IT 2019

n. 20

Relazione speciale

I sistemi di informazione dell'UE a supporto delle verifiche di frontiera costituiscono uno strumento potente, ma occorre maggiore attenzione alla completezza e attualità dei dati

CORTE
DEI CONTI
EUROPEA

Indice

Sintesi

I La creazione dello spazio Schengen ha abolito le verifiche di frontiera tra i paesi partecipanti, che comprendono 22 Stati membri dell'UE e altri quattro paesi europei. Tuttavia, l'abolizione delle frontiere interne accresce l'importanza di un controllo e una sorveglianza efficaci delle frontiere esterne dello spazio Schengen. Il controllo delle frontiere esterne riveste grande interesse per i cittadini dell'UE e per altri portatori di interessi.

II Per aiutare le guardie di frontiera nel controllo delle frontiere esterne dello spazio Schengen, l'UE ha creato i seguenti sistemi di informazione o quadri comuni per lo scambio di informazioni: il Sistema di informazione Schengen (SIS II); il Sistema di informazione visti (VIS); Eurodac (banca dati di dattiloscopia dell'asilo europeo – sistema per il confronto delle impronte digitali). Inoltre, il Sistema europeo di sorveglianza delle frontiere (Eurosur) e i sistemi di codice di prenotazione (PNR) forniscono ulteriore supporto alle autorità di frontiera.

III L'istituzione e la manutenzione di questi sistemi ha richiesto notevoli investimenti, sia da parte dell'UE che degli Stati Schengen partecipanti. Sulla base delle informazioni disponibili, la Corte stima che il bilancio dell'UE abbia erogato oltre 600 milioni di euro per la creazione di tali sistemi. Considerando la crescente pressione sulle frontiere esterne dell'UE dovuta ai recenti flussi migratori e ai problemi di sicurezza, l'audit della Corte ha inteso individuare alcuni aspetti dell'impostazione e dell'utilizzo dei sistemi sopra indicati che possono aiutare le guardie di frontiera a svolgere in modo più efficiente il proprio lavoro. Inoltre, le osservazioni e le raccomandazioni della Corte possono contribuire ad utilizzare in modo mirato i finanziamenti UE che saranno resi disponibili nel prossimo quadro finanziario pluriennale per sostenere questi sistemi.

IV Il principale quesito di audit era "**I principali sistemi di informazione dell'UE per la sicurezza interna supportano in modo efficiente il controllo alle frontiere?**" La Corte conclude che le guardie di frontiera utilizzano e fanno affidamento in misura crescente su tali sistemi al momento di eseguire le verifiche di frontiera. Tuttavia, alcuni dati non sono attualmente registrati nei sistemi, mentre altri dati sono incompleti o non sono inseriti tempestivamente nei sistemi. Ciò riduce l'efficienza di alcune verifiche di frontiera.

V La Corte ha rilevato che i sistemi sono generalmente ben concepiti per facilitare le verifiche di frontiera e che gli Stati membri visitati dagli auditor della Corte (Finlandia, Francia, Italia, Lussemburgo e Polonia) rispettavano generalmente il quadro normativo

applicabile. Ciononostante, le componenti nazionali dei sistemi SIS II e VIS di alcuni paesi consentono di svolgere verifiche di frontiera in modo più efficiente rispetto a quelle di altri paesi.

VI La realizzazione delle soluzioni informatiche per Eurosur e PNR ha richiesto tempi lunghi, sia a livello nazionale che dell'UE, privando così le guardie di frontiera e altre autorità dei benefici di questi sistemi.

VII Il meccanismo di valutazione di Schengen svolge un ruolo importante nel garantire la sicurezza delle frontiere esterne dell'UE. Le valutazioni sono generalmente approfondite e metodiche e prendono in esame le caratteristiche fondamentali dei sistemi. Tuttavia, gli Stati membri impiegano molto tempo per ovviare alle debolezze individuate. Questo perché non esistono termini vincolanti per l'adozione delle relazioni di valutazione e per l'attuazione delle azioni correttive.

VIII Anche se gli Stati membri utilizzano in misura crescente le informazioni registrate nei sistemi, questo utilizzo dovrebbe essere più sistematico. La Corte ha condotto una indagine presso le guardie di frontiera e ha rilevato che oltre la metà di queste aveva consentito ad alcune persone di varcare le frontiere senza consultare i sistemi. La Corte ha rilevato inoltre una serie di discrepanze tra il numero di visti rilasciati e il numero di visti verificati.

IX Le guardie di frontiera utilizzano i dati registrati nei sistemi come base per prendere decisioni da cui dipende la sicurezza dei cittadini europei. La qualità di tali dati è quindi della massima importanza. In base alla normativa UE, la responsabilità per la qualità dei dati compete agli Stati membri. La Corte ha rilevato pochi riferimenti al controllo della qualità dei dati negli atti giuridici che disciplinano i sistemi di informazione europei. Anche se eu-LISA esegue mensilmente controlli automatizzati sulla qualità dei dati registrati in SIS II, i risultati sono disponibili solo per gli Stati membri interessati e pertanto l'Agenzia o la Commissione non sono in grado di valutare i progressi compiuti dai singoli paesi nell'affrontare i problemi relativi alla qualità dei dati. Né eu-LISA né la Commissione dispongono di poteri esecutivi per imporre agli Stati membri di correggere tempestivamente i problemi relativi alla qualità dei dati.

X Le guardie di frontiera non ottengono sempre dati completi ed aggiornati dai sistemi di informazione. Ad esempio, quando le guardie di frontiera verificano un nominativo in SIS II, possono ricevere centinaia di risultati (per lo più falsi positivi) che, in base alla normativa, sono tenuti a verificare manualmente. Ciò non solo rende meno efficienti le verifiche di frontiera, ma aumenta anche il rischio di non individuare i "veri" riscontri positivi. Le registrazioni incomplete in SIS II incidono inoltre sull'efficienza di altri sistemi ad esso collegati.

XI Eccetto che per Eurodac, non esistono in genere termini obbligatori entro cui procedere all'inserimento dei dati. Ad esempio, Eurosur dovrebbe fornire informazioni in tempo reale sulla situazione alle frontiere. Tuttavia, mentre alcuni paesi oggetto del presente audit registrano effettivamente le informazioni in tempo reale, altri vi provvedono solo una volta alla settimana. Da quando Eurodac ha iniziato a funzionare nel 2003, non vi è stato un anno in cui tutti gli Stati membri abbiano trasmesso le informazioni richieste entro i termini stabiliti. Un ritardo nella trasmissione può far sì che la competenza per l'esame della domanda di asilo venga attribuita allo Stato membro sbagliato.

XII La Corte rivolge alla Commissione le seguenti raccomandazioni:

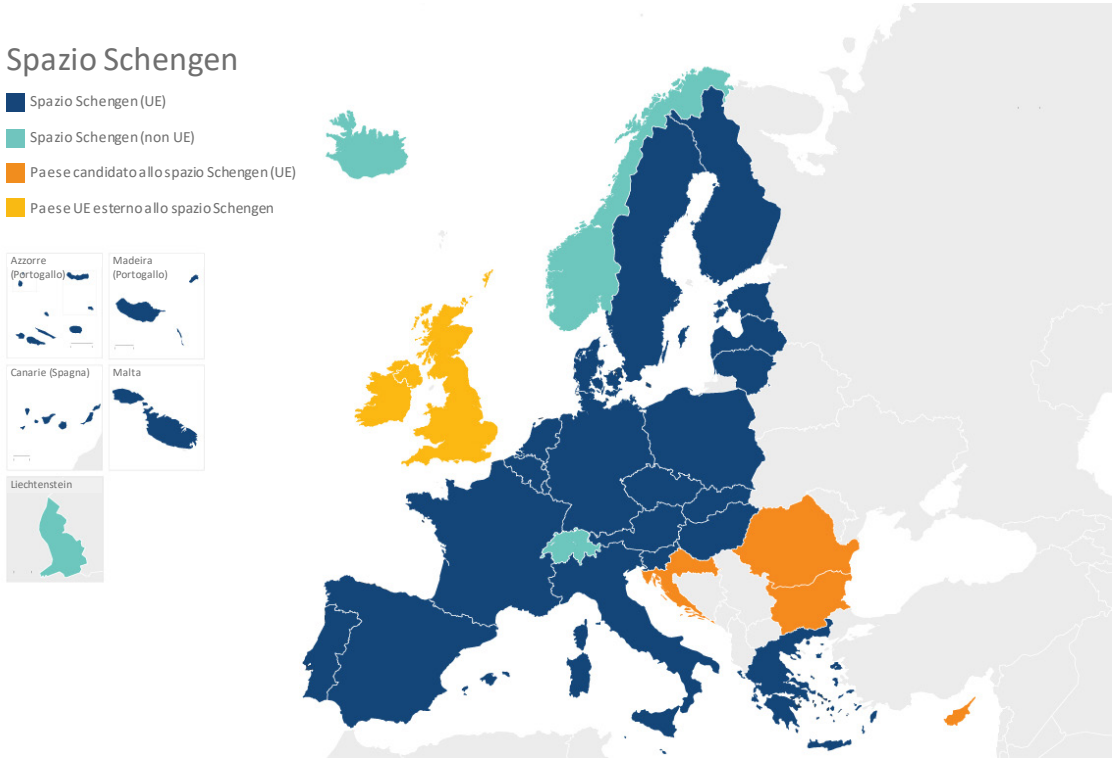
- promuovere l'uso degli ambienti di formazione per SIS II e VIS;
- accelerare la correzione delle debolezze constatate durante le valutazioni Schengen;
- analizzare le discrepanze relative alle verifiche dei visti;
- migliorare le procedure per il controllo della qualità dei dati;
- ridurre i tempi per l'inserimento dei dati.

Introduzione

Lo spazio Schengen

01 La creazione dello spazio Schengen, che attualmente include 26 Stati Schengen (cfr. ***figura 1***), ha permesso a tutti i viaggiatori di attraversare le frontiere interne senza essere soggetti alle verifiche di frontiera. Oltre ad abolire tali verifiche, i paesi partecipanti hanno adottato una politica comune in materia di visti e una cooperazione di polizia e giudiziaria formalizzata.

Figura 1 – Carta attuale dello spazio Schengen



Fonte: Parlamento europeo.

02 Due terzi dei cittadini dell'UE considerano lo spazio Schengen uno dei principali successi dell'UE. Circa il 70 % di essi, però, si aspetta che l'UE faccia di più per proteggere le frontiere esterne[1].

[1] Eurobarometro 89.2, 2018.

I sistemi di informazione utilizzati per controllare le frontiere esterne dello spazio Schengen

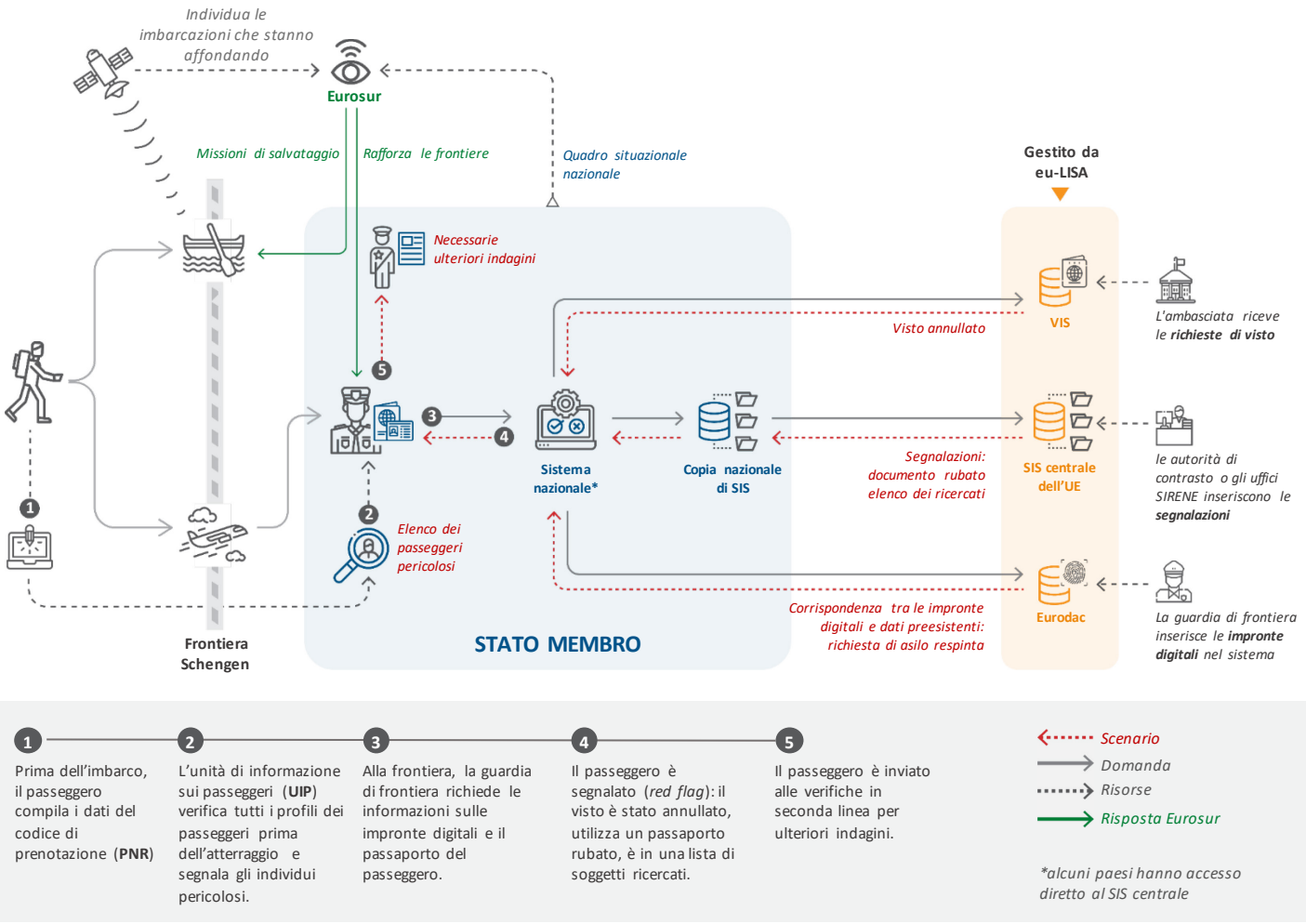
03 L'abolizione delle frontiere interne richiede un controllo ed una sorveglianza efficaci delle frontiere esterne, per prevenire la criminalità ed il terrorismo e controllare l'immigrazione. Per agevolare i controlli svolti dalle guardie di frontiera alle frontiere esterne dello spazio Schengen, l'UE ha creato una serie di sistemi di informazione o quadri comuni per lo scambio di informazioni. I sistemi più comunemente usati sono: il Sistema di informazione Schengen (SIS II); il Sistema di informazione visti (VIS); Eurodac (banca dati di dattiloscopia dell'asilo europeo – sistema per il confronto delle impronte digitali); il Sistema europeo di sorveglianza delle frontiere (Eurosur) e i sistemi di codice di prenotazione (PNR) (cfr. ***figura 2***). Inoltre, l'UE sta sviluppando due sistemi di informazione supplementari per la sicurezza delle frontiere, il sistema di ingressi/uscite e il sistema europeo di informazione e autorizzazione ai viaggi, che dovrebbero essere operativi rispettivamente nel 2020 e nel 2021.

Figura 2 – Sistemi di informazione prima di arrivare a un valico di frontiera esterna e alle frontiere esterne

Fonte: Corte dei conti europea.

04 Le guardie di frontiera negli Stati dello spazio Schengen utilizzano SIS II, VIS e Eurodac per controllare gli individui ai posti di frontiera. Eurosur e PNR sono utilizzati per ottenere informazioni su eventi verificatisi alle frontiere esterne dell'UE e al di là di esse e sui passeggeri di voli che giungono alle nostre frontiere. Consentono di anticipare eventi pertinenti ai fini della sicurezza alle frontiere. La ***figura 3*** mostra come le guardie di frontiera dovrebbero usare questi sistemi durante le verifiche di frontiera, mentre una descrizione più dettagliata, indicante anche quali sistemi di informazione sono a disposizione di quali paesi, è fornita nell'***allegato***.

Figura 3 – Uso dei sistemi di informazione selezionati per la sicurezza delle frontiere



Fonte: Corte dei conti europea.

05 Utenti dei sistemi sono anche diverse autorità nazionali di contrasto, nonché autorità doganali, autorità responsabili dei visti e autorità giudiziarie. Al tempo stesso, queste sono responsabili per l'inserimento dei relativi dati in tali sistemi. Nel caso del PNR, le informazioni sono fornite dalle compagnie aeree.

06 Le guardie di frontiera (e altre autorità) che utilizzano i sistemi negli Stati membri hanno accesso ai sistemi centrali UE attraverso i propri sistemi nazionali, che sono stati appositamente sviluppati a tal fine. I legislatori dell'UE hanno stabilito i requisiti minimi per l'attuazione di questi sistemi di informazione nazionali nell'ordinamento UE[2].

07 A livello dell'UE, la Commissione europea, in particolare la direzione generale della Migrazione e degli affari interni (DG HOME), ha la responsabilità complessiva dello sviluppo e del finanziamento dei sistemi di informazione, ad eccezione del PNR che non ha una componente centrale a livello dell'UE (ma può beneficiare di finanziamenti UE). Dal 2012, la Commissione ha incaricato l'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia ("eu-LISA") dell'archiviazione dei dati e della manutenzione di SIS II, Eurodac e VIS. Eurosur, invece, è gestito dall'Agenzia europea della guardia di frontiera e costiera (EBCGA), nota come Frontex, e dagli Stati membri.

[2] Regolamento (CE) n. 1987/2006 per SIS II, decisione 2007/533/GAI del Consiglio sul SIS II, regolamento (CE) n. 767/2008 per VIS, regolamento (UE) n. 603/2013 per Eurodac, regolamento (UE) n. 1052/2013 per Eurosur e direttiva (UE) 2016/681 per il PNR.

08 Sulla base delle informazioni disponibili, la Corte stima che il bilancio dell'UE abbia stanziato in totale 600 milioni di euro[3] per coprire i costi per l'istituzione delle componenti dei sistemi oggetto del presente audit a livello dell'UE. Il costo totale annuo del funzionamento dei sistemi era di circa 61,5 milioni di euro[4]. Inoltre, gli Stati membri contribuiscono al costo dello sviluppo e della manutenzione dei sistemi nazionali con finanziamenti erogati dai rispettivi bilanci nazionali. Sebbene le informazioni sulle spese sostenute dagli Stati membri per i sistemi nazionali non siano sempre disponibili, vi sono elementi che indicano che si tratta di importi significativi. Ad esempio, gli Stati membri hanno speso circa 235 milioni di euro per l'istituzione di SIS II, oltre ai 95 milioni di euro versati dal bilancio UE[5].

[3] Tale importo è stato calcolato sulla base delle informazioni presentate nei documenti pubblicati dalla Commissione o delle informazioni ottenute dai sistemi contabili (per SIS II e VIS). Questo importo non include il costo dello sviluppo di Eurodac, riguardo al quale non sono disponibili cifre aggregate.

[4] Tale importo include gli impegni 2017 di eu-LISA direttamente correlati ai sistemi di informazione oggetto dell'audit e gli impegni 2017 di Frontex relativi a Eurosur, nonché l'esecuzione degli stanziamenti di pagamento 2017 per SIS/VIS/Eurodac ad opera della DG HOME.

[5] Corte dei conti europea, relazione speciale n. 3/2014 "Insegnamenti da trarre dallo sviluppo del Sistema d'informazione Schengen di seconda generazione (SIS II) ad opera della Commissione europea".

Estensione e approccio dell'audit

09 L'UE lavora costantemente per migliorare la sicurezza delle frontiere dell'UE, un tema importante per i cittadini dell'UE. Considerando la crescente pressione sulle frontiere esterne dell'UE dovuta ai recenti flussi migratori e ai problemi di sicurezza, l'audit della Corte ha inteso individuare alcuni aspetti dell'impostazione e dell'utilizzo dei sistemi sopra indicati che possono aiutare le guardie di frontiera a svolgere in modo più efficiente il proprio lavoro. Inoltre, le osservazioni e le raccomandazioni della Corte possono contribuire ad utilizzare in modo mirato i finanziamenti UE che saranno resi disponibili nel prossimo quadro finanziario pluriennale per sostenere questi sistemi.

10 Il principale quesito di audit era:

- i principali sistemi di informazione dell'UE per la sicurezza interna supportano in modo efficiente il controllo alle frontiere?

11 Tale quesito è stato articolato nei seguenti sottoquesiti:

- i sistemi di informazione UE per la sicurezza interna sono ben concepiti ed in grado di facilitare efficienti verifiche di frontiera?
- i sistemi di informazione UE per la sicurezza interna forniscono alle guardie di frontiera informazioni pertinenti, tempestive e complete durante le verifiche di frontiera?

12 L'audit della Corte ha riguardato i seguenti cinque sistemi: il Sistema di informazione Schengen (SIS II); il Sistema di informazione visti (VIS); Eurodac (banca dati di dattiloscopia dell'asilo europeo – sistema per il confronto delle impronte digitali); il Sistema europeo di sorveglianza delle frontiere (Eurosur) e i sistemi di codice di prenotazione (PNR).

13 La Corte ha valutato in che misura i sistemi (sia le componenti nazionali che quelle centrali dei sistemi UE) hanno consentito alle guardie di frontiera e agli altri agenti di verificare i singoli individui che entrano nello spazio Schengen attraverso i posti di frontiera autorizzati[6]. Questi includono i valichi di frontiera terrestri, i porti marittimi e gli aeroporti (che, per alcuni Stati membri, sono le uniche frontiere esterne dell'UE).

14 Gli auditor della Corte hanno esaminato ed analizzato i documenti strategici, le valutazioni e le statistiche relative ai cinque sistemi oggetto dell'audit, nonché una serie di documenti attuativi sia a livello nazionale che UE. Hanno inoltre visitato i posti di frontiera e intervistato le autorità di frontiera in Finlandia, Francia, Italia, Lussemburgo e Polonia. In aggiunta, hanno intervistato il personale della DG HOME, di Frontex e di eu-LISA.

15 La Corte ha inoltre svolto un sondaggio presso le guardie di frontiera nei 28 Stati membri dell'UE e nei 4 Stati associati Schengen (Islanda, Liechtenstein, Norvegia e Svizzera) per conoscere il loro parere in quanto utenti dei sistemi. Alla Corte sono pervenute 951 risposte.

---

[6] La Corte aveva già trattato alcuni temi riguardanti l'immigrazione irregolare nella relazione speciale n. 6/2017 "La risposta dell'UE alla crisi dei rifugiati: il "sistema basato sui punti di crisi"(*hotspot approach*)" ed analizzerà ulteriormente tali questioni in prossime pubblicazioni.

Osservazioni

La concezione dei sistemi di informazione facilita verifiche di frontiera efficienti, ma porre rimedio alle debolezze richiede molto tempo

16 La Corte ha valutato se gli Stati Schengen visitati abbiano posto in essere i sistemi di informazione secondo le modalità e nei tempi stabiliti dalla normativa UE applicabile. Ha esaminato inoltre il meccanismo di valutazione Schengen e in che misura gli Stati Schengen abbiano utilizzato i finanziamenti UE disponibili per porre in essere e migliorare i rispettivi sistemi nazionali.

I sistemi di informazione sono generalmente conformi ai requisiti UE, ma operano con gradi di efficienza variabili

17 Se da un lato ogni Stato Schengen ha la responsabilità esclusiva della protezione delle proprie frontiere, una efficace cooperazione tra di essi per proteggere lo spazio Schengen richiede un determinato grado di armonizzazione delle verifiche di frontiera. Requisiti minimi in termini di governance contribuiscono alla coerenza e alla qualità delle verifiche di frontiera e dei dati inseriti nei sistemi di informazione.

18 Ogni Stato Schengen deve porre in essere sistemi nazionali complementari, collegati ai sistemi centrali dell'UE. Tutti gli Stati Schengen visitati avevano ottemperato agli obblighi previsti dalla normativa applicabile. Gli auditor hanno però rilevato che, anche se tutti i sistemi presentavano i requisiti minimi comuni, non tutti i sistemi nazionali erano ugualmente efficienti. I paragrafi che seguono illustrano alcuni esempi al riguardo.

19 Alcuni paesi non rendono disponibili attraverso i rispettivi sistemi nazionali tutte le funzionalità offerte dai sistemi centrali UE, riducendo così l'efficienza delle verifiche di frontiera. Ad esempio, il sistema centrale SIS II offre l'opzione di archiviazione e verifica delle impronte digitali. Si tratta di una funzionalità importante giacché non è sempre possibile identificare in modo univoco una persona sulla base dei dati personali di base, come il nome o la data di nascita. Tali dati possono essere contraffatti o la persona può rifiutarsi di fornirli. Le impronte digitali consentono di identificare una persona con un grado di certezza molto maggiore. Tuttavia, l'opzione per l'esecuzione di ricerche biometriche sulla base delle impronte digitali archiviate nel SIS non è ancora disponibile in tutti i sistemi nazionali degli Stati Schengen, in quanto alcuni

hanno bisogno di più tempo rispetto ad altri per realizzare le necessarie soluzioni tecniche. Quando l'identificazione delle impronte digitali è stata disponibile a livello centrale, solo 10 Stati Schengen hanno confermato di essere pronti ad utilizzarla.

20 Le guardie di frontiera che verificano un visto o un passaporto ricevono talvolta messaggi di errore dai sistemi. Le cause possono essere diverse, come l'insufficiente qualità delle impronte digitali, problemi di connettività o di lettura del visto. Anche se i sistemi centrali UE indicano in genere la natura dell'errore, alcuni sistemi nazionali, come quelli di Lussemburgo e Finlandia, segnalano soltanto la presenza di un errore senza fornire una diagnosi. Le guardie di frontiera devono quindi indagare sulla causa dell'errore e potenzialmente sottoporre il passeggero ad una ulteriore verifica (nota come "verifica in seconda linea"), prolungando così i controlli e la durata del viaggio del passeggero.

21 Nel caso di SIS II, gli Stati Schengen possono accedere o inviare richieste alla banca dati centrale oppure creare copie nazionali della banca dati a tale scopo. Anche se la maggior parte di essi utilizza le proprie copie nazionali, alcuni (Danimarca, Finlandia, Liechtenstein, Norvegia e Slovenia) si connettono direttamente alla banca dati UE. Dove gli Stati Schengen utilizzano copie nazionali di SIS II, queste devono essere continuamente sincronizzate con la banca dati centrale UE per far sì che le verifiche di frontiera possano avvalersi delle informazioni più aggiornate. Tuttavia, in due paesi del campione selezionato dalla Corte (Polonia e Francia), le valutazioni hanno indicato discrepanze tra le registrazioni delle copie nazionali e quelle della banca dati centrale.

22 La Corte ha riscontrato inoltre che alcuni vincoli giuridici a livello di Stato membro (norme sulla protezione dei dati e norme di sicurezza nazionale) impedivano una efficiente condivisione delle risorse umane. In effetti, le guardie di frontiera che si recano in un altro Stato Schengen (ad esempio, per prestare assistenza in caso di controlli rafforzati durante la crisi migratoria in Grecia ed Italia) non possono utilizzare i sistemi nazionali di tale paese. In linea di principio, non possono effettuare autonomamente le verifiche, ma solo assistere le guardie di frontiera nazionali. Anche se possono offrire assistenza in misura variabile durante le verifiche in seconda linea (ad esempio, uno Stato Schengen potrebbe avvalersi di un esperto in documenti contraffatti di un altro Stato Schengen), possono aiutare ben poco durante i controlli dei documenti ai posti di frontiera (verifiche in prima linea). Un altro ostacolo è rappresentato dalla barriera linguistica quando si opera in un altro Stato Schengen.

23 I benefici che i sistemi possono offrire alle guardie di frontiera dipendono dal livello di formazione ricevuto su come utilizzarli. La Corte ha rilevato che, poiché non

esisteva un ambiente di formazione all'uso di SIS II e VIS realizzato a livello nazionale negli Stati membri visitati, le guardie di frontiera dovevano fare pratica sul campo invece che in un ambiente "sicuro" dove sperimentare situazioni e scenari che non incontrano di frequente nella pratica (ad esempio, un risultato che segnala un sospetto terrorista ad un posto di frontiera o un minore scomparso).

A causa di ritardi nell'attuazione di Eurosur e PNR, le autorità di frontiera non hanno potuto condividere informazioni importanti

24 Le procedure per l'introduzione di Eurosur e PNR erano diverse da quelle dei sistemi sviluppati e gestiti da eu-LISA. Per diverse ragioni, l'introduzione di questi due sistemi ha conosciuto alcuni casi di ritardi e scadenze disattese. Di conseguenza, informazioni importanti che questi sistemi avrebbero dovuto fornire non sono state disponibili per diversi mesi.

25 Eurosur è stato sviluppato da Frontex (per la componente europea) e dagli Stati membri (per le componenti nazionali). L'interfaccia utente finale è la stessa per tutte le autorità nazionali partecipanti. Il sistema dovrebbe rafforzare la cooperazione tra Frontex e gli Stati membri dell'UE per favorire una maggiore conoscenza delle situazioni alle frontiere esterne dell'UE e reagire più prontamente. Gli Stati membri dovrebbero contribuire fornendo informazioni sulla situazione alle loro frontiere (note come "quadri situazionali nazionali", che mostrano informazioni su attraversamenti delle frontiere non autorizzati, reati transnazionali, situazioni di crisi o altri eventi riguardanti il controllo delle frontiere esterne), in modo da creare una capacità di intelligence condivisa ed un quadro della situazione in tutta l'Europa. Tali informazioni servono, ad esempio, per decidere dove inviare prioritariamente le guardie di frontiera o per individuare veicoli/imbarcazioni sospetti.

26 Per quanto riguarda Eurosur, vi sono stati ritardi nella creazione dei centri nazionali di coordinamento. Tali centri coordinano lo scambio di informazioni tra tutte le autorità responsabili della sorveglianza delle frontiere esterne. In base al regolamento Eurosur, gli Stati membri dovevano costituire i propri centri nazionali di coordinamento entro dicembre 2014. Tuttavia, una valutazione svolta quasi quattro anni più tardi ha rilevato che diversi Stati membri non avevano ancora pienamente ottemperato a tale obbligo[7]. Inoltre, solo metà degli Stati membri condivideva le

[7] COM(2018) 632 *final* "Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione del sistema europeo di sorveglianza delle frontiere (EUROSUR)".

informazioni non obbligatorie sull'impiego delle risorse di sorveglianza o informazioni aggiuntive sui rispettivi quadri situazionali nazionali.

27 Anche l'attuazione di Eurosur a livello UE ha subito ritardi. Frontex ha ottenuto la certificazione di sicurezza richiesta per la sua rete solo alla fine del 2017, ossia tre anni dopo l'entrata in vigore della normativa. Senza questa certificazione, non era possibile condividere informazioni classificate sulla rete Eurosur. A causa dei ritardi nell'attuazione di Eurosur, i quadri situazionali a livello UE erano incompleti, ostacolando così la cooperazione tra Stati membri.

28 Anche il PNR non è ancora pienamente operativo. A differenza degli altri sistemi, il PNR è stato istituito da una direttiva invece che da un regolamento. Di conseguenza, sono stati gli Stati membri a dover creare, ciascuno per sé, i propri sistemi PNR, senza alcuna piattaforma comune europea. La decisione di adottare una attuazione decentrata era stata principalmente motivata dal mancato consenso su protezione, archiviazione e comunicazione dei dati personali.

29 Molti Stati membri non hanno attuato tempestivamente il PNR. Quattordici Stati membri non hanno attuato le norme sui dati PNR[8] entro il termine stabilito dalla direttiva[9], ossia il 25 maggio 2018. Tuttavia, alla fine di marzo 2019, vale a dire dieci mesi dopo tale termine, Spagna, Paesi Bassi e Finlandia non avevano ancora notificato alla Commissione eventuali misure adottate a livello nazionale per dare attuazione al PNR[10].

30 Il PNR richiede la trasmissione dei dati dei passeggeri di tutti i voli in partenza da e in arrivo nello spazio Schengen. Al momento dell'audit, nessuno degli Stati membri visitati, eccetto il Lussemburgo, aveva concluso accordi a tal fine con tutte le compagnie aeree interessate.

31 Il PNR è stato concepito come uno strumento per prevenire, accertare e indagare sui reati di terrorismo e altri reati gravi. Il confronto tra i dati dei PNR e le informazioni contenute nelle banche dati della sicurezza consente alle autorità nazionali di individuare individui pericolosi. Il fatto che alcuni sistemi di PNR non siano ancora stati

---

[8] https://europa.eu/rapid/press-release_MEMO-18-4486_it.htm.

[9] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

[10] http://europa.eu/rapid/press-release_MEMO-19-1472_it.htm.

istituiti priva le autorità di frontiera di quei paesi di informazioni anticipate sui soggetti ad alto rischio che attraversano le loro frontiere.

32 Poiché il PNR raccoglie solo i dati identificativi dei passeggeri e quelli relativi ai loro spostamenti, occorre verificare altre banche dati per sapere se un dato passeggero costituisce una minaccia per la sicurezza. La maggior parte degli Stati membri utilizza il SIS II a tal fine. Tuttavia, la normativa si presta a varie interpretazioni. Ad esempio, la Francia ha interpretato il regolamento SIS II in modo tale che non consente di interrogare il SIS II riguardo a elenchi di passeggeri. In pratica, per verificare un elenco di passeggeri al fine di individuare eventuali presunti terroristi, la Francia utilizza soltanto le informazioni contenute nelle proprie banche dati nazionali. Se un sospetto è segnalato in SIS II ed è noto ad altre autorità UE ma non a quelle francesi, la verifica da queste effettuata attraverso il PNR non lo individuerà.

Le valutazioni Schengen analizzano le verifiche di frontiera, ma ovviare alle debolezze richiede molto tempo

33 Sin dal 2013, gli Stati Schengen e la Commissione condividono la responsabilità di attuare il meccanismo di monitoraggio e valutazione previsto dalle norme relative allo spazio Schengen ("acquis di Schengen"). L'obiettivo del meccanismo è far sì che gli Stati Schengen applichino le norme Schengen in modo efficace, uniforme e trasparente. La Corte ha esaminato se l'obiettivo del meccanismo sia stato raggiunto.

34 Il programma di valutazione pluriennale attualmente in corso è stato istituito nel 2014 per il periodo 2015-2019 e copre tutti i 26 Stati Schengen. Ogni paese è valutato una volta durante tale quinquennio.

35 Il ***riquadro 1*** descrive una visita di valutazione standard. I membri del gruppo di valutazione sono designati dagli Stati Schengen a seguito di un invito della Commissione per designazioni (un invito per ogni valutazione, con un termine di due settimane per la designazione dei valutatori da parte degli Stati Schengen). I valutatori di eu-LISA possono partecipare a tali visite, ma non vi prendono parte regolarmente. Il costo delle valutazioni Schengen è relativamente basso rispetto alla spesa per i sistemi di informazione. Per il periodo 2014-2018, la Commissione ha assegnato alle valutazioni Schengen 11,9 milioni di euro. L'attuale programma pluriennale è stato attuato come pianificato, attraverso programmi di valutazione annuali.

Riquadro 1

Visite del gruppo di valutatori Schengen negli Stati Schengen

Nel luglio dell'anno precedente la visita di valutazione, gli Stati membri interessati ricevono un questionario standard, a cui devono rispondere entro otto settimane. Il gruppo di valutazione prepara la visita sulla base delle risposte ricevute.

Le visite di valutazione durano di norma una settimana. Il gruppo è composto da al massimo otto esperti nominati dagli Stati Schengen, più due rappresentanti della Commissione. I membri del gruppo dispongono di tipi di competenze diversi, il che consente loro di coprire tutti gli aspetti dell'acquis di Schengen. Ogni gruppo è presieduto da due esperti principali (uno nominato dagli Stati membri e uno dalla Commissione), responsabili del contenuto e della qualità della relazione finale.

La visita inizia a livello strategico, con riunioni presso i ministeri e la sede dell'autorità di frontiera, seguite da attività a livello operativo. I componenti del gruppo di valutazione sono assegnati in base alle diverse aree di competenza e incontrano i diversi operatori nazionali, come le guardie di frontiera, gli agenti di polizia e gli esperti informatici.

Ad esempio, durante la valutazione Schengen 2017 sull'attuazione del SIS II in Francia, il gruppo ha visitato 38 siti in loco, compreso il centro nazionale informatico SIS II, le stazioni di polizia, gli uffici doganali, i porti, gli aeroporti e le stazioni ferroviarie.

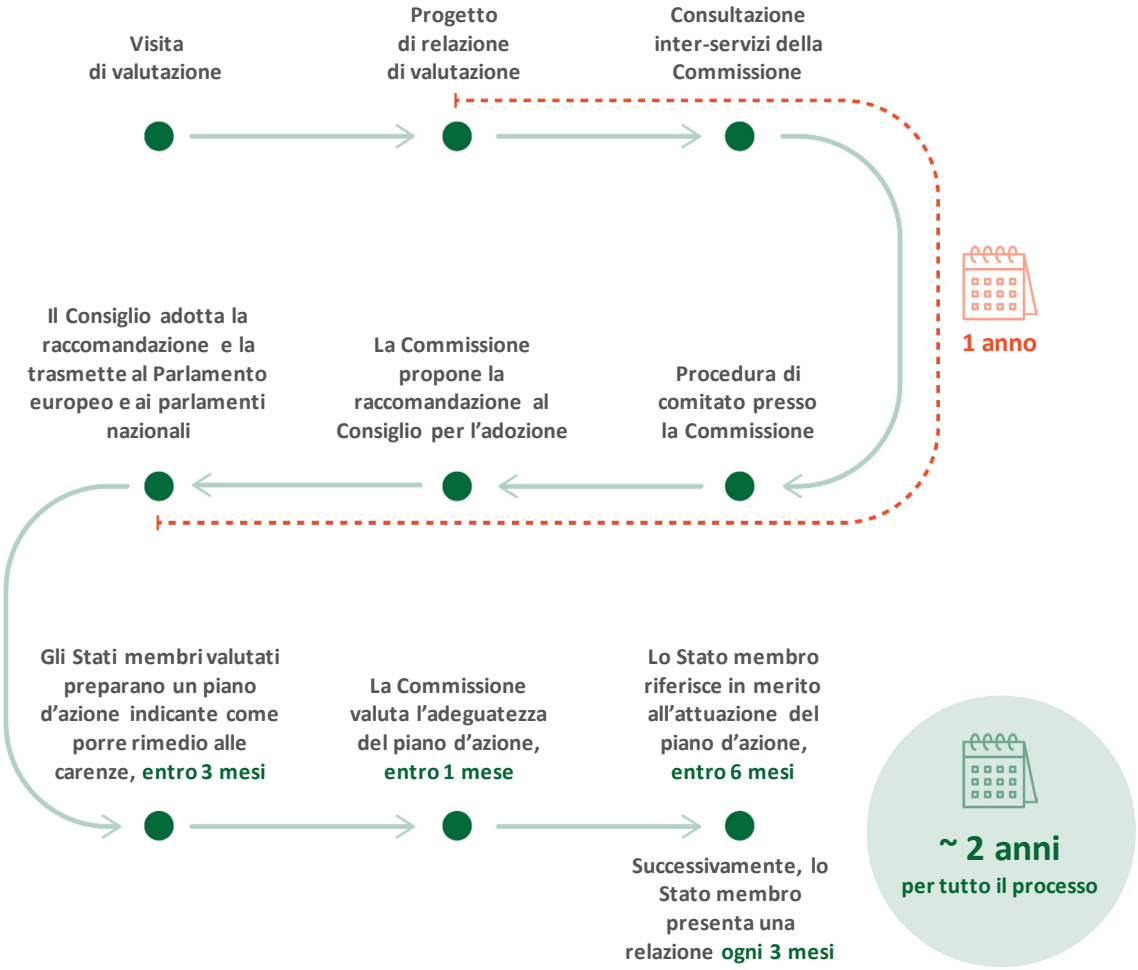
36 La Corte ha esaminato le valutazioni Schengen dei paesi visitati dagli auditor. Ha constatato che queste erano approfondite e metodiche, e prendevano in esame le caratteristiche fondamentali di sistemi. Fornivano una serie di raccomandazioni operative e di raccomandazioni specifiche su come migliorare i sistemi di informazione. Tuttavia, ci sono voluti diversi anni per ovviare alle debolezze segnalate.

37 Il progetto di relazione di valutazione è completato sei settimane dopo la missione di valutazione, ma l'adozione della relazione da parte della Commissione e delle raccomandazioni da parte del Consiglio può richiedere un anno. La procedura prevede numerose consultazioni con gli Stati Schengen e con la Commissione, per le quali non sono stabiliti termini.

38 Dopo che il Consiglio ha adottato le raccomandazioni, gli Stati Schengen interessati hanno tre mesi per presentare un piano d'azione per intervenire sulla base delle raccomandazioni del Consiglio. Questo piano d'azione deve essere esaminato ed approvato dalla Commissione e dal gruppo di valutazione.

39 Non esiste un termine entro cui dare attuazione a tali piani d'azione, anche se gli Stati Schengen devono iniziare a riferire in merito all'attuazione sei mesi dopo l'approvazione del piano. Ciò significa che, dal momento in cui viene individuata una carenza, ci vogliono quasi due anni prima che uno Stato Schengen inizi a riferire sull'intervento correttivo adottato. La ***figura 4*** illustra la procedura seguita dopo la visita di valutazione.

Figura 4 – Fasi procedurali del meccanismo di valutazione Schengen



Fonte: Corte dei conti europea.

40 Fino ad ora, nessuno Stato Schengen è stato oggetto di più di una visita di valutazione annunciata nel quadro dell'attuale ciclo di valutazioni. La Commissione fa affidamento sulle relazioni prodotte dagli stessi Stati Schengen riguardo all'attuazione del piano d'azione concordato. Vi è quindi il rischio che le carenze non siano affrontate sino al successivo giro di valutazioni cinque anni dopo. Ci possono poi volere altri due anni prima che le autorità di un paese intraprendano azioni correttive.

41 La Commissione può suggerire di effettuare visite di follow-up se uno Stato Schengen non attua il piano d'azione, ma non esistono altri meccanismi per imporne l'attuazione. In teoria, se vengono individuate carenze gravi e persistenti in uno Stato Schengen riguardanti la gestione della frontiera esterna, il Consiglio potrebbe, su proposta della Commissione, raccomandare al paese di reintrodurre i controlli alle frontiere con altri Stati Schengen.

42 In base al regolamento del 2013 sul meccanismo di valutazione dell'applicazione dell'acquis di Schengen[11], ogni anno la Commissione è tenuta a presentare al Parlamento europeo e al Consiglio una relazione esauriente sulle valutazioni effettuate, sulle raccomandazioni espresse e sullo stato d'avanzamento dei provvedimenti correttivi. La Commissione non ha ancora presentato tale relazione.

43 Ad eccezione della Finlandia, la cui relazione di valutazione non era stata completata al momento dell'audit, tutti gli Stati Schengen visitati dagli auditor della Corte erano stati oggetto di valutazione. La Corte ha seguìto i progressi compiuti nell'attuazione dei piani d'azione e ha riscontrato diversi tassi di attuazione. Alla luce degli elementi probatori forniti, la Polonia aveva attuato il 79 % delle raccomandazioni ad essa relative due anni dopo la visita di valutazione, la Francia aveva attuato l'87 % delle raccomandazioni quattro anni dopo la visita di valutazione ed il Lussemburgo, che era stato valutato nel 2018, aveva attuato il 92 % delle raccomandazioni. Gli elementi forniti dall'Italia indicano che, due anni dopo la visita di valutazione, il paese stava attuando il 15 % delle raccomandazioni ad esso rivolte.

Gli Stati membri dell'UE utilizzano solo in misura limitata i finanziamenti UE disponibili per migliorare i sistemi di informazione per i controlli alle frontiere

44 Il principale strumento dell'UE per sostenere i controlli delle frontiere è il Fondo sicurezza interna (ISF), che dispone di una dotazione iniziale di 3,8 miliardi di euro per il periodo 2014-2020. Esso comprende:

- ISF – Frontiere e visti (2,76 miliardi di euro), che fornisce sostegno finanziario per la gestione delle frontiere esterne e la politica comune dei visti. Tutti gli Stati dell'UE, eccetto Irlanda e Regno Unito, partecipano all'attuazione dello strumento ISF – Frontiere e visti. I quattro paesi associati a Schengen (Islanda,

[11] Articolo 20 del regolamento (UE) n. 1053/2013 del Consiglio del 7 ottobre 2013.

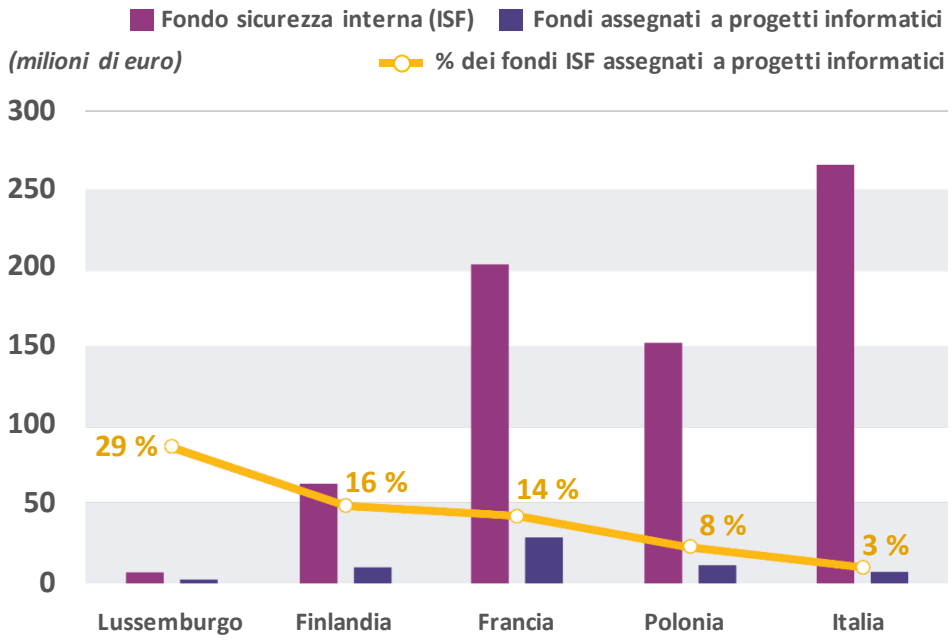
Liechtenstein, Norvegia e Svizzera) partecipano anche allo strumento ISF – Frontiere e visti.

- ISF – Polizia (1,04 miliardi di euro), che fornisce sostegno finanziario per la cooperazione di polizia, la prevenzione e la lotta alla criminalità, compreso il traffico di migranti. Tutti gli Stati dell'UE, eccetto Danimarca e Regno Unito, partecipano all'attuazione dello strumento ISF – Polizia.

45 La maggior parte degli Stati membri non ha dichiarato spese significative fino al 2017. Poiché le spese sono iniziate tardi, gli Stati membri hanno utilizzato i fondi lentamente. Secondo la Commissione, ciò è dovuto principalmente alle lunghe procedure di appalto che è necessario espletare. Gli Stati membri sottoposti ad audit hanno segnalato inoltre l'onere amministrativo supplementare che tali procedure comportano. Ad esempio, hanno notato che anche un modesto aumento dell'importo assegnato ad un programma nazionale richiede una completa revisione di tale programma.

46 I paesi oggetto del presente audit hanno destinato tra il 3 % e il 29 % degli stanziamenti del Fondo sicurezza interna (61,2 milioni di euro) ai cinque sistemi controllati (cfr. ***figura 5***). Di questi, hanno destinato il 43 % (26,5 milioni di euro) a progetti di manutenzione e il 57 % (34,7 milioni di euro) a progetti di estensione. Tali fondi sono stati principalmente utilizzati per la manutenzione di SIS II e di VIS e per l'estensione di Eurosur e di PNR.

Figura 5 – Percentuale dei fondi ISF assegnata a progetti informatici



Fonte: Corte dei conti europea, sulla base dei dati della Commissione europea.

Le guardie di frontiera non ottengono sempre dati completi dai sistemi, il che compromette l'efficienza delle verifiche

47 La Corte ha valutato in che misura gli Stati membri condividano informazioni pertinenti, tempestive e complete attraverso i sistemi di informazione oggetto del presente audit. Sono state esaminate le statistiche disponibili per valutare in che misura i paesi Schengen utilizzino i sistemi per le verifiche di frontiera e per lo scambio di informazioni. Inoltre, la Corte ha verificato se questi paesi abbiano tempestivamente inserito dati completi.

Gli Stati membri utilizzano in misura crescente i sistemi per condividere le informazioni, ma le verifiche potrebbero essere più sistematiche

48 A partire dal momento in cui una persona si presenta ad un posto di frontiera dello spazio Schengen, le guardie di frontiera hanno bisogno dei sistemi di informazione europei come ausilio per confermarne l'identità e verificare se è autorizzata ad entrare nello spazio Schengen.

SIS II

49 Ogni Stato Schengen in possesso di informazioni relative ad una persona che deve essere fermata alla frontiera (come prescritto dalla normativa applicabile) deve inserire una segnalazione in SIS II. Le guardie di frontiera di un qualsiasi paese partecipante possono così procedere al fermo quando si trovano in presenza di tale individuo durante le verifiche di frontiera (cfr. ***riquadro 2***).

Riquadro 2

Cogliere nel segno

Quando una persona presenta un documento di viaggio, la guardia di frontiera utilizza uno scanner che legge un identificativo sul documento di viaggio. La maggior parte dei documenti moderni contiene un chip elettronico, mentre quelli più vecchi presentavano uno speciale codice in fondo alla pagina (nello spazio noto come "zona a lettura ottica") e alcuni documenti non hanno alcun identificativo, come ad esempio la maggior parte delle carte d'identità italiane. Se il numero del documento non può essere letto dallo scanner, la guardia di frontiera può inserirlo nel sistema manualmente.

Sulla base dei dati trasferiti al computer, viene trasmessa una interrogazione alle banche dati SIS II nazionali o europee relativa alla persona in questione. La

corrispondenza tra una registrazione nella banca dati e i dati rilevati dalla guardia di frontiera, è denominata "riscontro positivo" (*hit*).

Se la segnalazione iniziale registrata nella banca dati era stata inserita in un paese diverso da quello che ha trasmesso l'interrogazione, il riscontro positivo è chiamato *foreign hit*.

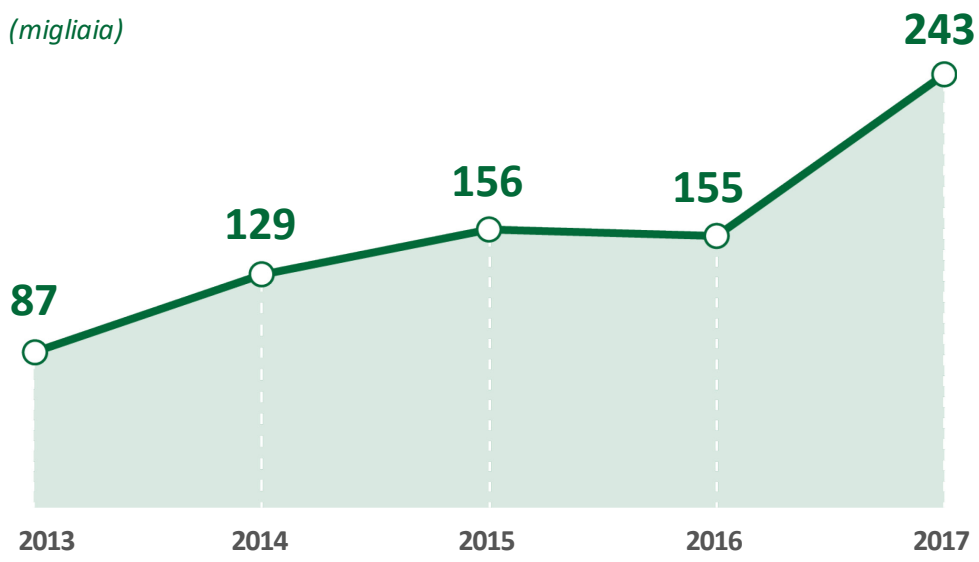
Si può ottenere un riscontro positivo se le autorità hanno registrato una persona come ricercata, o se il documento di viaggio è stato segnalato nel sistema (*flag*).

Tuttavia, talvolta le autorità che inseriscono una segnalazione non dispongono di tutte le informazioni necessarie per identificare una persona in modo univoco. Si può quindi ottenere un riscontro positivo in caso di omonimia con una persona ricercata. Questo tipo di riscontro è chiamato "falso positivo". In tali casi, le guardie di frontiera devono svolgere ulteriori verifiche per accertare l'identità della persona.

I dati biometrici (ad esempio, le impronte digitali) sono generalmente considerate un modo per identificare una persona in modo univoco: per tale ragione un crescente numero di segnalazioni in SIS II contiene informazioni sulle impronte digitali.

50 La Corte ha rilevato che, tra il 2013 e il 2017, il numero di riscontri positivi relative a persone o oggetti ricercati in base alle segnalazioni inserite in altri paesi è quasi triplicato (cfr. ***figura 6***).

Figura 6 – Numero di *hit* in SIS II basate su segnalazioni da altri paesi



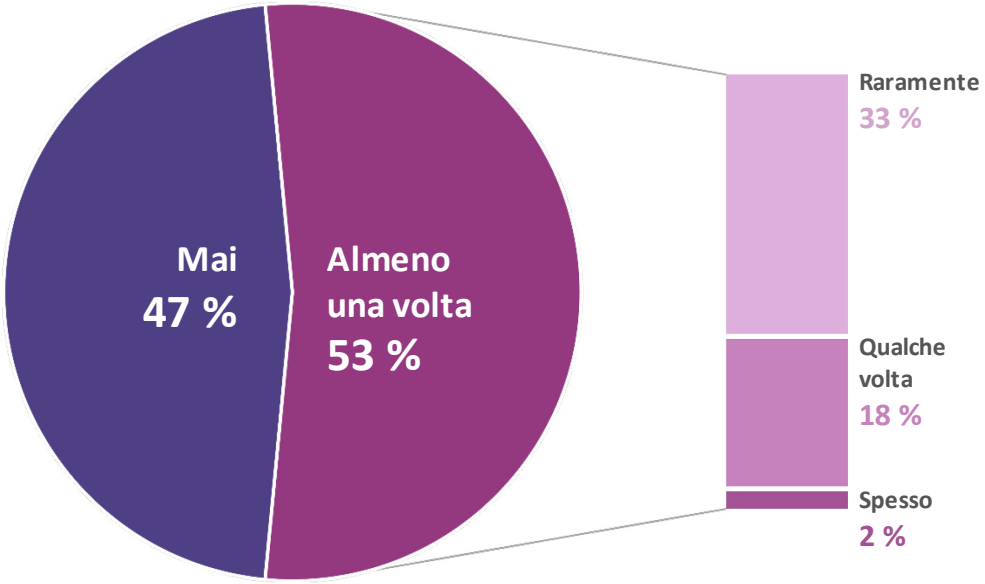
Fonte: Corte dei conti europea, sulla base di dati eu-LISA.

51 Il crescente numero di *hit* è in linea con il costante aumento del numero di segnalazioni in SIS II, da circa 50 milioni nel 2013 a oltre 76 milioni nel 2017. La maggior parte delle segnalazioni (76 %) riguarda documenti smarriti o rubati.

52 In base ai dati Eurostat[12], il numero di cittadini di paesi terzi a cui è stato rifiutato l'accesso alle frontiere esterne è oscillato tra un minimo di 440 000 nel 2017 e un massimo di quasi 500 000 nel 2009. I sistemi di informazione forniscono il necessario supporto per individuare le ragioni più comuni di tali rifiuti. Tuttavia, gli Stati Schengen non sempre specificano o registrano la ragione per cui viene rifiutato l'accesso di un individuo ad una frontiera esterna.

53 Come descritto in precedenza, il numero delle interrogazioni inserite nei sistemi di informazione è in costante crescita. Le autorità nazionali hanno dichiarato nelle interviste di audit di svolgere verifiche su ogni individuo che cerca di attraversare una frontiera esterna. Tuttavia, l'indagine condotta dalla Corte ha rivelato che oltre la metà delle guardie di frontiera si era trovata in una situazione in cui aveva dovuto decidere di ammettere qualcuno senza aver prima consultato i sistemi.

Figura 7 – Indagine: Ha mai dovuto prendere la decisione di ammettere qualcuno senza aver prima potuto consultare i dati nel sistema?



Fonte: indagine della Corte dei conti europea.

54 L'uso dei sistemi di informazione dipende anche dall'ambiente esterno in cui le verifiche vengono eseguite. Alcuni tipi di valichi di frontiera sono più difficili di altri. Ad

[12] https://ec.europa.eu/eurostat/web/products-datasets/-/migr_eirfs.

esempio, le verifiche svolte a bordo di imbarcazioni risentono spesso della difficoltà di connettersi ai sistemi. Durante le visite effettuate dagli auditor della Corte in due paesi, sono stati riscontrati problemi di questo tipo, che impediscono lo svolgimento di verifiche di frontiera complete. Analoghi problemi tecnici si incontrano nel caso di verifiche svolte su treni in movimento.

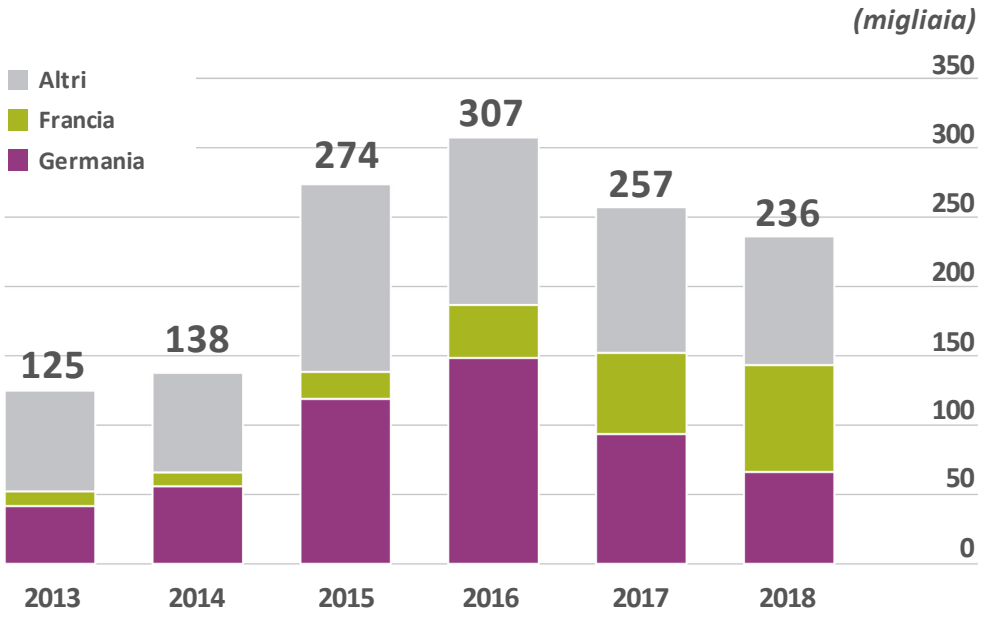
Eurodac

55 Un altro esempio di un accresciuto scambio di dati tra Stati Schengen è quello del sistema Eurodac, che consente di registrare i richiedenti asilo e le persone che tentano di effettuare un ingresso irregolare, rilevando le impronte digitali. Dal 2003 esiste un accordo[13] tra gli Stati membri dell'UE in base al quale le domande di asilo devono essere esaminate nel paese in cui il richiedente dichiara per la prima volta la propria intenzione di richiedere asilo. Quando una amministrazione nazionale confronta le impronte digitali di una persona con quelle registrate in Eurodac, ha un riscontro positivo se la persona ha precedentemente richiesto asilo in un altro paese dell'UE e in tale paese deve essere trasferita.

56 Il numero di domande di asilo presentate da individui che avevano già presentato una domanda di asilo in un altro Stato membro è aumentato significativamente fino al 2016, anno in cui si è registrato il picco della crisi migratoria. La maggior parte dei richiedenti che cercava di ottenere asilo in Francia o Germania era inizialmente arrivata in un altro paese dell'UE, come mostra la ***figura 8***.

[13] Regolamento (CE) n. 343/2003 del Consiglio, del 18 febbraio 2003, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda d'asilo presentata in uno degli Stati membri da un cittadino di un paese terzo ("regolamento di Dublino II").

Figura 8 – Richiedenti asilo che hanno già presentato domanda in un altro Stato membro



Fonte: Corte dei conti europea, sulla base di dati eu-LISA.

codice di prenotazione

57 Il PNR è un sistema nuovo. Anche se gli Stati membri dispongono di una base giuridica comune per la sua attuazione, la loro capacità di utilizzare il sistema per scambiare informazioni resta limitata, come spiegato nel paragrafo ***28***.

Eurosur

58 L'utilizzo di Eurosur varia enormemente da uno Stato membro all'altro. Tra il 2013 e il 2017, sono stati registrati in Eurosur oltre 140 000 episodi. Tuttavia, molti paesi partecipanti non hanno registrato un numero significativo di episodi[14]. Austria, Belgio, Cipro, Repubblica ceca, Germania, Danimarca, Francia, Lituania, Lussemburgo, Malta, Paesi Bassi, Portogallo, Svezia e Slovenia hanno registrato ciascuno meno di 5 000 episodi, mentre l'Ungheria, il paese più attivo, ne ha registrati oltre 25 000. Varia inoltre il tipo di informazioni che gli Stati membri condividono. Possono scegliere se inserire solo le informazioni obbligatorie (come i dati relativi alla migrazione irregolare e alla criminalità transfrontaliera e le informazioni provenienti dalla sorveglianza delle frontiere terrestri e marittime) oppure informazioni supplementari più ampie, come

[14] Valutazione del regolamento (UE) n. 1052/2013 del Parlamento europeo e del Consiglio, del 22 ottobre 2013, che istituisce il sistema europeo di sorveglianza delle frontiere (Eurosur), SWD(2018) 410 del 19.12.2018.

quelle relative a misure giuridiche o amministrative adottate dopo l'intercettazione e le informazioni sulle frontiere aeroportuali o sulle verifiche ai posti di frontiera. Ad esempio, la Finlandia ha scelto di condividere tutte le informazioni fornite dal suo quadro situazionale nazionale, sia quelle obbligatorie che facoltative, mentre Polonia e Francia inseriscono solo le informazioni obbligatorie.

VIS

59 Gli Stati Schengen hanno una politica comune in materia di visti. Possono rilasciare visti comuni per soggiorni di breve durata che consentono al titolare di soggiornare fino a 90 giorni in uno qualsiasi dei 26 Stati Schengen. Nel 2018 gli Stati Schengen hanno rilasciato oltre 14 milioni di visti Schengen per soggiorni di breve durata[15].

60 Il sistema consente di verificare l'identità di un titolare di visto Schengen ovunque all'interno dello spazio Schengen. Un titolare di visto Schengen può varcare più volte le frontiere esterne dello spazio Schengen e potrebbe farlo in diversi Stati Schengen. Le statistiche del VIS riportano il numero di volte che i visti sono stati richiesti alle frontiere. Nei primi nove mesi del 2017, sono state effettuate 35 milioni di verifiche di visti alle frontiere, rispetto a 12 milioni di visti rilasciati in quel periodo. Il numero di verifiche effettuate varia significativamente da uno Stato Schengen all'altro.

61 La Corte ha rilevato che, tra ottobre 2015 e settembre 2017, i cinque paesi che avevano rilasciato il maggior numero di visti (Francia, Germania, Italia, Spagna e Grecia) avevano eseguito alle rispettive frontiere un numero di verifiche sui visti inferiore al numero di visti rilasciati. Per un totale complessivo di quasi 18 milioni di visti rilasciati, questi paesi avevano svolto meno di 14 milioni di verifiche.

62 In teoria, tale differenza potrebbe essere dovuta al fatto che un numero significativo di viaggiatori con visti rilasciati da questi paesi è entrato nello spazio Schengen attraverso un altro paese oppure ha posticipato o annullato il proprio viaggio. Tuttavia, dato che la maggior parte dei viaggiatori richiede probabilmente il visto al paese in cui intende entrare, e che un visto Schengen comunque ha un suo costo[16], tale differenza potrebbe indicare che i visti non vengono sistematicamente controllati a tutti i posti di frontiera.

---

[15] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-policy#stats.

[16] Un visto Schengen costa 60 euro.

Le informazioni in alcuni sistemi erano incomplete

63 La qualità dei dati registrati nei sistemi di informazione è della massima importanza. L'inserimento dei dati nel sistema è di competenza delle autorità giudiziarie e di contrasto, nonché delle autorità di frontiera nazionali degli Stati membri. Sulla base di tali dati, le guardie di frontiera prendono decisioni da cui dipende la sicurezza dei cittadini europei.

64 In base alla normativa UE, la responsabilità per la qualità dei dati compete agli Stati membri. Pertanto, la Corte ha riscontrato scarse informazioni sulle procedure di controllo della qualità dei dati a livello dell'UE. Solo il regolamento Eurodac pone le basi di un quadro di controllo sulla qualità delle impronte digitali attribuendo ad eu-LISA la responsabilità di definire norme di qualità.

65 Il regolamento SIS II non prevede un coinvolgimento della Commissione o di eu-LISA nel processo volto a garantire la qualità dei dati. Rende invece responsabili gli Stati membri per l'esattezza, l'attualità e la liceità di inserimento dei dati nel sistema[17]. Gli uffici nazionali coordinano il funzionamento di SIS II e sono responsabili del coordinamento della verifica della qualità delle informazioni inserite nei sistemi[18].

66 La qualità dei dati ha assunto maggiore importanza nel 2018 con il nuovo regolamento eu-LISA[19] che attribuisce alla Commissione ed a eu-LISA responsabilità relative al processo di controllo della qualità dei dati. Il regolamento introduce l'obbligo che eu-LISA effettui controlli automatizzati sulla qualità dei dati e fornisca indicatori sulla qualità dei dati per SIS II, VIS e Eurodac.

67 Da aprile 2017, eu-LISA esegue controlli automatizzati mensili sulla qualità dei dati su determinate segnalazioni in SIS II (ad esempio, per problemi con la traslitterazione dei nomi da lingue con alfabeti non latini oppure su controlli automatizzati non effettuati per la presenza di termini generici come "SCONOSCIUTO"). Questi controlli generano un tabulato in cui sono elencate le singole segnalazioni che presentano potenziali problemi di qualità; tale tabulato viene trasmesso direttamente al paese interessato. Tuttavia, in ottemperanza alla normativa

---

[17] Articolo 34 del regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio del 20 dicembre 2016.

[18] Articolo 7, ibidem.

[19] Articolo 12 del regolamento (UE) 2018/1726 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA).

in materia di protezione dei dati, eu-LISA non può vedere le singole segnalazioni, ma solo il numero aggregato dei problemi di qualità rilevati per ciascun tipo di segnalazione e per ciascun paese.

68 I tabulati estratti con cadenza mensile riportano circa 3 milioni di segnalazioni di potenziali problemi di qualità dei dati (su un totale di 82 milioni registrazioni in media), il che significa che i dati potrebbero non essere conformi ai criteri di qualità dei dati per SIS II. La Corte ha riscontrato che né eu-LISA né la Commissione avevano poteri esecutivi per imporre agli Stati membri di correggere tempestivamente i problemi dovuti alla qualità dei dati. Di fatto, i tabulati mensili non mostrano alcuna riduzione significativa del numero di segnalazioni relative alla qualità dei dati in SIS II. Inoltre, poiché eu-LISA non può vedere le singole segnalazioni, non ha modo di sapere se le segnalazioni in un dato mese sono nuove o sono quelle di tabulati precedenti rimaste irrisolte. Oltre a questi tabulati, di utilità limitata come strumento di gestione di qualità, la Corte non ha ottenuto alcun elemento attestante lo svolgimento di altri controlli automatizzati sulla qualità dei dati a livello UE.

69 In base alla relazione di valutazione della Commissione su SIS II[20], gli Stati Schengen indicano che la scarsa qualità dei dati costituisce un problema frequente e ricorrente. In generale, nei paesi visitati dagli auditor della Corte emergono due principali problemi relativi alla qualità dei dati: uno riguarda la completezza dei dati e l'altro la tempistica di inserimento dei dati nei sistemi.

70 I dati presenti nel sistema dovrebbero consentire alle guardie di frontiera di identificare in modo univoco la persona oggetto della verifica e di decidere se farla entrare o meno. La Corte ha riscontrato che, talvolta, le guardie di frontiera non ottengono dalla consultazione del sistema informazioni adeguate per prendere tale decisione.

71 Ad esempio, la Corte ha rilevato segnalazioni in cui il nome della persona era inserito come cognome, oppure la data di nascita era incompleta o mancante,

[20] Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione del sistema d'informazione Schengen di seconda generazione (SIS II) ai sensi dell'articolo 24, paragrafo 5, dell'articolo 43, paragrafo 3, e dell'articolo 50, paragrafo 5, del regolamento (CE) n. 1987/2006 e ai sensi dell'articolo 59, paragrafo 3, e dell'articolo 66, paragrafo 5, della decisione 2007/533/GAI; 21.12.2016, pag. 12.

rendendo così difficile l'identificazione della persona[21]. A causa di tali problemi, quando le guardie di frontiera verificano un nominativo in SIS II, potrebbero ricevere centinaia di risultati (per lo più falsi positivi), che devono poi verificare manualmente. Ciò non solo rende meno efficienti le verifiche di frontiera, ma aumenta anche il rischio di non individuare i "veri" riscontri positivi.

72 Le registrazioni incomplete in SIS II riducono inoltre l'efficienza di altri sistemi ad esso collegati. Ad esempio, quando le autorità degli Stati Schengen verificano le informazioni sui passeggeri su un elenco PNR, le confrontano in genere con le segnalazioni di SIS II. Le segnalazioni incomplete generano un alto numero di falsi positivi che indicano che un passeggero è "sospetto". Poiché molte segnalazioni devono essere verificate manualmente, si genera un notevole carico di lavoro per le unità d'informazione sui passeggeri che verificano gli elenchi PNR. Inoltre, anche i dati PNR possono essere incompleti. I dati forniti dai sistemi di prenotazione possono contenere solo i nominativi dei passeggeri e il numero del volo.

73 Il VIS può solo registrare i visti Schengen per soggiorni di breve durata, anche se gli Stati Schengen usano ancora più di 200 tipi diversi di visti e di permessi di soggiorno nazionali per consentire a cittadini di paesi terzi di entrare e lavorare nello spazio Schengen. Questi permessi sono registrati soltanto su banche dati nazionali, che non sono condivise con altri paesi. Nel 2017 sono stati rilasciati quasi 2,6 milioni di permessi di questo tipo nello spazio Schengen[22]. Attualmente, non esiste una base giuridica indicante come procedere alla registrazione di questi permessi nel sistema centrale VIS.

---

[21] Molti Stati membri segnalano la scarsa qualità dei dati come un problema frequente e ricorrente, in base alla relazione di valutazione della Commissione su SIS II. Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione del sistema d'informazione Schengen di seconda generazione (SIS II) ai sensi dell'articolo 24, paragrafo 5, dell'articolo 43, paragrafo 3, e dell'articolo 50, paragrafo 5, del regolamento (CE) n. 1987/2006 e ai sensi dell'articolo 59, paragrafo 3, e dell'articolo 66, paragrafo 5, della decisione 2007/533/GAI; 21.12.2016.

[22] Statistiche Eurostat, *First permits in 2017:* http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=migr_resfirst&lang=en.

74 La Commissione ha individuato questa lacuna del sistema di informazioni e sta attualmente lavorando ad un regolamento che affronti la questione[23]. Tuttavia, poiché questi documenti di viaggio possono essere validi fino a 10 anni, resteranno esclusi dal sistema per anni prima che questa lacuna del sistema venga colmata.

75 Per quanto riguarda Eurosur, una debolezza dipende dal fatto che gli Stati membri trasmettono le relazioni in formati diversi, per cui le informazioni non possono essere aggregate facilmente e possono addirittura non essere accessibili ad altri Stati membri per ragioni tecniche.

76 I dati vengono generalmente inseriti in Eurosur manualmente. Quando alle frontiere vi è un aumento del numero di eventi, un operatore può avere difficoltà a registrarli velocemente nel sistema. Di conseguenza, la qualità dei dati potrebbe risentirne[24]. Inoltre, alcuni Stati membri segnalano i singoli episodi, mentre altri forniscono solo dati aggregati. Alcuni Stati membri registrano un episodio per ogni individuo, altri registrano un episodio che riguarda più persone. Ciò rende le statistiche sul numero di episodi segnalati dagli Stati membri non pertinenti, in quanto non mostrano la reale entità del problema. Diventa inoltre difficile per Frontex monitorare gli sviluppi e stabilire l'ordine di priorità nell'assegnazione delle risorse aggiuntive necessarie.

Gli eventi non sono sempre registrati prontamente nei sistemi

77 Le guardie di frontiera devono aver accesso a informazioni aggiornate sulle persone che varcano la frontiera per poter svolgere efficacemente il proprio compito. Talvolta, però, gli Stati membri non inseriscono le informazioni non appena ne vengono a conoscenza.

---

[23] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (CE) n. 767/2008, il regolamento (CE) n. 810/2009, il regolamento (UE) 2017/2226, il regolamento (UE) 2016/399, il regolamento (UE) 2018/XX [regolamento sull'interoperabilità] e la decisione 2004/512/CE, e che abroga la decisione 2008/633/GAI del Consiglio, COM(2018) 302.

[24] Fonte: *Evaluation of Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur)*, 12.9.2018, pag. 44.

78 I dati PNR sono generati durante le prenotazioni e sono previste sanzioni per le compagnie aeree che comunicano tardivamente gli elenchi dei passeggeri. Per quanto riguarda il VIS, i dati sono generati automaticamente quando viene rilasciato un visto. Per Eurodac, vi è un termine legale per l'inserimento delle informazioni sui richiedenti asilo. SIS II e Eurosur non prevedono invece scadenze specifiche entro cui registrare le informazioni[25].

79 Eurosur dovrebbe fornire informazioni in tempo reale sulla situazione alle frontiere, ma l'attualità delle informazioni dipende dalla tempestività con cui gli Stati membri le inseriscono. Alcuni paesi oggetto del presente audit registrano effettivamente le informazioni in tempo reale, altri invece lo fanno solo una volta alla settimana. Il che significa che un episodio alla frontiera (ad esempio, l'arrivo di un gran numero di migranti) potrebbe apparire nel sistema europeo solo una settimana più tardi.

80 Il regolamento di Dublino[26] stabilisce che il paese competente per l'esame di una domanda di asilo è quello in cui il richiedente asilo è entrato per la prima volta nell'UE. Gli Stati membri hanno al massimo 72 ore[27] per procedere al rilevamento delle impronte digitali e trasmetterle ad Eurodac, a partire dal momento in cui la persona presenta domanda di asilo o è fermata durante l'attraversamento irregolare di una frontiera. Se la persona richiedente asilo si trasferisce in un altro Stato membro, il ritardo nella trasmissione può far sì che la competenza per l'esame della domanda di asilo venga attribuita allo Stato membro sbagliato (cfr. paragrafi ***55***-***56***).

---

[25] I dati PNR sono generati durante le prenotazioni e sono previste sanzioni se le compagnie aeree comunicano tardivamente gli elenchi dei passeggeri. Per quanto riguarda il VIS, i dati sono generati automaticamente quando viene rilasciato un visto.

[26] Regolamento (UE) n. 604/2013.

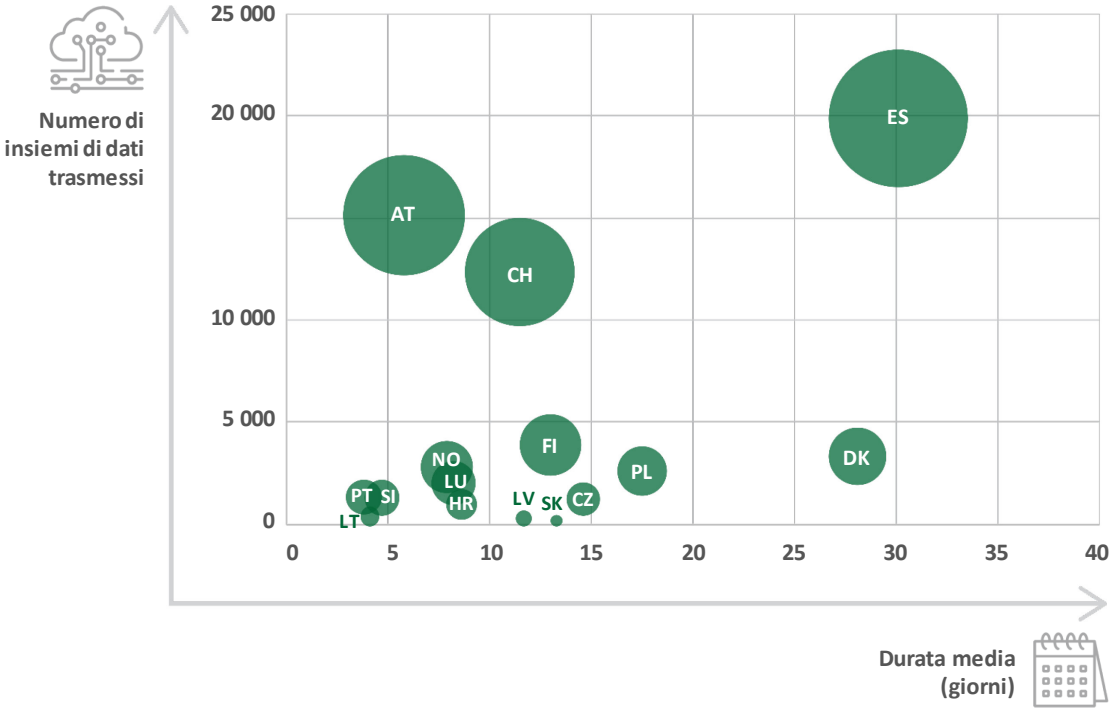
[27] Articolo 9, paragrafo 1, e articolo 14, paragrafo 2 del regolamento Eurodac.

Foto 1 - Raccolta delle impronte digitali per la registrazione in Eurodac

© UE, 2015/Fonte: CE – Servizio audiovisivo/Fotografo: Angelos Tzortzinis

81 Da quando Eurodac ha iniziato a funzionare, non vi è stato un anno in cui tutti gli Stati membri abbiano trasmesso le informazioni richieste entro i termini stabiliti. Nel 2017, i tempi medi di trasmissione di 15 paesi hanno superato i termini per la registrazione delle impronte digitali (cfr. ***figura 9***). Anche se il regolamento prevede deroghe ai termini per la registrazione dei dati, non esiste un meccanismo per distinguerle dai ritardi irregolari.

Figura 9 – Tempi medi per la trasmissione delle impronte digitali nel 2017



Fonte: Corte dei conti europea, sulla base di dati eu-LISA, Relazione annuale del 2017 sulle attività del sistema centrale dell'Eurodac.

82 Come mostra la ***figura 9***, nel 2017 la Spagna ha impiegato in media 30 giorni per trasmettere le impronte digitali ad Eurodac. Il che significa che una persona fermata durante un attraversamento irregolare della frontiera in Spagna ha avuto in media 30 giorni per raggiungere un altro Stato membro e presentare lì domanda di asilo. Le autorità di questo altro Stato membro, al momento di verificare le impronte digitali confrontandole con i dati Eurodac, non avrebbero trovato alcun corrispondenza nel sistema. Di conseguenza, l'altro paese sarebbe stato obbligato a esaminare la domanda di asilo presentata dal soggetto fermato.

Conclusioni e raccomandazioni

83 La Corte ha esaminato se i principali sistemi di informazione dell'UE per la sicurezza interna supportano in modo efficiente il controllo alle frontiere. La Corte ha concluso che, al momento di eseguire le verifiche di frontiera, le guardie di frontiera utilizzano e fanno affidamento su tali sistemi in misura crescente. Tuttavia, alcuni dati non sono attualmente registrati nei sistemi, mentre altri dati sono incompleti o non sono inseriti tempestivamente. Ciò riduce l'efficienza di alcune verifiche di frontiera.

84 La Corte ha riscontrato che i sistemi di informazione dell'UE sono generalmente ben concepiti, per facilitare le verifiche di frontiera. I paesi visitati dagli auditor della Corte hanno posto in essere i propri sistemi conformemente al quadro normativo applicabile. Ciononostante, alcune componenti nazionali SIS II e VIS hanno consentito di svolgere verifiche di frontiera in modo più efficiente rispetto ad altre (cfr. paragrafi ***17***-***21***).

85 Anche se gli Stati membri condividono sempre di più informazioni attraverso tali sistemi, i vincoli di natura giuridica (norme relative alla protezione dei dati e alla sicurezza nazionale) impediscono la condivisione di risorse umane. Le guardie di frontiera che si recano in altri Stati membri non possono avere accesso ai sistemi di informazione del paese ospite per svolgere le verifiche di frontiera. La Corte ha rilevato inoltre che i sistemi sono stati sviluppati senza prevedere un ambiente di formazione in cui le guardie di frontiera possano esercitarsi su situazioni che non incontrano frequentemente nel corso del loro lavoro (cfr. paragrafi ***22***-***23***).

Raccomandazione 1 – Promuovere l'uso degli ambienti di formazione per SIS II e VIS

La Commissione dovrebbe promuovere l'uso, da parte degli Stati membri, degli ambienti di formazione centrali per SIS II e VIS, che consentirebbe alle guardie di frontiera di sperimentare situazioni reali durante la formazione.

Termine ultimo: fine 2020.

86 L'operatività di soluzioni informatiche è stata talvolta posticipata, sia a livello UE che nazionale. Quattro anni dopo l'entrata in vigore del regolamento Eurosur, solo metà degli Stati membri condivideva tutte le informazioni, facoltative o obbligatorie, sulla piattaforma Eurosur. Quattordici paesi non hanno attuato le norme sui dati PNR entro il termine previsto. Ciò ha impedito alle autorità di frontiera di disporre di un

quadro completo della situazione alle frontiere esterne dello spazio Schengen nonché di ricevere in anticipo informazioni sull'attraversamento di frontiere da parte di individui ad alto rischio (cfr. paragrafi ***24***-***32***).

87 Il meccanismo di valutazione Schengen svolge un ruolo importante nel monitoraggio dell'attuazione della normativa Schengen da parte degli Stati Schengen. La Corte ha constatato che queste valutazioni erano generalmente approfondite e metodiche, e prendevano in esame le caratteristiche fondamentali dei sistemi. Tuttavia, gli Stati Schengen impiegano molto tempo per ovviare alle debolezze individuate durante le valutazioni. Non esistono infatti termini per l'adozione delle relazioni di valutazione e per l'attuazione dei piani d'azione correttivi (cfr. paragrafi ***33***-***41***).

88 La Commissione non ha ancora adempiuto all'obbligo di presentare annualmente una relazione al Parlamento e al Consiglio sulle valutazioni effettuate. La Corte ha constatato che, quattro anni dopo le valutazioni, nessuno degli Stati Schengen oggetto del presente audit aveva attuato integralmente i rispettivi piani d'azione. Ciò indica che il processo di valutazione non consente di porre rapidamente rimedio alle debolezze constatate (cfr. paragrafi ***42***-***43***).

Raccomandazione 2 – Accelerare la correzione delle debolezze constatate durante le valutazioni Schengen

La Commissione dovrebbe:

a) nel presentare la relazione di valutazione di cui all'articolo 22 del regolamento (UE) n. 1053/2013 al Parlamento e al Consiglio, includere informazioni sui tempi di attuazione dei piani di azione approntati dagli Stati Schengen per rispondere alle raccomandazioni del Consiglio;

b) proporre misure legislative e procedurali idonee per abbreviare i tempi del ciclo di valutazione Schengen.

Termine ultimo: fine 2020.

89 L'UE fornisce agli Stati membri finanziamenti erogati dal Fondo sicurezza interna per lo sviluppo e la manutenzione dei sistemi di informazione oggetto del presente audit. In media, i paesi visitati dagli auditor della Corte hanno destinato il 15 % degli stanziamenti del Fondo sicurezza interna loro assegnati a questi cinque sistemi. Essi

hanno principalmente utilizzato tali fondi per la manutenzione di SIS II e di VIS e per l'estensione di Eurosur e di PNR (cfr. paragrafi ***44***-***46***).

90 La Corte ha rilevato che gli Stati membri utilizzano tali sistemi in misura crescente. Tra il 2013 e il 2017, il numero di *hit* in SIS II relative a persone o oggetti ricercati in base alle segnalazioni inserite in altri paesi è quasi triplicato (cfr. paragrafi ***47***-***58***).

91 Tuttavia, tale utilizzo dovrebbe essere più sistematico. Dall'indagine condotta dalla Corte emerge che oltre la metà delle guardie di frontiera si è trovata in una situazione in cui ha dovuto decidere di ammettere qualcuno senza aver prima consultato i sistemi. In particolare, la Corte ha rilevato una serie di discrepanze tra il numero di visti rilasciati e il numero di visti verificati. Inoltre, il VIS può gestire solo i visti Schengen per soggiorni di breve durata e non è attualmente predisposto per l'inserimento dei dati sui visti nazionali che consentono ai titolari di entrare in un qualsiasi Stato Schengen. Solo nel 2017, sono stati rilasciati quasi 2,6 milioni di visti di questo tipo (cfr. paragrafi ***59***-***62***).La Commissione ha individuato questa lacuna del sistema di informazioni e ha presentato una proposta per rivedere il quadro giuridico relativo al VIS.

Raccomandazione 3 – Analizzare le discrepanze relative alle verifiche dei visti

La Commissione dovrebbe analizzare le ragioni delle discrepanze tra il numero di visti Schengen rilasciati ed il numero di quelli verificati e proporre misure correttive.

Termine ultimo: fine 2020.

92 Le guardie di frontiera utilizzano i dati registrati nei sistemi come base per prendere decisioni da cui dipende la sicurezza dei cittadini europei. La qualità di tali dati è quindi della massima importanza. La Corte ha rilevato pochi riferimenti alla questione della qualità dei dati negli atti giuridici che disciplinano i sistemi di informazione europei. Il regolamento SIS II ha conferito agli Stati membri la responsabilità della qualità dei dati e non ha previsto un coinvolgimento della Commissione o di eu-LISA (cfr. paragrafi ***63***-***65***).

93 Anche se eu-LISA esegue mensilmente controlli automatizzati sulla qualità dei dati registrati in SIS II e trasmette i risultati agli Stati membri interessati, l'Agenzia può solo vedere il numero dei problemi di qualità aggregato per ciascun tipo di

segnalazione e per ciascun paese. Queste rilevazioni non sono sufficientemente dettagliate per poter vedere i progressi compiuti nel porre rimedio ai problemi di qualità. Inoltre, né eu-LISA né la Commissione hanno poteri esecutivi per imporre agli Stati Schengen di correggere tempestivamente i problemi relativi alla qualità dei dati (cfr. paragrafi ***67***-***70***).

94 La Corte ha osservato che le guardie di frontiera non ottengono sempre dati completi ed aggiornati dai sistemi di informazione, il che limita l'efficienza delle verifiche di frontiera. Ad esempio, quando le guardie di frontiera verificano un nominativo in SIS II, possono ricevere centinaia di risultati (per lo più falsi positivi), che devono poi verificare manualmente. Ciò non solo rende meno efficienti le verifiche di frontiera, ma aumenta anche il rischio di non individuare i "veri" riscontri positivi (cfr. paragrafi ***71***-***76***).

Raccomandazione 4 – Migliorare le procedure per il controllo della qualità dei dati

La Commissione dovrebbe:

a) chiedere ad eu-LISA di includere, nel monitoraggio mensile da questa svolto, le statistiche delle rettifiche introdotte dagli Stati Schengen.

b) se il monitoraggio della qualità dei dati non indica un miglioramento, adottare adeguati provvedimenti, ad esempio attraverso orientamenti o i gruppi consultivi esistenti, per incoraggiare gli Stati Schengen a intensificare le azioni correttive.

Termine ultimo: entro fine 2020.

95 Eccetto che per Eurodac, non esistono in genere termini obbligatori entro cui procedere all'inserimento dei dati. Ad esempio, Eurosur dovrebbe fornire informazioni in tempo reale sulla situazione alle frontiere esterne. Tuttavia, mentre alcuni paesi oggetto del presente audit registrano effettivamente le informazioni in tempo reale, altri vi provvedono solo una volta alla settimana. Da quando Eurodac ha iniziato a funzionare nel 2003, non vi è stato un anno in cui tutti gli Stati membri abbiano trasmesso le informazioni richieste entro i termini stabiliti. Un ritardo nella trasmissione può far sì che la competenza per l'esame della domanda di asilo venga attribuita allo Stato membro sbagliato (cfr. paragrafi ***77***-***82***).

Raccomandazione 5 – Ridurre i tempi per l'inserimento dei dati

La Commissione dovrebbe:

a) analizzare le cause dei ritardi irregolari nell'inserimento dei dati in Eurodac e intraprendere azioni adeguate nei confronti degli Stati membri interessati;

b) proporre, durante la prossima revisione della normativa applicabile a Eurosur, l'introduzione di termini obbligatori per l'inserimento dei dati.

Termine: fine 2021.

La presente relazione è stata adottata dalla Sezione III, presieduta da Bettina JAKOBSEN, Membro della Corte dei conti europea, a Lussemburgo, nella riunione dell'8 ottobre 2019.

Per la Corte dei conti europea

Klaus-Heiner Lehne
Presidente

Allegato

Breve descrizione dei sistemi di informazione selezionati

SIS II

Il sistema d'informazione Schengen (SIS) è il sistema di condivisione delle informazioni più vasto e più ampiamente utilizzato per la sicurezza e la gestione delle frontiere in Europa. Il SIS II consente alle autorità nazionali competenti, quali la polizia e le guardie di frontiera, di inserire e consultare segnalazioni su persone o oggetti. Una segnalazione SIS non solo contiene informazioni su persone o oggetti specifici, ma anche istruzioni per le autorità sulle iniziative da prendere quando un oggetto o una persona sono stati individuati.

Il SIS II comprende tre principali componenti: un sistema centrale, i sistemi nazionali ed una infrastruttura di comunicazione (rete) tra tali sistemi. Una segnalazione inserita nel SIS II in uno Stato Schengen è trasferita in tempo reale al sistema centrale e diventa subito disponibile in tutti gli altri Stati Schengen.

Ogni Stato Schengen che utilizza il SIS II è responsabile dell'istituzione, del funzionamento e della manutenzione del sistema nazionale e dell'ufficio SIRENE nazionale, che funge da punto di contatto unico per lo scambio di informazioni supplementari e per il coordinamento delle attività relative alle segnalazioni SIS II.

L'Agenzia UE per la gestione operativa dei sistemi IT su larga scala (eu-LISA) è responsabile della gestione operativa del sistema centrale e dell'infrastruttura di comunicazione.

La Commissione europea è responsabile della supervisione generale e della valutazione del sistema e dell'adozione delle misure attuative.

Il SIS II è operativo in 30 paesi europei, tra cui 26 Stati membri dell'UE (solo Irlanda e Cipro non sono ancora connessi al SIS II) e quattro paesi associati Schengen (Svizzera, Norvegia, Liechtenstein e Islanda).

VIS

Il Sistema di informazione visti (VIS) sostiene l'attuazione di una politica comune dell'UE in materia di visti. Consente agli Stati Schengen di scambiare dati sui visti. Il

sistema può eseguire confronti biometrici, principalmente delle impronte digitali, a fini di identificazione e verifica.

Il VIS consente alle guardie di frontiera di verificare che la persona che presenta un visto ne sia il legittimo titolare, che il visto sia autentico e che la persona soddisfi in quel momento i requisiti per disporre del visto.

Alle persone che richiedono un visto viene richiesta una fotografia digitale e vengono rilevate le 10 impronte digitali. Questi dati biometrici, insieme ai dati forniti nella domanda di visto, sono registrate in una banca dati centrale sicura. L'utilizzo dei dati biometrici per confermare l'identità del titolare del visto consente verifiche più rapide, accurate e sicure. Il sistema facilita inoltre il processo di rilascio del visto.

Il VIS comprende un sistema informatico centrale ad una infrastruttura di comunicazione che collega il sistema centrale ai sistemi nazionali. Il VIS collega i consolati dei paesi non-UE e tutti i posti di frontiera esterni degli Stati Schengen. Elabora e archivia i dati e le decisioni relative alle domande di visti per soggiorni di breve durata.

Quale strumento Schengen, il VIS si applica a tutti i paesi dello spazio Schengen. L'Agenzia UE per la gestione operativa dei sistemi IT su larga scala (eu-LISA) è responsabile della gestione operativa del VIS.

Eurodac

Eurodac è una banca dati delle impronte digitali dei richiedenti asilo dell'UE. Il suo principale obiettivo è consentire l'attuazione del regolamento (UE) n. 604/2013 ("il regolamento di Dublino"). Quando qualcuno presenta domanda di asilo, indipendentemente da dove si trovi nell'UE, le sue impronte digitali vengono trasmesse al sistema centrale Eurodac.

Dalla sua istituzione nel 2003, Eurodac aiuta a stabilire lo Stato membro competente per l'esame della domanda di asilo.

Eurodac contiene soltanto le impronte digitali (insieme ai dati e al luogo della registrazione), ma non altre informazioni personali. Il sistema è utilizzato dai 28 Stati membri dell'UE e dai paesi associati Schengen: Islanda, Liechtenstein, Norvegia e Svizzera.

Eurosur

Il Sistema europeo di sorveglianza delle frontiere (Eurosur) istituisce un quadro di governance per la cooperazione tra gli Stati membri e l'Agenzia europea della guardia di frontiera e costiera (**EBCGA - "Frontex"**) al fine di migliorare la conoscenza situazionale europea e di aumentare la capacità di reazione alle frontiere esterne. L'obiettivo è prevenire la migrazione irregolare e la criminalità transfrontaliera e contribuire a proteggere la vita dei migranti.

In base al regolamento Eurosur, ogni Stato Schengen istituisce un centro nazionale di coordinamento che provvede al coordinamento e allo scambio di informazioni tra tutte le autorità incaricate della sorveglianza delle frontiere esterne nonché con gli altri centri nazionali di coordinamento e con Frontex.

Frontex è responsabile del coordinamento della cosiddetta "applicazione comune di strumenti di sorveglianza": gli Stati membri possono richiedere l'assistenza di Frontex per monitorare aree o navi selezionate di interesse ai fini di Eurosur, utilizzando strumenti quali le immagini satellitari o i sistemi di notifica delle navi. Tale dispositivo può essere utilizzato per individuare casi di migrazione irregolare o di criminalità transfrontaliera, ma anche per localizzare un'imbarcazione in difficoltà.

Eurosur è utilizzato in tutti i paesi dello spazio Schengen, nonché in Bulgaria, Romania e Croazia.

PNR

Il codice di prenotazione (*Passenger Name Record* – PNR) descrive le informazioni fornite dai passeggeri alle compagnie aeree al momento della prenotazione e durante il check-in. Possono includere informazioni quali le date e l'itinerario del viaggio, le informazioni sul biglietto, l'agenzia di viaggio, i recapiti, i mezzi di pagamento, il numero di sedile e le informazioni sul bagaglio. Il 27 aprile 2016, il Parlamento europeo e il Consiglio hanno adottato la direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

Tutti gli Stati membri dell'UE, eccetto la Danimarca[28], sono tenuti a individuare soggetti specifici responsabili della raccolta, archiviazione e trattamento dei dati PNR, le "unità d'informazione sui passeggeri" (UIP). Le UIP raccolgono i dati PNR dai vettori aerei utilizzando sistemi informatici dedicati e confrontano i dati PNR con le banche dati delle autorità di contrasto. Le esaminano inoltre in base a criteri prestabiliti, in modo da identificare le persone che potrebbero essere implicate in reati di terrorismo o in altri reati gravi. Le UIP sono incaricate anche di trasmettere i dati PNR alle guardie di frontiera e alle altre autorità nazionali competenti, a Europol e alle UIP di altri Stati membri.

[28] In base al protocollo 22 dei trattati, la Danimarca non è soggetta alle disposizioni della direttiva PNR.

Acronimi e abbreviazioni

DG HOME: direzione generale della Migrazione e degli affari interni

EBCGA: Agenzia europea della guardia di frontiera e costiera

eu-LISA: Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia

Eurodac: sistema europeo di dattiloscopia

Eurosur: Sistema europeo di sorveglianza delle frontiere

Frontex: *si veda EBCG*

ISF: Fondo sicurezza interna

NCC: centro nazionale di coordinamento

PNR: codice di prenotazione

SIS II: Sistema d'informazione Schengen II

VIS: Sistema di informazione visti

Glossario

Guardia di frontiera: pubblico ufficiale assegnato, conformemente alla legislazione nazionale, ad un posto di frontiera oppure lungo la frontiera o nelle immediate vicinanze di quest'ultima, che assolve compiti di controllo di frontiera.

Interoperabilità: generalmente definita come la capacità di diversi sistemi di informazione di comunicare tra loro, di scambiarsi dati e di utilizzare le informazioni che sono state scambiate.

Paesi dello spazio Schengen: 26 paesi europei che hanno eliminato il controllo dei passaporti alle frontiere comuni, di cui 22 sono Stati membri dell'UE e 4 sono paesi dell'EFTA: Belgio, Repubblica ceca, Danimarca, Germania, Estonia, Grecia, Spagna, Francia, Italia, Lettonia, Lituania, Lussemburgo, Ungheria, Malta, Paesi Bassi, Austria, Polonia, Portogallo, Slovenia, Slovacchia, Finlandia, Svezia, Islanda, Liechtenstein, Norvegia, Svizzera.

Posto di frontiera: valico autorizzato dalle autorità competenti per il passaggio delle frontiere esterne.

Prima linea: luogo in cui tutte le persone sono sottoposte a verifiche presso i posti di frontiera.

Stati Schengen associati: quattro stati membri dell'EFTA (*European Free Trade Association* – Associazione europea di libero scambio) (Islanda, Liechtenstein, Norvegia e Svizzera), che non sono membri dell'UE, ma che hanno sottoscritto convenzioni per essere associati all'accordo di Schengen.

Verifica in seconda linea: una verifica supplementare che può essere effettuata in un luogo specifico, diverso da quello in cui sono effettuate le verifiche su tutte le persone (prima linea).

RISPOSTE DELLA COMMISSIONE ALLA RELAZIONE SPECIALE DELLA CORTE DEI CONTI EUROPEA

"I SISTEMI DI INFORMAZIONE DELL'UE A SUPPORTO DELLE VERIFICHE DI FRONTIERA COSTITUISCONO UNO STRUMENTO POTENTE, MA OCCORRE MAGGIORE ATTENZIONE ALLA COMPLETEZZA E ATTUALITÀ DEI DATI"

SINTESI

II È importante evidenziare che i dati del codice di prenotazione (PNR) raccolti a norma della direttiva sul PNR non possono essere impiegati a fini di controllo delle frontiere/dell'immigrazione, ma esclusivamente a fini di contrasto delle forme gravi di criminalità e del terrorismo.

VI Il termine per il recepimento della direttiva sul PNR è scaduto il 25 maggio 2018. Si tratta pertanto di uno strumento relativamente recente rispetto ad altri sistemi oggetto dell'audit della Corte dei conti europea.

Gli Stati membri sono tenuti a dotare le rispettive unità d'informazione sui passeggeri di hardware e software per la raccolta e il trattamento dei dati PNR. Stabilire un collegamento con un vettore aereo è un processo lungo e complicato, che non dipende interamente dalle autorità nazionali. Inoltre, i dati PNR non possono essere raccolti e trattati in assenza di una base giuridica, ossia prima dell'adozione e dell'entrata in vigore di misure nazionali di recepimento. Tutti questi fattori giustificano il motivo per cui potrebbe essere necessario del tempo prima che le unità nazionali d'informazione sui passeggeri diventino pienamente operative. La Commissione ha sostenuto gli Stati membri nel processo di attuazione, stanziando anche fondi dell'UE per l'acquisizione e lo sviluppo dell'hardware e del software necessari.

La Commissione non ritiene che vi siano stati lunghi ritardi nell'attuazione di soluzioni informatiche per il sistema Eurosur.

La rete di comunicazione Eurosur, che permette di collegare i centri nazionali di coordinamento degli Stati membri per la sorveglianza delle frontiere tra loro e con l'Agenzia europea della guardia di frontiera e costiera (Frontex), è stata istituita in modo tempestivo, consentendo ad esempio lo scambio di informazioni su episodi connessi alla migrazione irregolare e alla criminalità transfrontaliera.

Tuttavia, vi è stato effettivamente un ritardo nel portare a termine il processo di accreditamento per lo scambio di alcune informazioni a causa di disposizioni in materia di riservatezza.

VII La Commissione concorda con la Corte dei conti europea sul fatto che scadenze concrete e vincolanti per l'attuazione delle raccomandazioni da parte degli Stati membri interessati rafforzerebbero notevolmente l'efficienza del meccanismo di valutazione Schengen e colmerebbero più rapidamente le lacune individuate.

Per quanto riguarda il periodo di tempo necessario per l'adozione delle relazioni di valutazione, la Commissione sta esaminando possibili modifiche procedurali per ridurre tale periodo.

VIII Poiché il flusso dei passeggieri è in costante aumento, è importante investire in soluzioni che consentano un controllo sistematico di ogni passeggero in tutti i sistemi pertinenti, indipendentemente dalla situazione specifica o dall'affluenza.

IX Per quanto riguarda i poteri esecutivi ad essa conferiti, la Commissione è tenuta a verificare la corretta applicazione della normativa UE da parte degli Stati membri. Pertanto, sebbene non abbia accesso ai dati SIS e non possa valutare i singoli casi, la Commissione può verificare che a livello nazionale siano stati istituiti meccanismi e strutture volti a garantire un'elevata qualità dei dati nel sistema SIS.

X Per quanto riguarda i dati presenti nel SIS, è stata concordata una serie di dati obbligatori senza i quali non è possibile creare una segnalazione; pertanto, qualsiasi segnalazione nel SIS è sempre completa. Ma vi sono anche dati presenti solo se disponibili o considerati sicuri dalle autorità emittenti. È inoltre possibile accedere ad informazioni supplementari presso gli uffici SIRENE. Nella segnalazione, gli utenti finali sono sempre invitati a contattare il proprio ufficio SIRENE nazionale (in alcuni casi, immediatamente).

Per quanto concerne il sistema VIS e la questione dei falsi positivi, va evidenziato che il VIS contiene di norma dati biometrici (10 impronte digitali di buona qualità); pertanto, tale sistema non risente dell'inconveniente dei falsi positivi, ammesso che i controlli vengano svolti in modo appropriato (verificando le impronte digitali di una persona). Per di più, le costatazioni risultanti dalla valutazione REFIT del 2016 sul sistema VIS evidenziano che nel sistema sono presenti dati, tra cui quelli biometrici, di qualità elevata.

XI Nella relazione di valutazione di Eurosur elaborata nel 2018, la Commissione ha inoltre sottolineato che non tutti gli Stati membri inseriscono informazioni nel sistema in modo tempestivo. Tale questione è stata dunque affrontata nel nuovo regolamento relativo alla guardia di frontiera e costiera europea (che ora include anche Eurosur), consentendo di concordare norme di attuazione vincolanti sullo scambio futuro di informazioni nel quadro di Eurosur.

XII La Commissione accoglie le raccomandazioni.

INTRODUZIONE

03 La direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, conosciuta come direttiva sul PNR, non prevede la creazione di un sistema informatico centralizzato a livello dell'UE. Ogni Stato membro dispone di una propria unità d'informazione sui passeggeri (UIP), incaricata di raccogliere, trattare e archiviare i dati PNR. Le UIP nazionali di ogni Stato membro possono trasferire o richiedere dati PNR alle UIP di altri Stati membri, conformemente alle procedure stabilite all'articolo 9 della direttiva sul PNR.

Eurosur non costituisce un sistema d'informazione specifico paragonabile ai sistemi SIS, VIS o PNR, ma rappresenta "un quadro comune per lo scambio di informazioni e per la cooperazione tra gli Stati membri" e l'Agenzia europea della guardia di frontiera e costiera (Frontex). I dati contenuti in Eurosur possono essere raccolti da diversi sistemi d'informazione.

OSSERVAZIONI

20 Le componenti nazionali dei sistemi SIS II e VIS sono di competenza degli Stati membri.

24 La struttura di Eurosur, che consiste di diverse componenti, rappresenta un quadro di riferimento non solo per lo scambio di informazioni, ma anche per la cooperazione. La rete di comunicazione di Eurosur è stata istituita nei tempi previsti, consentendo di collegare tutti gli Stati membri partecipanti nel 2013/2014 tra loro e con l'Agenzia europea della guardia di frontiera e costiera (Frontex). Tuttavia, vi sono stati alcuni ritardi nel completamento dell'accreditamento della rete di comunicazione di Eurosur per quanto riguarda lo scambio di informazioni classificate.

27 L'accreditamento di sicurezza per lo scambio di informazioni classificate nella rete di comunicazione di Eurosur è stato ritardato, ma va notato che questo tipo di informazioni riguarda solo una parte molto limitata delle informazioni scambiate.

28 La Commissione ha costantemente sostenuto gli Stati membri nel processo di attuazione e di applicazione tramite finanziamenti e assistenza, e ha agevolato lo scambio tra pari organizzando riunioni e seminari periodici, e garantendo attività di formazione organizzate principalmente dall'agenzia CEPOL.

29. Nel frattempo, i Paesi Bassi e la Finlandia hanno notificato il pieno recepimento della direttiva sul PNR, rispettivamente l'8 luglio 2019 e il 25 giugno 2019.

30 Stabilire un collegamento con le compagnie aeree costituisce un processo lungo e complesso dal punto di vista tecnico che può richiedere fino a 6-9 mesi per ciascuna compagnia, e che interessa aziende che forniscono servizi di prenotazione alle compagnie aeree. Dall'adozione della direttiva sul PNR sono aumentate le richieste per collegare i vettori aerei alle UIP.

Va inoltre osservato che dal marzo 2019 molti Stati membri hanno compiuto considerevoli progressi nel campo della connettività.

31 Il sistema in questione è relativamente recente e ancora in fase di attuazione.

I dati PNR non solo sono sottoposti a controlli incrociati con le banche dati, ma possono anche essere verificati in base a norme prestabilite di profilazione per l'identificazione dei passeggeri che corrispondono a determinati profili, sulla base delle informazioni disponibili.

Questa tecnica permette di identificare individui sconosciuti alle autorità, ma coinvolti in attività illegali come il terrorismo o traffici illeciti.

32 Secondo quanto stabilito dalla direttiva sul PNR, i dati PNR possono essere impiegati esclusivamente per combattere il terrorismo e reati gravi. L'ambito di applicazione della normativa riguardante il sistema SIS è invece più ampio, poiché, ad esempio, possono essere introdotte segnalazioni in caso di reati non contemplati dalla direttiva sul PNR.

I dati PNR corrispondono ai dati forniti dai passeggeri al momento della prenotazione del volo. Nel caso dei voli intra-UE, tali dati non contengono dati API, ossia dati provenienti da documenti d'identità ufficiali, come la data di nascita, fondamentale per l'identificazione delle persone. Di conseguenza, da un punto di vista delle attività di contrasto, i dati PNR risultano essere incompleti e non sottoposti a verifica.

I vettori aerei trasferiscono i dati di tutti i passeggeri. Confrontare questi dati con le banche dati, tramite norme mirate, permette di identificare sospetti noti o sconosciuti.

SIS II è una delle banche dati impiegate dalle autorità nazionali per trattare i dati PNR.

40 Oltre alle visite periodiche, ogni anno vengono effettuate anche diverse valutazioni non previste. Durante tali visite è possibile valutare se le raccomandazioni precedenti siano state attuate o meno. Sono state effettuate una visita non prevista e quattro nuove visite riguardanti il sistema SIS II.

41 La Commissione organizza una nuova visita al fine specifico di valutare l'attuazione delle raccomandazioni precedenti.

Riquadro 2 – Cogliere nel segno

Va notato che si verifica una corrispondenza in SIS quando una ricerca rivela l'esistenza di una segnalazione da parte di un altro Stato membro (risultato di una ricerca automatizzata). L'utente finale (ad esempio una guardia di frontiera) visualizza una serie di potenziali "corrispondenze" che devono essere verificate. Secondo quanto disposto dal diritto dell'UE sulla protezione dei dati, è necessario che avvenga sempre una verifica manuale, solo in seguito alla quale è possibile confermare una corrispondenza che diventa un "riscontro positivo" (*hit*).

58 La questione è stata affrontata nel nuovo regolamento relativo alla guardia di frontiera e costiera europea che entrerà in vigore nel corso dell'anno e che abrogherà l'attuale regolamento Eurosur.

In particolare, l'Agenzia europea della guardia di frontiera e costiera (EBCGA) si occuperà di controllare i dati scambiati e informerà in tempo reale tutti gli Stati membri sullo stato delle segnalazioni.

La trasmissione di informazioni riguardanti i valichi di frontiera esterni diventerà obbligatoria.

61 Ricorrere al VIS per controllare i titolari di visto alla frontiera è un obbligo derivante dal codice frontiere Schengen. Si potrebbe impiegare il meccanismo di valutazione Schengen per analizzare questa possibile discrepanza al fine di garantire un controllo sistematico dei visti rispetto al VIS.

68 Si tratta di potenziali problemi che l'autorità responsabile deve sottoporre a controlli incrociati e non di errori attestati sulla qualità dei dati. Va inoltre osservato che il numero comprende anche tutte le segnalazioni già verificate dagli Stati membri e per le quali si conferma che non rappresentano un problema di qualità dei dati. Le segnalazioni verificate non vengono eliminate dalla relazione dettagliata finché la segnalazione non sarà rimossa.

71 La normativa sul sistema SIS definisce una serie di dati che possono essere inseriti nella segnalazione (articolo 20 della decisione SIS II e del regolamento SIS II). La minimizzazione dei dati è un principio importante della protezione dei dati. Inoltre, la normativa stabilisce anche i dati indispensabili senza i quali non può essere creata alcuna segnalazione. Pertanto, qualsiasi segnalazione contenente tale serie di dati è considerata completa. Devono inoltre essere inseriti altri dati (facoltativi), se disponibili. Se tali dati facoltativi non vengono inseriti, la Commissione può solo presumere che i dati non siano a disposizione dell'autorità emittente.

72 L'obbligo di effettuare una verifica manuale è un requisito disposto dalla normativa dell'UE sulla protezione dei dati [regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) e direttiva sulla protezione dei dati trattati a fini di contrasto (direttiva (UE) 2016/680)]. Si tratta inoltre di una disposizione nel quadro della direttiva sul PNR.

La maggior parte dei dati PNR è insufficiente, non pertinente e talvolta troppo inaffidabile ai fini dei controlli nel sistema SIS: ad esempio, i dati PNR privi di valori API possono essere verificati solo con una serie molto limitata di dati SIS. Inoltre, il fatto che i dati PNR siano basati su autodichiarazioni solleva questioni di affidabilità.

74 La Corte sottolinea giustamente che la proposta della Commissione di rivedere il quadro giuridico del VIS (COM(2018) 302), attualmente discussa dai colegislatori, prevede l'inclusione dei visti e dei permessi di soggiorno nazionali nel VIS. La lacuna informativa cui fa riferimento la Corte verrebbe così colmata. Se è vero che sarebbero inclusi solo i documenti per soggiorni di lunga durata di nuova emissione, tale problematica andrebbe a scomparire nel tempo in quanto i documenti per soggiorni di lunga durata hanno un periodo di validità limitato e devono essere rinnovati/sostituiti.

75 La questione riguardante i diversi formati delle relazioni presentate dagli Stati membri è stata affrontata nel nuovo regolamento relativo alla guardia di frontiera e costiera europea che dovrebbe entrare in vigore entro la fine del 2019 e che abrogherà l'attuale regolamento Eurosur.

Il sistema relativo alla presentazione delle relazioni nel quadro di Eurosur sarà armonizzato tramite un atto di esecuzione.

76 Cfr. la risposta della Commissione al paragrafo 75.

Inoltre, la Commissione sosterrà lo sviluppo di gateway di scambio automatizzato di informazioni per limitare la doppia immissione di dati.

79 La questione riguardante la tempistica della trasmissione delle relazioni da parte degli Stati membri nel quadro di Eurosur è stata affrontata nel nuovo regolamento relativo alla guardia di frontiera e costiera europea che dovrebbe entrare in vigore entro la fine del 2019 e che abrogherà l'attuale regolamento Eurosur.

L'atto di esecuzione relativo al sistema Eurosur riguarderà le tempistiche per la trasmissione delle informazioni in Eurosur e il livello di responsabilità in materia di comunicazione.

CONCLUSIONI E RACCOMANDAZIONI

84 Le componenti nazionali dei sistemi SIS II e VIS sono di competenza degli Stati membri.

85 La Commissione, gli Stati membri, CEPOL ed eu-LISA hanno assicurato attività di formazione regolari per i funzionari SIRENE nel campo di SIS II/SIRENE. È stata inoltre effettuata un'analisi delle esigenze in ambito formativo.

Gli Stati membri stanno valutando sempre più spesso la possibilità di investire in ambienti di formazione pratica integrati/online.

La normativa modificata che istituisce i sistemi informatici pertinenti (ad esempio, SIS II) prevede la possibilità per l'Agenzia EBCG (Frontex) di mettere a punto interfacce specifiche che possano essere utilizzate dagli agenti distaccati in qualsiasi Stato membro.

Raccomandazione 1 – Promuovere l'uso di ambienti di formazione per i sistemi SIS II e VIS

La Commissione accoglie la raccomandazione 1.

86 Per quanto riguarda Eurosur, va osservato che solo una parte delle informazioni scambiate è obbligatoria. Ad esempio, gli Stati membri senza frontiere esterne terrestri e marittime hanno la possibilità, ma non l'obbligo, di scambiare informazioni sulle frontiere aeree. Tuttavia, con il nuovo regolamento relativo alla guardia di frontiera e costiera europea, anche i controlli alle frontiere e la sorveglianza delle frontiere aeree sono stati inclusi in Eurosur come requisito obbligatorio; ciò significa che in futuro quasi tutti gli Stati membri forniranno attivamente informazioni nel quadro di Eurosur.

Cfr. risposte della Commissione ai paragrafi da 24 a 32.

Raccomandazione 2 – Accelerare la correzione delle debolezze constatate durante le valutazioni Schengen

La Commissione accoglie la raccomandazione 2.

Raccomandazione 3 – Analizzare le discrepanze relative alle verifiche dei visti

La Commissione accoglie la raccomandazione 3.

Raccomandazione 4 – Migliorare le procedure per il controllo della qualità dei dati

La Commissione accoglie la raccomandazione 4.

La Commissione ed eu-LISA stanno già provvedendo a migliorare il meccanismo. La questione viene regolarmente esaminata dal comitato SIS-VIS.

95 La questione riguardante la tempistica per la trasmissione delle informazioni è stata affrontata nel nuovo regolamento relativo alla guardia di frontiera e costiera europea che dovrebbe entrare in vigore entro la fine del 2019 e che abrogherà l'attuale regolamento Eurosur. L'atto di esecuzione relativo al sistema Eurosur riguarderà le tempistiche per la trasmissione delle informazioni in Eurosur e il livello di responsabilità in materia di comunicazione.

Raccomandazione 5 – Ridurre i tempi per l'inserimento dei dati

La Commissione accetta la raccomandazione 5, lettera a).

La Commissione accoglie la raccomandazione 5, lettera b).

La Commissione conviene sulla parte relativa a Eurosur. La questione riguardante le scadenze per l'inserimento dei dati è stata affrontata nel nuovo regolamento relativo alla guardia di frontiera e costiera europea che dovrebbe entrare in vigore entro la fine del 2019, che abrogherà l'attuale regolamento Eurosur e che consentirà di concordare norme di attuazione vincolanti sullo scambio futuro di informazioni nel quadro di Eurosur.

Équipe di audit

Le relazioni speciali della Corte dei conti europea illustrano le risultanze degli audit espletati su politiche e programmi dell'UE o su temi relativi alla gestione concernenti specifici settori di bilancio. La Corte seleziona e pianifica detti incarichi di audit in modo da massimizzarne l'impatto, tenendo conto dei rischi per la performance o la conformità, del livello delle entrate o delle spese, dei futuri sviluppi e dell'interesse pubblico e politico.

Il presente controllo di gestione è stato espletato dalla Sezione di audit III, competente per l'audit della spesa per azioni esterne, sicurezza e giustizia e presieduta da Bettina Jakobsen, Membro della Corte, che ha anche diretto l'audit. A tal fine è stata coadiuvata da: Katja Mattfolk, capo di Gabinetto, e Kim Storup, attaché di Gabinetto; Alejandro Ballester Gallardo, primo manager; Piotr Senator, Alexandre Tan e Mirko Iaconisi, auditor. Michael Pyper ha fornito assistenza linguistica.

Da sinistra a destra: Mirko Iaconisi, Piotr Senator, Michael Pyper, Bettina Jakobsen, Alejandro Ballester Gallardo, Katja Mattfolk.

Cronologia

Evento	Data
Adozione del piano di indagine (APM) / Inizio dell'audit	17.4.2018
Trasmissione ufficiale del progetto di relazione alla Commissione (o ad altra entità sottoposta ad audit)	11.7.2019
Adozione della relazione finale dopo la procedura in contraddittorio	8.10.2019
Ricezione, in tutte le lingue, delle risposte ufficiali della Commissione (o di altra entità sottoposta ad audit)	31.10.2019

IT	PDF	ISBN 978-92-847-3856-4	doi:10.2865/84412	QJ-AB-19-020-IT-N
IT	HTML	ISBN 978-92-847-3822-9	doi:10.2865/96625	QJ-AB-19-020-IT-Q

L’abolizione dei controlli alle frontiere all’interno dello spazio Schengen ha reso più importanti un controllo e una sorveglianza efficaci alle sue frontiere esterne. Per agevolare le guardie di frontiera nello svolgimento di tali controlli, l’UE ha creato una serie di sistemi di informazione. La Corte ha esaminato se i principali sistemi di informazione dell’UE per la sicurezza interna supportino in modo efficiente il controllo alle frontiere. La Corte ha rilevato che, al momento di eseguire le verifiche di frontiera, le guardie di frontiera utilizzano e fanno affidamento su tali sistemi in misura crescente. Tuttavia, alcuni dati non sono attualmente registrati nei sistemi, mentre altri dati sono incompleti o non sono inseriti tempestivamente nei sistemi. Ciò riduce l’efficienza di alcune verifiche di frontiera. La Corte formula una serie di raccomandazioni, ad esempio il miglioramento delle procedure per garantire la qualità dei dati e la riduzione dei ritardi nell’inserimento dei dati e dei tempi per correggere le debolezze individuate.

Relazione speciale della Corte dei conti europea presentata in virtù dell’articolo 287, paragrafo 4, secondo comma, del TFUE.

CURIA RATIONUM
CORTE DEI CONTI EUROPEA

Ufficio delle pubblicazioni

CORTE DEI CONTI EUROPEA
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Modulo di contatto: eca.europa.eu/it/Pages/ContactForm.aspx
Sito Internet: eca.europa.eu
Twitter: @EUAuditors