Directiva 95/46/CE, JO L 281, 23.11.1995, p. 31.

În urma atentatelor din 11 septembrie 2001, statele membre au luat hotărârea de a accelera punerea în aplicare a unei politici comune în materie de vize prin crearea unui sistem de schimb de informații cu privire la vizele de scurtă ședere[20]. Prin eliminarea frontierelor interne a fost posibilă fraudarea cu mai multă ușurință a regimului de vize ale statelor membre. **Sistemul de Informații privind Vizele—***Visa Information System* (VIS) urmărește să răspundă ambelor preocupări: scopul acestuia este de a contribui la punerea în aplicare a unei politici comune în materie de vize prin facilitarea examinării cererilor de viză și a controalelor la frontierele externe, contribuind în același timp la prevenirea amenințărilor la securitatea internă a statelor membre[21]. VIS va fi un sistem centralizat de informații și va cuprinde o componentă națională în fiecare stat participant și o funcție de suport tehnic în Franța. Va folosi un sistem de corespondențe biometrice pentru a asigura compararea fiabilă a datelor dactiloscopice și a verifica identitatea titularilor de vize la frontierele externe. VIS va include date privind cererile de viză, fotografii, amprente digitale, deciziile aferente luate de autoritățile competente în materie de vize și legăturile între aplicațiile conexe. Autoritățile în materie de vize, azil, imigrație și control al frontierelor vor avea acces la această bază de date cu scopul de a verifica identitatea titularilor de vize și a autenticității vizelor; poliția și Europol pot consulta baza de date în scopul prevenirii și combaterii terorismului și a altor forme de criminalitate gravă[22]. Dosarele cu cererile pot fi păstrare timp de cinci ani. Datele cu caracter personal introduse în VIS trebuie prelucrate conform normelor specifice cuprinse în actele legislative de bază care reglementează acest sistem [Regulamentul (CE) nr. 767/2008 și Decizia 2008/633/JAI a Consiliului] care completează dispozițiile Directivei 95/46/CE, ale Regulamentului (CE) nr. 45/2001, ale Deciziei-cadru 2008/977/JAI a Consiliului, ale Convenției 108 a Consiliului Europei, ale Protocolului adițional 181 la aceasta și ale Recomandării privind sectorul polițienesc[23]. VIS se va aplica în fiecare stat membru (cu excepția Regatului Unit și Irlandei), precum și în Elveția, Norvegia și Islanda. Va funcționa în baza rețelei s-TESTA a Comisiei. Comisia va evalua acest sistem la trei ani de la lansarea sa și apoi la fiecare patru ani.

La inițiativa spaniolă, Consiliul a adoptat în 2004 o directivă de reglementare a transmiterii **informațiilor prealabile privind pasagerii -** *Advance Passenger Information* (API) de către transportatorii aerieni în atenția autorităților de control la frontiere[24]. Obiectivul acestui instrument este îmbunătățirea controlului la frontiere și combaterea migrației ilegale. La cerere, transportatorii aerieni trebuie să comunice autorităților de control la frontieră numele, data nașterii, naționalitatea, punctul de îmbarcare și punctul de trecere a frontierei pe teritoriul UE în cazul pasagerilor care călătoresc în UE din țări terțe. Datele cu caracter personal de

---

20 Consiliul Extraordinar Justiție și Afaceri Interne, 20.9.2001.

21 Decizia 2004/512/CE a Consiliului, JO L 213, 15.6.2004, p. 5; Regulamentul (CE) nr. 767/2008, JO L 218, 13.8.2008, p. 60; Decizia 2008/633/JAI a Consiliului, JO L 218, 13.8.2008, p. 129. A se vedea, de asemenea, Declarația privind combaterea terorismului, Consiliul European, 25.3.2004.

22 Decizia 2008/633/JAI a Consiliului, JO L 218, 13.8.2008, p. 129.

23 Regulamentul (CE) nr. 767/2008, JO L 218, 13.8.2008, p. 60; Decizia 2008/633/JAI a Consiliului, JO L 218, 13.8.2008, p. 129; Directiva 95/46/CE, JO L 281, 23.11.1995, p. 31; Regulamentul (CE) nr. 45/2001, JO L 8, 12.1.2001, p.1. Decizia-cadru 2008/977/JAI a Consiliului, JO L 350, 30.12.2008, p. 60; Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181), Consiliul Europei, 8.11.2001 (Protocol adițional 181); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

24 Directiva 2004/82/CE a Consiliului, JO L 261, 6.8.2004, p. 24.

acest tip sunt preluate de obicei din secțiunea cu citire optică a pașapoartelor pasagerilor și sunt transmise autorităților după încheierea procedurii de îmbarcare. După sosirea unui avion, autoritățile și transportatorii aerieni pot păstra datele API pentru 24 de ore. Sistemul API funcționează în mod descentralizat prin împărtășirea informațiilor între operatorii privați și autoritățile publice. Acest instrument nu permite schimbul de date API între statele membre; cu toate acestea, autoritățile de aplicare a legii, altele decât grănicerii, pot solicita accesul la aceste informații în scopul aplicării legii. Datele cu caracter personal nu pot fi utilizate decât de autoritățile publice în scopul controlului la frontieră și combaterii migrației ilegale și trebuie prelucrate conform Directivei 95/46/CE[25]. În vigoare în UE, acest instrument este utilizat numai de un număr restrâns de state membre. Comisia va revizui această directivă în 2011.

O parte importantă a Programului Comisiei din 1992, care a instituit piața internă, se referea la eliminarea tuturor controalelor și formalităților pentru bunurile care circulă în Comunitate[26]. Eliminarea acestor proceduri la frontierele interne a crescut riscul de fraudă, ceea ce a făcut necesar ca statele membre să instituie, pe de o parte, un mecanism de asistență administrativă reciprocă pentru a contribui la prevenirea, anchetarea și trimiterea în instanță a operațiunilor care contravin legislației Comunității în domeniul vamal și agricol și, pe de altă parte, a făcut necesar instituirea unei cooperări vamale cu scopul de a permite identificarea și trimiterea în instanță a cazurilor de încălcare a dispozițiilor vamale naționale, în special prin consolidarea schimbului transfrontalier de informații. Fără a aduce atingere competenței UE în materie de uniune vamală[27], **Convenția Napoli II** privind asistența reciprocă și cooperarea între administrațiile vamale are obiectivul de a permite administrațiilor vamale naționale să prevină și să identifice încălcarea dispozițiilor vamale naționale și să contribuie la trimiterea în instanță și la sancționarea cazurilor de încălcare a dispozițiilor vamale comunitare și naționale[28]. În temeiul acestui instrument, o serie de unități centrale de coordonare solicită asistență în scris de la omologii din alte state membre în vederea anchetelor penale cu privire la încălcarea normelor vamale naționale și comunitare. Aceste unități nu pot prelucra date cu caracter personal decât în scopul prevăzut de Convenția Napoli II. Unitățile centrale pot transmite aceste informații autorităților vamale naționale, autorităților de anchetă și organelor judiciare precum și altor autorități, sub rezerva acordului prealabil al statului membru care furnizează datele. Datele pot fi păstrate pentru o perioadă care nu depășește ceea ce este necesar pentru scopul în care au fost furnizate. În statul membru destinatar, datele cu caracter personal beneficiază cel puțin de același nivel de protecție ca și în statul membru care le-a furnizat, iar prelucrarea acestora trebuie să respecte dispozițiile Directivei 95/46/CE și ale Convenției 108 a Consiliului Europei[29]. Convenția Napoli II a fost ratificată de toate statele membre. Statele membre pot propune amendamente la această convenție, în urma cărora textul modificat va trebui să fie adoptat de Consiliul de Miniștri și ratificat de către statele membre.

---

25 Directiva 95/46/CE, JO L 281, 23.11.1995, p. 31.

26 Regulamentul (CEE) 2913/92 al Consiliului, JO L 302, 19.10.1992.

27 Regulamentul (CE) nr. 515/97 al Consiliului din 13 martie 1997 privind asistența reciprocă între autoritățile administrative ale statelor membre și cooperarea dintre acestea și Comisie în vederea asigurării aplicării corespunzătoare a legislației din domeniile vamal și agricol, JO L 82, 22.3.1997, p. 1, modificat prin Regulamentul (CE) nr. 766/2008, JO L 218, 13.8.2008, p. 48.

28 Convenție redactată în baza articolului K.3 din Tratatul privind Uniunea Europeană, privind asistența reciprocă și cooperarea între administrațiile vamale, JO C 24/2, 23.1.1998 (Convenția Napoli II).

29 Directiva 95/46/CE, JO L 281, 23.11.1995, p. 31; Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei).

În completarea Convenției Napoli II, Convenția CIS desfășoară **Sistemul de informații al vămilor** (CIS) pentru a asista în prevenirea, anchetarea și trimiterea în instanță a diferitelor cazuri de încălcare a legilor naționale, prin diseminarea rapidă a informațiilor, prin eficiența cooperării între administrațiile vamale ale statelor membre[30]. CIS, gestionat de Comisie, este un sistem centralizat de informații accesibil prin intermediul terminalelor în fiecare stat membru și în incinta Comisiei, Europol și Eurojust. Cuprinde date cu caracter personal cu referire la mărfuri, mijloace de transport, întreprinderi, persoane, bunuri și mijloace bănești reținute, sub sechestru sau confiscate. Datele cu caracter personal sunt numele și pseudonimele, data și locul nașterii, naționalitatea, sexul, trăsăturile fizice, documentele de identitate, adresa, antecedente de violență, motivul pentru introducerea datelor în CIS, acțiunea sugerată și înregistrarea mijloacelor de transport. În cazul bunurilor și mijloacelor bănești reținute, puse sub sechestru sau confiscate, în CIS nu pot fi introduse decât datele biografice și adresa. Aceste informații pot fi utilizate exclusiv în scopul observării, raportării, efectuării anumitor inspecții sau controale specifice ori în scopul analizelor strategice sau operaționale cu privire la persoanele suspectate de încălcarea dispozițiilor vamale naționale. Datele CIS pot fi accesate de către autoritățile naționale vamale, fiscale, agricole, din domeniul sănătății publice și de autoritățile naționale polițienești, de Europol și Eurojust[31]. Prelucrarea datelor cu caracter personal trebuie să respecte normele specifice stabilite de Convenția CIS și dispozițiile Directivei 95/46/CE, ale Regulamentului (CE) nr. 45/2001, ale Convenției 108 a Consiliului Europei și ale Recomandării privind sectorul polițienesc[32]. Datele cu caracter personal nu pot fi copiate din CIS decât pe alte sisteme de prelucrare a datelor în vederea analizelor operaționale sau de gestionare a riscului, la care pot avea acces numai analiștii desemnați de statele membre. Datele cu caracter personal copiate din CIS nu pot fi păstrate decât pentru durata necesară în vederea atingerii scopului pentru care au fost copiate și pentru cel mult 10 ani. De asemenea, CIS creează o **bază de date pentru identificarea dosarelor de anchetă vamale** (FIDE) pentru a contribui la prevenirea, anchetarea și trimiterea în instanță a cazurilor grave de încălcare a legilor naționale[33]. FIDE permite autorităților naționale responsabile de efectuarea anchetelor vamale, ca în momentul în care deschid un dosar de anchetă, să identifice alte autorități care au anchetat o anumită persoană sau întreprindere. Aceste autorități pot introduce date în FIDE din dosarele de anchetă, inclusiv datele biografice ale persoanelor care fac obiectul anchetei, precum și denumirea întreprinderii, denumirea comercială, numărul TVA și adresa întreprinderilor care fac obiectul anchetei. Datele care provin din dosare de anchetă în care nu s-a constatat o

---

30 Convenție elaborată în temeiul articolului K.3 din Tratatul privind Uniunea Europeană, privind utilizarea tehnologiei informației în domeniul vamal, JO C 316, 27.11.1995, p. 34, modificată prin Decizia 2009/917/JAI a Consiliului, JO L 323, 10.12.2009, p. 20.

31 Cu începere din luna mai 2011, Europol și Eurojust vor avea acces la CIS pentru consultare în baza Deciziei 2009/917/JAI a Consiliului (JO L 323, 10.12.2009, p. 20).

32 Convenție elaborată în temeiul articolului K.3 din Tratatul privind Uniunea Europeană, privind utilizarea tehnologiei informației în domeniul vamal, JO C 316, 27.11.1995, p. 34, modificată prin Decizia 2009/917/JAI a Consiliului, JO L 323, 10.12.2009, p. 20; Directiva 95/46/CE, JO L 281, 23.11.1995, p. 31; Regulamentul (CE) nr. 45/2001, JO L 8, 12.1.2001, p.1; Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

33 FIDE, abrevierea pentru *Fichier d'Identification des Dossiers d'Enquêtes douanières* (bază de date pentru identificarea dosarelor de anchetă vamale), se întemeiază pe Regulamentul (CE) nr. 766/2008 al Consiliului și pe Protocolul instituit în conformitate cu articolul 34 din Tratatul privind Uniunea Europeană, de modificare în ceea ce privește constituirea unei baze de date pentru identificarea dosarelor vamale, a Convenției privind utilizarea tehnologiei informațiilor de către serviciile vamale, JO C 139, 13.6.2003, p. 1.

fraudă vamală pot fi stocate pentru o perioadă de maximum trei ani; cele care provin din dosare în care s-a constatat existența unei fraude vamale pot fi stocate pentru o perioadă de maximum șase ani; iar cele care provin din dosare în care s-a pronunțat o condamnare sau s-a aplicat o sancțiune pot fi păstrate pentru o durată de maximum 10 ani. CIS și FIDE utilizează rețeaua comună de comunicație, interfața comună a sistemelor sau accesul internet securizat furnizat de Comisie. CIS este în vigoare în toate statele membre. Comisia, în cooperare cu statele membre, prezintă în fiecare an un raport Parlamentului European și Consiliului cu privire la funcționarea CIS.

Instrumente UE care au ca scop prevenirea și combaterea terorismului, precum și a altor forme de criminalitate transfrontalieră gravă

Atacurile teroriste din martie 2004 din Madrid au dus la noi inițiative la nivelul UE. La cererea Consiliului European, Comisia a prezentat în 2005 o propunere pentru un instrument care reglementează schimbul de informații conform principiului disponibilității[34]. În loc să aprobe această propunere, Consiliul a adoptat în 2006 **Inițiativa suedeză**, care simplifică partajarea oricărei informații existente sau a datelor operative în materie penală între statele membre care ar putea fi necesare în vederea unei anchete penale sau a unei operațiuni de colectare a datelor operative în materie penală[35]. Acest instrument își are fundamentul în principiul de politică „acces echivalent", potrivit căruia condițiile aplicabile schimbului transfrontalier de date nu ar trebui să fie mai stricte decât cele care reglementează accesul intern. Inițiativa suedeză funcționează în mod descentralizat și permite poliției, vămilor și oricărei alte autorități cu competențe de anchetare a infracțiunilor (cu excepția serviciilor de informații, care de obicei tratează informațiile cu privire la securitatea națională sau de stat) să partajeze informații și date operative în materie penală cu omologii lor din UE. Statele membre trebuie să desemneze punctele naționale de contact pentru tratarea cererilor urgente de informații. Această măsură stabilește termene clare pentru schimbul de informații, statele membre având obligația de a completa un formular atunci când solicită date. Statele membre trebuie să dea curs solicitărilor de informații și date operative în termen de 8 ore în cazurile urgente, în termen de o săptămână în cazurile care nu sunt urgente și în termen de două săptămâni în toate celelalte cazuri. Utilizarea informațiilor și datelor operative obținute prin intermediul acestui instrument face obiectul legilor interne de protecție a datelor, iar statele membre nu pot aplica tratament diferențial datelor obținute intern și celor obținute din alte state membre. Cu toate acestea, statul membru care furnizează informația poate stabili condiții pentru utilizarea informațiilor sau datelor operative în alte state membre. Datele cu caracter personal trebuie prelucrate în conformitate cu legislația națională de protecție a datelor, precum și cu Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta și cu Recomandarea privind sectorul polițienesc[36]. Din cei 31 de semnatari ai acestei măsuri (inclusiv statele membre UE, precum și Norvegia, Islanda, Elveția și Liechtenstein), 12 au adoptat legislație națională în vederea aplicării; cinci state completează periodic formularul de solicitare de informații; însă numai două state îl folosesc în mod frecvent pentru schimb de

---

34 COM(2005) 490, 12.10.2005; Concluziile președinției — Programul de la Haga, 4/5.11.2004. A se vedea, de asemenea, Declarația privind combaterea terorismului, Consiliul European, 25.3.2004.

35 Decizia-cadru 2006/960/JAI a Consiliului, JO L 386, 29.12.2006, p. 89.

36 Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181), Consiliul Europei, 8.11.2001 (Protocol adițional 181); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

informații[37]. Comisia va prezenta Consiliului raportul de evaluare înainte de sfârșitul anului 2010.

Decizia Prüm are la bază un acord încheiat în 2005 de Germania, Franța, Spania, statele Benelux și Austria pentru intensificarea cooperării în lupta împotriva terorismului, criminalității transfrontaliere și migrației ilegale. Ca răspuns la interesul exprimat de mai multe state membre în aderarea la acest acord, Germania a propus în cursului președinției din 2007 a Consiliului transformarea acestuia într-un instrument UE. Decizia Prüm din 2008, care urmează a fi pusă în aplicare până în august 2011, stabilește normele pentru schimbul transfrontalier de profiluri ADN, amprente digitale, date privind înmatricularea vehiculelor și informații cu privire la persoanele suspectate de planificarea unor atacuri teroriste[38]. Decizia urmărește consolidarea prevenirii infracțiunilor, în special a terorismului și a criminalității transfrontaliere, și menținerea ordinii publice în legătură cu evenimente importante. Acest sistem va funcționa în mod descentralizat prin interconectarea, prin intermediul punctelor naționale de contact, a bazelor de date ale statelor participante care conțin informații privind ADN-ul, amprentele digitale și înmatricularea vehiculelor. Utilizând rețeaua s-TESTA a Comisiei, punctele de contact vor trata cererile primite și trimise pentru compararea transfrontalieră a datelor privind profilurile ADN, amprentele digitale și înregistrarea vehiculelor. Competențele acestora de a transmite datele de acest tip utilizatorilor finali sunt reglementate prin legislația națională. Începând cu august 2011, compararea datelor va fi complet automată. Cu toate acestea, statele membre trebuie să facă obiectul unui proces riguros de evaluare (în special a evaluării respectării cerințelor privind protecția datelor și a cerințelor tehnice) pentru a primi autorizare împărtășirii în mod automat a datelor. Datele cu caracter personal nu pot face obiectul schimbului în temeiul prezentului instrument decât atunci când statele membre au garantat un nivel al protecției datelor cel puțin egal cu cel care rezultă din Convenția 108 a Consiliului Europei, din Protocolul adițional 181 la aceasta și din Recomandarea privind sectorul polițienesc[39]. Consiliul va decide prin unanimitate dacă această condiție a fost întrunită. Informațiile cu caracter personal nu vor fi folosite decât pentru scopul în care au fost furnizate, cu excepția cazului în care statul membru care furnizează informațiile își dă acordul pentru folosirea acestora în alte scopuri. De asemenea, persoanele fizice se pot adresa autorităților naționale responsabile de protecția datelor, desemnate în temeiul Directivei 95/46/CE, pentru asigurarea aplicării drepturilor lor cu privire la prelucrarea datelor cu caracter personal în temeiul prezentului instrument. Compararea profilurilor ADN și a amprentelor digitale va funcționa în baza unui sistem „hit/no hit” (anonim), prin care autoritățile vor putea să solicite numai informații cu caracter personal cu privire la subiectul datelor în cazul în care căutarea inițială a dus la un rezultat. Cererile de informații suplimentare de acest tip vor fi canalizate de obicei prin Inițiativa suedeză. Decizia

---

37 Această informație are la bază răspunsurile la un chestionar, rezultatele fiind prezentate de președinția spaniolă a Consiliului în cadrul unei reuniuni a Grupului de lucru ad hoc al Consiliului privind schimbul de informații din 22 iunie 2010.

38 Decizia 2008/615/JAI a Consiliului, JO L 210, 6.8.2008, p. 1; Decizia 2008/616/JAI a Consiliului, JO L 210, 6.8.2008, p. 12.

39 Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181), Consiliul Europei, 8.11.2001 (Protocol adițional 181); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

Prüm este pusă în aplicare în UE-27, în timp ce Norvegia și Islanda sunt în curs de aderare la aceasta[40]. În 2012, Comisia va prezenta Consiliului raportul său de evaluare.

Ca răspuns la atacurile cu bombă din Londra din iulie 2005, Marea Britanie, Irlanda, Suedia și Franța au propus adoptarea unui instrument UE de armonizare a normelor naționale aplicabile păstrării datelor. **Directiva privind păstrarea datelor** din 2006 prevede obligația ca furnizorii de servicii de telefonie și de internet să păstreze, în scopul anchetării, detectării și urmăririi penale a criminalității grave, datele de trafic și localizare ale comunicațiilor electronice, precum și informații cu privire la abonați (inclusiv numărul de telefon al acestora, adresa IP și elementele de identificare ale echipamentelor mobile)[41]. Directiva privind păstrarea datelor nu reglementează nici condițiile de acces și nici modul de utilizare a datelor păstrate de autoritățile naționale. Sfera de aplicare a directivei exclude în mod explicit conținutul comunicațiilor electronice; cu alte cuvinte, interceptarea convorbirilor telefonice nu este posibilă în temeiul acestui instrument. Conform acestei măsuri, statele membre sunt cele care definesc „criminalitatea gravă". De asemenea, statele membre stabilesc autoritățile naționale care pot accesa aceste date de la caz la caz, precum și procedurile și condițiile de acordare a accesului la informații. Perioadele pentru care datele pot fi păstrate variază de la 6 la 24 de luni. Directiva 95/46/CE și Directiva 2002/58/CE reglementează protecția datelor cu caracter personal în temeiul acestui instrument[42]. Șase state membre nu au transpus încă integral această măsură, iar Curtea Constituțională din Germania și cea din România au declarat neconstituțională legislația națională de punere în aplicare. Curtea Constituțională din Germania a constatat că normele care reglementează accesul la date și utilizarea datelor, conform dispozițiilor legii naționale, sunt neconstituționale[43]. Curtea Constituțională din România a constatat că păstrarea datelor *per se* încalcă articolul 8 al Convenției pentru apărarea drepturilor omului și a libertăților fundamentale (Convenția europeană privind drepturile omului) fiind așadar neconstituțională[44]. În prezent, Comisia evaluează acest instrument și urmează să prezinte raportul de evaluare Parlamentului European și Consiliului la sfârșitul anului 2010.

Sistemul european de informații cu privire la cazierele judiciare (ECRIS), în curs de instituire, are la bază o inițiativă belgiană din 2004 al cărei obiectiv era împiedicarea persoanelor condamnate pentru abuzuri sexuale de a lucra cu copii în alte state membre. În trecut, statele membre se bazau pe Convenția Consiliului Europei de asistență judiciară în materie penală pentru schimbul de informații cu privire la condamnările emise în numele resortisanților lor, însă sistemul s-a dovedit a fi ineficient[45]. Consiliul a efectuat un prim demers în vederea reformării prin adoptarea Deciziei 2005/876/JAI a Consiliului, în temeiul căreia fiecare stat membru trebuia să instituie o autoritate centrală care să transmită, la intervale regulate, condamnările cu privire la neresortisanți statului (statelor) membru (membre) ai căror resortisanți sunt persoanele care fac obiectul condamnării[46]. De asemenea,

---

40 Până în prezent, zece state membre au primit autorizarea de a începe schimbul automat de profiluri ADN, cinci statele membre au primit autorizare pentru amprente digitale, iar șapte pentru datele cu privire în înmatricularea vehiculelor. Germania, Austria, Spania și Țările de Jos au prezentat Comisiei statistici parțiale privind utilizarea de către acestea a prezentului instrument.

41 Directiva 2006/24/CE, JO L 105, 13.4.2006, p. 54.

42 Directiva 95/46/CE, JO L 281, 23.11.1995, p. 31; Directiva 2002/58/CE, JO L 201, 31.7.2002, p. 37 (Directiva asupra confidențialității și comunicațiilor electronice).

43 Hotărârea Curții Constituționale din Germania, Bundesverfassunggericht 1 BvR 256/08, 11.3.2008.

44 Decizia 1258 a Curții Constituționale a României, 8.10.2009.

45 Convenția europeană privind asistența judiciară reciprocă în materie penală (ETS nr. 30), Consiliul Europei, 20.4.1959. A se vedea, de asemenea, COM(2005) 10, 25.1.2005.

46 Decizia 2005/876/JAI a Consiliului, JO L 322, 9.12.2005, p. 33.

acest instrument a permis statelor membre să obțină, pentru prima dată și sub rezerva legislației naționale, condamnările anterioare pronunțate împotriva resortisanților proprii în alte state membre. Statele membre pot solicita informații de acest tip prin completarea unui formular standardizat mai degrabă decât prin proceduri de asistență juridică reciprocă. În 2006 și 2007, Comisia a prezentat un pachet legislativ general care cuprindea trei instrumente: Decizia-cadru 2008/675/JAI a Consiliului, care prevedea obligativitatea statelor membre de a ține seama de condamnările anterioare în noile proceduri penale; Decizia-cadru 2009/315/JAI a Consiliului privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare; și Decizia 2009/316/JAI a Consiliului de instituire a ECRIS ca mijloc tehnic pentru schimbul de informații extrase din cazierele judiciare[47]. Urmând a fi puse în aplicare până în aprilie 2012, Deciziile-cadru 2009/315/JAI și 2009/316/JAI ale Consiliului au ca scop definirea modalităților în care un stat membru care emite o condamnare trebuie să transmită informații privind o nouă condamnare către statul (statele) membru (membre) al cărui cetățean este persoana care face obiectul condamnării, obligațiile de arhivare și un cadru pentru un sistem computerizat de schimb de informații. ECRIS va fi un sistem descentralizat de informații care interconectează bazele de date cu cazierele judiciare ale statelor membre prin intermediul rețelei s-TESTA a Comisiei. O serie de autorități centrale vor schimba date cu privire la noile condamnări ale cetățenilor și cu privire la antecedentele acestora. Datele vor fi criptate, structurate conform unui format prestabilit și vor include următoarele: detalii biografice; condamnarea, sentința și infracțiunea de bază; precum și informații suplimentare (inclusiv amprente digitale, dacă sunt disponibile). Începând cu aprilie 2012, extrasele din cazierele judiciare trebuie prezentate pentru procedurile penale în desfășurare și trebuie trimise autorităților judiciare sau autorităților administrative competente, ca de exemplu organismelor împuternicite să verifice persoanele care ocupă funcții sensibile sau care posedă arme de foc. Datele cu caracter personal furnizate pentru procedurile penale nu pot fi folosite decât în acest scop; pentru utilizarea în alt scop este nevoie de consimțământul statului membru care furnizează datele. Prelucrarea datelor cu caracter personal trebuie să fie conformă cu dispozițiile specifice instituite prin Decizia-cadru 2009/315/JAI a Consiliului, care include normele Deciziei 2005/876/JAI a Consiliului, precum și ale Deciziei-cadru 2008/977/JAI a Consiliului și ale Convenției 108 a Consiliului Europei[48]. În cazul prelucrării datelor cu caracter personal de către instituțiile UE care folosesc ECRIS, de exemplu pentru a asigura securitatea datelor, se aplică Regulamentul (CE) 45/2001[49]. Acest pachet legislativ nu conține norme privind păstrarea datelor, întrucât stocarea informațiilor privind condamnările penale este reglementată de legea națională. În prezent, cincisprezece state membre participă la un proiect pilot, dintre care nouă au început schimbul electronic de informații extrase din cazierele judiciare. Comisia trebuie să prezinte Parlamentului European și Consiliului două rapoarte de evaluare privind funcționarea acestui pachet legislativ: Decizia-cadru 2008/675/JAI urmează a fi revizuită în 2011; Decizia-cadru 2009/315/JAI urmează a fi revizuită în 2015. Cu începere din 2016, Comisia trebuie să publice, de asemenea, rapoarte periodice privind funcționarea ECRIS.

---

47 Decizia-cadru 2008/675/JAI a Consiliului, JO L 220, 15.8.2008, p. 32; Decizia-cadru 2009/315/JAI a Consiliului, JO L 93, 7.4.2009, p. 23; Decizia 2009/316/JAI a Consiliului, JO L 93, 7.4.2009, p. 33. A se vedea, de asemenea, COM(2005) 10, 25.1.2005.

48 Decizia-cadru 2009/315/JAI a Consiliului, JO L 93, 7.4.2009, p. 23; Decizia 2005/876/JAI a Consiliului, JO L 322, 9.12.2005, p. 33; Decizia-cadru 2008/977/JAI a Consiliului, JO L 350, 30.12.2008, p. 60; Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei).

49 Regulamentul (CE) nr. 45/2001, JO L 8, 12.1.2001, p.1.

Conform unei inițiative finlandeze, Consiliul a adoptat în 2000 un instrument de organizare a schimbului de informații între **unitățile de informații financiare -** *Financial Intelligence Units* (FIU) ale statelor membre în scopul combaterii spălării banilor și, ulterior, finanțării terorismului[50]. Unitățile de informații financiare sunt de obicei instituite în cadrul agențiilor de aplicare a legii, autorităților judiciare sau organismelor administrative care raportează autorităților financiare. Aceste unități au obligația de a împărtăși datele financiare și de aplicare a legii necesare, inclusiv detaliile tranzacțiilor financiare, cu omologii din UE, cu excepția cazurilor în care divulgarea datelor ar fi disproporționată în raport cu interesele persoanelor fizice sau juridice. Informațiile furnizate în scopul analizării sau investigării spălării banilor sau finanțării terorismului pot fi utilizate pentru anchete sau urmăriri penale cu excepția cazului în care statul membru care furnizează informațiile interzice utilizarea în acest scop. Prelucrarea datelor cu caracter personal trebuie să respecte dispozițiile Deciziei-cadru 2008/977/JAI a Consiliului, ale Convenției 108 a Consiliului Europei și ale Recomandării privind sectorul polițienesc[51]. În 2002, mai multe state membre au instituit FIU.net, o aplicație de rețea descentralizată care tratează schimbul de date între FIU și care operează pe rețeaua s-TESTA a Comisiei[52]. Această inițiativă numără douăzeci de unități de informații financiare în calitate de membri. În prezent se poartă discuții privind desfășurarea aplicației securizate a Europol, SIENA, pentru funcționarea FIU.net[53]. După ce au evaluat respectarea de către statele membre a acestui instrument, Consiliul a împuternicit FIU, prin A treia directivă de combatere a spălării banilor, să primească, să analizeze și să difuzeze rapoartele privind tranzacțiile suspecte în legătură cu spălarea banilor *și* finanțarea terorismului[54]. Ca parte a Planului de acțiune privind serviciile financiare, Comisia a revizuit punerea în aplicare a celei de A treia directive privind combaterea spălării banilor din 2009[55].

Dând curs inițiativei propuse de Austria, Belgia și Finlanda, Consiliul a adoptat în 2007 un instrument care are ca obiectiv consolidarea cooperării între **oficiile de recuperare a creanțelor -** *Asset Recovery Offices* (ARO) în urmărirea și identificarea produselor infracțiunii[56]. Similar unităților de informații financiare, oficiile de recuperare a creanțelor cooperează pe o bază descentralizată, deși fără ajutorul unei platforme online. Oficiile de recuperare a creanțelor au obligația de a utiliza Inițiativa suedeză pentru a schimba informații, indicând date cu privire la proprietatea vizată, precum conturi bancare, bunuri imobiliare și vehicule, precum și date cu privire la persoanele fizice sau juridice căutate, inclusiv numele acestora, adresa, data nașterii, precum și informații privind acționarii sau societatea comercială. Utilizarea informațiilor schimbate în temeiul acestui instrument face obiectul legilor interne de protecție a datelor, iar statele membre nu pot aplica un tratament diferențial datelor obținute intern și celor obținute din alte state membre. Prelucrarea datelor cu caracter personal trebuie să respecte dispozițiile Convenției 108 a Consiliului Europei, ale Protocolului

---

50 Decizia 2000/642/JAI a Consiliului, JO L 271, 24.10.2000, p. 4.

51 Decizia-cadru 2008/977/JAI a Consiliului, JO L 350, 30.12.2008, p. 60; Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

52 http://www.fiu.net/

53 SIENA este acronimul de la „Secure Information Exchange Network Application" (Aplicația de rețea a Europol pentru schimbul de informații securizate).

54 Directiva 2005/60/CE, JO L 309, 25.11.2005, p. 15 (A treia directivă privind combaterea spălării banilor).

55 A se vedea, de exemplu, Evaluarea impacturilor economice ale Planului de acțiune privind serviciile financiare — Raport final (pentru Comisia Europeană, DG MARKT), CRA International, 03.2009.

56 Decizia 2007/845/JAI a Consiliului, JO L 332, 18.12.2007, p. 103.

adițional 181 la aceasta și ale Recomandării privind sectorul polițienesc[57]. Până în prezent, peste douăzeci de state membre au instituit ARO. Având în vedere caracterul sensibil al informațiilor schimbate, în prezent au loc discuții privind desfășurarea aplicației SIENA a Europol pentru partajarea datelor între ARO. În cadrul unui proiect pilot lansat în mai 2010, douăsprezece oficii de recuperare a creanțelor au început să utilizeze SIENA pentru a partaja informațiile relevante pentru depistarea activelor. Comisia trebuie să prezinte Consiliului un raport de evaluare în 2010.

În 2008, președinția franceză a Consiliului a invitat statele membre să instituie **platforme** naționale **de alertă privind criminalitatea informatică**, iar pe Europol să instituie o platformă europeană de alertă privind criminalitatea informatică în scopul culegerii, analizării și schimbului de informații privind infracțiunile comise pe internet[58]. Cetățenii pot raporta platformelor naționale cazurile de conținuturi sau comportamente ilegale identificate pe internet. Platforma europeană împotriva criminalității informatice - *European Cybercrime Platform* (ECCP), gestionată de către Europol, ar funcționa ca un centru de informații, analizând și schimbând cu autoritățile naționale de aplicare a legii informațiile legate de criminalitatea informatică care intră în mandatul Europol[59]. Până în prezent, aproape toate statele membre au creat platforme naționale de alertă privind criminalitatea informatică. Europol lucrează la aplicarea din punct de vedere tehnic a ECCP și ar putea desfășura în curând aplicația SIENA pentru a consolida partajarea datelor cu platformele naționale. În măsura în care partajarea informațiilor de acest tip se referă la prelucrarea datelor cu caracter personal de către Europol, se aplică normele speciale privind protecția datelor cuprinse în Decizia privind Europol (Decizia 2009/371/JAI a Consiliului), precum și în Regulamentul (CE) 45/2001, Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta și Recomandarea privind sectorul polițienesc[60]. Dispozițiile Deciziei-cadru 2008/977/JAI a Consiliului reglementează schimbul de date cu caracter personal între statele membre și Europol[61]. În lipsa unui instrument legislativ, nu există un mecanism oficial de revizuire pentru platformele de alertă privind criminalitatea informatică. Cu toate acestea, Europol

---

57 Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181), Consiliul Europei, 8.11.2001 (Protocol adițional 181); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

58 Concluziile Consiliului privind instituirea platformelor naționale de alertă și a unei platforme europene de alertă pentru raportarea infracțiunilor constatate pe internet, Consiliul Justiție și Afaceri Interne, 24.10.2008; Concluziile Consiliului privind un plan de acțiune pentru aplicarea strategiei concertate de combatere a criminalității, Consiliul Afaceri Generale, 26.4.2010. Europol a redenumit proiectul „Platforma europeană împotriva criminalității informatice" (ECCP).

59 Obiectivul Europol este prevenirea și combaterea criminalității organizate, a terorismului și a altor forme de criminalitate gravă care afectează două sau mai multe state membre. A se vedea Decizia 2009/371/JAI a Consiliului, JO L 121, 15.5.2009, p. 37.

60 Decizia 2009/371/JAI a Consiliului, JO L 121, 15.5.2009, p. 37; Regulamentul (CE) nr. 45/2001, JO L 8, 12.1.2001, p.1; Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181), Consiliul Europei, 8.11.2001 (Protocol adițional 181); Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

61 Decizia-cadru 2008/977/JAI a Consiliului, JO L 350, 30.12.2008, p. 60.

acoperă deja acest domeniu important, iar în viitor va raporta cu privire la activitățile ECCP în raportul anual prezentat Consiliului pentru aprobare și Parlamentului European pentru informare.

Agenții și organisme ale UE mandatate să asiste statele membre în vederea prevenirii și combaterii criminalității grave transfrontaliere

Înființat în 1995, **Oficiul European de Poliție** (Europol) și-a început activitatea în 1999 și a devenit o agenție UE în ianuarie 2010[62]. Obiectivul său este de a sprijini statele membre în vederea prevenirii și combaterii criminalității organizate, a terorismului și a altor forme grave de criminalitate care afectează două sau mai multe state membre. Funcțiile sale principale includ colectarea, stocarea, prelucrarea, analiza și schimbul de informații publice și secrete; asistența în cazul anchetelor și furnizarea de informații secrete și sprijin analitic statelor membre. Principalul organism de legătură între Europol și statele membre sunt unitățile naționale Europol (UNE), care detașează ofițeri de legătură pe lângă Europol. Șefii UNE se întâlnesc în mod regulat pentru a oferi asistență Europol în chestiuni operaționale, iar funcționarea agenției este supervizată de consiliul său de administrație și de director. Instrumentele de gestionare a informației ale Europol includ sistemul informațional Europol (EIS – *Europol Information System*), fișierele de lucru pentru analiză (AWF - *Analysis Work Files*) și aplicația SIENA. EIS conține datele cu caracter personal, inclusiv, *inter alia*, elementele de identificare biometrică, condamnările penale și legăturile cu criminalitatea organizată ale persoanelor suspectate de săvârșirea unor infracțiuni care intră sub incidența mandatului Europol. Accesul este limitat, fiind posibil doar pentru UNE, ofițerii de legătură, personalul autorizat al Europol și directorul. AWF, deschise în scopul de ajuta anchetele penale, includ date privind persoane și orice alte informații pe care UNE pot hotărî să le adauge. Accesul este permis ofițerilor de legătură, însă numai analiștii Europol pot introduce date în aceste fișiere. Un sistem de index le permite UNE și ofițerilor de legătură să verifice dacă un AWF conține informații de interes pentru statul lor membru. Aplicația SIENA a Europol este din ce în ce mai utilizată de statele membre pentru a partaja date sensibile în vederea aplicării legii. Europol poate prelucra informații publice și secrete, inclusiv date cu caracter personal, pentru îndeplinirea funcțiilor sale; statele membre pot doar utiliza informații extrase din fișierele de date ale Europol în scopul prevenirii și combaterii criminalității grave de natură transfrontalieră. Orice restricție plasată asupra utilizării informațiilor de către un stat membru care le furnizează se aplică și altor utilizatori care extrag astfel de date din fișierele de date ale Europol. De asemenea, Europol poarte face schimb de informații cu caracter personal cu țări terțe care au încheiat acorduri operaționale cu Europol și care garantează un nivel adecvat de protecție a datelor. Acesta poate păstra datele numai atâta timp cât este necesar pentru îndeplinirea funcțiilor sale. AWF pot fi păstrate cel mult trei ani, cu o prelungire posibilă de încă trei ani. Prelucrarea datelor cu caracter personal de către Europol trebuie să se facă în conformitate cu normele specifice privind protecția datelor conținute în propriul său instrument de reglementare [Decizia 2009/371/JAI a Consiliului, precum și Regulamentul (CE) 45/2001, Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta și Recomandarea privind sectorul polițienesc[63]]. Dispozițiile Deciziei-

---

62 Decizia 2009/371/JAI a Consiliului, JO L 121, 15.5.2009, p. 37, care înlocuieşte Convenția în temeiul articolului K.3 din Tratatul privind Uniunea European, privind înființarea Oficiului European de Poliție, JO C 316, 27.11.1995, p. 2.

63 Decizia 2009/371/JAI a Consiliului, JO L 121, 15.5.2009, p. 37; Regulamentul (CE) nr. 45/2001, JO L 8, 12.1.2001, p.1. Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenția 108 a Consiliului Europei); Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a

cadru 2008/977/JAI a Consiliului se aplică schimbului de date cu caracter personal dintre statele membre și Europol[64]. Un organism comun de supraveghere, format din membri ai organismelor naționale de supraveghere, monitorizează prelucrarea datelor cu caracter personal de către Europol, precum și transmiterea de Europol a datelor cu caracter personal către alte părți. Acesta prezintă rapoarte periodice Parlamentului European și Consiliului. Europol prezintă un raport anual privind activitățile sale Consiliului pentru aprobare și Parlamentului European pentru informare.

În plus față de impactul lor asupra celor câteva instrumente descrise anterior, atacurile teroriste de la 11 septembrie 2001 au determinat înființarea, în 2002, a **Unității de Cooperare Judiciară a Uniunii Europene** (Eurojust)[65]. Eurojust este un organism UE al cărui obiectiv constă în îmbunătățirea coordonării anchetelor și urmăririlor penale în statele membre, precum și intensificarea cooperării dintre autoritățile naționale competente. Acesta tratează aceleași tipuri de criminalitate și infracțiuni ca și Europol. În cadrul acestui mandat și pentru îndeplinirea funcțiilor lor, cei 27 de membri naționali ai Eurojust, care constituie colegiul acestuia, au acces la datele cu caracter personal ale suspecților și infractorilor. Astfel de date cuprind, *inter alia*, următoarele: informații biografice, date de contact, date privind înmatricularea vehiculelor, profiluri ADN, fotografii, amprente digitale, precum și date de trafic, localizare și abonare puse la dispoziție de furnizorii de servicii de telecomunicații. Se așteaptă ca statele membre să partajeze astfel de informații cu Eurojust pentru a-i permite acestuia să își îndeplinească funcțiile. Toate datele cu caracter personal legate de un caz trebuie introduse în sistemul informatizat de gestionare a cazurilor al Eurojust, care funcționează pe rețeaua s-TESTA a Comisiei. Un sistem de index înregistrează date cu caracter personal și nepersonal relevante pentru cercetări în curs. Eurojust poate prelucra date cu caracter personal pentru îndeplinirea funcțiilor sale, însă astfel de operațiuni trebuie să respecte normele specifice conținute în propriul instrument de reglementare al Eurojust (Decizia 2009/426/JAI a Consiliului), precum și Convenția 108 a Consiliului Europei, Protocolului adițional 181 la aceasta, și Recomandarea privind sectorul polițienesc. Dispozițiile Deciziei-cadru a Consiliului 2008/977/JAI se aplică schimbului de date cu caracter personal dintre statele membre și Eurojust[66]. Eurojust poate face schimb de date cu autorități naționale și cu țări terțe cu care a încheiat un acord, cu condiția ca membrul național care a furnizat datele să fi fost de acord cu un astfel de transfer și ca țara terță să garanteze un nivel adecvat de protecție a datelor cu caracter personal. Datele cu caracter personal pot fi păstrate atâta timp cât este necesar pentru ca Eurojust să își îndeplinească obiectivele, însă trebuie șterse odată ce cazul este închis. Statele membre trebuie să aplice temeiul juridic modificat al Eurojust până în iunie 2011. Până în iunie 2014, Comisia trebuie să revizuiască schimbul de informații între membrii naționali ai Eurojust și poate propune orice modificări pe care le consideră potrivite privind acesta. Până în iunie 2013, Eurojust trebuie să raporteze Consiliului și Comisiei în legătură cu experiența referitoare la furnizarea de acces la nivel național la sistemul său de gestionare a cazurilor. Statele membre pot revizui drepturile de acces național pe această bază. Un organism comun de supraveghere, format din judecători

---

datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor (ETS nr. 181), Consiliul Europei, 8.11.2001 (Protocol adițional 181). Recomandarea nr. R (87) 15 a Comitetului de Miniștri ce reglementează utilizarea datelor personale în sectorul polițienesc, Consiliul Europei, 17.9.1987 (Recomandarea privind sectorul polițienesc).

64 Decizia-cadru 2008/977/JAI a Consiliului, JO L 350, 30.12.2008, p. 60.

65 Decizia 2002/187/JAI a Consiliului, JO L 63, 6.3.2002, p. 1, modificată prin Decizia 2009/426/JAI a Consiliului, JO L 138, 4.6.2009, p. 14. A se vedea și Consiliul Extraordinar Justiție și Afaceri Interne, 20.9.2001.

66 Decizia-cadru 2008/977/JAI a Consiliului, JO L 350, 30.12.2008, p. 60.

numiți de statele membre, monitorizează prelucrarea datelor cu caracter personal de către Eurojust și raportează anual către Consiliu. Președintele colegiului prezintă Consiliului un raport anual privind activitățile Eurojust, pe care Consiliul îl transmite Parlamentului European.

Acorduri internaționale care vizează prevenirea și combaterea terorismului, precum și a altor forme de criminalitate gravă transnațională

Ca urmare a atacurilor teroriste de la 11 septembrie 2001, SUA au adoptat o legislație care obligă transportorii aerieni care operează zboruri către, dinspre sau pe teritoriul său, să furnizeze autorităților SUA datele privind **registrele cu numele pasagerilor** (PNR) înregistrate în sistemele lor de rezervare informatizată. La puțin timp după aceasta, Canada și Australia au hotărât să facă același lucru. Întrucât legislația UE relevantă impune evaluarea prealabilă a nivelului de protecție a datelor garantat de țările terțe, Comisia a făcut eforturi pentru a îndeplini această funcție și a negociat acorduri PNR cu aceste țări[67]. A semnat acordul cu SUA în iulie 2007, cel cu Australia în iunie 2008 și acordul API/PNR cu Canada în octombrie 2005[68]. Acordurile cu SUA și cu Australia se aplică provizoriu, iar cel cu Canada rămâne în vigoare în ciuda expirării în septembrie 2009, a deciziei Comisiei de evaluare a caracterului adecvat privind standardele canadiene de protecție a datelor[69]. Exprimând critici în legătură cu conținutul acestora, Parlamentul European a invitat Comisia să renegocieze toate cele trei acorduri pe baza unui set clar de principii[70]. Transmise cu mult înaintea plecării unui zbor, datele PNR ajută autoritățile de aplicare a legii să verifice pasagerii în ceea ce privește eventuale legături cu terorismul și cu alte forme de criminalitate gravă. În consecință, scopul fiecărui acord este prevenirea și combaterea terorismului și a altor forme transnaționale de criminalitate gravă. În schimbul datelor PNR provenind din UE, Departamentul pentru Securitate Internă al SUA (DHS) transmite „piste" care rezultă din analiza sa privind PNR autorităților de aplicare a legii ale UE, Europol și Eurojust; iar atât Canada, cât și SUA, s-au angajat în acordurile semnate cu acestea să coopereze cu UE la constituirea propriului său sistem PNR. Acordurile cu SUA și cu Australia conțin 19 categorii de date, inclusiv informații biografice, privind rezervarea, plata și informații suplimentare; acordul cu Canada conține 25 de tipuri de date similare. Informațiile suplimentare includ, *inter alia*, date privind bilete dus, statutul în așteptare și statutul „neprezentare". Acordul cu SUA permite, în anumite condiții speciale, utilizarea unor informații sensibile. DHS poate prelucra astfel de informații dacă viața unei persoane vizate sau a altor persoane este în pericol, însă trebuie să le șteargă în termen de 30 de zile. Datele PNR sunt transmise unui grup de unități centrele din cadrul DHS, Agenția de Servicii Frontaliere a Canadei și Serviciul Vamal australian, care pot să transfere astfel de date unor alte autorități naționale responsabile cu aplicarea legii sau cu combaterea terorismului. În acordul cu SUA, DHS se așteaptă ca nivelul de protecție a datelor pe care trebuie să îl aplice prelucrării datelor PNR provenind de la UE să nu fie „mai strict" decât cel aplicat de autoritățile UE în sistemele lor PNR naționale. În cazul în care această cerință nu este îndeplinită, acesta poate suspenda anumite părți din acord. UE consideră că Australia și

---

67 Directiva 95/46/CE (Directiva privind protecția datelor), JO L 281, 23.11.1995, p. 31.

68 Pachetul canadian constă într-un angajament canadian privind tratarea datelor API/PNR, decizia Comisiei de evaluare a caracterului adecvat privind standardele de protecție a datelor și un acord internațional (a se vedea JO L 91, 29.3.2006, p. 49; JO L 82, 21.3.2006, p. 14). Acordul cu SUA poate fi găsit în JO L 204, 4.8.2007, p. 16; cel cu Australia în JO L 213, 8.8.2008, p. 47.

69 În 2009, Canada s-a angajat în fața Comisiei, a Președinției Consiliului și a statelor membre ale UE că va continua să aplice angajamentul său anterior din 2005 privind utilizarea datelor PNR ale UE. Decizia Comisiei de evaluare a caracterului adecvat s-a bazat pe acel angajament anterior.

70 Rezoluția Parlamentului European, P7_TA(2010)0144, 5.5.2010.

Canada oferă un nivel de protecție „adecvat” pentru datele PNR provenind de la UE dacă acestea respectă condițiile din acordurile încheiate cu fiecare dintre ele. În SUA, datele PNR provenind de la UE sunt păstrate timp de șapte ani într-o bază de date activă și timp de alți opt ani într-o bază de date pasivă. În Australia, acestea sunt introduse într-o bază de date activă timp de 3,5 ani și apoi într-o bază de date pasivă timp de doi ani. În ambele țări, baza de date pasivă este accesibilă numai cu autorizație specială. În Canada, datele sunt păstrate timp de 3,5 ani, informațiile fiind transformate în date anonime după 72 de ore. Fiecare acord prevede revizuiri periodice, în timp ce acordurile cu Canada și cu Australia includ și o clauză de denunțare. În UE, numai Regatul Unit are un sistem PNR. Franța, Danemarca, Belgia, Suedia și Țările de Jos fie au adoptat acte legislative relevante sau testează în prezent utilizarea datelor PNR în pregătirea creării unor sisteme PNR. Câteva alte state membre examinează posibilitatea creării unor sisteme PNR și toate statele membre utilizează, de la caz la caz, date PNR în vederea aplicării legii.

În urma atacurilor de la 11 septembrie 2001, Departamentul de Trezorerie al SUA a dezvoltat un **program de urmărire a finanțărilor în scopuri teroriste** (TFTP) pentru a identifica, a supraveghea și a urmări penal teroriștii și susținătorii lor financiari. În cadrul TFTP, Departamentul de Trezorerie al SUA a cerut, prin intermediul unor citații administrative, filialei americane a unei societăți belgiene să transfere Departamentului de Trezorerie seturi limitate de date de mesagerie financiară transferate prin rețeaua sa. În ianuarie 2010, această societate și-a modificat arhitectura de sistem, ceea ce a redus cu mai mult de jumătate volumul de date aflate sub jurisdicția SUA care făceau, în general, obiectul citațiilor Departamentului de Trezorerie. În noiembrie 2009, Președinția Consiliului Uniunii Europene și Guvernul Statelor Unite au semnat un acord intermediar privind prelucrarea și transferul de date de mesagerie financiară din UE către SUA în scopuri TFTP, care nu a fost aprobat de Parlamentul European[71]. Pe baza unui nou mandat, Comisia Europeană a negociat un nou proiect de acord cu SUA, prezentând Consiliului la 18 iunie 2010 o propunere de decizie a Consiliului referitoare la încheierea unui acord între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste (Acordul TFTP UE-SUA)[72]. Parlamentul European a aprobat încheierea acestui acord la 8 iulie 2010[73]. Se așteaptă acum adoptarea de către Consiliu a unei decizii a Consiliului privind încheierea acestui acord, în urma căreia acordul ar intra în vigoare prin intermediul unui schimb de scrisori între cele două părți. Scopul Acordului TFTP UE-SUA este de a preveni, a cerceta, a detecta sau a urmări penal terorismul și finanțarea sa. Acest lucru obligă furnizorii desemnați de servicii de mesagerie financiară să transfere Departamentului de Trezorerie al SUA, pe baza unor evaluări specifice geografice a amenințării și a unor cereri adaptate, seturi de date de mesagerie financiară care conțin, *inter alia*, numele, numărul de cont, adresa și numărul de identificare al inițiatorului și destinatarului (destinatarilor) de tranzacții financiare. Departamentul de Trezorerie poate doar efectua căutări de astfel de date în scopuri legate de TFTP și numai dacă are un motiv să creadă că o persoană identificată are legătură cu terorismul sau cu finanțarea acestuia. Extragerea de date și transferul de date referitoare la tranzacții în cadrul Zonei unice de plăți în euro sunt interzise. SUA furnizează statelor membre UE, Europol și Eurojust orice „piste” privind eventuale comploturi teroriste în UE și va ajuta UE să își creeze propriul său sistem echivalent cu TFTP. În cazul în care UE instituie un astfel de program, cele două părți pot

---

71 Rezoluția Parlamentului European, P7_TA(2010)029, 11.2.2010.

72 COM(2010)316 final/2, 18.6.2010.

73 Rezoluția Parlamentului European, P7_TA-PROV(2010)0279, 8.7.2010.

reajusta condițiile acestui acord. Înainte ca vreo dată să poată fi transferată, fiecare cerere de informații din partea SUA trebuie controlată de Europol pentru a se asigura că îndeplinește condițiile acestui acord. Informațiile extrase din mesaje financiare nu pot fi păstrate mai mult timp decât este necesar pentru cercetări sau urmăriri penale specifice; datele neextrase pot fi păstrate timp de maximum 5 ani. În caz de nevoie pentru cercetarea, prevenirea sau urmărirea penală a terorismului sau a finanțării acestuia, Departamentul de Trezorerie poate transfera autorităților de aplicare a legii, de siguranță publică sau de combatere a terorismului din SUA, statelor membre UE, Europol sau Eurojust, orice date cu caracter personal extrase din mesaje FIN. De asemenea, poate transmite unor țări terțe orice piste privind resortisanți și rezidenți UE, sub rezerva consimțământului statului membru vizat. Respectarea de către părți a limitării stricte a scopului acordului la combaterea terorismului și respectarea celorlalte garanții fac obiectul unei monitorizări de către supraveghetori independenți, inclusiv de către o persoană desemnată de Comisie. Acesta are o durată de cinci ani și poate fi denunțat sau suspendat de oricare dintre părți. O echipă de revizuire a UE condusă de Comisie și care include reprezentați a două autorități de protecție a datelor și o persoană care provine din mediul judiciar va revizui acest acord la șase luni de la intrarea sa în vigoare, evaluând în special punerea în aplicare de către părți a dispozițiilor acestuia privind limitarea scopului și proporționalitatea, precum și respectarea obligațiilor acestora în materie de protecție a datelor Raportul Comisiei va fi prezentat Parlamentului European și Consiliului.

2.2. Inițiative în cadrul Planului de acțiune privind Programul de la Stockholm

Propuneri legislative care urmează să fie prezentate Comisiei

În Programul de la Stockholm, Consiliul European a invitat Comisia să prezinte trei propuneri cu relevanță directă pentru prezenta comunicare: un sistem PNR al UE pentru prevenirea, detectarea și urmărirea penală a terorismului și a criminalității grave; un sistem de intrare/ieșire și un program privind călătorii înregistrați. Ultimele două, a subliniat Consiliul European, ar trebui prezentate „cât de curând posibil”. Comisia a încorporat toate cele trei cerințe în Planul său de acțiune privind Programul de la Stockholm[74]. Aceasta va avea acum ca obiectiv punerea în aplicare a acestor cerințe și, în viitor, evaluarea acestor instrumente pe baza principiilor de elaborare a politicilor prevăzute în secțiunea 4.

În noiembrie 2007, Comisia a prezentat o propunere de decizie-cadru a Consiliului privind utilizarea datelor PNR în scopul aplicării legii[75]. Această inițiativă a primit sprijin în Consiliu și a fost modificată ulterior pentru a ține seama de amendamentele propuse de Parlamentul European și de opiniile Autorității Europene pentru Protecția Datelor. Odată cu intrarea în vigoare a Tratatului de la Lisabona, aceasta a devenit caducă. După cum se indică în Planul de acțiune privind Programul de la Stockholm, Comisia lucrează acum pentru a prezenta, la începutul anului 2011, un **pachet privind registrele cu numele pasagerilor** care constă în următoarele: o comunicare privind o strategie a UE în legătură cu PNR externe, care definește principiile esențiale care ghidează negocierea de acorduri cu țări terțe; directive de negociere pentru renegocierea de acorduri PNR cu SUA și Australia și directive de negociere pentru un nou acord cu Canada. De asemenea, Comisia se află în plin proces de pregătire a unei noi propuneri a UE privind PNR.

---

74 Programul de la Stockholm — O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora, Documentul Consiliului 5731/10, 3.3.2010; COM(2010)171, 20.4.2010 (Planul de acțiune privind Programul de la Stockholm).

75 COM(2007) 654, 6.11.2007.

În 2008, Comisia a prezentat mai multe sugestii de dezvoltare a gestionării integrate a frontierelor UE prin facilitarea deplasărilor pentru resortisanții țărilor terțe, concomitent cu consolidarea securității interne[76]. Având în vedere că persoanele care depășesc termenul legal de ședere constituiau cel mai mare grup de imigranți clandestini, s-a sugerat posibila introducere a unui **sistem de intrare/ieșire** (EES – *Entry/Exit System*) pentru resortisanții țărilor terțe care intră pe teritoriul UE pentru perioade scurte de până la trei luni. Acest sistem ar înregistra data și locul de intrare, precum și durata șederii autorizate și ar transmite semnalări automate autorităților competente, care identifică persoanele ca depășind termenul legal de ședere. Pe baza verificării datelor biometrice, ar desfășura același sistem de corespondențe biometrice și aceleași echipament operațional care sunt utilizate de către SIS II și VIS. În prezent, Comisia desfășoară o evaluarea de impact și, după cum se afirmă în Planul de acțiune privind Programul de la Stockholm, aceasta se va strădui să prezinte o propune legislativă în 2011.

Un **Program privind călătorii înregistrați** (RTP - *Registered Travellers Programme*) a fost cea de a treia propunere de examinat[77]. Acest program ar permite unor anumite grupuri de călători care se deplasează frecvent, provenind din țări terțe, să intre în UE, cu condiția unei verificări prealabile corespunzătoare, utilizând controale simplificate la frontieră, la porți automate. De asemenea, RTP ar fi bazat pe verificarea identității prin utilizarea datelor biometrice și ar permite o trecere treptată de la abordarea actuală a controlului general la frontieră către o abordare bazată pe riscul individual. Comisia a realizat o evaluare de impact și, în conformitate cu Planul de acțiune privind Programul de la Stockholm, intenționează să prezinte o propune legislativă în 2011.

Inițiative care urmează să fie studiate de Comisie

În Programul de la Stockholm, Consiliul European a invitat Comisia să studieze trei inițiative cu relevanță pentru prezenta comunicare: posibilitățile de a supraveghea finanțarea teroristă pe teritoriul UE; posibilitatea și utilitatea de a dezvolta un sistem european de autorizare a călătoriilor și necesitatea de a se crea un sistem european de inventariere a evidențelor poliției, precum și valoarea adăugata a acestuia. De asemenea, Comisia a încorporat aceste inițiative în Planul său de acțiune privind Programul de la Stockholm. Acum, va evalua fezabilitatea acestora și va decide dacă le va continua și în ce fel o va face, pe baza principiilor de elaborare a politicilor prezentate în secțiunea 4.

Acordul TFTP UE-SUA invită Comisia Europeană să efectueze un studiu privind eventuala introducere a unui **sistem UE de urmărire a finanțărilor în scopuri teroriste**, echivalent cu TFTP în SUA, care să permită un transfer „mai punctual" al datelor dinspre UE către SUA. Proiectul de decizie a Consiliului privind încheierea acestui acord invită, de asemenea, Comisia să prezinte Parlamentului European și Consiliului, cel târziu la un an de la intrarea în vigoare a Acordului TFTP UE-SUA, un cadru juridic și tehnic pentru extragerea datelor pe teritoriul UE[78]. În termen de trei ani de la intrarea în vigoare a acestui acord, Comisia va prezenta un raport privind progresele înregistrate în legătură cu dezvoltarea unui astfel de sistem UE echivalent. În cazul în care un astfel de sistem nu va fi fost creat în termen de cinci ani de la intrarea în vigoare a acordului, UE poate hotărî să denunțe acordul. De asemenea, prin Acordul TFTP UE-SUA, SUA se angajează să coopereze cu UE și să furnizeze asistență

---

76 COM(2008) 69, 13.2.2008.

77 COM(2008) 69, 13.2.2008.

78 Documentul Consiliului 11222/1/10 REV1, 24.6.2010; Documentul Consiliului 11222/1/10 REV1 COR1, 24.6.2010.

și consultanță în cazul în care UE hotărăște să creeze un astfel de sistem. Fără a aduce atingere oricărei decizii eventuale, Comisia a început să examineze protecția datelor, resursele și implicațiile practice ale acestei acțiuni. După cum se indică în Planul de acțiune privind Programul de la Stockholm, Comisia va prezenta în 2011 o comunicare privind fezabilitatea creării unui program de urmărire a finanțărilor în scopuri teroriste (TFTP UE).

În comunicarea sa din 2008 privind gestionarea integrată a frontierelor, Comisia a sugerat crearea eventuală a unui **sistem electronic de autorizare a călătoriilor** (ESTA) pentru resortisanți din țări terțe care nu au nevoie de viză[79]. În cadrul acestui program, resortisanților eligibili din țări terțe li s-ar cere să introducă o solicitare electronică în care să furnizeze, înainte de călătorie, informațiile lor biografice, cele din pașaport și legate de călătorie. Comparativ cu procedura de eliberare a vizei, ESTA ar oferi o metodă mai rapidă și mai simplă de verificare a măsurii în care o persoană îndeplinește condițiile necesare de intrare. În prezent, Comisia realizează un studiu privind avantajele, dezavantajele și implicațiile practice ale introducerii ESTA. După cum se indică în Planul de acțiune privind Programul de la Stockholm, aceasta intenționează să prezinte în 2011 o comunicare privind fezabilitatea creării unui astfel de program.

În cursul președinției Consiliului exercitate în 2007, Germania a lansat o discuție privind crearea eventuală a unui **sistem european de inventariere a evidențelor poliției** (EPRIS - *European Police Records Index System*)[80]. EPRIS ar ajuta agenții responsabili de aplicarea legii să localizeze informațiile pe teritoriul UE, în special privind legăturile dintre indivizi suspectați de a participa la criminalitatea organizată. În 2010, Comisia va prezenta Consiliului proiectul său de termeni de referință pentru studiul său de fezabilitate privind EPRIS. După cum se afirmă în Planul de acțiune privind Programul de la Stockholm, aceasta se va strădui să prezinte în 2012 o comunicare privind fezabilitatea creării unui astfel de program.

3. ANALIZA INSTRUMENTELOR OPERAȚIONALE, ÎN CURS DE APLICARE SAU ÎN CURS DE EXAMINARE

Prezentarea anterioară conduce la următoarele observații preliminare:

Structură descentralizată

Dintre diversele instrumente care sunt în prezent operaționale, în curs de aplicare sau în curs de examinare, numai șase implică o colectare sau stocare a datelor cu caracter personal la nivel UE, și anume, SIS (și SIS II), VIS, EURODAC, CIS, Europol și Eurojust. Toate celelalte măsuri reglementează schimbul descentralizat transfrontalier sau transferul către țări terțe de informații cu caracter personal colectate la nivel național de autorități publice sau de societăți private. Majoritatea datelor cu caracter personal sunt colectate și stocate la nivel național; UE se străduiește să confere valoare adăugată permițând, în anumite condiții, schimbul unor astfel de informații cu parteneri UE și cu țări terțe. Recent, Comisia a prezentat Parlamentului European și Consiliului o propunere modificată de instituire a Agenției pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție[81]. Viitoarea funcție a Agenției IT va fi să realizeze gestionarea operațională a SIS II, VIS și EURODAC și a oricărui alt sistem informatic viitor în spațiul de

[79] COM(2008) 69, 13.2.2008.
[80] Documentul 15526/1/09 al Consiliului, 2.12.2009.
[81] COM(2010) 93, 19.3.2010.

libertate, securitate și justiție, astfel încât să permită funcționarea acestor sisteme în mod permanent, asigurând astfel fluxul neîntrerupt de informații.

Scop limitat

Majoritatea instrumentelor analizate anterior au un scop unitar: EURODAC se străduiește să consolideze funcționarea sistemului Dublin; API să îmbunătățească controlul la frontiere; inițiativa suedeză să consolideze anchetele penale și operațiunile de culegere de informații; Convenția Napoli II să ajute la prevenirea, detectarea, urmărirea penală și sancționarea fraudei vamale; CIS să ofere asistență pentru prevenirea, cercetarea și urmărirea penală a încălcărilor grave ale legilor naționale prin creșterea eficacității cooperării între autoritățile vamale naționale; ECRIS, FIU și ARO să simplifice schimbul de date la nivel transfrontalier în anumite domenii și Decizia Prüm, Directiva privind păstrarea datelor, TFTP și PNR să combată terorismul și criminalitatea gravă. SIS, SIS II și VIS par să fie principalele excepții de la acest model: scopul inițial al VIS era să faciliteze schimbul transfrontalier de date privind vizele, însă acesta a fost extins ulterior la prevenirea și combaterea terorismului și criminalității grave. SIS și SIS II au ca scop asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție, precum și facilitarea circulației persoanelor utilizând informațiile comunicate prin intermediul acestui sistem. Cu excepția acestor sisteme centralizate de informații, limitarea scopului pare să reprezinte un factor esențial în elaborarea măsurilor de gestionare a informațiilor la nivelul UE.

Eventuale suprapuneri în funcționare

Aceleași informații cu caracter personal pot fi colectate prin intermediul unor instrumente diferite, însă pot fi utilizate doar pentru un scop limitat în cadrul unui anumit instrument (cu excepția VIS, SIS și SIS II). De exemplu, datele biografice ale unei persoane, inclusiv numele său, data și locul nașterii, precum și cetățenia, pot fi prelucrate prin intermediul SIS, SIS II, VIS, API, CIS, inițiativa suedeză, Decizia Prüm, ECRIS, FIU, ARO, Europol, Eurojust și acordurile PNR și TFTP. Cu toate acestea, astfel de date pot fi prelucrate doar în scopul controlului la frontiere în cazul API; al prevenirii, cercetării și urmăririi penale a fraudei vamale, în cazul CIS; al anchetelor penale și al operațiunilor de culegere de informații, în cazul inițiativei suedeze; al prevenirii terorismului și criminalității transfrontaliere, în cazul Deciziei Prüm; al examinării antecedentelor penale ale unei persoane, în cazul ECRIS; al cercetării legăturilor unei persoane cu criminalitatea organizată și cu rețelele teroriste, în cazul FIU; al depistării activelor, în cazul ARO; al cercetării și sprijinirii urmăririi penale a criminalității transfrontaliere grave, în cazul Europol și Eurojust; al prevenirii și combaterii terorismului și a altor forme de criminalitate transnațională gravă, în cazul PNR și al identificării și urmăririi penale a teroriștilor și a finanțatorilor acestora, în cazul TFTP. Datele biometrice, precum amprentele digitale și fotografiile, pot fi prelucrate în cadrul SIS II, VIS, EURODAC, inițiativa suedeză, Decizia Prüm, ECRIS, Europol și Eurojust – din nou, pentru scopul limitat al fiecărei măsuri. Decizia Prüm este singurul instrument care permite schimbul transfrontalier de profiluri ADN anonime (chiar dacă astfel de date pot fi transferate și Europol și Eurojust). Alte măsuri prelucrează informații cu caracter personal foarte specializate, relevante pentru obiectivele unice ale acestora: sistemele PNR prelucrează datele privind rezervarea zborului de către pasageri; FIDE, datele relevante pentru cercetarea fraudei vamale; Directiva privind păstrarea datelor, adresele IP și elementele de identificare a echipamentelor mobile; ECRIS, cazierele judiciare; ARO, activele private și datele privind societățile; platformele privind criminalitatea informatică, infracțiunile pe internet; Europol, legăturile cu rețelele criminale și TFTP, datele de mesagerie financiară. Schimbul transfrontalier de informații publice și secrete pentru anchete penale oferă singurul exemplu

de suprapunere substanțială în funcții. Din punct de vedere juridic, inițiativa suedeză ar fi suficientă pentru a face schimb de *orice* tip de informații relevante pentru astfel de anchete (cu condiția ca schimbul de astfel de date cu caracter personal să fie permis în cadrul legislației naționale). Cu toate acestea, din perspectivă operațională, decizia Prüm poate fi preferabilă pentru schimbul de profiluri ADN și de amprente digitale, întrucât sistemul său de tip „hit/no hit" asigură răspunsuri instantanee și metoda sa de schimb de date informatizat garantează un nivel ridicat de securitate a datelor[82]. În mod similar, poate fi mai eficient pentru FIU, ARO și platformele privind criminalitatea informatică să contacteze direct omologii lor din UE fără să completeze formularele necesare conform inițiativei suedeze pentru a solicita informații.

Drepturi de acces controlate

Drepturile de acces pentru instrumentele puse în mișcare de logica combaterii terorismului și a criminalității grave tind să fie limitate la o definiție mai restrânsă a autorităților de aplicare a legii, adică poliția, autoritățile de control la frontiere și autoritățile vamale. Drepturile de acces pentru măsurile determinate de logica "Schengen" sunt acordate în general autorităților de imigrație și, în anumite condiții, poliției, autorităților de control la frontiere și autorităților vamale. Fluxul de informații este controlat de interfețe naționale în cazul SIS și VIS centralizate și prin puncte naționale de contact sau prin unități centrale de coordonare în cazul unor instrumente descentralizate, precum Decizia Prüm, inițiativa suedeză, Convenția Napoli II, ECRIS, TFTP, acordurile PNR, FIU, ARO și platformele privind criminalitatea informatică.

Norme variabile privind păstrarea datelor

Termenele de păstrare a datelor variază foarte mult în funcție de obiectivele diverselor instrumente. Acordul PNR cu SUA are cel mai lung termen de păstrare a datelor - 15 ani, în timp ce API are cel mai scurt termen - 24 de ore. Acordurile PNR introduc o distincție interesantă între date cu o utilizare activă sau pasivă: după un anumit termen, informațiile trebuie arhivate și pot fi „deblocate" doar cu o autorizație specială. Utilizarea în Canada a datelor PNR ale UE oferă un bun exemplu: informațiile trebuie transformate în date anonime după 72 de ore, dar rămân la dispoziția agenților autorizați timp de 3,5 ani.

Gestionarea eficace a identității

Mai multe măsuri analizate anterior, inclusiv viitorul SIS II și VIS, au ca scop să permită verificarea identității prin utilizarea unor date biometrice. Se așteaptă ca implementarea SIS II să consolideze securitatea în spațiul de libertate, securitate și justiție prin sprijinul acordat, de exemplu, la identificarea indivizilor pentru care au fost emise mandate europene de arestare, a celor cărora li s-a refuzat intrarea în spațiul Schengen și a celor solicitați din alte motive specifice legate de o anchetă (cum ar fi persoane dispărute sau martori în procese) indiferent de disponibilitatea sau autenticitatea unor documente de identificare. Implementarea VIS trebuie să faciliteze procesul de eliberare și gestionare a vizelor.

---

82 Decizia Prüm (Decizia 2008/615/JAI a Consiliului, JO L 210, 6.8.2008, p. 1) are o decizie de punere în aplicare corespondentă (Decizia 2008/616/JAI a Consiliului, JO L 210, 6.8.2008, p. 12), care vizează garantarea utilizării celor mai recente măsuri tehnice pentru a asigura protecția și securitatea datelor, în special confidențialitatea și integritatea datelor, precum și a unor proceduri de criptare și de autorizare pentru accesarea datelor și care include norme specifice care reglementează admisibilitatea căutărilor.

Securitatea datelor prin intermediul soluțiilor UE

Pentru schimbul de informații sensibile dincolo de frontierele europene, statele membre preferă soluții UE. Mai multe instrumente cu diferite dimensiuni, structură și scop se bazează pe rețeaua s-TESTA de comunicare a datelor finanțată de Comisie pentru partajarea datelor sensibile. Acestea includ sistemele centralizate SIS II, VIS și EURODAC, instrumentele descentralizate Prüm, ECRIS și FIU, precum și Europol și Eurojust. CIS și FIDE utilizează rețeaua comună de comunicație, interfața comună a sistemelor sau accesul internet securizat furnizat de Comisie. Între timp, aplicația de rețea de schimb de informații SIENA a Europol pare să fi devenit aplicația preferată pentru unele inițiative recente care se bazează pe transferul securizat de date: sunt în curs discuții în legătură cu posibilitatea ca FIU.net, ARO și platformele de alertă privind criminalitatea informatică să opereze pe baza acestei aplicații.

Mecanisme de revizuire divergente

Instrumentele analizate anterior conțin o serie de diferite mecanisme de revizuire. În cazul unor sisteme complexe de informații, precum SIS II, VIS și EURODAC, Comisia trebuie să prezinte Parlamentului European și Consiliului rapoarte anuale sau bianuale privind funcționarea sau gradul de implementare al acestor sisteme. Instrumentele descentralizate de schimb de informații impun Comisiei să prezinte celorlalte instituții un singur raport de evaluare la câțiva ani de la implementare: Directiva privind păstrarea datelor, inițiativa suedeză și măsurile ARO trebuie evaluate în 2010; Decizia Prüm în 2012 și ECRIS în 2016. Cele trei acorduri PNR prevăd revizuiri periodice și *ad hoc*, iar două dintre ele includ și clauze privind încetarea de drept a efectelor juridice. Europol și Eurojust prezintă rapoarte anuale Consiliului, care le transmite pentru informare Parlamentului European. Aceste considerații sugerează faptul că structura actuală de gestionare a informațiilor în UE nu favorizează adoptarea unui singur mecanism de evaluare pentru toate instrumentele. Având în vedere această diversitate, este esențial ca viitoarea modificare a oricărui instrument din domeniul gestionării informațiilor să țină seama de eventualul său impact asupra tuturor celorlalte măsuri care reglementează colectarea, stocarea sau schimbul de date cu caracter personal în spațiul de libertate, securitate și justiție.

4. PRINCIPII DE DEZVOLTARE A POLITICILOR

Secțiunea 2 a descris mai multe inițiative pe care Comisia Europeană le-a aplicat, le-a prezentat sau le-a examinat în ultimii ani. Numărul mare de idei noi și cadrul legislativ în creștere în domeniul securității interne și al gestionării migrației fac necesară definirea unui set esențial de principii care să servească drept criterii de referință pentru inițierea și evaluarea unor propuneri de politici în anii următori. Aceste principii se întemeiază pe principiile generale prevăzute în tratatele UE, în jurisprudența Curții Europene de Justiție și a Curții Europene a Drepturilor Omului, precum și în acordurile interinstituționale relevante între Parlamentul European, Consiliu și Comisia Europeană și încearcă să le completeze pe acestea. Comisia propune să se dezvolte și să se implementeze noi inițiative și să se evalueze instrumentele actuale pe baza următoarelor două seturi de principii:

Principii esențiale

Garantarea drepturilor fundamentale, în special a dreptului la viață privată și la protecția datelor

Garantarea drepturilor fundamentale ale persoanelor astfel cum sunt consacrate în Carta drepturilor fundamentale a Uniunii Europene, în special a dreptului acestora la viață privată și la protecția datelor cu caracter personal, va fi o preocupare principală a Comisiei la elaborarea de noi propuneri care implică prelucrarea de date cu caracter personal în domeniul securității interne și a al gestionării migrației. Articolele 7 și 8 din cartă proclamă dreptul oricărei persoane la „respectarea vieții private și de familie" și la „protecția datelor cu caracter personal care o privesc"[83]. Articolul 16 din Tratatul privind funcționarea Uniunii Europene (TFUE), care are un caracter obligatoriu în ceea ce privește activitățile statelor membre, ale instituțiilor Uniunii, ale agențiilor și ale organismelor, reafirmă dreptul fiecărei persoane la „protecția datelor cu caracter personal care o privesc"[84]. La elaborarea de noi instrumente care se bazează pe utilizarea tehnologiei informațiilor, Comisia se va strădui să urmeze abordarea cunoscută sub sintagma „luarea în considerare a vieții private începând cu momentul conceperii". Aceasta înseamnă includerea protecției datelor cu caracter personal în baza tehnologică a unui instrument propus, limitând prelucrarea datelor la cele necesare pentru un scop propus și acordând accesul la date numai acelor entități care „trebuie să le cunoască[85]".

Necesitatea

Interferența unei autorități publice cu dreptul persoanelor la viață privată poate fi necesară în interesul securității naționale, siguranței publice sau al prevenirii criminalității[86]. Jurisprudența Curții Europene a Drepturilor Omului stabilește trei condiții în care pot fi justificate astfel de restricții: dacă sunt legale, dacă urmăresc un scop legitim și dacă sunt necesare într-o societate democratică. Interferența cu dreptul la viața privată este considerată necesară dacă răspunde unei nevoi sociale presante, dacă este proporțională cu scopul urmărit și dacă motivele prezentate de autoritatea publică pentru a o justifica sunt relevante și suficiente[87]. În toate propunerile viitoare de politici, Comisia va evalua impactul așteptat al inițiativei asupra dreptului persoanelor la viață privată și la protecția datelor cu caracter personal și va stabili de ce un astfel de impact este necesar și de ce soluția propusă este proporțională cu scopul legitim de menținere a securității interne pe teritoriul Uniunii Europene, de prevenire a criminalității și de gestionare a migrației. Respectarea normelor privind protecția datelor cu caracter personal va face, în toate cazurile, obiectul controlului de către o autoritate independentă la nivel național sau la nivelul UE.

---

83 Carta drepturilor fundamentale a Uniunii Europene (JO C 83, 30.3.2010, p. 389).

84 Versiunile consolidate ale Tratatului privind Uniunea Europeană și ale Tratatului privind funcționarea Uniunii Europene, JO C 83, 30.3.2010, p. 1.

85 Pentru o descriere cuprinzătoare a sintagmei de „luare în considerare a vieții private începând cu momentul conceperii", a se vedea Avizul Autorității europene pentru protecția datelor privind promovarea încrederii în societatea informațională prin favorizarea protecției datelor și a vieții private, Autoritatea europeană pentru protecția datelor, 18.3.2010.

86 A se vedea articolul 8, Convenția pentru Apărarea drepturilor omului și a libertăților fundamentale (ETS nr. 5), Consiliul Europei, 4.11.1950.

87 A se vedea *Marper/Regatul Unit*, hotărârea Curții Europene a Drepturilor Omului, Strasbourg, 4.12.2008.

Subsidiaritatea

Comisia se va strădui să își justifice noile propuneri prin prisma principiilor de subsidiaritate și de proporționalitate, în conformitate cu articolul 5 din Protocolul nr. 2 anexat la Tratatul privind Uniunea Europeană. Orice nouă propunere legislativă va conține o fișă care permite evaluarea respectării principiului subsidiarității, astfel cum se prevede la articolul 5 din Tratatul privind Uniunea Europeană. Fișa aceasta va cuprinde o evaluare a impactului financiar, economic și social al propunerii și, în cazul unei directive, a implicațiilor acesteia asupra normelor care urmează să fie puse în aplicare de statele membre[88]. Motivele care conduc la concluzia că un obiectiv al UE poate fi îndeplinit mai bine la nivelul UE se vor baza pe indicatori calitativi. Propunerile de acte legislative vor avea în vedere necesitatea de a proceda astfel încât orice obligație care revine UE, guvernelor naționale, autorităților regionale sau locale, agenților economici și cetățenilor să fie cât mai redusă posibil și proporțională cu obiectivul urmărit. În cazul unor propuneri care solicită noi acorduri internaționale, această fișă va analiza impactul așteptat al propunerii asupra relațiilor cu țările terțe respective.

Gestionarea exactă a riscurilor

Schimbul de informații în spațiul de libertate, securitate și justiție se face în general pentru a se analiza amenințările la adresa securității, pentru a se identifica tendințe în activitatea cu caracter infracțional sau pentru a se evalua riscurile în domenii de politică conexe[89]. Riscul este adesea, dar nu în mod necesar, legat de persoane al căror comportament în trecut sau al căror tip de comportament indică un risc continuu în viitor. Cu toate acestea, riscurile ar trebui să se bazeze pe dovezi și nu să fie ipotetice. Teste de necesitate și limitarea scopului sunt esențiale pentru orice măsură de gestionare a informațiilor. Dezvoltarea de profile de risc – a nu se confunda cu profilurile rasiale sau cu alte tipuri de profile discriminatorii, care sunt incompatibile cu drepturile fundamentale – este relevantă. Astfel de profile pot ajuta la concentrarea resurselor asupra anumitor persoane în scopul identificării amenințărilor la adresa securității și al protejării victimelor criminalității.

Principii orientate către proces[90]

Raport cost-eficacitate

Serviciile publice bazate pe tehnologia informațiilor ar trebui să permită furnizarea unor servicii mai bune și cu un raport mai bun calitate-preț pentru contribuabili. Având în vedere situația economică actuală, toate noile propuneri, în special atunci când se referă la înființarea sau modernizarea sistemelor de informații, vor avea ca scop obținerea celui mai bun raport cost-eficacitate. O astfel de abordare va ține cont de soluțiile deja existente pentru a minimiza suprapunerea și pentru a maximiza sinergiile posibile. Comisia va evalua dacă este posibilă îndeplinirea obiectivelor unei propuneri printr-o mai bună utilizare a instrumentelor existente.

---

88 Principiile de bază ale evaluărilor impactului sunt stabilite în Orientările privind evaluarea impactului [(SEC(2009)92, 15.1.2009).

89 Exemple practice de riscuri gestionate cu succes includ împiedicarea unei persoane expulzate care a comis o infracțiune gravă într-un stat membru să reintre în spațiul Schengen printr-un alt stat membru (SIS) sau împiedicarea unei persoane să ceară azil în mai multe state membre (EURODAC).

90 Aceste principii se bazează pe Concluziile Consiliului privind o strategie de gestionare a informațiilor pentru securitatea internă a UE, Consiliul Justiție și Afaceri Interne, 30.11.2009.

De asemenea, aceasta va lua în considerare adăugarea unor funcții auxiliare sistemelor informatice existente înainte de a propune sisteme noi.

Elaborare a politicilor în mod ascendent

Dezvoltarea unor noi inițiative trebuie, cât mai devreme posibil, să se bazeze pe contribuția tuturor părților interesate relevante, inclusiv autoritățile naționale responsabile pentru punerea în aplicare, actorii economici și societatea civilă. Elaborarea politicilor care iau în considerare interesele utilizatorilor finali necesită o gândire orizontală și o consultare la scară largă.[91] Din acest motiv, Comisia va încerca să stabilească o legătura permanentă cu funcționari din cadrul autorităților naționale și cu practicieni prin intermediul structurilor Consiliului, comitetelor de gestionare și formațiunilor ad-hoc.

Repartizare clară a responsabilităților

Având în vedere complexitatea tehnică a proiectelor privind colectarea și schimbul de informații în spațiul de libertate, securitate și justiție, trebuie acordată o atenție deosebită elaborării inițiale a structurilor de guvernare. Experiența de pe urma proiectului SIS II demonstrează că lipsa definirii de la bun început a unor obiective, roluri și responsabilități clare, stabile și cuprinzătoare poate duce la depășiri de costuri și întârzieri semnificative în punerea în aplicare. O evaluare timpurie a experienței de pe urma punerii în aplicare a Deciziei Prüm sugerează de asemenea că o structură de guvernanță descentralizată nu reprezintă un panaceu, deoarece statele membre nu au un conducător de proiect căruia să i se adreseze pentru consiliere cu privire la aspectele financiare sau tehnice ale punerii în aplicare. Viitoarea Agenție IT poate fi în măsură să furnizeze o astfel de consultanță tehnică responsabililor cu sistemele de informații în spațiul de libertate, securitate și justiție. Aceasta poate oferi, de asemenea, o platformă pentru o implicarea largă a părților interesate în gestionarea operațională și dezvoltarea sistemelor informatice. Ca măsură posibilă de prevenire a depășirii costurilor și a întârzierilor care rezultă din schimbarea cerințelor, orice nou sistem de informații în spațiul de libertate, securitate și justiție, în special în cazul în care implică un sistem informatic la scară largă, nu va fi dezvoltat înainte de adoptarea definitivă a instrumentelor juridice de referință care stabilesc scopul, domeniul de aplicare, funcțiile și detaliile tehnice ale sistemului.

Revizuire și clauze privind încetarea de drept a efectelor juridice

Comisia va evalua fiecare instrument cuprins în prezenta comunicare. Evaluarea se va face în raport cu întreaga gamă de instrumente care există în domeniul gestionării informațiilor. Aceasta ar trebui să ofere o imagine fiabilă a modului în care instrumentele individuale se încadrează în peisajul mai larg al securității interne și gestionării migrației. Viitoarele propuneri vor include, după caz, o obligație de raportare anuală, revizuiri periodice și ad-hoc, precum și o clauză privind încetarea de drept a efectelor juridice. Instrumentele existente vor fi menținute doar dacă continuă să servească scopului legitim pentru care au fost proiectate. Anexa II stabilește data revizuirii și mecanismul pentru fiecare instrument cuprins în prezenta comunicare.

---

[91] Principiile generale și standardele minime privind consultarea publică sunt stabilite în COM (2002) 704, 11.12.2002.

5. CALEA DE URMAT

Această comunicare oferă, pentru prima dată, un rezumat clar și cuprinzător al măsurilor instituite la nivelul UE, în vigoare sau în curs de examinare, care reglementează aspectele legate de colectarea, stocarea și schimbul transfrontalier de informații cu caracter personal în scopul aplicării legislației și al gestionării migrației.

Comunicarea oferă cetățenilor o imagine de ansamblu asupra tipului de informații referitoare la aceștia care sunt colectate, stocate și schimbate, asupra scopului acestor acțiuni și asupra celor care fac acest lucru. Aceasta reprezintă un instrument de referință transparent pentru părțile interesate care doresc să se angajeze în dezbaterea cu privire la direcția pe care o va urma politica UE în acest domeniu. În același timp, oferă un prim răspuns la apelul lansat de Consiliul European în vederea dezvoltării instrumentelor de gestionare a informațiilor la nivelul UE, în conformitate cu Strategia UE de gestionare a informațiilor[92] și în vederea angajării într-un proces de reflecție privind necesitatea unui model european de schimb de informații[93].

Comisia își propune ca, în urma acestei comunicări, să prezinte o comunicare privind modelul european de schimb de informații în 2012[94]. În acest scop, Comisia a lansat în ianuarie 2010 un exercițiu de „cartografiere a informațiilor" cu privire la bazele juridice și funcționarea practică a schimbului între statele membre de informații și date operative în materie penală, ale cărui rezultate Comisia își propune să le prezinte Consiliului și Parlamentului European în 2011[95].

În final, prezenta comunicare stabilește pentru prima dată viziunea Comisiei privind principiile generale pe care aceasta intenționează să le urmeze în dezvoltarea viitoare a instrumentelor de colectare, stocare sau schimb de date. Aceste principii vor fi de asemenea utilizate la evaluarea instrumentelor existente. Adoptarea unei astfel de abordări principiale privind dezvoltarea și evaluarea politicilor poate spori coerența și eficiența instrumentelor actuale și viitoare astfel încât să fie pe deplin respectate drepturile fundamentale ale cetățenilor.

---

92 Concluziile Consiliului privind o strategie de gestionare a informațiilor pentru securitatea internă a UE, Consiliul Justiție și Afaceri Interne, 30.11.2009 (Strategia UE de gestionare a informațiilor).

93 Programul de la Stockholm — O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora, Documentul 5731/10 al Consiliului, 3.3.2010, secțiunea 4.2.2.

94 Acest lucru este indicat în Planul de acțiune al Comisiei pentru punerea în aplicare a Programului de la Stockholm [COM(2010)171, 20.4.2010].

95 Acest exercițiu de cartografiere a informațiilor se desfășoară în strânsă cooperare cu o echipă de lucru responsabilă cu cartografierea informațiilor formată din reprezentanți ai UE și ai statelor membre AELS, Europol, Eurojust, Frontex și Autoritatea europeană pentru protecția datelor.

ANEXA I

Următoarele date şi exemple au scopul de a ilustra funcţionarea în practică a măsurilor de gestionare a informaţiilor utilizate în prezent.

Sistemul de Informaţii Schengen (SIS)

Numărul total de semnalări SIS introduse în baza de date centrală a SIS (C.SIS)[96]			
Categorii de semnalări	**2007**	**2008**	**2009**
Bancnote	177 327	168 982	134 255
Documente în alb	390 306	360 349	341 675
Arme de foc	314 897	332 028	348 353
Documente eliberate	17 876 227	22 216 158	25 685 572
Vehicule	3 012 856	3 618 199	3 889 098
Persoane căutate (pseudonime)	299 473	296 815	290 452
Persoane căutate (nume principal)	859 300	927 318	929 546
din care:			
Persoane căutate pentru arestare în vederea extrădării	19 119	24 560	28 666
Resortisanţi din ţările terţe aflaţi pe lista persoanelor cu interdicţie de intrare	696 419	746 994	736 868
Persoane adulte dispărute	24 594	23 931	26 707
Persoane minore dispărute	22 907	24 628	25 612
Martori sau persoane convocate să compară în faţa unei instanţe	64 684	72 958	78 869
Persoane supuse unei monitorizări excepţionale pentru prevenirea ameninţărilor la adresa securităţii publice	31 568	34 149	32 571
Persoane supuse unei monitorizări excepţionale pentru prevenirea ameninţărilor la adresa securităţii naţionale	9	98	253
Total	**22 933 370**	**27 919 849**	**31 618 951**

[96] Documentul Consiliului 6162/10, 5.2.2010; Documentul Consiliului 5764/09, 28.1.2009; Documentul Consiliului 5441/08, 30.1.2008.

EURODAC – Circulația solicitanților de azil care au depus cereri noi în același stat membru sau în alte state membre (2008)

Numărul de cazuri în care statele membre au trimis amprente în vederea comparării și au obținut rezultate pozitive de la statele membre (în coloane) în care o persoană a depus anterior o cerere de azil	Statul membru în care a fost depusă prima cerere de azil[97]																													Total cereri depuse a doua oară	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	Rezultate naționale	Total rezultate
AT	1 725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1 371	1	42	111	17	260	61	**1 725**	**4 694**
BE	180	5 450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5 450**	**8 129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1 852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1 852**	**4 718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1 341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1 759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1 739	8	9	286	37	75	190	**860**	**5 497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1 717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3 290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3 290**	**6 263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1 240	95	16	8	9	289	8	22	129	**1 240**	**3 017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3 078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1 208	1	1	43	1	13	4	**1 208**	**1 760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1 914	11	26	122	**1 914**	**4 882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3 141	**3 141**	**5 607**
Total prime cereri	**4 407**	**7 298**	**245**	**4**	**125**	**1 155**	**5 487**	**589**	**4**	**2 067**	**480**	**773**	**2 734**	**1 670**	**663**	**15**	**6 600**	**46**	**204**	**5**	**542**	**2 363**	**1 833**	**5 581**	**55**	**313**	**5 791**	**283**	**1 082**	**5 475**	**24 433**	**57 889**

97 COM(2009) 494, 25.9.2009. „Rezultate naționale” se referă la depunerea unei noi cereri de azil în statul membru în care a fost depusă cererea anterioară.

Sistemul de informații prealabile privind pasagerii (API)

Utilizarea de către Regatul Unit a informațiilor prealabile privind pasagerii în vederea îmbunătățirii controlului la frontiere și a combaterii migrației ilegale[98]	
Numărul de acțiuni întreprinse în 2009	
Antecedente defavorabile (intrări refuzate persoanei)	379
Pașapoarte pierdute, furate sau anulate (documente confiscate)	56

[98] UK Border Agency (Agenția britanică pentru gestionarea frontierelor) a furnizat aceste informații Comisiei în scopul prezentei comunicări.

Sistemul de informații al vămilor (CIS)

Numărul total de cazuri introduse în baza de date CIS (2009)[99]	
Acțiune	**CIS (pe baza convenției privind CIS)**
Cazuri deschise	2 007
Cazuri în curs	274
Cazuri contestate	11 920
Cazuri anulate	1 355

[99] Aceste informații au fost furnizate de Comisie.

Inițiativa suedeză

Exemple ale utilizării inițiativei suedeze în anchetarea infracțiunilor[100]	
Omucidere	În 2009, într-o capitală a unui stat membru, a avut loc o tentativă de omucidere. Poliția a colectat o probă biologică de pe o sticlă din care a băut suspectul. Prin extragerea ADN-ului de pe acest eșantion, specialiștii în medicină legală au generat un profil ADN. O comparare a acestui profil cu alte profiluri de referință din baza națională de date ADN nu a generat nicio corespondență. Prin urmare, organele de anchetă au trimis, prin intermediul punctului de contact Prüm o cerere pentru compararea profilului cu profilurile ADN de referință deținute de celelalte state membre care au fost autorizate să facă schimb de astfel de date pe baza Deciziei Prüm sau a Acordului de la Prüm. Această comparație transfrontalieră a produs un „rezultat”. Pe baza inițiativei suedeze, organele de anchetă au solicitat date suplimentare cu privire la suspect. Punctul de contact național al acestora a primit un răspuns din partea mai multor alte state membre în termen de 36 de ore, ceea ce a permis poliției să identifice suspectul.
Viol	În 2003, un suspect neidentificat a violat o femeie. Poliția a colectat probe de la victimă, însă profilul ADN generat pe baza acestor probe nu a corespuns niciunui profil de referință din baza națională de date ADN. O cerere privind compararea ADN-ului, trimisă de punctul de contact Prüm celorlalte state membre care au fost autorizate să facă schimb de profiluri ADN de referință pe baza Deciziei Prüm sau a Acordului de la Prüm, a produs un „rezultat”. Organele de anchetă au solicitat apoi informații suplimentare privind suspectul în cadrul inițiativei suedeze. Punctul de contact național al acestora a primit un răspuns în termen de 8 ore, ceea ce a permis poliției să identifice suspectul.

[100] Aceste exemple au fost oferite Comisiei de către forțele de poliție ale unui stat membru în scopul prezentei comunicări.

Rezultate obținute de Germania în cadrul comparației transfrontaliere a profilurilor ADN, în funcție de tipul infracțiunii (2009)[101]

Rezultate în funcție de tipul infracțiunii	**Austria**	**Spania**	**Luxemburg**	**Țările de Jos**	**Slovenia**
Infracțiuni care aduc atingere unor activități de interes public	32	4	0	5	2
Infracțiuni contra libertății persoanei	9	3	5	2	0
Infracțiuni privitoare la viața sexuală	40	22	0	31	4
Infracțiuni contra persoanei	49	24	0	15	2
Alte infracțiuni	3 005	712	18	1 105	71

[101] Răspunsul Guvernului german la întrebarea parlamentară înaintată de Ulla Jelpke, Inge Höger și Jan Korte (cu nr. de referință 16/14120), Bundestag, sesiunea 16, nr. de referință 16/14150, 22.10.2009. Aceste cifre se referă la perioada care începe cu demararea unui schimb de date între un stat membru și Germania, care se încheie la 30 septembrie 2009.

Exemple privind detectarea de către statele membre a cazurilor de infracțiuni grave prin intermediul păstrării datelor[102]	
Omor	Autoritățile polițienești ale unui stat membru au reușit să identifice un grup de criminali responsabili pentru uciderea motivată rasial a șase persoane. Autorii au încercat să se sustragă urmăririi prin schimbarea cartelor SIM, însă listele acestora cu numerele formate și elementele de identificare a echipamentelor mobile i-au dat de gol.
Omucidere	O autoritate polițienească a fost în măsură să dovedească implicarea a doi suspecți într-un caz de omucidere prin analizarea datelor de trafic de pe telefonul mobil al victimei. Acest lucru a permis detectivilor să reconstituie traseul pe care victima și cei doi suspecți au călătorit împreună.
Tâlhărie	Autoritățile au depistat un infractor responsabil pentru 17 tâlhării prin studierea datelor de trafic de pe cartela SIM preplătită anonimă a acestuia. Prin identificarea partenerei sale, autoritățile au reușit de asemenea să localizeze infractorul.
Fraudă	Anchetatorii au descoperit o înșelătorie în care o grupare criminală care făcea publicitate pe internet pentru vânzarea unor automobile scumpe „contra numerar” jefuia sistematic pe cei veneau să intre în posesia vehiculelor cumpărate. O adresa IP a permis poliției să localizeze abonatul și să aresteze infractorii.

[102] Aceste exemple anonime se bazează pe răspunsurile statelor membre la un chestionar al Comisiei din 2009 privind transpunerea Directivei 2006/24/CE (Directiva privind păstrarea datelor).

Cooperarea între unitățile de informații financiare (FIU)

Numărul total de cereri de informații formulate de FIU naționale prin intermediul FIU.net[103]		
Anul	**Cereri de informații**	**Utilizatori activi**
2007	3 133	12 state membre
2008	3 084	13 state membre
2009	3 520	18 state membre

[103] Oficiul FIU.net a furnizat aceste informații Comisiei în scopul prezentei comunicări.

Cooperarea între oficiile de recuperare a creanțelor (ARO)

Cereri privind depistarea activelor, formulate de statele membre și tratate de Europol[104]				
Anul	**2004**	**2005**	**2006**	**2007**
Cereri	5	57	53	133
din care:				
Cazuri legate de fraudă				29
Cazuri legate de spălarea banilor				26
Cazuri legate de droguri				25
Cazuri legate de alte infracțiuni				18
Cazuri legate de droguri și spălarea banilor				19
Cazuri legate de fraudă și spălarea banilor				7
Cazuri legate de o diversitate de infracțiuni				9

Cazuri de confiscare a activelor tratate de Eurojust (2006-2007)[105]			
Tipuri de cazuri		**Cazuri inițiate de**	
Cazuri legate de infracțiuni împotriva mediului	1	Germania	27%
Cazuri legate de participarea la o organizație criminală	5	Țările de Jos	21%
Cazuri legate de traficul de droguri	15	Regatul Unit	15%
Cazuri legate de frauda fiscală	8	Finlanda	13%
Cazuri legate de fraudă	8	Franța	8%
Cazuri legate de frauda în materie de TVA	1	Spania	6%
Cazuri legate de spălarea banilor	9	Portugalia	4%
Cazuri legate de corupție	1	Suedia	2%
Cazuri legate de infracțiuni contra proprietății	2	Danemarca	2%
Cazuri legate de traficul de arme	1	Letonia	2%
Cazuri legate de contrafacerea și piratarea produselor	2		
Cazuri legate de frauda privind plățile în avans	2		
Cazuri legate de falsificarea documentelor administrative	1		
Cazuri privind criminalitatea legată de autovehicule	1		
Cazuri legate de terorism	1		
Cazuri legate de falsificare	2		
Cazuri legate de traficul de ființe umane	1		

104 Evaluarea eficienței practicilor din statele membre ale UE privind identificarea, urmărirea, înghețarea și confiscarea activelor de origine criminală – raport final (destinat Comisiei Europene, DG JLS), Matrix Insight, 6.2009.

105 Ibid.

Platforme de alertă privind criminalitatea informatică

Exemple ale unor cazuri de criminalitate informatică investigate de platforma franceză de alertă privind criminalitatea informatică, Pharos[106]	
Pornografie infantilă	Un utilizator de internet a alertat Pharos cu privire la existența unui blog care conținea fotografii și imagini de tip desen animat redând imagini ale unor abuzuri sexuale asupra copiilor. De asemenea, redactorul blogului, care apare nud într-o fotografie, atrăgea copii pe blogul său. Anchetatorii au identificat ca principal suspect un profesor de matematică. O percheziție efectuată la locuința acestuia a scos la iveală aproximativ 49 de videoclipuri care conțineau imagini de pornografie infantilă. De asemenea, investigația a dezvăluit că acesta a făcut pregătirile necesare în vederea organizării unor meditații la domiciliu. Inculpatul a fost condamnat ulterior și a primit o pedeapsă cu închisoarea cu suspendare.
Abuzuri sexuale asupra copiilor	Poliția franceză a primit informații cu privire la un individ care oferea bani pe internet în schimbul unor relații sexuale cu copii. Un detectiv din cadrul Pharos, dându-se drept minor, a luat legătura cu suspectul, care i-a oferit bani în schimbul unor relații sexuale. Convorbirile ulterioare pe internet au permis Pharos să identifice adresa IP a suspectului, acesta fiind localizat într-un oraș cunoscut pentru incidența ridicată de abuzuri sexuale asupra copiilor. Inculpatul a fost condamnat ulterior și a primit o pedeapsă cu închisoarea cu suspendare.

[106] Pharos înseamnă „plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements".

Europol

Exemple privind contribuția Europol în lupta împotriva criminalității grave transfrontaliere[107]	
Operațiunea Andromeda	În decembrie 2009, Europol a contribuit la desfășurarea unei operațiuni polițienești transfrontaliere de mare amploare împotriva unei rețele de traficanți de droguri având contacte în 42 de țări. Această rețea avea sediul în Belgia și Norvegia și trafica droguri din Peru, prin Țările de Jos, în Belgia, Marea Britanie, Italia și alte state membre. Cooperarea polițienească a fost coordonată de Europol, iar cooperare judiciară de către Eurojust. Autoritățile participante au înființat un birou mobil în Pisa, iar Europol un centru operațional la Haga. Europol a efectuat corelări între informațiile privind suspecții și a produs un raport în care era descrisă rețeaua infracțională.
Participanți	Italia, Țările de Jos, Germania, Belgia, Marea Britanie, Lituania, Norvegia și Eurojust.
Rezultate	Forțele de poliție participante au confiscat 49 kg de cocaină, 10 kg de heroină, 6 000 de pastile de Ecstasy, două arme de foc, cinci documente de identitate false și 43 000 EUR în numerar și au arestat 15 persoane.
Operațiunea Typhon	În perioada aprilie 2008 - februarie 2010, Europol a furnizat suport analitic forțelor de poliție din 20 de țări implicate în operațiunea Typhon. În cadrul acestei operațiuni de mare amploare împotriva unei rețele de pedofili care distribuia imagini de pornografie infantilă prin intermediul unui site internet austriac, Europol a furnizat suport tehnic și a efectuat analize ale datelor operative în materie penală pe baza imaginilor primite de la autoritățile austriece. Ulterior, a evaluat fiabilitatea datelor și le-a restructurat înainte de a pregăti propriile materiale de informații. Prin corelarea datelor cu informațiile conținute în fișierul de lucru pentru analiză al Europol, au fost elaborate 30 de rapoarte de informații pe baza cărora au fost demarate investigații în mai multe țări.
Participanți	Austria, Belgia, Bulgaria, Canada, Danemarca, Franța, Germania, Ungaria, Italia, Lituania, Luxemburg, Malta, Țările de Jos, Polonia, România, Slovacia, Slovenia, Spania, Elveția și Regatul Unit.
Rezultate	Forțele de poliție participante au identificat 286 de suspecți, din care au arestat 118 suspecți și au salvat cinci victime în patru țări, care au suferit abuzuri în acest caz.

[107] Europol a furnizat aceste informații Comisiei în scopul prezentei comunicări. Informații suplimentare cu privire la operațiunea Andromeda sunt disponibile la http://www.eurojust.europa.eu/.

Exemple privind coordonarea de către Eurojust a unor operațiuni judiciare transfrontaliere de mare amploare împotriva criminalității grave[108]	
Trafic de ființe umane și finanțarea terorismului	În mai 2010, Eurojust a coordonat o operațiune transfrontalieră care a dus la arestarea a cinci membri ai unei rețele de criminalitate organizată activă în Afganistan, Pakistan, România, Albania și Italia. Grupul furniza documente falsificate unor cetățeni afgani și pakistanezi pe care îi ajuta să ajungă în mod fraudulos în Italia, prin Iran, Turcia și Grecia. La sosirea în Italia, imigranții erau trimiși în Germania, Suedia, Belgia, Marea Britanie și Norvegia. Fondurile obținute de pe urma traficului erau destinate finanțării terorismului.
Fraudă cu carduri bancare	Prin coordonarea cooperării polițienești și judiciare transfrontaliere, Europol și Eurojust au contribuit la lichidarea unei rețele având ca obiect frauda cu carduri bancare, activă în Irlanda, Italia, Țările de Jos, Belgia și România. Această rețea a furat datele de identificare ale aproximativ 15 000 de carduri de plată, provocând o pierdere de 6,5 milioane EUR. Anterior acestei operațiuni care a condus la efectuarea a 24 de arestări în iulie 2009, magistrații belgieni, irlandezi, italieni, olandezi și români au facilitat emiterea unor mandate europene de arestare și a unor cereri privind interceptarea convorbirilor telefonice ale suspecților.
Trafic de ființe umane și de droguri	În urma unei reuniuni de coordonare organizate de Eurojust în martie 2009, autoritățile italiene, olandeze și columbiene au arestat 62 de persoane suspectate de trafic de ființe umane și de droguri. Rețeaua era specializată în traficul de femei vulnerabile din Nigeria către Țările de Jos, acestea fiind forțate să se prostitueze în Italia, Franța și Spania. Fondurile obținute din prostituție erau folosite pentru finanțarea achiziționării de către rețea de cocaină din Columbia, care era expediată în UE pentru consum.

[108] Aceste exemple au fost preluate de pe site-ul internet http://www.eurojust.europa.eu/.

Exemple de analize PNR care au permis obținerea de informații în vederea anchetării criminalității grave transfrontaliere[109]	
Trafic de copii	Analiza PNR a arătat că trei copii neînsoțiți călătoreau dintr-un stat membru al UE către o țară terță, fără indicarea celor care urmau să-i întâmpine la sosire. Alertate de către autoritățile polițienești din statul membru după plecarea copiilor, autoritățile din țara terță au arestat persoana care a venit să-i întâmpine: o persoană condamnată pentru abuzuri sexuale, înregistrată în statul membru.
Trafic de ființe umane	Analiza PNR a permis demascarea unui grup de traficanți de ființe umane care călătoreau întotdeauna pe aceeași rută. Aceștia foloseau documente false pentru a se îmbarca pe un zbor intra-UE și, simultan, foloseau documente autentice pentru a se îmbarca pe un zbor către o țară terță. Odată ajunși în sala de așteptare a aeroportului, traficanții se îmbarcau pe zborul intra-UE.
Fraudă cu carduri de credit	Mai multe familii au călătorit către un stat membru cu bilete cumpărate cu carduri de credit furate. Cercetările au arătat că un grup infracțional a folosit aceste carduri pentru cumpărarea biletelor pe care ulterior le vindea în mod ilegal în cadrul unor centre pentru apeluri internaționale. Datele PNR au fost cele care au permis efectuarea legăturii între călători, cardurile de credit și vânzători.
Trafic de droguri	Autoritățile polițienești ale unui stat membru dețineau informații care sugerau că un bărbat era implicat în traficul de droguri dintr-o țară terță, însă polițiștii de frontieră nu a găsit nimic asupra acestuia la sosirea în UE. Analiza PNR a arătat că bărbatul călătorea întotdeauna împreună cu un asociat. O percheziționare a asociatului a dus la descoperirea unei mari cantități de droguri.

[109] Aceste exemple au fost furnizate în mod anonim în vederea protejării surselor din care provin informațiile.

Programul de urmărire a finanțărilor în scopuri teroriste (TFTP)

Exemple de cazuri în care TFTP a permis obținerea de informații în vederea anchetării unor comploturi teroriste[110]	
Complotul terorist de la Barcelona din 2008	În ianuarie 2008, zece suspecți au fost arestați la Barcelona în legătură cu o tentativă dejucată de a organiza un atac asupra sistemului public de transport al orașului. Au fost folosite date TFTP pentru identificarea legăturilor suspecților cu Asia, Africa și America de Nord.
Complotul privind organizarea unor atentate cu explozibili lichizi pe zboruri transatlantice în 2006	Informațiile TFTP au fost folosite pentru anchetarea și condamnarea indivizilor implicați într-o tentativă dejucată de a arunca în aer, în august 2006, zece zboruri transatlantice cu destinația SUA și Canada care plecau din Marea Britanie.
Atentatele cu bombă de la Londra din 2005	Datele TFTP au fost utilizate pentru a oferi noi piste anchetatorilor, pentru a confirma identitatea suspecților și pentru a dezvălui relațiile dintre persoanele responsabile de aceste atentate.
Atentatele cu bombă de la Madrid din 2004	Datele TFTP au fost furnizate mai multor state membre ale UE pentru a le sprijini în investigațiile lansate în urma acestui atac.

110 Al doilea raport privind prelucrarea de către Departamentul de Trezorerie al Statelor Unite a datelor cu caracter personal provenite din UE pentru investigațiile în materie de combatere a terorismului, judecătorul Jean-Louis Bruguière, ianuarie 2010.

ANEXA II

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Sistemul de Informații Schengen (SIS)	Inițiat de statele membre.	Menținerea securității publice, inclusiv securitatea națională, în spațiul Schengen și facilitarea circulației persoanelor utilizând informații comunicate prin intermediul acestui sistem.	Centralizată: N.SIS (componentele naționale) conectate prin interfață la C.SIS (componenta centrală).	Numele și pseudonimele, trăsăturile fizice, locul și data nașterii, cetățenia și mențiunea dacă persoana este înarmată și violentă. Semnalările SIS privesc diferite grupuri de persoane.	Poliția, autoritățile de frontieră, autoritățile vamale și judiciare au acces la toate datele; autoritățile de imigrație și oficiile consulare au acces la lista persoanelor cu interdicție de intrare și semnalările cu privire la documentele pierdute și furate. Europol și Eurojust pot accesa doar anumite date.	Convenția 108 a Consiliului Europei și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	Datele cu caracter personal introduse în SIS în scopul localizării persoanelor urmărite pot fi păstrate numai atâta timp cât este necesar pentru atingerea scopului pentru care au fost furnizate și cel mult trei ani. Datele cu privire la persoanele care fac obiectul monitorizării excepționale ca urmare a riscului pe care îl reprezintă pentru securitatea națională sau publică trebuie șterse după un an.	SIS se aplică integral în 22 de state membre, precum și în Elveția, Norvegia și Islanda. Regatul Unit și Irlanda participă la SIS cu excepția semnalărilor legate de resortisanții țărilor terțe incluși pe lista persoanelor cu interdicție de intrare. Se așteaptă ca Bulgaria, România și Liechtenstein să pună în aplicare această măsură în curând.	Semnatarii pot propune modificări ale Convenției Schengen. Textul modificat va trebui adoptat în unanimitate și ratificat de parlamente.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Sistemul de Informații Schengen II (SIS II)	Inițiat de Comisie.	Asigurarea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție, precum și facilitarea circulației persoanelor utilizând informațiile comunicate prin intermediul acestui sistem.	Centralizată: N.SIS II (componentele naționale) conectate prin interfață la C.SIS (componenta centrală). SIS II va opera pe rețeaua securizată s-TESTA.	Categoriile de date din SIS, împreună cu amprente și fotografii, copii ale mandatului european de arestare, semnalări privind uzurparea identității și legăturile între diferitele semnalări. Semnalările SIS II privesc diferite grupuri de persoane.	Poliția, autoritățile de frontieră, autoritățile vamale și judiciare vor avea acces la toate datele; autoritățile de imigrație și oficiile consulare au acces la lista persoanelor cu interdicție de intrare și semnalările cu privire la documentele pierdute și furate. Europol și Eurojust vor putea accesa doar anumite date.	Normele specifice cuprinse în actele legislative de bază care reglementează SIS II, precum și în Directiva 95/46/CE, Regulamentul (CE) nr. 45/2001, Decizia-cadru 2008/977/JAI a Consiliului, Convenția 108 a Consiliului Europei și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	Datele cu caracter personal introduse în SIS în scopul localizării persoanelor urmărite pot fi păstrate numai atâta timp cât este necesar pentru atingerea scopului pentru care au fost furnizate și cel mult trei ani. Datele cu privire la persoanele care fac obiectul monitorizării excepționale ca urmare a riscului pe care îl reprezintă pentru securitatea națională sau publică trebuie șterse după un an.	SIS II este în curs de aplicare. De îndată ce va fi operațional, acest sistem se va aplica în UE-27, Elveția, Liechtenstein, Norvegia și Islanda. Regatul Unit și Irlanda vor participa la SIS II cu excepția semnalărilor legate de resortisanții țărilor terțe incluși pe lista persoanelor cu interdicție de intrare.	Comisia trebuie să prezinte Parlamentului European (PE) și Consiliului un raport bianual privind progresele înregistrate cu privire la dezvoltarea SIS II și posibila migrare de la SIS.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
EURODAC	Inițiat de Comisie.	Oferirea de asistență în vederea stabilirii statului membru care ar trebui să fie responsabil de examinarea unei anumite cereri de azil.	Centralizată, constând din puncte naționale de acces conectate printr-o interfață la unitatea centrală a EURODAC. EURODAC funcționează pe rețeaua s-TESTA.	Date privind amprentele, sexul, locul și data depunerii cererii de azil, numărul de referință folosit de statul membru de origine, data luării amprentelor, a transmiterii și înregistrării acestora în sistem.	Statele membre trebuie să indice lista autorităților care au acces la aceste date, care de obicei cuprinde autoritățile cu responsabilități în domeniul azilului și migrației, polițiștii de frontieră și poliția.	Directiva 95/46/CE.	10 ani în cazul amprentelor solicitanților de azil; 2 ani în cazul resortisanților țărilor terțe care au fost reținuți pentru trecerea ilegală a frontierei externe.	Regulamentul EURODAC este în vigoare în fiecare stat membru, precum și în Norvegia, Islanda și Elveția. Este în curs de încheiere un acord care să permită conectarea Principatului Liechtenstein la rețea.	Comisia trebuie să prezinte Parlamentului European și Consiliului un raport anual privind funcționarea unității centrale a EURODAC.
Sistem de Informații privind Vizele (VIS)	Inițiat de Comisie.	Contribuția la punerea în aplicare a unei politici comune în materie de vize și la prevenirea amenințărilor la adresa securității interne.	Centralizată, constând din componente naționale care vor fi conectate printr-o interfață la componenta centrală. VIS va funcționa pe rețeaua s-TESTA.	Cereri de viză, fotografii, amprente digitale, deciziile aferente în materie de vize și legăturile între aplicațiile conexe.	Autoritățile în materie de vize, azil, imigrație și control al frontierelor vor avea acces la toate datele. Poliția și Europol pot consulta VIS în scopul prevenirii, depistării și cercetării formelor de criminalitate gravă.	Normele specifice stabilite prin actele legislative de bază care reglementează VIS, precum și prin Directiva 95/46/CE, Regulamentul (CE) nr. 45/2001, Decizia-cadru 2008/977/JAI a Consiliului, Convenția 108 a Consiliului Europei, Protocolului adițional 181 la aceasta și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	5 ani.	VIS este în curs de aplicare și se va aplica în fiecare stat membru (cu excepția Regatului Unit și Irlandei), precum și în Norvegia, Islanda și Elveția.	Comisia trebuie să prezinte Parlamentului European și Consiliului un raport privind funcționarea VIS la trei ani după lansarea acestuia și ulterior la fiecare patru ani.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Sistemul de informații prealabile privind pasagerii (API)	Inițiat de Spania.	Îmbunătățirea controlului la frontiere și combaterea migrației ilegale.	Descentralizată.	Date cu caracter personal colectate din pașapoarte, de la punctul de îmbarcare și punctul de intrare pe teritoriul UE.	Autoritățile de control la frontiere și, la cerere, autoritățile de aplicare a legii.	Directiva 95/46/CE.	Datele trebuie șterse după 24 de ore de la sosirea unui zbor în UE.	API este în vigoare în toate statele membre, însă este utilizat doar de câteva din acestea.	Comisia va face o evaluare a sistemului API în 2011.
Convenția Napoli II	Inițiată de statele membre.	Sprijinirea administrațiilor vamale naționale în prevenirea și identificarea încălcării dispozițiilor vamale naționale și în trimiterea în instanță și sancționarea cazurilor de încălcare a dispozițiilor vamale comunitare și naționale.	Descentralizată, funcționând prin intermediul unei serii de unități centrale de coordonare.	Orice informații privind o persoană identificată sau identificabilă.	Unitățile centrale de coordonare transmit datele autorităților vamale naționale, autorităților de cercetare și organismelor judiciare și, sub rezerva acordului prealabil al statului membru care furnizează datele, altor autorități.	Directiva 95/46/CE și Convenția 108 a Consiliului Europei. În statul membru destinatar, datele trebuie să beneficieze cel puțin de același nivel de protecție ca și în statul membru care le-a furnizat.	Datele pot fi păstrate pentru o perioadă care nu depășește ceea ce este necesar pentru scopul în care au fost furnizate.	Convenția Napoli II a fost ratificată de toate statele membre.	Semnatarii pot propune modificări ale Convenției Napoli II. Textul modificat va trebui adoptat de Consiliu și ratificat de statele membre.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Sistemul de informații al vămilor (CIS)	Inițiat de statele membre.	Sprijinirea autorităților competente în prevenirea, anchetarea și aducerea în instanță a cazurilor grave de încălcare a legislației vamale naționale.	Centralizat, accesibil prin intermediul terminalelor în fiecare stat membru și în incinta Comisiei. CIS și FIDE funcționează pe baza AFIS care utilizează rețeaua comună de comunicație, interfața comună a sistemelor sau accesul internet securizat furnizat de Comisie.	Numele și pseudonimele, data și locul nașterii, cetățenia, sexul, trăsături fizice, documente de identitate, adresa, antecedente de violență, motivul pentru introducerea datelor în CIS, acțiunea sugerată și înregistrarea mijloacelor de transport.	Datele CIS pot fi accesate de către autoritățile naționale vamale, Europol și Eurojust.	Normele specifice stabilite prin Convenția CIS și prin Directiva 95/46/CE, Regulamentul (CE) nr. 45/2001, Convenția 108 a Consiliului Europei, și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	Datele cu caracter personal copiate din CIS pe alte sisteme de prelucrare a datelor în vederea analizelor operaționale sau de gestionare a riscului nu pot fi păstrate decât pentru durata necesară realizării scopului în care au fost copiate și pentru cel mult 10 ani.	Sistemul este în vigoare în toate statele membre.	Comisia, în cooperare cu statele membre, prezintă în fiecare an un raport Parlamentului European și Consiliului cu privire la funcționarea CIS.
Inițiativa suedeză	Inițiată de Suedia.	Simplificarea schimbului de informații necesare în vederea anchetelor penale și a operațiunilor de colectare a datelor operative în materie penală.	Descentralizată; statele membre trebuie să desemneze punctele naționale de contact pentru tratarea cererilor urgente de informații.	Orice informații sau date operative în materie penală existente, disponibile autorităților de aplicare a legii.	Poliție, autorități vamale și orice alte autorități cu competențe de anchetare a infracțiunilor (cu excepția serviciilor de informații).	Normele naționale în materie de protecție a datelor, precum și Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	Informațiile și datele operative furnizate prin intermediul acestui instrument nu vor fi folosite decât pentru scopul în care au fost furnizate și cu respectarea condițiilor specifice stabilite de statul membru care le furnizează.	12 din cei 31 de semnatari (state membre ale UE și AELS) au adoptat legi naționale în vederea punerii în aplicare a acestui instrument; cinci state completează formularul de solicitare de informații, iar două state îl folosesc în mod frecvent pentru schimbul de informații.	Comisia urmează să prezinte Consiliului un raport de evaluare în 2010.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Decizia Prüm	Inițiată de statele membre.	Consolidarea prevenirii infracțiunilor, în special a terorismului, și menținerea ordinii publice.	Descentralizată, interconectată prin intermediul rețelei s-TESTA. Punctele naționale de contact tratează cererile primite și trimise pentru compararea datelor.	Profiluri ADN anonime și amprente digitale, date de înmatriculare a autovehiculelor și informații cu privire la persoanele suspectate de legături teroriste.	Punctele naționale de contact transmit cererile; accesul pe plan național este reglementat de legislația națională.	Normele specifice stabilite prin Decizia Prüm, precum și prin Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc. Persoanele fizice se pot adresa autorităților naționale responsabile de protecția datelor pentru asigurarea aplicării drepturilor lor cu privire la prelucrarea datelor cu caracter personal.	Datele cu caracter personal trebuie șterse atunci când nu mai sunt necesare pentru scopul pentru care au fost furnizate. Termenul maxim de păstrare a datelor la nivel național în statul care le-a furnizat are caracter obligatoriu pentru statul care le primește.	Decizia Prüm este în curs de aplicare. Zece state membre au primit autorizația de a face schimb de profiluri ADN, cinci state membre de a face schimb de amprente digitale, iar șapte state de date de înmatriculare a vehiculelor. Norvegia și Islanda sunt pe punctul de a adera la acest instrument.	Comisia urmează să prezinte Consiliului un raport de evaluare în 2012.
Directiva privind păstrarea datelor	Inițiată de statele membre.	Consolidarea anchetării, depistării și urmăririi penale a criminalității grave prin păstrarea datelor de trafic și localizare ale telecomunicațiilor.	Descentralizată; acest instrument prevede obligația ca furnizorii de servicii de telecomunicații să păstreze datele.	Număr de telefon, adresă IP și elemente de identificare ale echipamentelor mobile.	Autoritățile cu drept de acces sunt definite la nivel național.	Directiva 95/46/CE și Directiva 2002/58/CE.	Între 6 și 24 de luni.	Șase state membre nu au transpus încă această directivă, iar Curțile Constituționale din Germania și România au hotărât că legile privind punerea în aplicare a acesteia sunt neconstituționale.	Comisia urmează să prezinte Consiliului și PE un raport de evaluare în 2010.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Sistemul european de informații cu privire la cazierele judiciare (ECRIS)	Inițiat de Belgia la propunerea Comisiei.	Îmbunătățirea schimbului de date la nivel transfrontalier privind cazierele judiciare ale cetățenilor UE.	Descentralizată; sistemul este interconectat prin intermediul unei serii de autorități centrale care vor face schimb de informații extrase din cazierele judiciare prin intermediul rețelei s-TESTA.	Date biografice; condamnarea, sentința și infracțiunea, precum și informații suplimentare, inclusiv amprente digitale (dacă sunt disponibile).	Autorități judiciare și autorități administrative competente.	Normele specifice stabilite prin Decizia-cadru 2009/315/JAI a Consiliului, care includ normele prevăzute în Decizia 2005/876/JAI a Consiliului, Decizia-cadru 2008/977/JAI a Consiliului, Convenția108 a Consiliului Europei și Regulamentul (CE) nr. 45/2001.	Sunt aplicabile normele naționale privind păstrarea datelor, deoarece acest instrument reglementează doar schimbul de date.	ECRIS este în curs de aplicare. Nouă state membre au început schimbul electronic de informații.	Comisia urmează să prezinte PE și Consiliului două rapoarte de evaluare: un raport privind Decizia-cadru 2008/675/JAI în 2011; un raport privind Decizia-cadru 2009/315/JAI în 2015. Cu începere din 2016, Comisia trebuie să publice rapoarte periodice privind funcționarea Deciziei 2009/316/JAI a Consiliului (ECRIS).
Cooperarea între unitățile de informații financiare (FIU.net)	Inițiată de Țările de Jos.	Schimbul de informații necesare în vederea analizării și anchetării activităților de spălare a banilor și finanțare a terorismului.	Descentralizată; FIU fac schimb de date prin intermediul FIU.net care operează pe rețeaua s-TESTA. Este posibil ca, în curând, aplicația Europol, SIENA, să fie utilizată în vederea consolidării FIU.net.	Orice date relevante în vederea analizării și anchetării activităților de spălare a banilor și finanțare a terorismului.	Unități de informații financiare (în cadrul poliției, autorităților judiciare sau administrative care raportează autorităților financiare).	Decizia-cadru 2008/977/JAI a Consiliului, Convenția 108 a Consiliului Europei și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	Sunt aplicabile normele naționale privind păstrarea datelor, deoarece acest instrument reglementează doar schimbul de date.	20 de state membre participă în cadrul FIU.net, o aplicație de partajare a datelor pe internet, care funcționează pe rețeaua s-TESTA.	Ca parte a Planului de acțiune privind serviciile financiare, Comisia revizuiește din 2009 punerea în aplicare a Directivei 2005/60/CE.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Cooperarea între oficiile de recuperare a creanțelor (ARO)	Inițiată de statele membre.	Schimbul de informații necesare în vederea urmăririi și identificării produselor infracțiunii.	Descentralizată; ARO au obligația de a utiliza inițiativa suedeză în vederea schimbului de informații. Este posibil ca, în curând, aplicația Europol, SIENA, să fie utilizată în vederea consolidării cooperării între ARO.	Date cu privire la proprietatea vizată, precum conturi bancare, bunuri imobiliare și vehicule, precum și date cu privire la persoanele căutate, cum ar fi numele, adresa, informații privind acționarii sau societatea comercială.	Oficii de recuperare a creanțelor.	Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	Sunt aplicabile normele naționale privind păstrarea datelor, deoarece acest instrument reglementează doar schimbul de date.	Au fost înființate ARO în peste 20 de state membre; 12 ARO participă în cadrul unui proiect pilot prin care se utilizează aplicația Europol, SIENA, în vederea schimbului de date relevante pentru depistarea activelor.	Comisia urmează să prezinte Consiliului un raport de evaluare în 2010.
Platforme naționale și europene de alertă privind criminalitatea informatică	Inițiate de Franța.	Colectarea, analizarea și schimbul de informații privind infracțiunile comise pe internet.	Descentralizată; această structură reunește platformele naționale de alertă cu Platforma europeană împotriva criminalității informatice din cadrul Europol. Este posibil ca, în curând, aplicația Europol, SIENA, să fie utilizată în vederea consolidării schimbului de date între platformele de alertă.	Conținuturi sau comportamente ilegale identificate pe internet.	Platformele naționale primesc semnalări din partea cetățenilor; Platforma europeană împotriva criminalității informatice din cadrul Europol primește semnalări din partea autorităților de aplicare a legii privind forme de criminalitate gravă transfrontalieră.	Normele specifice stabilite prin Decizia Europol și Decizia-cadru 2008/977/JAI a Consiliului, Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta, Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc și Regulamentul (CE) 45/2001.	Sunt aplicabile normele naționale privind păstrarea datelor, deoarece această măsură reglementează doar schimbul de informații.	Aproape toate statele membre au creat platforme naționale de alertă. Europol lucrează în continuare la Platforma europeană împotriva criminalității informatice.	Europol acoperă domeniul criminalității informatice iar, în viitor, va raporta cu privire la activitățile Platformei europene împotriva criminalității informatice în raportul anual prezentat Consiliului pentru aprobare și Parlamentului European pentru informare.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Europol	Inițiat de statele membre.	Sprijinirea statelor membre în vederea prevenirii și combaterii criminalității organizate, a terorismului și a altor forme de criminalitate gravă care afectează două sau mai multe state membre.	Europol este o agenție a UE cu sediul la Haga. În prezent, Europol dezvoltă propria aplicație securizată de rețea de schimb de informații, denumită SIENA.	Sistemul informațional Europol (EIS) conține datele cu caracter personal, inclusiv elementele de identificare biometrică, condamnările și legăturile cu criminalitatea organizată ale persoanelor suspectate de săvârșirea unor infracțiuni care intră în mandatul Europol. Fișierele de lucru pentru analiză (AWF) conțin toate datele cu caracter personal relevante.	EIS poate fi accesat de unitățile naționale ale Europol, ofițerii de legătură, personalul și directorul Europol. Accesul la AWF este acordat ofițerilor de legătură. Sunt posibile schimburile de date cu caracter personal cu țările terțe care au încheiat acorduri cu Europol.	Normele specifice stabilite prin Decizia Europol și Decizia-cadru 2008/977/JAI a Consiliului, Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta, Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc și Regulamentul (CE) 45/2001.	Fișierele AWF pot fi păstrate cel mult trei ani, cu o prelungire posibilă de încă trei ani.	Europol colaborează în mod activ cu fiecare stat membru și cu țările terțe cu care a încheiat acorduri operaționale. Noul temei juridic al Europol a fost pus în aplicare în toate statele membre.	Un organism comun de supraveghere monitorizează prelucrarea de către Europol a datelor cu caracter personal și transmiterea acestora către alte părți.. Acesta prezintă rapoarte periodice Parlamentului European și Consiliului. De asemenea, Europol prezintă un raport anual privind activitățile sale Consiliului pentru aprobare și Parlamentului European pentru informare.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Eurojust	Inițiat de statele membre.	Îmbunătățirea coordonării cercetărilor și urmăririlor penale în statele membre, precum și intensificarea cooperării dintre autoritățile relevante.	Eurojust este un organism al UE cu sediul la Haga, care utilizează rețeaua s-TESTA în vederea schimbului de date.	Datele cu caracter personal ale suspecților și infractorilor în cazul unor forme de criminalitate gravă care afectează două sau mai multe state membre, inclusiv informații biografice, date de contact, profiluri ADN, amprente digitale, fotografii precum și date de trafic și localizare ale telecomunicațiilor.	Cei 27 de membri naționali ai Europol care pot partaja date cu autoritățile naționale și țările terțe, sub rezerva consimțământului sursei informațiilor.	Normele specifice stabilite prin Decizia Eurojust, Decizia-cadru 2008/977/JAI a Consiliului, Convenția 108 a Consiliului Europei, Protocolul adițional 181 la aceasta și Recomandarea R (87) 15 a Consiliului Europei privind sectorul polițienesc.	Informațiile trebuie șterse după atingerea scopului pentru care au fost furnizate și după închiderea cazului.	Temeiul juridic modificat al Eurojust este pus în aplicare, în prezent, de statele membre.	Până în iunie 2014, Comisia trebuie să revizuiască schimbul de date între membrii naționali ai Eurojust. Până în iunie 2013, Eurojust trebuie să raporteze Consiliului și Comisiei în legătură cu furnizarea de acces la nivel național la sistemul său de gestionare a cazurilor. Un organism comun de supraveghere monitorizează prelucrarea de către Eurojust a datelor cu caracter personal și prezintă un raport anual Consiliului. Președintele colegiului Eurojust prezintă Consiliului un raport anual privind activitățile Eurojust, pe care Consiliul îl transmite Parlamentului European.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Acorduri PNR cu SUA și Australia; Acord API/PNR cu Canada	Inițiate de Comisie.	Prevenirea și combaterea terorismului, precum și a altor forme de criminalitate gravă transnațională.	Acorduri internaționale.	Acordurile cu SUA și cu Australia conțin 19 categorii de date PNR, inclusiv informații biografice, informații privind rezervarea, plata și alte informații suplimentare; acordul cu Canada conține 25 de tipuri de date similare.	Departamentul pentru Securitate Internă al SUA, Agenția de Servicii Frontaliere a Canadei și Serviciul Vamal Australian, care pot să transfere astfel de date unor alte autorități naționale responsabile cu aplicarea legii sau cu combaterea terorismului.	Normele privind protecția datelor sunt prevăzute în acordurile internaționale specifice.	SUA: șapte ani într-o bază de date activă și opt ani într-o bază de date pasivă; Australia: 3,5 ani într-o bază de date activă și doi ani într-o bază de date pasivă; Canada: 72 de ore într-o bază de date activă și 3,5 ani într-o bază de date pasivă.	Acordurile cu SUA și cu Australia se aplică provizoriu; cel cu Canada a intrat în vigoare. Comisia va renegocia aceste acorduri. Șase state membre ale UE au adoptat legi prin care se permite utilizarea datelor PNR în scopul aplicării legii.	Fiecare acord prevede o revizuire periodică, în timp ce acordurile cu Canada și cu Australia includ și o clauză de denunțare.

Tabel recapitulativ al instrumentelor operaționale, în curs de aplicare sau în curs de examinare

Instrument	Context	Scop (scopuri)	Structură	Sfera datelor cu caracter personal	Accesul la date	Protecția datelor	Păstrarea datelor	Stadiul punerii în aplicare	Reexaminare
Acordul TFTP UE-SUA	Inițiat de Comisie.	Prevenirea, cercetarea, detectarea sau urmărirea penală a terorismului și finanțării acestuia.	Acord internațional.	Date de mesagerie financiară care conțin, inter alia, numele, numărul de cont, adresa și numărul de identificare al inițiatorului și destinatarilor de tranzacții financiare.	Departamentul de Trezorerie al SUA poate partaja date cu caracter personal extrase din mesaje financiare autorităților de aplicare a legii, de securitate publică sau de combatere a terorismului din SUA, cu statele membre UE, Europol sau Eurojust. Transferul ulterior al datelor către țări terțe se face cu consimțământul statelor membre.	Acordul prevede dispoziții stricte privind limitarea scopului și proporționalitatea.	Datele cu caracter personal extrase din mesaje financiare nu pot fi păstrate mai mult timp decât este necesar pentru cercetări sau urmăriri penale specifice; datele neextrase pot fi păstrate timp de maximum 5 ani.	Parlamentul European a aprobat încheierea Acordului TFTP UE-SUA la 8 iulie 2010. Se așteaptă acum adoptarea de către Consiliu a unei decizii a Consiliului privind încheierea acestui acord, în urma căreia acordul ar intra în vigoare prin intermediul unui schimb de scrisori între părți.	Comisia trebuie să revizuiască acest acord la șase luni de la intrarea sa în vigoare. Raportul de evaluare a acordului trebuie trimis PE și Consiliului.