COMMISSIONE
EUROPEA

Bruxelles, 6.4.2016
COM(2016) 205 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza

1. INTRODUZIONE

L'Europa è una società mobile. Milioni di cittadini dell'Unione e di paesi terzi attraversano le frontiere interne ed esterne ogni giorno. Nel 2015 più di 50 milioni di cittadini di paesi terzi hanno visitato l'UE, con oltre 200 milioni di attraversamenti delle frontiere esterne dello spazio Schengen.

Oltre a questi flussi di viaggiatori regolari, il conflitto siriano e le crisi in altre aree hanno indotto, nel solo 2015, 1,8 milioni di attraversamenti irregolari delle frontiere esterne dell'Europa. I cittadini dell'UE si aspettano che i controlli sulle persone alle frontiere esterne siano efficaci, consentano una gestione adeguata della migrazione e contribuiscano alla sicurezza interna. Gli attentati terroristici perpetrati a Parigi nel 2015 e a Bruxelles nel marzo 2016 sono la tragica dimostrazione delle minacce a cui è costantemente sottoposta la sicurezza interna dell'Europa.

Questi due eventi hanno ulteriormente evidenziato la necessità di unire gli sforzi e di potenziare complessivamente i quadri della cooperazione dell'UE in materia di gestione delle frontiere, migrazione e sicurezza e gli strumenti di informazione. La gestione delle frontiere, le attività di contrasto della criminalità e il controllo della migrazione sono interconnessi in modo dinamico. È noto che alcuni cittadini dell'UE hanno attraversato la frontiera esterna per recarsi in aree di conflitto a fini terroristici e che quindi rappresentano un rischio al loro ritorno. È comprovato che le rotte della migrazione irregolare sono state utilizzate da terroristi per entrare nell'UE e poi spostarsi all'interno dello spazio Schengen senza essere scoperti.

L'agenda europea sulla sicurezza e quella sulla migrazione hanno definito l'orientamento per lo sviluppo e l'attuazione di una politica dell'UE volta ad affrontare le sfide parallele della gestione della migrazione e della lotta contro il terrorismo e la criminalità organizzata. La presente comunicazione si basa sulle sinergie tra le due agende e costituisce il punto di partenza per un dibattito su come i sistemi d'informazione presenti e futuri possano contribuire a rafforzare sia la gestione delle frontiere esterne che la sicurezza interna nell'UE. Essa è complementare alla proposta del dicembre 2015 concernente l'istituzione di una guardia costiera e di frontiera europea e il miglioramento della prevenzione delle crisi e degli interventi alle frontiere esterne.

A livello dell'UE esistono vari sistemi d'informazione che forniscono alle guardie di frontiera e ai funzionari di polizia informazioni sulle persone, ma l'architettura della gestione dei dati dell'UE non è perfetta. La presente comunicazione illustra alcune possibili opzioni per massimizzare i benefici dei sistemi di informazione esistenti ed elaborare nuove azioni complementari per colmare eventuali lacune. Essa sottolinea anche, come obiettivo a lungo termine, la necessità di migliorare l'interoperabilità dei sistemi di informazione, così come indicato anche dal Consiglio europeo e dal Consiglio[1], e presenta idee su come sviluppare in futuro i sistemi informativi per garantire che le guardie di frontiera, le autorità doganali, i funzionari di polizia e le autorità giudiziarie dispongano delle necessarie informazioni.

Ogni iniziativa futura sarà elaborata in base ai principi di una migliore regolamentazione, mediante consultazione pubblica e valutazione d'impatto anche per quanto riguarda i diritti fondamentali e in particolare il diritto alla protezione dei dati personali.

[1] Conclusioni del Consiglio europeo del 17 e 18 dicembre 2015; Dichiarazione comune dei ministri della giustizia e degli interni dell'UE e dei rappresentanti delle istituzioni dell'UE sugli attentati terroristici di Bruxelles del 22 marzo 2016 (24 marzo 2016); Conclusioni del Consiglio dell'Unione europea e degli Stati membri riuniti in sede di Consiglio sulla lotta al terrorismo (20 novembre 2015).

2. SFIDE DA AFFRONTARE

L'assenza di frontiere interne nello spazio Schengen richiede una gestione solida e affidabile dei movimenti di persone alle frontiere esterne, condizione essenziale per garantire un elevato livello di sicurezza e la libera circolazione delle persone al suo interno. Al tempo stesso l'assenza di frontiere interne significa che anche le autorità di contrasto degli Stati membri hanno accesso ai pertinenti dati relativi alle persone. A livello dell'UE esistono vari sistemi di informazione e banche dati che forniscono informazioni sulle persone alle guardie di frontiera, ai funzionari di polizia e alle altre autorità, in linea con le loro rispettive finalità[2].

Tuttavia questi sistemi di informazione presentano delle carenze che ostacolano il lavoro delle autorità nazionali. Per questo motivo l'agenda europea sulla sicurezza ha indicato il miglioramento dello scambio di informazioni tra le priorità fondamentali. Le principali carenze sono le seguenti: a) funzionalità non ottimali dei sistemi di informazione esistenti; b) lacune nell'architettura della gestione dei dati dell'UE; c) complessità dovuta all'esistenza di sistemi di informazione gestiti in maniera diversa; e d) frammentarietà dell'architettura della gestione dei dati per il controllo delle frontiere e la sicurezza.

I sistemi di informazione esistenti nell'UE per la gestione delle frontiere e la sicurezza interna offrono un'ampia gamma di funzionalità. Tuttavia le **funzionalità dei sistemi esistenti presentano ancora delle carenze**. Esaminando i processi di controllo alle frontiere che si applicano alle diverse categorie di viaggiatori risulta evidente che alcuni di questi processi sono lacunosi ed esistono difetti di funzionamento tra i sistemi di informazione utilizzati per il controllo delle frontiere. Analogamente è necessario ottimizzare le prestazioni degli strumenti esistenti per le attività di contrasto della criminalità. È pertanto opportuno prendere in considerazione misure per migliorare i sistemi di informazione esistenti (sezione 5).

Vi sono inoltre **lacune nell'architettura della gestione dei dati dell'UE**. Permangono problemi per quanto concerne i controlli alle frontiere di specifiche categorie di viaggiatori, ad esempio i cittadini di paesi terzi titolari di un visto per soggiorno di lunga durata. Inoltre, per quanto concerne i cittadini di paesi terzi che sono esenti dall'obbligo del visto, non esistono informazioni che precedano il loro arrivo alla frontiera. Si dovrebbe valutare se sia necessario colmare tali lacune sviluppando un sistema di informazioni aggiuntivo laddove necessario (sezione 6).

Le guardie di frontiera e in particolare gli agenti di polizia devono far fronte alla **complessità dovuta all'esistenza di sistemi di informazione gestiti in maniera diversa** a livello dell'UE. Tale complessità comporta difficoltà pratiche connesse soprattutto alla scelta delle banche dati da controllare in ogni specifica situazione. Inoltre non tutti gli Stati membri sono collegati a tutti i sistemi esistenti[3]. L'attuale complessità di accesso ai sistemi d'informazione a livello dell'UE potrebbe essere ridotta creando un'unica interfaccia di ricerca a livello nazionale che rispetti le diverse finalità di accesso (sezione 7.1).

---

[2] Si veda la sezione 4 per una panoramica dei sistemi di informazione per le frontiere e la sicurezza e l'allegato 2 per un elenco più dettagliato.

[3] Fatte salve le specifiche disposizioni del protocollo n. 22 per quanto riguarda la Danimarca e dei protocolli n. 21 e n. 36 per quanto riguarda il Regno Unito e l'Irlanda e i rispettivi atti di adesione.

L'attuale architettura della gestione dei dati dell'UE per il controllo delle frontiere e la sicurezza è caratterizzata da una **frammentazione** dovuta alla diversità dei contesti istituzionali, giuridici e politici in cui sono stati sviluppati i sistemi. Le informazioni sono archiviate separatamente in vari sistemi, che raramente sono interconnessi. Esistono incompatibilità tra le banche dati e pratiche differenti per l'accesso ai dati da parte delle autorità competenti. Ciò può creare zone d'ombra, in particolare per le autorità di contrasto, in quanto può risultare assai difficile riconoscere le connessioni tra i vari frammenti di dati. È quindi necessario e urgente realizzare soluzioni integrate per migliorare l'accessibilità dei dati per la gestione delle frontiere e la sicurezza, nel pieno rispetto dei diritti fondamentali. A tal fine occorre avviare un processo volto a conseguire l'interoperabilità dei sistemi di informazione esistenti (sezione 7).

3. DIRITTI FONDAMENTALI

Il pieno rispetto dei diritti fondamentali e delle norme in materia di protezione dei dati costituisce una condizione essenziale per affrontare queste sfide.

Per rispettare i diritti fondamentali è necessario che le tecnologie e i sistemi di informazione siano ben strutturati e utilizzati correttamente. Tecnologie e sistemi di informazione possono aiutare le amministrazioni pubbliche a tutelare i diritti fondamentali dei cittadini. La tecnologia biometrica può ridurre il rischio di errori d'identità, di discriminazione e di profilazione su base razziale. Inoltre può contribuire a migliorare la gestione dei rischi nel settore della protezione di minori per quanto riguarda i casi di scomparsa o tratta di minori, a condizione che vada di pari passo con la salvaguardia dei diritti fondamentali e con misure di protezione. Infine può ridurre il rischio di fermi e arresti ingiustificati e fornire una maggiore sicurezza ai cittadini residenti nello spazio Schengen favorendo la lotta contro il terrorismo e i reati gravi.

L'esistenza di sistemi d'informazione su vasta scala implica anche potenziali rischi per la vita privata, che occorre prevedere e affrontare in maniera adeguata. La raccolta e l'uso dei dati personali in tali sistemi comporta ricadute sul diritto al rispetto della vita privata e alla protezione dei dati personali sancito dalla Carta dei diritti fondamentali dell'Unione europea. Tutti i sistemi devono essere conformi ai principi di protezione dei dati e rispettare i requisiti di necessità, proporzionalità, limitazione delle finalità e qualità dei dati. Devono essere predisposte salvaguardie per tutelare i diritti degli interessati in relazione alla protezione della vita privata e dei dati personali. I dati dovrebbero essere conservati soltanto per il tempo necessario a conseguire le finalità per le quali sono raccolti. È inoltre necessario prevedere meccanismi volti a garantire un'accurata gestione del rischio e un'effettiva tutela dei diritti degli interessati.

Nel dicembre 2015 i colegislatori hanno raggiunto un accordo politico sulla riforma della protezione dei dati. Una volta adottati, il nuovo regolamento generale sulla protezione dei dati e la direttiva sulla protezione dei dati destinata alle autorità di polizia e le autorità giudiziarie penali[4], che entreranno in vigore nel 2018, forniranno un quadro armonizzato per il trattamento dei dati personali.

La limitazione delle finalità è un principio fondamentale per la protezione dei dati quale sancita nella Carta dei diritti fondamentali. A causa dei diversi contesti istituzionali, giuridici e politici in cui sono stati messi a punto i sistemi di informazione a livello dell'UE, il principio della limitazione delle finalità è stato attuato attraverso una gestione

[4] Si veda http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

compartimentata delle informazioni[5]. È questo uno dei motivi dell'attuale frammentazione dell'architettura della gestione dei dati dell'UE per il controllo delle frontiere e la sicurezza interna. Grazie all'attuazione del nuovo quadro generale di protezione dei dati personali nell'UE e ai significativi progressi nel campo delle tecnologie e della sicurezza informatica, il principio della limitazione delle finalità potrà essere applicato più facilmente per quanto concerne l'accesso ai dati archiviati e il loro utilizzo, in piena conformità con la Carta dei diritti fondamentali dell'Unione europea e con la recente giurisprudenza della Corte di giustizia. Salvaguardie quali la compartimentazione dei dati all'interno di un sistema unico e specifiche regole di accesso e utilizzo per ciascuna categoria di dati e di utenti dovrebbero garantire la necessaria limitazione delle finalità all'interno di soluzioni integrate della gestione dei dati. Ciò apre la strada all'interoperabilità dei sistemi di informazione, in parallelo con il necessario rigore delle norme in materia di accesso e utilizzo, senza compromettere l'attuale limitazione delle finalità.

La "protezione dei dati fin dalla progettazione" e la "protezione dei dati di default" sono ora principi che informano le norme dell'UE sulla protezione dei dati. Nello sviluppare nuovi strumenti basati sull'uso delle tecnologie dell'informazione, la Commissione si impegnerà a seguire tale approccio. Ciò significa integrare la protezione dei dati personali nella base tecnologica dello strumento proposto, limitando il trattamento dei dati a quanto necessario per un determinato scopo e concedendo l'accesso ai dati soltanto ai soggetti che hanno la "necessità di conoscere"[6].

Le disposizioni della Carta dei diritti fondamentali e in particolare i nuovi strumenti della riforma della protezione dei dati guideranno la Commissione nell'affrontare le attuali lacune e carenze nell'architettura della gestione dei dati dell'UE per il controllo delle frontiere e la sicurezza. Ciò garantirà che in futuro i sistemi d'informazione in questi settori siano sviluppati in linea con gli standard più elevati in materia di protezione dei dati e che rispettino e supportino i diritti garantiti dalla Carta dei diritti fondamentali.

4. PANORAMICA DEI SISTEMI DI INFORMAZIONE PER LA GESTIONE DELLE FRONTIERE E LA SICUREZZA[7]

I sistemi di informazione esistenti nell'UE per la gestione delle frontiere e la sicurezza interna hanno ognuno obiettivi, finalità, basi giuridiche[8], gruppi di utenti e contesto istituzionale propri. Insieme costituiscono un quadro complesso di banche dati.

I tre principali **sistemi di informazione centralizzati** sviluppati dall'UE sono: i) il sistema di informazione Schengen (SIS) con un ampio spettro di segnalazioni relative a persone e oggetti; ii) il sistema di informazione visti (VIS) contenente i dati sui visti per soggiorni di breve durata; e iii) il sistema EURODAC per i dati relativi alle impronte digitali di richiedenti asilo e cittadini di paesi terzi che hanno attraversato le frontiere esterne in maniera irregolare. Questi tre sistemi sono complementari e, ad eccezione del

---

5 COM(2010) 385 definitivo.

6 Per una descrizione esaustiva del principio della "tutela della vita privata fin dalla progettazione" (*privacy by design*) si veda il parere del Garante europeo della protezione dei dati relativo alla promozione della fiducia nella società dell'informazione mediante il rafforzamento della protezione dei dati e della privacy (*Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*) del 18.3.2010.

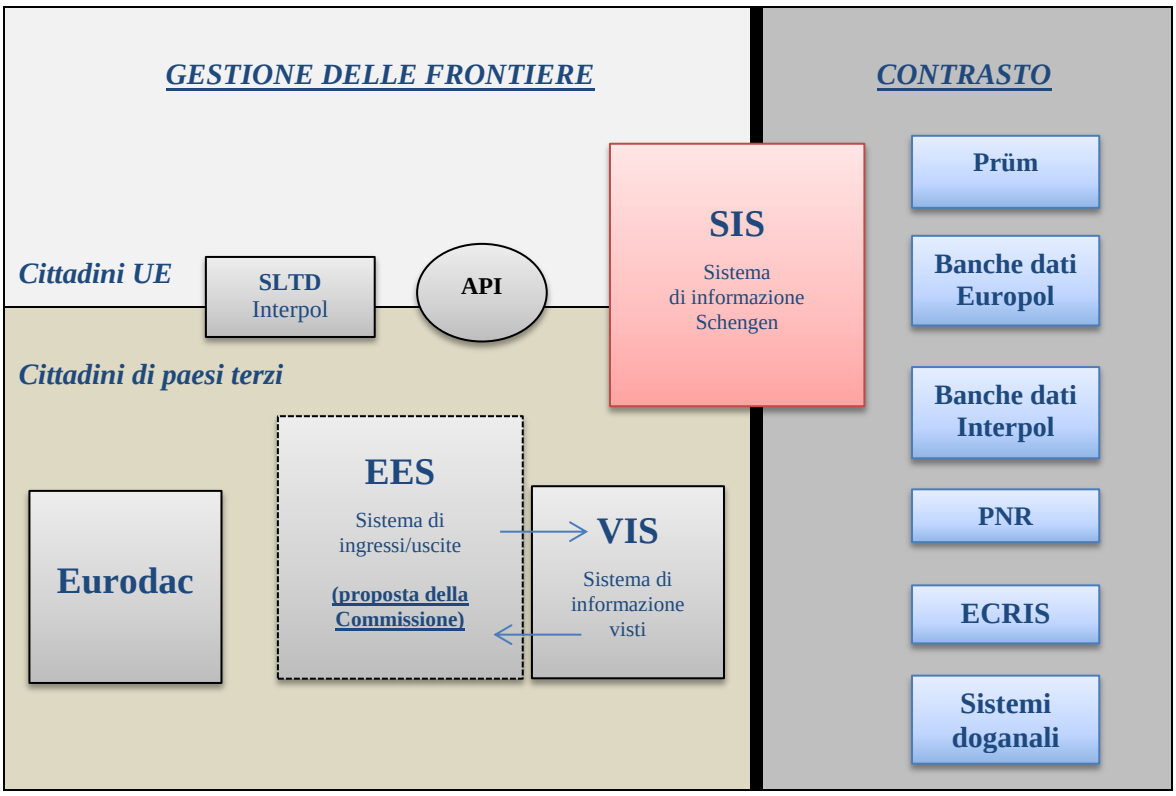
7 Si veda l'allegato 2 per un inventario dei sistemi di informazione esistenti per la gestione delle frontiere e il contrasto.

8 Fatte salve le specifiche disposizioni del protocollo n. 22 per quanto riguarda la Danimarca e dei protocolli n. 21 e n. 36 per quanto riguarda il Regno Unito e l'Irlanda.

SIS, riguardano essenzialmente i cittadini di paesi terzi. Essi aiutano anche le autorità nazionali nella lotta contro la criminalità e il terrorismo[9]. Ciò vale in particolare per il SIS, che costituisce oggi lo strumento più utilizzato per la condivisione delle informazioni. Lo scambio di informazioni su tali sistemi è effettuato tramite una specifica infrastruttura di comunicazione protetta denominata sTESTA[10].

Oltre a questi sistemi, la Commissione propone di istituire un quarto sistema centralizzato di gestione delle frontiere, il **sistema di ingressi/uscite** (EES, *Entry-Exit System*)[11], che dovrebbe essere realizzato entro il 2020, anch'esso riguardante i cittadini di paesi terzi.

Figura 1 *Schema generale dei principali sistemi di informazione per la gestione delle frontiere e il contrasto della criminalità:*



Altri strumenti esistenti per la gestione delle frontiere sono la banca dati dell'Interpol sui documenti di viaggio rubati e smarriti (SLTD) e le informazioni anticipate sui passeggeri (API), che contengono dati sui passeggeri che si imbarcheranno su voli da paesi terzi diretti nell'UE. Tali strumenti riguardano sia i cittadini dell'UE che i cittadini di paesi terzi.

L'UE ha anche sviluppato **strumenti decentrati per lo scambio di informazioni** concepiti espressamente a fini di contrasto, indagini penali e cooperazione giudiziaria, vale a dire: i) il quadro di Prüm per lo scambio di DNA, impronte digitali e dati di

[9] L'accesso dei servizi di contrasto al VIS e all'EURODAC è esercitato con particolari limitazioni a causa del fatto che il contrasto della criminalità è un obiettivo secondario di tali sistemi. Per quanto riguarda il VIS, gli Stati membri devono designare un'autorità responsabile di controllare l'accesso a fini di contrasto e la polizia deve provare che tale accesso le è necessario nel quadro delle indagini penali. Per quanto riguarda l'EURODAC, prima di essere autorizzata ad accedervi l'autorità inquirente deve effettuare ricerche nelle basi nazionali AFIS e Prüm e nel VIS.

[10] A breve sarà sostituita da TESTA-NG.

[11] COM(2016) 194 final.

immatricolazione dei veicoli; ii) il sistema europeo di informazione sui casellari giudiziali (ECRIS) per lo scambio delle informazioni dei casellari giudiziali nazionali. L'ECRIS consente lo scambio di informazioni, attraverso una rete protetta, sulle condanne pronunciate a carico di una determinata persona dagli organi giurisdizionali penali all'interno dell'UE. Le richieste riguardano principalmente dati identificativi alfanumerici, ma è possibile anche lo scambio di dati biometrici.

L'**Europol** agevola lo scambio di informazioni tra le autorità di polizia nazionali fungendo da piattaforma centrale dell'UE per lo scambio di informazioni sulla criminalità. Il sistema di informazione Europol (SIE) è una banca dati centralizzata in cui gli Stati membri possono archiviare e ricercare i dati relativi a reati gravi e terrorismo. I punti di contatto dell'Europol offrono archivi di lavoro per fini di analisi, specializzati per materia, che contengono informazioni sulle operazioni in corso negli Stati membri. L'applicazione di rete per lo scambio di informazioni protetta (SIENA) dell'Europol consente agli Stati membri di scambiare informazioni in maniera rapida, sicura e semplice tra loro, con l'Europol o con terzi che abbiano un accordo di cooperazione con l'Europol. Questa applicazione presenta anche una notevole interoperabilità con altri sistemi dell'Europol, ad esempio per lo scambio diretto di dati con i punti di contatto, e consente di alimentare le banche dati dell'Europol con le informazioni scambiate fra gli Stati membri. Pertanto SIENA dovrebbe essere la scelta di elezione degli Stati membri come canale per lo scambio di informazioni in materia di contrasto della criminalità nell'UE.

Un altro sistema di trattamento di dati personali sarà messa a punto negli Stati membri: il sistema dei **codici di prenotazione** (PNR)[12]. I dati PNR contengono le informazioni fornite dai passeggeri al momento della prenotazione e del check-in.

Infine anche le **autorità doganali** sono soggetti imprescindibili nella cooperazione tra agenzie alle frontiere esterne. Essi dispongono di vari sistemi[13] e banche dati contenenti informazioni sui movimenti di merci, sull'identificazione degli operatori economici e sui rischi, che possono essere utilizzati per rafforzare la sicurezza interna. Questi sistemi sono dotati di una loro infrastruttura controllata, limitata e sicura - la rete comune di comunicazione (CCN) - che ha dimostrato la propria validità. Sarebbe opportuno analizzare ulteriormente le sinergie e la convergenza possibili tra i sistemi di informazione e le relative infrastrutture ai fini della gestione delle frontiere dell'UE e delle operazioni doganali.

5. MIGLIORARE I SISTEMI DI INFORMAZIONE ESISTENTI

I sistemi di informazione esistenti nell'UE per la gestione delle frontiere e la sicurezza interna offrono un'ampia gamma di funzionalità. Tuttavia presentano ancora delle carenze che devono essere affrontate per ottimizzarne l'efficacia.

Sistema di informazione Schengen (SIS)

I controlli alla frontiera con il **sistema d'informazione Schengen** (SIS) attualmente sono effettuati sulla base di ricerche alfanumeriche (ossia nome e data di nascita). Le impronte

[12] Si veda la sezione 6.2.

[13] I sistemi d'informazione doganale comprendono tutti i sistemi creati a norma del codice doganale comunitario (regolamento (CEE) n. 2913/92) e del futuro codice doganale dell'Unione (regolamento (UE) n. 952/2013), della decisione concernente un ambiente privo di supporti cartacei per le dogane e il commercio (decisione n. 70/2008/CE) e del sistema d'informazione doganale istituito nell'ambito della convenzione SID del 1995. Lo scopo è facilitare la lotta contro reati doganali agevolando la cooperazione tra le autorità doganali europee.

digitali possono essere usate solo per verificare e confermare l'identità di una persona il cui nome è già conosciuto. Questa lacuna in materia di sicurezza consente alle persone oggetto di una segnalazione di utilizzare documenti falsi per evitare una perfetta corrispondenza nel SIS.

Questo grave problema sarà affrontato aggiungendo al SIS una funzione di ricerca delle impronte digitali attraverso un **sistema automatizzato di identificazione delle impronte digitali (AFIS)**, come previsto dal quadro normativo in vigore[14]. L'AFIS dovrebbe essere operativo entro la metà del 2017[15]. Una volta sviluppato, l'AFIS sarà accessibile all'Europol, completandone così i sistemi per le indagini penali e l'antiterrorismo e gli scambi di impronte digitali effettuati nell'ambito del quadro di Prüm. La Commissione ed eu-LISA valuteranno il potenziale di un tale ampliamento d'uso in relazione al nuovo AFIS.

Sulla base della valutazione in corso e di uno studio tecnico, la Commissione sta esaminando **eventuali ulteriori funzionalità del SIS** al fine di presentare proposte di revisione della base giuridica di quest'ultimo. Tra gli aspetti all'esame figurano:

- la creazione di segnalazioni SIS sui migranti irregolari oggetto di decisioni di rimpatrio;
- l'uso delle immagini dei volti per l'identificazione biometrica, oltre alle impronte digitali;
- la trasmissione automatizzata delle informazioni sui riscontri (*hit*) ottenuti a seguito di un controllo;
- la memorizzazione nel sistema centrale del SIS delle informazioni su tali riscontri in caso di segnalazioni ai fini di un controllo discreto o di un controllo specifico;
- la creazione di una nuova categoria di segnalazioni su persone ricercate sconosciute per le quali possono esistere dati forensi nelle banche dati nazionali (ad es. un'impronta latente lasciata sul luogo del reato)[16].

La Commissione continuerà a sostenere con i finanziamenti dell'UE l'attuazione di progetti che consentano di effettuare ricerche simultanee nel SIS e nelle banche dati dell'Interpol sui documenti di viaggio rubati e smarriti (SLTD) e su latitanti, veicoli o armi da fuoco (iARMS), che sono complementari ai sistemi d'informazione dell'UE[17].

Banca dati dell'Interpol sui documenti di viaggio rubati e smarriti (SLTD)

Per un'efficace gestione delle frontiere è essenziale che i documenti di viaggio di tutti i cittadini dei paesi terzi e dell'UE siano controllati utilizzando la **banca dati SLTD**. Anche le autorità di contrasto dovrebbero utilizzare la banca dati SLTD per le interrogazioni all'interno dello spazio Schengen. In seguito agli attacchi terroristici

[14] Articolo 22, lettera c), del regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) e decisione 533/2007/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 381 del 28.12.2006, pag. 4 e GU L 2015 del 7.8.2007, pag. 63).

[15] Nel marzo 2016 la Commissione ha presentato una relazione al Parlamento europeo e al Consiglio sullo stato di evoluzione e la disponibilità della tecnologia che permette di identificare una persona in base alle impronte digitali conservate nel sistema d'informazione Schengen di seconda generazione (SIS II).

[16] La creazione di questa nuova segnalazione sarà valutata avendo come obiettivo la complementarità ed evitando sovrapposizioni con l'attuale quadro di Prüm per la ricerca delle impronte digitali nelle diverse banche dati nazionali degli Stati membri dell'UE.

[17] Gli strumenti per la ricerca di informazioni messi a punto dall'Interpol, quali la banca dati Interpol in rete fissa (FIND) e la banca dati Interpol in rete mobile (MIND), sono volti a facilitare le ricerche simultanee nei sistemi dell'Interpol e nel SIS.

perpetrati a Parigi il 13 novembre 2015, il Consiglio ha chiesto la creazione di collegamenti elettronici alle pertinenti banche dati dell'Interpol presso tutti i valichi delle frontiere esterne e il controllo automatico dei documenti di viaggio entro marzo 2016[18]. Tutti gli Stati membri dovrebbero stabilire tali collegamenti elettronici e porre in essere sistemi che consentano l'aggiornamento automatico dei dati sui documenti di viaggio rubati o smarriti nella banca dati SLTD.

Informazioni anticipate sui passeggeri (API)

In linea con le migliori pratiche esistenti, gli Stati membri dovrebbero anche accrescere il valore aggiunto delle **informazioni anticipate sui passeggeri** (API) mediante l'istituzione di procedure automatizzate di verifica incrociata di tali dati con il SIS e la banca dati SLTD dell'Interpol. La Commissione valuterà se sia necessario rivedere la base giuridica per il trattamento dei dati API al fine di garantirne una più ampia attuazione e di includere l'obbligo per gli Stati membri di richiedere e utilizzare i dati API per tutti i voli in arrivo e in partenza. Ciò assume particolare rilevanza nel contesto dell'applicazione della futura direttiva sui codici di prenotazione, dato che l'uso combinato dei dati API e dei dati PNR rafforza ulteriormente l'efficacia di questi ultimi nella lotta contro il terrorismo e i reati gravi[19].

Sistema di informazione visti (VIS)

La Commissione sta inoltre conducendo una valutazione globale del **sistema di informazione visti** (VIS), che dovrebbe concludersi nel 2016. La valutazione esamina, tra l'altro, in che modo viene utilizzato il VIS per le verifiche sia alle frontiere esterne che all'interno del territorio degli Stati membri, e in che modo esso contribuisce alla lotta contro i furti d'identità e le frodi relative ai visti. Su questa base, la Commissione esaminerà le possibilità di potenziamento delle funzionalità del VIS, provvedendo in particolare a:

- migliorare la qualità delle immagini dei volti per consentire confronti biometrici;
- utilizzare i dati biometrici dei richiedenti il visto per interrogare il futuro sistema automatizzato di identificazione delle impronte digitali da sviluppare per il SIS;
- ridurre il limite di età per il rilevamento delle impronte digitali dei bambini di età compresa tra i 6 e i 12 anni, pur fornendo solide garanzie in materia di diritti fondamentali e misure di protezione[20];
- facilitare l'interrogazione della banca dati SLTD dell'Interpol in fase di richiesta del visto.

Per quanto riguarda le possibilità di accesso ai dati VIS **a fini di contrasto** previste dall'attuale quadro giuridico, la loro applicazione negli Stati membri non è uniforme. In questo contesto gli Stati membri hanno riferito di problemi pratici per le procedure di accesso al VIS da parte delle autorità di contrasto. Allo stesso modo, l'attuazione dell'accesso all'EURODAC a fini di contrasto è ancora molto limitata. La Commissione esaminerà l'eventuale necessità di rivedere il quadro giuridico in materia di accesso al VIS e all'EURODAC da parte dei servizi di contrasto.

---

[18] Conclusioni del Consiglio dell'UE e degli Stati membri riuniti in sede di Consiglio sulla lotta al terrorismo, 20 novembre 2015.

[19] Si veda la sezione 6.2 sulla proposta di direttiva sui codici di prenotazione.

[20] Questo è stato indicato come tecnicamente fattibile nello studio del Centro comune di ricerca "Fingerprint Recognition for children" (Il riconoscimento delle impronte digitali per i minori); EUR 26193 EN; ISBN 978-92-79-33390-3Children', 2013.

EURODAC

Come definito nella comunicazione "Riformare il sistema europeo comune di asilo e potenziare le vie legali di accesso all'Europa"[21], la Commissione presenterà una proposta di riforma dell'**EURODAC** per rafforzarne ulteriormente le funzioni in materia di migrazione irregolare e rimpatrio. Ciò consentirà di colmare l'attuale divario tra gli Stati membri nella capacità di monitoraggio dei movimenti secondari dei migranti irregolari. Inoltre la proposta intende migliorare l'efficacia delle procedure di rimpatrio e di riammissione, fornendo mezzi per identificare migranti irregolari e rilasciare loro nuovi documenti d'identità a fini di rimpatrio. In tale contesto la proposta riguarderà anche lo scambio delle informazioni contenute nell'EURODAC con i paesi terzi, tenendo presenti le necessarie garanzie in materia di protezione dei dati.

Europol

L'UE ha consentito all'**Europol** di accedere alle principali banche dati centrali, ma l'Agenzia non ha ancora sfruttato appieno questa opportunità. L'Europol ha il diritto di accedere ai dati inseriti nel SIS e di consultarli direttamente per quanto concerne arresti, controlli discreti o specifici e sequestro di oggetti. Ad oggi l'Europol ha eseguito solo un numero relativamente limitato di ricerche nel SIS. L'accesso al VIS per la consultazione è stato giuridicamente possibile per Europol dal settembre 2013. Dal luglio 2015 la base giuridica dell'EURODAC consente l'accesso da parte di Europol. L'Agenzia dovrebbe accelerare i lavori in corso per stabilire il collegamento al VIS e all'EURODAC. Più in generale, la Commissione valuterà se sia necessario fornire un ulteriore accesso ai sistemi di informazione ad altre agenzie dell'UE nel settore degli affari interni, e in particolare alla futura guardia costiera e di frontiera europea.

Quadro di Prüm

Attualmente le potenzialità del **quadro di Prüm** non sono sfruttate appieno poiché non tutti gli Stati membri hanno assolto i propri obblighi giuridici in termini di integrazione della rete con i rispettivi sistemi. Avendo ricevuto un notevole sostegno finanziario e tecnico per l'attuazione del quadro di Prüm, gli Stati membri dovrebbero adesso attuarlo pienamente. La Commissione sta facendo uso dei poteri ad essa attribuiti per garantire la piena applicazione degli obblighi giuridici contratti dagli Stati membri e nel gennaio 2016 ha avviato un dialogo strutturato (EU Pilot) con gli Stati membri interessati. Se le risposte degli Stati membri saranno insoddisfacenti la Commissione non esiterà ad avviare procedimenti di infrazione.

Sistema europeo di informazione sui casellari giudiziali (ECRIS)

Il sistema europeo di informazione sui casellari giudiziali **ECRIS** consente lo scambio delle informazioni relative alle condanne per i cittadini dei paesi terzi e gli apolidi, ma non vi è alcuna procedura in atto per farlo in modo efficiente. Nel gennaio 2016 la Commissione ha adottato una proposta legislativa per colmare questa lacuna[22]. In questo contesto la Commissione ha proposto di consentire alle autorità nazionali di cercare i cittadini di paesi terzi sulla base delle impronte digitali al fine di garantirne un'identificazione più sicura. Il Parlamento europeo e il Consiglio dovrebbero adottare il testo legislativo nel 2016.

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

Questioni orizzontali

Una preoccupazione generale in relazione ai sistemi di informazione riguarda il **livello di attuazione** da parte degli Stati membri. L'attuazione diseguale del quadro di Prüm e la mancanza di collegamenti elettronici alla banca dati SLTD ne sono esempi evidenti. Per migliorare il livello di attuazione in relazione ai sistemi d'informazione, la Commissione monitorerà da vicino i progressi compiuti da ogni Stato membro[23]. Questo monitoraggio valuterà non solo se gli Stati membri rispettino i loro obblighi giuridici nel settore dei sistemi informatici, ma anche in che modo utilizzino gli strumenti esistenti e se applichino le migliori pratiche. La Commissione si baserà su diverse fonti per monitorare e promuovere il livello di attuazione, comprese le notifiche degli Stati membri e le visite effettuate nel quadro del meccanismo di valutazione e monitoraggio Schengen.

Un'altra preoccupazione generale in relazione ai sistemi di informazione riguarda la **qualità dei dati inseriti**. Se gli Stati membri non rispettano requisiti minimi di qualità, l'affidabilità e il valore dei dati archiviati è assai limitato e il rischio di ottenere corrispondenze errate o di non trovare riscontri compromette il valore intrinseco dei sistemi. Per migliorare la qualità dei dati inseriti eu-LISA svilupperà una **capacità di monitoraggio centrale della qualità dei dati** per tutti i sistemi di sua competenza.

La maggior parte dei sistemi di informazione nel settore dei controlli alle frontiere e di sicurezza gestisce i dati di identificazione provenienti dai documenti di viaggio e d'identità. Per migliorare i controlli alle frontiere e la sicurezza, oltre a disporre di sistemi ben funzionanti, è necessario autenticare in maniera rapida e sicura i documenti di viaggio e d'identità. A questo fine la Commissione presenterà una serie di misure volte a migliorare la gestione dell'identità e la **sicurezza dei documenti** in modalità elettronica e a rafforzare la lotta contro la frode documentale. I livelli interoperabili di identificazione sicura raggiungibili mediante il regolamento eIDAS[24] potrebbero offrire uno strumento in tal senso.

Azioni volte a migliorare i sistemi di informazione esistenti

Sistema di informazione Schengen (SIS)

- La Commissione ed eu-LISA svilupperanno e attueranno nel SIS una funzionalità per il sistema automatizzato di identificazione delle impronte digitali (AFIS) entro la metà del 2017.
- La Commissione presenterà entro la fine del 2016 proposte per la revisione della base giuridica del SIS per migliorarne ulteriormente il funzionamento.
- Gli Stati membri massimizzeranno l'uso del SIS, sia inserendo tutte le informazioni pertinenti, sia consultando il sistema ogni qualvolta sia necessario.

Banca dati dell'Interpol sui documenti di viaggio rubati e smarriti (SLTD)

- Gli Stati membri stabiliranno collegamenti elettronici con gli strumenti dell'Interpol a tutti i valichi delle frontiere esterne.
- Gli Stati membri rispetteranno l'obbligo di inserire e consultare contemporaneamente i dati sui documenti di viaggio rubati o smarriti nel SIS e della banca dati SLTD.

[23] Fatte salve le specifiche disposizioni del protocollo n. 22 per quanto riguarda la Danimarca e dei protocolli n. 21 e n. 36 per quanto riguarda il Regno Unito e l'Irlanda.

[24] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

Informazioni anticipate sui passeggeri (API)

- Gli Stati membri automatizzeranno l'utilizzo dei dati API per effettuare ricerche nel SIS e nella banca dati sui documenti di viaggio rubati e smarriti (SLTD) dell'Interpol, in linea con le migliori pratiche esistenti.
- La Commissione valuterà se sia necessario rivedere la base giuridica per il trattamento dei dati API.

Sistema di informazione visti (VIS)

- La Commissione valuterà ulteriori miglioramenti del VIS prima della fine del 2016.

EURODAC

- La Commissione presenterà una proposta di revisione della base giuridica dell'EURODAC per potenziarne ulteriormente le funzioni in materia di migrazione irregolare e rimpatrio.

Europol

- L'Europol si avvarrà pienamente dei diritti di accesso di cui dispone per la consultazione del SIS, del VIS e dell'EURODAC.
- La Commissione e l'Europol valuteranno e promuoveranno sinergie tra il sistema di informazione Europol (SIE) e altri sistemi, in particolare il SIS.
- La Commissione ed eu-LISA valuteranno se il sistema di identificazione automatizzato delle impronte digitali (AFIS) da sviluppare per il SIS possa integrare i sistemi di Europol per le indagini penali e l'antiterrorismo.

Quadro di Prüm

- Gli Stati membri attueranno e utilizzeranno appieno il quadro di Prüm.
- Se necessario, la Commissione avvierà procedimenti d'infrazione contro gli Stati membri che non si sono collegati al quadro di Prüm.
- La Commissione ed eu-LISA valuteranno se il sistema di identificazione automatizzato delle impronte digitali (AFIS) da sviluppare per il SIS possa integrare lo scambio di dati sulle impronte digitali effettuato nell'ambito del quadro di Prüm.

Sistema europeo di informazione sui casellari giudiziali (ECRIS)

- Il Parlamento europeo e il Consiglio dovrebbero adottare nel 2016 una proposta legislativa per consentire alle autorità nazionali di cercare nell'ECRIS i cittadini di paesi terzi sulla base delle impronte digitali.

Questioni orizzontali

- La Commissione **monitorerà e promuoverà il livello di attuazione** per quanto concerne i sistemi informatici.
- Eu-LISA svilupperà una **capacità di monitoraggio centrale della qualità dei dati** per tutti i sistemi di sua competenza.
- La Commissione presenterà misure volte a migliorare **la gestione dell'identità e la sicurezza dei documenti** in modalità elettronica e a rafforzare la lotta contro la frode documentale.
- La Commissione analizzerà ulteriormente le sinergie e la convergenza possibili tra i sistemi di informazione e le relative infrastrutture ai fini della gestione delle frontiere dell'UE e delle **operazioni doganali**.

6. SVILUPPO DI ULTERIORI SISTEMI D'INFORMAZIONE ED ELIMINAZIONE DELLE LACUNE

Benché i sistemi di informazione esistenti gestiscano un'ampia gamma di dati necessari per la gestione delle frontiere e il contrasto, permangono notevoli lacune. Per colmare alcune di queste lacune la Commissione ha presentato proposte legislative quali quella relativa ad un sistema di ingressi/uscite e quella sul codice di prenotazione (PNR) dell'UE. Per le altre lacune individuate è necessaria un'attenta valutazione al fine di stabilire se siano necessari strumenti supplementari a livello dell'UE.

1. Sistema di ingressi/uscite

La Commissione ha presentato le proposte legislative riviste per l'istituzione di un sistema di ingressi/uscite (*Entry-Exit System*, EES) in parallelo alla presente comunicazione. Dopo l'adozione da parte dei colegislatori, spetterà ad eu-LISA sviluppare e attuare il sistema, in cooperazione con gli Stati membri di Schengen.

Il sistema registrerà i passaggi alla frontiera (sia in ingresso che in uscita) di tutti i cittadini di paesi terzi che si recano nello spazio Schengen per un soggiorno di breve durata (massimo 90 giorni in qualsiasi periodo di 180 giorni), per i viaggiatori che hanno l'obbligo del visto, per quelli che ne sono esentati e per coloro che soggiornano con il nuovo visto di circolazione (fino a un anno). Gli obiettivi dell'EES sono i seguenti: a) migliorare la gestione delle frontiere esterne; b) ridurre la migrazione irregolare, affrontando il fenomeno del superamento dei termini del soggiorno; e c) favorire la lotta contro il terrorismo e i reati gravi, contribuendo in tal modo a garantire un livello elevato di sicurezza interna.

Il sistema registrerà l'identità dei cittadini di paesi terzi (dati alfanumerici, quattro impronte digitali e immagine del volto) e i dati dei loro documenti di viaggio, e li collegherà ai dati elettronici di ingresso e uscita. L'attuale prassi di apposizione di timbri sui documenti di viaggio sarà sospesa. L'EES permetterà una gestione efficace dei soggiorni di breve durata autorizzati, una maggiore automazione dei controlli alle frontiere e un miglioramento nell'individuazione delle frodi d'identità e documentali. La registrazione centralizzata consentirà l'individuazione di coloro che soggiornano oltre la scadenza del visto e l'identificazione delle persone prive di documenti nello spazio Schengen. Il sistema di ingressi/uscite proposto colma pertanto un'importante lacuna nel panorama dei sistemi di informazione esistenti.

2. Codice di prenotazione

I dati del codice di prenotazione (PNR) sono costituiti dalle informazioni relative alla prenotazione, comprendenti i recapiti, tutti i dati relativi al viaggio e alle prenotazioni, le note particolari, le informazioni sul bagaglio e il posto a sedere e i sistemi di pagamento. I dati PNR sono utili e necessari per identificare i passeggeri ad alto rischio nel contesto della lotta contro il terrorismo, il traffico di stupefacenti, la tratta di esseri umani, lo sfruttamento sessuale dei minori e altri reati gravi. La proposta di direttiva PNR garantirà una migliore cooperazione tra i sistemi nazionali e ridurrà le lacune in materia di sicurezza tra gli Stati membri. Essa colmerà quindi un'importante lacuna per quanto concerne la disponibilità dei dati necessari per la lotta contro i reati gravi e il terrorismo. **La direttiva PNR dovrebbe essere adottata e attuata con urgenza**.

La direttiva stabilirà che gli Stati membri istituiscano unità d'informazione sui passeggeri (PIU) incaricate di ricevere i dati PNR dai vettori. Pur non prevedendo la creazione di un sistema o di una banca dati centrale, la direttiva garantirà un certo grado di standardizzazione delle soluzioni tecniche e delle procedure nazionali, facilitando così lo

scambio di dati PNR tra le unità d'informazione sui passeggeri. La Commissione sosterrà gli Stati membri nell'analizzare i diversi scenari per l'interconnettività tra queste unità al fine di proporre soluzioni e procedure standardizzate. Una volta adottata la direttiva, la Commissione intende accelerare i lavori sui protocolli comuni e formati di dati supportati per il trasferimento dei dati PNR da parte dei vettori aerei alle unità d'informazione sui passeggeri. La Commissione preparerà un progetto di atto di esecuzione entro tre mesi dall'adozione della direttiva.

3. Mancanza di informazioni precedenti all'arrivo di cittadini di paesi terzi esenti dall'obbligo di visto

Mentre per quanto concerne i titolari di visto l'identità, i recapiti e le altre informazioni sono registrati nel VIS, per le persone esenti dall'obbligo di visto le uniche informazioni disponibili sono quelle contenute nel documento di viaggio. Per i viaggiatori che arrivano per via aerea o marittima queste informazioni possono essere completate prima dell'arrivo con i dati API. Sulla base della proposta di direttiva PNR, per coloro che giungono nell'Unione per via aerea saranno raccolti anche i dati PNR. Per le persone che entrano nell'UE per via terrestre non sono disponibili informazioni prima dell'arrivo alle frontiere esterne dell'UE.

Mentre le autorità di contrasto, laddove necessario per la lotta contro i reati gravi e il terrorismo, possono ottenere informazioni sui titolari di visto tramite il VIS, sulle persone esenti dall'obbligo di visto non sono disponibili dati comparabili. Questa mancanza di informazioni è particolarmente importante per quanto concerne la gestione delle frontiere terrestri dell'UE, in una situazione in cui un numero considerevole di viaggiatori esenti dall'obbligo di visto arrivano in automobile, in pullman o in treno. Diversi paesi limitrofi dell'UE sono già esenti dall'obbligo di visto, mentre con altri è in corso il dialogo sulla liberalizzazione dei visti. Ciò potrebbe portare nel prossimo futuro a un considerevole incremento dei viaggiatori esenti.

La Commissione valuterà la necessità, fattibilità e proporzionalità di un nuovo strumento dell'UE per affrontare tale questione. Un'opzione che potrebbe essere valutata è la creazione di un **sistema dell'UE di informazione e autorizzazione ai viaggi** (ETIAS), in cui i viaggiatori esenti dall'obbligo di visto dovrebbero registrare le informazioni sul viaggio che intendono compiere. Il trattamento automatico di tali informazioni potrebbe aiutare le guardie di frontiera a valutare i visitatori di paesi terzi che arrivano per un soggiorno di breve durata. Paesi quali gli Stati Uniti, il Canada e l'Australia hanno già attuato sistemi analoghi, anche per i cittadini dell'UE.

I sistemi di autorizzazione al viaggio prevedono una domanda online in cui il richiedente fornisce, prima della partenza, informazioni sulla sua identità, i recapiti, le finalità del viaggio, l'itinerario, ecc. Una volta ottenuta l'autorizzazione, le procedure di frontiera all'arrivo diventano più rapide e semplici. Al di là dei vantaggi in termini di sicurezza e gestione delle frontiere, e della potenziale utilità nel contesto della reciprocità dei visti, un sistema come l'ETIAS potrebbe servire anche da strumento di facilitazione dei viaggi.

4. Sistema UE d'indice dei registri di polizia giudiziali (EPRIS)

Come indicato nell'agenda europea sulla sicurezza, la disponibilità in tempo reale di dati della polizia in tutti gli Stati membri è un'area su cui si dovranno concentrare i lavori futuri per quanto concerne lo scambio di informazioni. La Commissione valuterà la necessità, la fattibilità tecnica e la proporzionalità di un sistema UE d'indice degli schedari di polizia (EPRIS) per facilitare l'accesso transfrontaliero alle informazioni contenute nelle banche dati nazionali sulle attività di contrasto. In questo contesto, la Commissione sostiene con finanziamenti dell'UE l'attuazione di un progetto pilota da

parte di un gruppo di cinque Stati membri per istituire un meccanismo automatico di ricerca transfrontaliera negli indici nazionali tramite un sistema "*hit/no hit*"[25]. Nella sua valutazione la Commissione terrà conto dei risultati del progetto.

Azioni volte a sviluppare ulteriori sistemi d'informazione e a fornire le informazioni mancanti

Sistema di ingressi/uscite (EES)

- Il Parlamento europeo e il Consiglio dovrebbero considerare le proposte legislative concernenti il sistema di ingressi/uscite con la massima urgenza, con l'obiettivo di adottarle entro la fine del 2016.

Codice di prenotazione (PNR)

- Il Parlamento europeo e il Consiglio dovrebbero adottare la direttiva PNR entro l'aprile del 2016.
- Una volta che la direttiva PNR sarà stata adottata, gli Stati membri la attueranno con la massima urgenza.
- La Commissione sosterrà lo scambio di dati tra le unità d'informazione sui passeggeri attraverso soluzioni e procedure standardizzate.
- La Commissione elaborerà un progetto di decisione di esecuzione sui protocolli comuni e i formati di dati supportati per il trasferimento dei dati PNR da parte dei vettori aerei alle unità d'informazione sui passeggeri entro tre mesi dall'adozione della direttiva PNR.

Mancanza di informazioni precedenti all'arrivo di cittadini di paesi terzi esenti dall'obbligo di visto

- La Commissione valuterà nel 2016 la necessità, la fattibilità tecnica e la proporzionalità dell'istituzione di un nuovo strumento dell'UE, quale ad esempio il sistema dell'UE di informazione e autorizzazione ai viaggi.

Sistema UE d'indice degli schedari di polizia (EPRIS)

- La Commissione valuterà nel 2016 la necessità, la fattibilità tecnica e la proporzionalità dell'istituzione di un EPRIS.

7. VERSO L'INTEROPERABILITÀ DEI SISTEMI DI INFORMAZIONE

L'interoperabilità è la capacità di sistemi di informazione di scambiare dati e di consentire la condivisione delle informazioni. Si possono distinguere **quattro aspetti dell'interoperabilità**, ciascuno dei quali solleva questioni giuridiche[26], tecniche e operative, anche in materia di protezione dei dati:

- un'interfaccia di ricerca unica per l'interrogazione contemporanea di diversi sistemi di informazione, che consente di ottenere risultati combinati su una sola schermata;

[25] Il progetto pilota relativo al processo di scambio automatizzato di dati (ADEP) mira a creare un sistema tecnico che consenta, mediante un indice, di verificare se esistano verbali di polizia su una persona o un'indagine di polizia giudiziaria in uno o più altri Stati membri. La risposta automatica a una ricerca nell'indice si limiterebbe ad indicare se sono disponibili dati (risposta "*hit/no hit*"). In caso di risposta positiva ulteriori dati personali dovrebbero essere richiesti in un secondo tempo, attraverso i normali canali utilizzati per la cooperazione di polizia.

[26] Fatte salve le specifiche disposizioni del protocollo n. 22 per quanto riguarda la Danimarca e dei protocolli n. 21 e n. 36 per quanto riguarda il Regno Unito e l'Irlanda.

- l'interconnettività dei sistemi di informazione, grazie alla quale i dati registrati in un sistema vengono consultati automaticamente da un altro sistema;
- la creazione di un servizio comune di confronto biometrico a sostegno dei vari sistemi di informazione;
- un archivio comune di dati per i diversi sistemi di informazione (modulo centrale).

Al fine di avviare un processo volto a conseguire l'interoperabilità dei sistemi di informazione a livello europeo, la Commissione istituirà un **gruppo di esperti sui sistemi di informazione e l'interoperabilità** a livello di alti funzionari con le agenzie dell'UE, gli esperti nazionali e i pertinenti interlocutori istituzionali. Il gruppo di esperti avrà il compito di affrontare gli aspetti giuridici, tecnici e operativi delle diverse opzioni per l'interoperabilità dei sistemi di informazione, analizzando tra l'altro la necessità, la fattibilità tecnica e la proporzionalità delle opzioni disponibili e le loro implicazioni per la protezione dei dati. Esso si occuperà delle lacune e della mancanza di informazioni che si riscontrano attualmente a causa della complessità e della frammentazione dei sistemi a livello europeo, adottando una prospettiva ampia e globale in materia di gestione delle frontiere e di contrasto e tenendo conto anche dei ruoli, delle responsabilità e dei sistemi delle autorità doganali in questi ambiti. Il metodo di lavoro adottato dal gruppo di esperti punterà a creare sinergie tra tutte le esperienze in materia, che in passato troppo spesso sono state sviluppate in modo compartimentato.

L'obiettivo di questo processo è fornire un quadro strategico generale dell'architettura dell'UE in materia di gestione dei dati per il controllo delle frontiere e la sicurezza, e offrire soluzioni per la sua attuazione.

Questo processo di consultazione **avrà i seguenti obiettivi**:

- Complementarità dei sistemi di informazione: occorre evitare sovrapposizioni, eliminare quelle già esistenti, e affrontate le lacune in modo adeguato.
- Dovrebbe essere applicato un approccio modulare, avvalendosi pienamente degli sviluppi tecnologici e basandosi sui principi della tutela della vita privata fin dalla progettazione.
- Pieno rispetto di tutti i diritti fondamentali sia dei cittadini dell'UE che dei cittadini di paesi terzi, garantito fin dall'inizio in linea con la Carta dei diritti fondamentali.
- Sistemi di informazione interconnessi e interoperabili, ove ciò sia necessario e praticabile. Dovrebbe essere agevolata la ricerca simultanea nei diversi sistemi affinché tutte le informazioni pertinenti siano a disposizione delle guardie di frontiera e dei funzionari di polizia, se e quando ciò sia necessario per i loro rispettivi compiti, senza modificare i diritti di accesso esistenti.

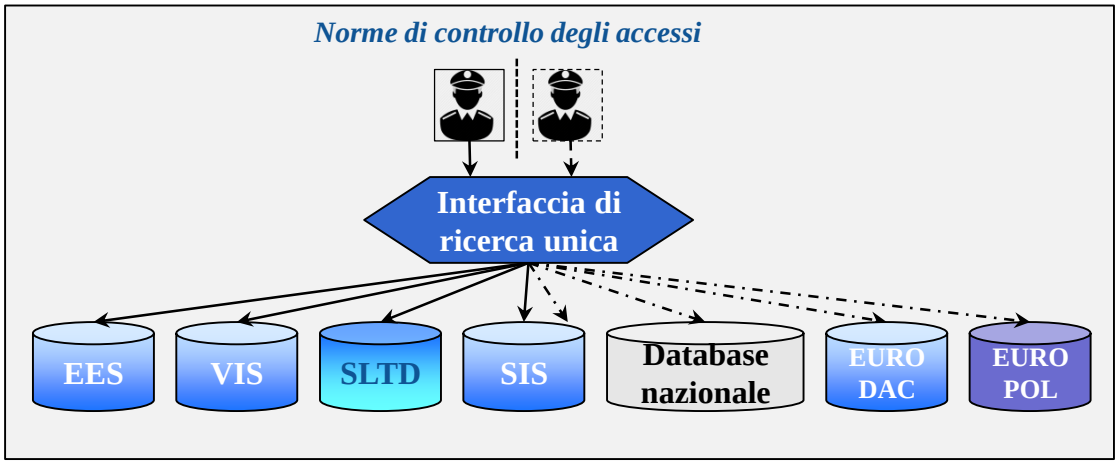
1. Interfaccia di ricerca unica

La prima dimensione dell'interoperabilità è la **capacità di interrogare contemporaneamente diversi sistemi di informazione ottenendo risultati combinati su una sola schermata** per le guardie di frontiera e gli agenti di polizia, nel pieno rispetto dei loro diritti di accesso e in linea con i rispettivi scopi. Ciò richiede piattaforme con un'interfaccia unica di ricerca che siano in grado di consultare contemporaneamente i sistemi di informazione con un'unica interrogazione. Ad esempio mediante la lettura del chip del documento di viaggio o utilizzando i dati biometrici la piattaforma potrebbe interrogare simultaneamente più banche dati. Il concetto di ricerca unica si applica a tutte le autorità (guardie di frontiera, autorità di contrasto, servizi per l'asilo) che hanno necessità di accedere ai dati e di utilizzarli nel rispetto della limitazione delle finalità e di norme rigorose per il controllo degli accessi. Tale ricerca può essere effettuata anche

utilizzando dispositivi mobili. La creazione di un'interfaccia di ricerca unica riduce la complessità dei sistemi d'informazione a livello europeo, poiché consente alle guardie di frontiera e ai funzionari di polizia di effettuare ricerche in diversi sistemi di informazione simultaneamente con un singolo processo e in conformità con i loro diritti di accesso.

Vari Stati membri hanno già installato piattaforme con un'interfaccia di ricerca unica. Sulla base delle migliori pratiche esistenti, la Commissione lavorerà insieme ad eu-LISA alla realizzazione di una soluzione standardizzata per un'interfaccia di ricerca unica. Gli Stati membri dovrebbero utilizzare i fondi dell'UE nell'ambito dei rispettivi programmi nazionali del Fondo sicurezza interna per finanziare l'installazione di tale funzionalità. La Commissione seguirà da vicino il modo in cui gli Stati membri utilizzano la funzionalità di interfaccia di ricerca unica a livello nazionale.

Figura 2 *Interfaccia di ricerca unica*



Effettuare una ricerca su più sistemi, centralizzati o nazionali, (come illustrato in figura) è più semplice che interrogare sistemi decentrati. La Commissione ed eu-LISA valuteranno se sia possibile utilizzare un'interfaccia di ricerca unica per effettuare ricerche simultanee in sistemi decentrati quali Prüm ed ECRIS. La Commissione ed eu-LISA svolgeranno questa analisi insieme al gruppo di esperti sui sistemi di informazione e l'interoperabilità, senza modificare i diritti di accesso esistenti.

2. Interconnettività dei sistemi di informazione

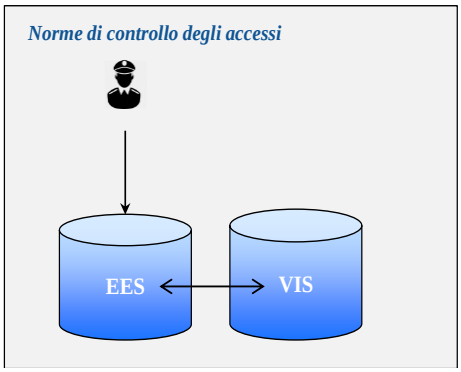
La seconda dimensione dell'interoperabilità è l'interconnettività dei sistemi di informazione. Ciò significa che le diverse banche dati o sistemi sono in grado di "dialogare" dal punto di vista tecnico. **I dati registrati in un sistema possono essere consultati automaticamente da un altro sistema a livello centrale**. Ciò presuppone la compatibilità tecnica tra i sistemi e l'interoperabilità dei dati in essi contenuti (ad es. le impronte digitali). L'interconnettività può ridurre la quantità di dati che circola sulle reti di comunicazione e che transita nei sistemi nazionali.

L'interconnettività richiede adeguate garanzie di protezione dei dati e norme rigorose di controllo degli accessi. L'accordo politico raggiunto dai colegislatori nel dicembre 2015 sulla riforma della protezione dei dati consentirà di creare un moderno quadro di protezione dei dati in tutta l'Unione europea in grado di prevedere tali garanzie. È importante che i colegislatori adottino senza indugio il regolamento generale sulla protezione dei dati e la direttiva sulla protezione dei dati.

Il concetto di interconnettività è parte integrante del futuro sistema di ingressi/uscite, che sarà in grado di comunicare direttamente con il VIS a livello centrale (e viceversa). Si

tratta di un passo importante per porre rimedio all'attuale frammentazione dell'architettura di gestione dei dati dell'UE per il controllo delle frontiere e la sicurezza interna. Il controllo incrociato automatizzato consente agli Stati membri di non dover consultare il VIS durante i controlli alle frontiere, riduce la manutenzione richiesta e migliora le prestazioni del sistema.

Figura 3 *Interconnettività dei sistemi: l'esempio del sistema di ingressi/uscite e del VIS*



Successivamente la Commissione ed eu-LISA valuteranno se l'interconnettività a livello centrale tra il futuro sistema di ingressi/uscite e il VIS possa essere estesa al SIS, e se possa essere stabilita un'interconnettività tra l'EURODAC e il SIS. La Commissione ed eu-LISA svolgeranno questa analisi insieme al gruppo di esperti sui sistemi di informazione e l'interoperabilità.

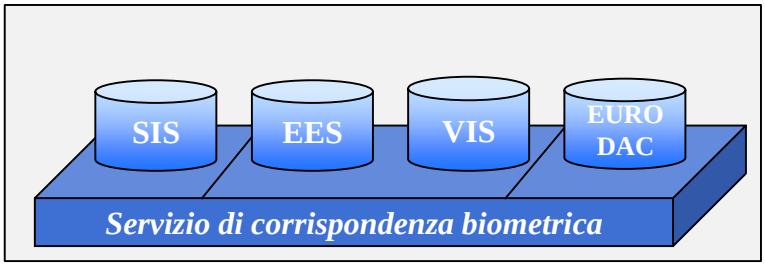
3. Servizio comune di corrispondenza biometrica

La terza dimensione dell'interoperabilità è costituta dal settore degli identificatori biometrici. Ad esempio è fondamentale che le impronte digitali raccolte con strumenti specifici presso il consolato di uno Stato membro possano essere confrontate mediante il VIS ad un posto di frontiera di un altro Stato membro utilizzando strumenti di altro tipo. Lo stesso requisito si applica alle interrogazioni relative alle impronte digitali in altri sistemi: i campioni biometrici devono soddisfare requisiti minimi di qualità e formato affinché sia possibile ottenere facilmente questo tipo di interoperabilità.

A livello di sistema l'interoperabilità degli identificatori biometrici consente l'utilizzo di un servizio comune di corrispondenza biometrica per diversi sistemi di informazione, rispettando nel contempo le norme sulla protezione dei dati personali mediante la suddivisione di questi ultimi in categorie, a ciascuna delle quali si applicano specifiche norme di controllo degli accessi[27]. Servizi condivisi di questo tipo offrono grandi vantaggi in termini finanziari, operativi e di manutenzione.

[27] Simile alla condivisione di un server di archivio fisico con una molteplicità di utenti, ciascuno dei quali ha diritti di accesso specifici relativi solo ad alcune cartelle.

Figure 4 *Servizio comune di corrispondenza biometrica*



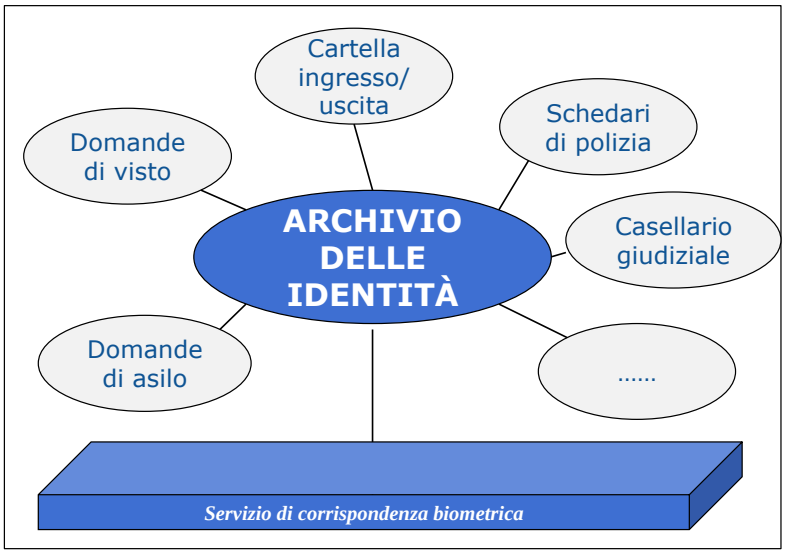
La Commissione ed eu-LISA valuteranno la necessità e la fattibilità tecnica dell'istituzione di un servizio comune di corrispondenza biometrica per tutti i sistemi d'informazione pertinenti. La Commissione ed eu-LISA svolgeranno questa analisi insieme al gruppo di esperti sui sistemi di informazione e l'interoperabilità.

4. Archivio comune di dati

Il progetto a lungo termine più ambizioso in materia di interoperabilità sarebbe un **archivio comune di dati a livello dell'UE per diversi sistemi di informazione**. L'archivio comune costituirebbe un modulo centrale contenente i dati di base (dati alfanumerici e biometrici), mentre altri dati e caratteristiche proprie dei diversi sistemi di informazione (ad es. i dati sui visti) sarebbero archiviati in moduli specifici. Il modulo centrale e i moduli specifici sarebbero collegati tra loro per consentire la connessione tra le rispettive serie di dati. In questo modo si verrebbe a creare una **gestione modulare e integrata dell'identità per le frontiere e sicurezza**. Sarebbe necessario garantire il rispetto delle norme sulla protezione dei dati, ad esempio mediante la suddivisione di questi ultimi in categorie, a ciascuna delle quali si applicherebbero specifiche norme di controllo degli accessi.

L'istituzione di archivio comune di dati consentirebbe di superare l'attuale frammentazione dell'architettura della gestione dei dati dell'UE per il controllo delle frontiere e la sicurezza interna. Questa frammentazione, che fa sì che gli stessi dati siano archiviati più volte, è in contrasto con il principio di minimizzazione dei dati. L'archivio comune dovrebbe consentire, laddove necessario, di riconoscere i collegamenti e fornire un quadro globale combinando i singoli dati archiviati nei diversi sistemi di informazione. In questo senso esso consentirebbe di superare l'attuale mancanza di informazioni e contribuirebbe al lavoro delle guardie di frontiera e degli agenti di polizia eliminando le zone d'ombra.

Figura 5 *Archivio comune di dati*



L'istituzione di un archivio comune di dati a livello dell'UE solleva importanti questioni di definizione delle finalità, della necessità, della fattibilità tecnica e della proporzionalità del trattamento dei dati che esso comporta. Richiedendo una revisione completa del quadro giuridico su cui si fondano i vari sistemi di informazione, questo obiettivo potrebbe essere raggiungibile solo nel lungo periodo. Il gruppo di esperti sui sistemi di informazione e l'interoperabilità si occuperà delle questioni giuridiche, tecniche e operative connesse a un archivio comune di dati, anche per quanto concerne la protezione dei dati.

Per tutte e quattro le dimensioni dell'interoperabilità sopra menzionate (interfaccia di ricerca unica, interconnettività dei sistemi, servizio comune di corrispondenza biometrica e archivio comune di dati) è necessario che i dati archiviati nei diversi sistemi di informazione o moduli siano compatibili. A tal fine è importante continuare a lavorare sul formato UMF (**Uniform Message Format**) per creare uno standard comune per tutti i sistemi d'informazione pertinenti[28].

Azioni per l'interoperabilità dei sistemi di informazione

- La Commissione istituirà un **gruppo di esperti sui sistemi di informazione e l'interoperabilità** in collaborazione con le agenzie dell'UE, gli Stati membri e gli interlocutori istituzionali per valutare le questioni legali, tecniche e operative connesse a una maggiore interoperabilità dei sistemi di informazione, tenendo conto della necessità, della fattibilità tecnica e della proporzionalità delle opzioni disponibili e delle loro implicazioni per la protezione dei dati.

[28] La Commissione ha sostenuto lo sviluppo continuo del formato UMF nella comunicazione del 2012 sul modello europeo di scambio delle informazioni (EIXM) e finanzia attualmente il terzo progetto pilota UMF, allo scopo di creare uno standard comune per tutte le banche dati pertinenti, da utilizzare a livello nazionale (degli Stati membri), a livello dell'UE (per i sistemi centrali e da parte delle agenzie) e a livello internazionale (Interpol).

Interfaccia di ricerca unica

- La Commissione ed eu-LISA forniranno un supporto agli Stati membri per l'installazione di un'interfaccia di ricerca unica per le interrogazioni nei sistemi centrali.
- La Commissione ed eu-LISA valuteranno, insieme al gruppo di esperti, se sia possibile utilizzare interfacce di ricerca uniche per effettuare ricerche simultanee in tutti i sistemi pertinenti senza modificare i diritti di accesso esistenti.

Interconnettività dei sistemi di informazione

- La Commissione ed eu-LISA valuteranno, insieme al gruppo di esperti, se sia possibile promuovere ulteriormente l'interconnettività tra sistemi di informazione centralizzati, al di là di quanto già proposto per l'interconnettività tra il sistema di ingressi/uscite e il sistema di informazione visti.

Servizio di corrispondenza biometrica

- La Commissione ed eu-LISA analizzeranno, in collaborazione con il gruppo di esperti, la necessità e la fattibilità tecnica dell'istituzione di un servizio comune di confronto biometrico per tutti i sistemi di informazione pertinenti.

Archivio comune di dati (modulo centrale)

- La Commissione ed eu-LISA valuteranno, in collaborazione con il gruppo di esperti, le implicazioni giuridiche, tecniche, operative e finanziarie dello lo sviluppo nel lungo termine di un archivio comune di dati.
- La Commissione ed eu-LISA prenderanno parte ai lavori in corso per la realizzazione di un formato UMF globale per tutti i sistemi d'informazione in questione.

8. CONCLUSIONI

La presente comunicazione avvia un dibattito sul modo in cui i sistemi di informazione dell'UE possono rafforzare la gestione delle frontiere e la sicurezza interna, basandosi su importanti sinergie tra l'agenda europea sulla sicurezza e quella sulla migrazione. I diversi sistemi di informazione attualmente in uso forniscono alle guardie di frontiera e ai funzionari di polizia informazioni utili, ma non sono perfetti. L'UE deve misurarsi con la sfida di costruire un'architettura più solida e più intelligente per la gestione dei dati, nel pieno rispetto dei diritti fondamentali e in particolare della protezione dei dati personali e del principio della limitazione delle finalità.

A questo scopo è anche necessario colmare le lacune esistenti nell'architettura della gestione dei dati dell'UE. Insieme alla presente comunicazione, la Commissione ha presentato una proposta relativa a un sistema di ingressi/uscite che dovrebbe essere adottata con urgenza. Anche la direttiva sul codice di prenotazione (PNR) dovrebbe essere adottata nelle prossime settimane. La proposta di una guardia costiera e di frontiera europea dovrebbe essere adottata prima dell'estate. Parallelamente la Commissione continuerà a lavorare per rafforzare e, se necessario, razionalizzare i sistemi esistenti, ad esempio sviluppando una funzionalità per il sistema automatizzato di identificazione delle impronte digitali da integrare nel sistema d'informazione Schengen.

Gli Stati membri devono utilizzare appieno i sistemi di informazione esistenti e realizzare i necessari collegamenti a tutti i sistemi di informazione e banche dati, in linea con i loro obblighi giuridici. Le carenze esistenti, in particolare per quanto concerne il quadro di Prüm, devono essere eliminate senza indugio. Sebbene questa comunicazione avvii un dibattito e un processo per affrontare le lacune e le carenze di sistema, spetta agli

Stati membri risolvere con urgenza le persistenti problematiche inerenti all'alimentazione delle banche dati e allo scambio di informazioni nell'Unione.

La comunicazione dà inoltre il via a un processo volto a conseguire l'interoperabilità dei sistemi di informazione al fine di migliorare strutturalmente l'architettura di gestione dei dati dell'UE per il controllo delle frontiere e la sicurezza, La Commissione istituirà un gruppo di esperti sui sistemi di informazione e l'interoperabilità per valutare le modalità e le opzioni giuridiche, tecniche e operative per conseguire l'interoperabilità dei sistemi di informazione e colmare eventuali lacune e carenze. Una volta ricevute le conclusioni del gruppo di esperti, la Commissione europea presenterà ulteriori proposte concrete al Parlamento europeo e al Consiglio quale base comune per una discussione sulle prospettive future. La Commissione richiederà anche il contributo del garante europeo della protezione dei dati e delle autorità nazionali per la protezione dei dati, che si riuniscono nel gruppo di lavoro "articolo 29".

L'obiettivo dovrebbe essere la messa a punto di una strategia comune per una gestione dei dati nell'UE più efficace ed efficiente, nel pieno rispetto dei requisiti in materia di protezione dei dati, al fine di proteggere meglio le frontiere esterne e rafforzare la sicurezza interna, a beneficio di tutti i cittadini.

ALLEGATO 1: ABBREVIAZIONI

API	Informazioni anticipate sui passeggeri
AFIS	Sistema di identificazione automatizzato delle impronte digitali: sistema in grado di acquisire, conservare, confrontare e verificare le impronte digitali.
SID	Sistema d'informazione doganale
ECRIS	Sistema europeo di informazione sui casellari giudiziali
EES	Sistema di ingressi/uscite (proposta)
EIXM	Modello europeo di scambio delle informazioni – EIXM;
SIE	Sistema di informazione Europol
EPRIS	Sistema dell'UE d'indice degli schedari di polizia
EURODAC	Sistema europeo di dattiloscopia
EUROPOL	Ufficio europeo di polizia (agenzia di contrasto dell'Unione europea)
ETIAS	(Eventuale) sistema dell'UE di informazione e autorizzazione ai viaggi
eu-LISA	Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia
FIND	Banca dati Interpol in rete fissa
FRONTEX	Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea
iARMS	Sistema dell'Interpol per la registrazione e la tracciabilità delle armi da fuoco illegali
INTERPOL	Organizzazione internazionale di polizia criminale
MIND	Banca dati Interpol in rete mobile
PIU	Unità d'informazione sui passeggeri; unità da istituire in ogni Stato membro per ricevere i dati PNR dai vettori.
PNR	Codice di prenotazione
Prüm	Meccanismo di cooperazione di polizia per lo scambio di informazioni su DNA, impronte digitali e dati di immatricolazione dei veicoli
SafeSeaNet	Piattaforma europea per lo scambio di dati marittimi fra le autorità responsabili del trasporto marittimo degli Stati membri
SBC	Codice frontiere Schengen
SIENA	Applicazione di rete per lo scambio di informazioni protetta
SIS	Sistema d'informazione Schengen (talvolta denominato SIS II, sistema d'informazione Schengen di seconda generazione)
SLTD	Banca dati (dell'Interpol) sui documenti di viaggio rubati e smarriti
sTESTA	Servizi transeuropei sicuri per la comunicazione telematica tra amministrazioni (diventerà TESTA-NG (prossima generazione))

UMF	Uniform Message Format: formato dei messaggi che consente la compatibilità tra i sistemi di informazione
VIS	Sistema d'informazione visti
VRD	Dati di immatricolazione dei veicoli

ALLEGATO 2: INVENTARIO DEI SISTEMI DI INFORMAZIONE ESISTENTI PER LA GESTIONE DELLE FRONTIERE E IL CONTRASTO

1. Sistema di informazione Schengen (SIS)

Il SIS è la più grande e più diffusa piattaforma di scambio di informazioni sull'immigrazione e il contrasto. Si tratta di un sistema centralizzato utilizzato da 25 Stati membri dell'UE[29] e quattro paesi associati a Schengen[30], che contiene attualmente 63 milioni di segnalazioni immesse e consultate dalle autorità competenti (polizia, controllo delle frontiere e immigrazione). Contiene le cartelle dei cittadini di paesi terzi cui è fatto divieto di entrare o di soggiornare nello spazio Schengen, dei cittadini dell'UE e di paesi terzi che sono scomparsi o ricercati (minori compresi) e degli oggetti ricercati (armi da fuoco, veicoli, documenti d'identità, attrezzature industriali, ecc.). La caratteristica distintiva del SIS rispetto ad altri strumenti per la condivisione delle informazioni è che le informazioni sono completate da istruzioni per gli interventi concreti da parte dei funzionari sul terreno, quali arresti o sequestri.

Le verifiche nel SIS sono obbligatorie per il trattamento delle domande di visti per soggiorni di breve durata, per i controlli alle frontiere dei cittadini di paesi terzi e, su base non sistematica[31], dei cittadini dell'UE e delle altre persone che godono del diritto di libera circolazione. Inoltre ogni controllo di polizia sul territorio dovrebbe includere una verifica automatica nel SIS.

2. Sistema di informazione visti (VIS)

Il VIS è un sistema centralizzato per lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata. Elabora i dati e le decisioni inerenti alle domande di visto per soggiorni di breve durata, a fini di visita o di transito attraverso l'area Schengen. Sono stati collegati al sistema tutti i consolati degli Stati Schengen (circa 2000) e tutti i loro valichi delle frontiere esterne (in totale circa 1800).

Il VIS contiene i dati sulle domande di visto e le relative decisioni, nonché sulle revoche, gli annullamenti e le proroghe dei visti rilasciati. Al momento contiene dati su 20 milioni di domande di visto e, nei periodi di picco, gestisce oltre 50 000 operazioni all'ora. Ciascun richiedente fornisce dati anagrafici dettagliati, una fotografia in formato digitale e dieci impronte digitali. Si tratta quindi di un sistema affidabile per verificare l'identità dei richiedenti il visto, per valutare eventuali casi di migrazione irregolare e di minacce alla sicurezza e per prevenire il cosiddetto "visa shopping" (richiesta del visto nel paese in cui le norme appaiono più favorevoli).

Il VIS è utilizzato ai valichi delle frontiere o all'interno del territorio degli Stati membri per verificare l'identità dei titolari di visto confrontandone le impronte digitali con quelle archiviate nel sistema. Questo processo garantisce che la persona che ha presentato domanda di visto sia la stessa persona che attraversa la frontiera. La ricerca delle impronte digitali nel VIS permette inoltre l'identificazione delle persone prive di documenti d'identità che abbiano richiesto un visto negli ultimi cinque anni.

---

[29] Tutti eccetto Cipro, Irlanda e Croazia.

[30] Svizzera, Liechtenstein, Norvegia e Islanda.

[31] Questa norma è passibile di modifica, come previsto dalla proposta della Commissione COM/2015/0670 sulla modifica del codice frontiere Schengen.

3. EURODAC

EURODAC, il sistema europeo di dattiloscopia, contiene le impronte digitali dei richiedenti asilo e dei cittadini di paesi terzi che attraversano irregolarmente le frontiere esterne di Schengen. Il suo scopo principale è stabilire quale paese dell'UE sia responsabile del trattamento delle domande di asilo, in conformità con il regolamento di Dublino. È disponibile ai valichi di frontiera ma, contrariamente al SIS e al VIS, non è un sistema di gestione delle frontiere.

Le impronte digitali dei migranti irregolari che entrano nell'UE illegalmente sono rilevate ai valichi di frontiera e archiviate nell'Eurodac per verificare l'identità della persona nel caso di una futura domanda di asilo. Le autorità per l'immigrazione e di polizia possono inoltre confrontare i dati delle impronte digitali dei migranti irregolari che si trovano negli Stati membri dell'UE per verificare se abbiano presentato domanda d'asilo in un altro Stato membro. Anche le autorità di contrasto e l'Europol possono consultare l'EURODAC ai fini della prevenzione, dell'accertamento e delle indagini per reati gravi o di terrorismo.

La registrazione in un sistema centralizzato delle impronte digitali dei richiedenti asilo e dei migranti irregolari consente l'identificazione e il controllo dei loro movimenti secondari[32] all'interno dell'UE fino alla presentazione della domanda di protezione internazionale o alla decisione di rimpatrio (in futuro sarà accompagnata dalla relativa segnalazione nel SIS). Più in generale l'identificazione e il monitoraggio dei migranti irregolari sono necessari per garantire il rilascio di nuovi documenti da parte delle autorità dei loro paesi di origine, favorendone così il rimpatrio.

4. Banca dati sui documenti di viaggio rubati e smarriti (SLTD)

La banca dati dell'Interpol sui documenti di viaggio rubati e smarriti (SLTD) è una banca dati centrale sui passaporti e altri documenti di viaggio che le autorità di emissione segnalano all'Interpol come rubati o smarriti. Comprende anche informazioni sui passaporti vergini rubati. I documenti di viaggio di cui sia stato denunciato lo smarrimento o il furto alle autorità dei paesi che partecipano al SIS sono inseriti sia nel SIS che nell'SLTD. Quest'ultimo contiene anche dati sui documenti di viaggio inseriti da paesi che non partecipano al SIS (Irlanda, Croazia, Cipro e paesi terzi).

Come affermato nelle conclusioni del Consiglio del 9 e 20 novembre 2015, e nella proposta della Commissione del 15 dicembre 2015 per un regolamento relativo a una modifica mirata del codice frontiere Schengen[33], i documenti di viaggio dei cittadini di paesi terzi e delle persone che godono del diritto di libera circolazione dovrebbero essere verificati nell'SLTD. Tutti i posti di controllo frontalieri devono essere collegati a questa banca dati. Inoltre la sua consultazione a fini di contrasto all'interno del vari paesi potrebbe produrre benefici anche in termini di sicurezza.

5. Informazioni anticipate sui passeggeri (API)

L'obiettivo dell'API è raccogliere informazioni sull'identità di una persona prima che salga a bordo di voli diretti nell'UE e identificare i migranti irregolari al loro arrivo. I dati API sono costituiti da informazioni contenute nei documenti di viaggio (nome, cognome,

[32] Ad esempio i profughi che, arrivati in Grecia, invece di chiedere asilo intendono proseguire il viaggio via terra verso altri Stati membri.

[33] COM(2015) 670 final, proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (CE) n. 562/2006 per quanto riguarda il rafforzamento delle verifiche nelle banche dati pertinenti alle frontiere esterne.

data di nascita, nazionalità, numero e tipo di documento di viaggio, informazioni sul valico di frontiera di uscita e di entrata e dati relativi ai trasporti. I dati API relativi al passeggero generalmente sono raccolti al momento del check-in.

Le informazioni pre-arrivo riguardanti il trasporto marittimo deve essere trasmesse, nel quadro della convenzione sulla facilitazione del traffico marittimo internazionale, 24 ore prima della data di arrivo prevista della nave. La direttiva 2010/65/UE[34] prevede la trasmissione elettronica dei dati attraverso un'unica finestra che collega SafeSeaNet, la dogana elettronica e altri sistemi elettronici.

Non esiste un sistema centrale dell'UE per la registrazione dei dati API.

6. Sistemi di informazione Europol

Il sistema di informazione Europol (SIE) è una banca dati centralizzata contenente informazioni sulla criminalità a scopo investigativo. Esso può essere utilizzato dagli Stati membri e dall'Europol per l'archiviazione e la ricerca dei dati su reati gravi e terrorismo. Le informazioni archiviate nel SIE riguardano dati relativi a persone, documenti d'identità, veicoli, armi da fuoco, numeri di telefono, posta elettronica, impronte digitali, DNA e informazioni connesse alla criminalità informatica, che possono essere collegati in diversi modi per creare un'immagine più dettagliata e strutturata per i casi di reato. Il SIE favorisce la cooperazione in materia di contrasto e non è utilizzabile da parte delle autorità preposte al controllo delle frontiere.

Per lo scambio di informazioni si utilizza la piattaforma SIENA[35], che è una rete di comunicazione elettronica sicura tra l'Europol, gli uffici di collegamento, le unità nazionali Europol, le autorità competenti designate (quali le dogane, gli uffici per il recupero dei beni, ecc.) e terzi collegati.

Nel maggio 2017 entrerà in vigore il nuovo quadro giuridico dell'Europol, che aumenterà la capacità operativa di quest'ultima in materia di analisi e favorirà l'individuazione dei collegamenti tra le informazioni disponibili.

7. Quadro di Prüm

Il quadro di Prüm si basa su un accordo multilaterale[36] tra gli Stati membri che consente lo scambio di DNA, impronte digitali e dati di immatricolazione dei veicoli. Si tratta di un meccanismo fondato sull'interconnessione tra i sistemi nazionali di tutti gli Stati membri dell'UE al fine di consentire ricerche incrociate a distanza. Se una ricerca produce un riscontro positivo nelle banche dati di altri Stati membri, i relativi dati sono condivisi mediante meccanismi di scambio bilaterale.

8. Sistema europeo di informazione sui casellari giudiziali (ECRIS)

L'ECRIS è un sistema elettronico per lo scambio di informazioni sulle condanne pronunciate a carico di una determinata persona dagli organi giurisdizionali penali all'interno dell'UE, ai fini di un procedimento penale contro l'interessato o, se consentito

---

[34] Direttiva 2010/65/UE del Parlamento europeo e del Consiglio, del 20 ottobre 2010, relativa alle formalità di dichiarazione delle navi in arrivo o in partenza da porti degli Stati membri e che abroga la direttiva 2002/6/CE.

[35] *Secure Information Exchange Network Application* (applicazione di rete per lo scambio di informazioni protetta).

[36] Convenzione di Prüm del 2005. La convenzione è stata integrata nella legislazione dell'UE nel 2008 con la decisione del Consiglio 2008/615/GAI.

dal diritto nazionale, a fini diversi. Gli Stati membri di condanna devono comunicare le condanne pronunciate a carico di un cittadino di un altro Stato membro allo Stato membro di cittadinanza. Lo Stato membro di cittadinanza deve archiviare tali informazioni ed è quindi in grado, su richiesta, di fornire informazioni aggiornate sui precedenti penali dei propri cittadini, indipendentemente dal paese dell'UE in cui sono state pronunciate le condanne.

L'ECRIS consente anche lo scambio di informazioni sulle condanne di cittadini di paesi terzi e apolidi. Le autorità centrali designate di ciascuno Stato membro rappresentano i punti di contatto della rete ECRIS e svolgono tutti i compiti per quanto concerne le informazioni del casellario giudiziale (comunicazione, archiviazione, richiesta, trasmissione, ecc.).