Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Questo testo è una versione provvisoria. La versione definitiva che sarà pubblicata su www.dirittofederale.admin.ch è quella determinante.

20.xxx

Messaggio relativo all'approvazione e alla trasposizione nel diritto svizzero degli scambi di note tra la Svizzera e l'UE concernenti il recepimento dei regolamenti (UE) 2019/817 e (UE) 2019/818 che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (sviluppi dell'acquis di Schengen)

del 2 settembre 2020

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di decreto federale che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento dei regolamenti (UE) 2019/817 e (UE) 2019/818 che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (sviluppi dell'acquis di Schengen).

Gradite, onorevoli presidenti e consiglieri, l'espressione della nostra alta considerazione.

… In nome del Consiglio federale svizzero:

La presidente della Confederazione, Simonetta Sommaruga
Il cancelliere della Confederazione, Walter Thurnherr

Compendio

L'interoperabilità metterà in collegamento diversi sistemi d'informazione dell'Unione europea (UE). Con un'unica interrogazione, le autorità di controllo delle frontiere, migratorie e di perseguimento penale potranno ottenere in futuro ampie informazioni da tutti i sistemi d'informazione per esse rilevanti. Sarà inoltre agevolata l'identificazione di persone grazie al confronto tra i dati biometrici contenuti in diversi sistemi d'informazione. In tal modo, le autorità potranno individuare casi di identità multiple e frodi di identità. L'interoperabilità intende migliorare la sicurezza in Svizzera e nello spazio Schengen, rendere più efficienti i controlli alle frontiere esterne e contribuire alla gestione della migrazione irregolare. Con l'introduzione dell'interoperabilità, i diritti di accesso delle autorità ai singoli sistemi resteranno immutati. Il presente messaggio illustra le misure giuridiche necessarie ai fini del recepimento e della trasposizione nel diritto svizzero dei due regolamenti UE sull'interoperabilità e fornisce una panoramica delle ripercussioni per la Confederazione e i Cantoni.

Situazione iniziale

Le autorità di controllo delle frontiere, migratorie e di perseguimento penale possono accedere a numerosi sistemi d'informazione dell'UE. Tuttavia, tali sistemi oggi non sono connessi tra loro. Per ottenere informazioni su una persona, occorre pertanto interrogare separatamente ogni singolo sistema d'informazione. Ciò non consente di sfruttare le sinergie. Grazie all'interoperabilità i sistemi d'informazione dell'UE saranno collegati in modo tale da rendere più efficace ed efficiente l'utilizzo delle informazioni disponibili. In futuro le autorità interessate potranno infatti effettuare un'interrogazione simultanea di diversi sistemi d'informazione, laddove dispongano dei diritti di accesso necessari per i sistemi interrogati. L'interoperabilità non implica l'ampliamento di tali diritti di accesso. Essa consente unicamente di individuare i collegamenti tra i dati esistenti.

Contenuto del progetto

Con l'interoperabilità viene creato un portale di ricerca europeo che consente di consultare simultaneamente tutti i pertinenti sistemi d'informazione. L'interoperabilità prevede la registrazione a livello centralizzato dei dati di identità e biometrici (impronte digitali e immagini del viso) di cittadini di Paesi terzi all'interno di un archivio comune e permette inoltre il confronto automatizzato di dati biometrici di una persona.

Grazie a un utilizzo più efficiente delle informazioni contenute nei sistemi, l'interoperabilità rafforzerà la sicurezza in Svizzera e nello spazio Schengen e migliorerà la gestione della migrazione. In tal modo, l'interoperabilità contribuisce al raggiungimento degli obiettivi del Consiglio federale 2020 nei settori della sicurezza e della migrazione. Nella lotta alla criminalità e nella gestione della migrazione, la Svizzera si trova davanti a sfide di carattere transnazionale. Per tale

motivo, è essenziale che le autorità svizzere possano collaborare a stretto contatto e scambiare rapidamente informazioni con gli altri Stati Schengen. L'interoperabilità faciliterà alle autorità di controllo delle frontiere, migratorie e di perseguimento penale l'identificazione delle persone che rappresentano una minaccia per la sicurezza o che forniscono informazioni false in merito alla propria identità.

La trasposizione dei due regolamenti UE (sviluppi dell'acquis di Schengen) comporta modifiche nella legge federale sugli stranieri e la loro integrazione, nella legge federale sul sistema d'informazione per il settore degli stranieri e dell'asilo, nella legge sulla responsabilità e nella legge federale sui sistemi d'informazione di polizia della Confederazione.

Tale trasposizione comporta oneri supplementari in termini finanziari e di personale per la Confederazione e i Cantoni. I sistemi d'informazione e i processi esistenti in Svizzera devono essere infatti adeguati per poter sfruttare a pieno le possibilità offerte dall'interoperabilità.

Indice

Decreto federale

che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento dei regolamenti (UE) 2019/817 e (UE) 2019/ 818 che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione dell'UE

(Sviluppi dell'acquis di Schengen) *(disegno)*

Scambio di note del …[1] tra la Svizzera e l'Unione europea concernente il recepimento del regolamento (UE) 2019/817 che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio;

Scambio di note del …[2] tra la Svizzera e l'Unione europea concernente il recepimento del regolamento (UE) 2019/818 che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816.

1 RS **0.362.380.xxx**; RU **xxxxx**
2 RS **0.362.380.xxx**; RU **xxxxx**

Messaggio

1 Introduzione

L'interoperabilità intende migliorare la sicurezza in Svizzera e nello spazio Schengen, rendere più efficienti i controlli alle frontiere esterne e contribuire alla gestione della migrazione. Grazie all'interoperabilità, gli attuali sistemi d'informazione dell'UE della cooperazione Schengen/Dublino in futuro saranno collegati in modo tale da permettere di confrontare in maniera automatizzata i dati di identità, dei documenti di viaggio e biometrici (impronte digitali e immagini del viso). In tal modo, le informazioni contenute potranno essere consultate in modo più semplice e veloce, contribuendo così a rafforzare la sicurezza nello spazio Schengen e a migliorare la gestione della migrazione. Potranno beneficiare dell'interoperabilità le autorità di perseguimento penale, di controllo delle frontiere e migratorie. In tale contesto i diritti d'accesso delle autorità ai singoli sistemi restano immutati. Il presente messaggio concerne il recepimento e la trasposizione dei regolamenti (UE) 2019/817[3] e (UE) 2019/818[4] concernenti la realizzazione dell'interoperabilità tra i sistemi d'informazione dell'UE nel settore delle frontiere, della migrazione e della polizia.

2 Situazione iniziale

2.1 Necessità d'intervento e obiettivi

Le autorità di controllo delle frontiere, migratorie e di perseguimento penale possono accedere già oggi a numerosi sistemi d'informazione dell'Unione europea. Tali sistemi, tuttavia, non sono connessi tra loro sul piano tecnico. I dati sono registrati separatamente nei singoli sistemi d'informazione. Le sinergie non possono dunque essere sfruttate. Vi è pertanto il rischio che, non potendo consultare i singoli sistemi d'informazione, le autorità non vengano a conoscenza delle informazioni importanti ivi contenute così come delle eventuali correlazioni. L'esempio qui di seguito evidenzia un'attuale lacuna in materia di sicurezza. Tale lacuna potrà essere colmata in futuro grazie all'interoperabilità:

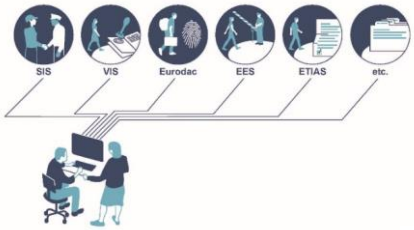
Un criminale proveniente da uno Stato terzo è segnalato in Svizzera nel Sistema d'informazione Schengen (SIS) ai fini di un divieto d'entrata ed è stato pertanto allontanato nel suo Paese d'origine. La stessa persona richiede un visto presso

3 Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, versione della GU L 135 del 22.5.2019, pag. 27.

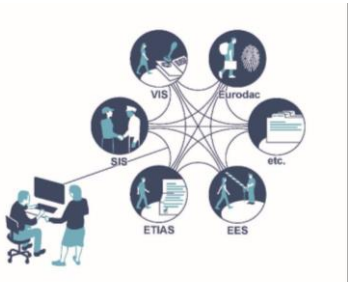
4 Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, versione della GU L 135 del 22.5.2019, pag. 85.

l'ambasciata di un altro Stato Schengen servendosi di una falsa identità. Le sue impronte digitali, sebbene siano registrate nel sistema d'informazione visti (VIS), non vengono confrontate con le impronte registrate nel SIS. La persona in questione riceve il visto riuscendo così a entrare nuovamente nello spazio Schengen.

L'interoperabilità tra i sistemi di informazione dell'UE permetterà di confrontare in futuro in maniera automatizzata i dati di identità, dei documenti di viaggio o biometrici (impronte digitali e immagini del viso) di cittadini di Stati terzi e di identificare i criminali che utilizzano false identità. Sarà così possibile consultare simultaneamente tutti i sistemi d'informazione (nel caso in questione il SIS e il VIS) effettuando un'unica interrogazione.



Senza l'interoperabilità ciascun sistema deve essere consultato separatamente.



Grazie all'interoperabilità le autorità potranno consultare simultaneamente tutti i sistemi d'informazione tramite un'unica interrogazione.

Interoperabilità significa dunque collegare i sistemi d'informazione dell'UE in modo tale da poter utilizzare le informazioni ivi contenute in modo più efficiente e mirato. Con l'interoperabilità, le autorità che hanno accesso ai sistemi interessati potranno in futuro disporre di tutte le informazioni rilevanti ai fini dell'adempimento dei propri compiti, riuscendo in tal modo ad avere un quadro completo di una persona in modo rapido ed efficiente. L'obiettivo è di permettere alle autorità di disporre in qualsiasi momento di tutte le informazioni essenziali per evitare ad esempio, come nel caso illustrato poc'anzi, che venga rilasciato un visto a un criminale proveniente da uno Stato terzo.

A tal fine, il 20 maggio 2019 il Parlamento europeo e il Consiglio dell'UE hanno approvato due regolamenti volti a istituire l'interoperabilità tra i sistemi d'informazione dell'UE:

- il regolamento (UE) 2019/817 concernente il settore delle frontiere e dei visti (di seguito: regolamento «IOP frontiere»);
- il regolamento (UE) 2019/818 concernente il settore della cooperazione di polizia e giudiziaria, asilo e migrazione (di seguito: regolamento «IOP po-

lizia»).

Con l'interoperabilità saranno create le componenti seguenti:

- il portale di ricerca europeo (ESP), che permette alle autorità competenti di consultare contemporaneamente più sistemi d'informazione;
- il servizio comune di confronto biometrico (sBMS) che permette il confronto di dati biometrici (impronte digitali e immagini del viso) contenuti in più sistemi;
- l'archivio comune di dati di identità (CIR) che contiene i dati di identità, i dati dei documenti di viaggio e i dati biometrici di cittadini di Stati terzi contenuti in più sistemi d'informazione dell'UE;
- il rilevatore di identità multiple (MID) che evidenzia le correlazioni esistenti tra i dati contenuti nei sistemi collegati (i cosiddetti collegamenti MID), contribuendo a individuare persone registrate sotto falsa identità o con più identità.

Tramite l'interoperabilità non sono rilevati nuovi dati, bensì sono semplicemente aggiunte nuove funzioni agli attuali e futuri sistemi d'informazione (SIS, VIS, il sistema di ingressi/uscite [EES], il sistema europeo di informazione e autorizzazione ai viaggi [ETIAS], la banca dati centrale dell'Unione europea in cui sono conservate le impronte digitali delle persone che hanno presentato una domanda d'asilo in uno Stato Dublino o che sono state arrestate nel tentativo di entrare illegalmente [Eurodac]). Per le autorità non vi sarà alcun cambiamento per quanto riguarda gli attuali diritti di accesso ai sistemi d'informazione sottostanti.

I due regolamenti UE sull'interoperabilità sono stati elaborati in seguito agli attacchi terroristici perpetrati a partire dal 2015 nello spazio Schengen e alla luce delle crescenti sfide nel settore della migrazione. Lo sviluppo e l'ampliamento della struttura IT dell'UE sono considerati elementi centrali per poter garantire un miglioramento della sicurezza nello spazio Schengen. L'interoperabilità dei sistemi d'informazione dell'UE assume un ruolo primario nel colmare le lacune esistenti nel settore della sicurezza. La semplificazione dello scambio di dati tra i diversi sistemi d'informazione consentirà, tuttavia, anche controlli più rapidi ed efficaci alle frontiere esterne dello spazio Schengen, contribuendo così al contrasto della migrazione illegale. In tal modo, le informazioni disponibili potranno essere utilizzate in modo più efficiente e mirato, apportando un importante valore aggiunto al lavoro delle autorità di perseguimento penale, di controllo delle frontiere e migratorie.

Con l'accordo di associazione a Schengen (AAS)[5], la Svizzera si è impegnata a recepire di principio tutti i nuovi sviluppi dell'acquis di Schengen (art. 2 par. 3 e

5 Accordo del 26 ottobre 2004 tra la Confederazione svizzera, l'Unione europea e la Comunità europea, riguardante l'associazione della Svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen, RS **0.362.31**

art. 7 AAS). Il recepimento di un nuovo atto si svolge secondo una procedura particolare che prevede la notifica dello sviluppo da parte degli organi responsabili dell'UE e la trasmissione di una nota di risposta da parte della Svizzera.

Il 21 maggio 2019 i due regolamenti UE sono stati notificati alla Svizzera come sviluppi dell'acquis di Schengen. Il 14 giugno 2019 il nostro Consiglio ha approvato gli scambi di note concernenti il recepimento dei regolamenti UE, con riserva di approvazione parlamentare. Il 19 giugno 2019 abbiamo trasmesso all'UE le rispettive note di risposta. L'obiettivo del presente disegno è di recepire entro i termini prestabiliti gli sviluppi dell'acquis di Schengen e di creare le necessarie basi giuridiche per la relativa trasposizione. La Svizzera dispone di un termine massimo di due anni. Il termine scade il 21 maggio 2021.

2.2 Svolgimento dei negoziati

Il 12 dicembre 2017 la Commissione europea ha presentato due proposte di regolamento sull'interoperabilità, che insieme costituiscono le basi giuridiche per l'istituzione dell'interoperabilità tra i sistemi d'informazione dell'UE nei settori delle frontiere, della migrazione e di polizia. Le discussioni in seno al Consiglio dell'UE si sono protratte da gennaio a settembre 2018, mentre i negoziati con il Parlamento europeo (trilogo) da ottobre 2018 a febbraio 2019. I rappresentanti della Svizzera hanno preso parte a tutte le riunioni, hanno avuto la possibilità di chiarire le questioni tecniche e di contribuire con le loro proposte di soluzione durante tutte le tappe dei negoziati.

Le discussioni sono state particolarmente intense, soprattutto per quanto riguarda i temi seguenti:

- Attuazione: oltre alle ripercussioni finanziarie per gli Stati Schengen, sono state discusse le conseguenze dell'attuazione sui controlli delle persone alle frontiere esterne dello spazio Schengen. Sono stati espressi dubbi in particolare per quanto riguarda la fattibilità tecnica di un'interrogazione simultanea di tutti i sistemi interoperabili durante i controlli delle persone alle frontiere esterne di Schengen.
- Aumento del fabbisogno di personale: è stata più volte inserita all'ordine del giorno la questione relativa all'aumento del fabbisogno di personale per gli Stati Schengen e agli oneri aggiuntivi per i servizi esistenti quali ad esempio gli uffici SIRENE nazionali, i quali sono competenti per lo scambio di informazioni e il coordinamento della procedura in caso di riscontro positivo nel SIS.
- «Geometria variabile»: tale espressione è utilizzata per indicare il problema della mancata adesione di singoli Stati a uno o più sistemi d'informazione dell'UE. Nel caso dei sistemi interoperabili, il minore o maggiore grado di integrazione implica risultati diversi nell'interrogazione dei sistemi centrali interoperabili. I Paesi maggiormente interessati attualmente da tale problematica sono soprattutto il Regno Unito e l'Irlanda, i quali essendo sprovvisti dell'accesso al SIS non possono usufruire della funzionalità del MID di rilevare le identità multiple, ma anche la Svizzera e altri Stati associati per via

dell'accesso limitato ai dati dell'Ufficio europeo di polizia (Europol) o del mancato accesso al sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di Paesi terzi (ECRIS-TCN).

- Interrogazione delle banche dati dell'Organizzazione internazionale di polizia criminale (Interpol): le basi giuridiche previste con l'interoperabilità per l'interrogazione delle banche dati Interpol sono tuttora oggetto di discussioni. Le questioni ancora in sospeso saranno disciplinate in un accordo tra l'UE e Interpol.
- Ulteriori temi: accesso al CIR a scopo di identificazione o di perseguimento penale o l'informazione dei cittadini degli Stati terzi interessati.

Il compromesso raggiunto è stato approvato in sessione plenaria dal Parlamento europeo il 16 aprile 2019 e dal Consiglio dei ministri il 14 maggio 2019. L'approvazione ufficiale dei regolamenti è avvenuta il 20 maggio 2019 tramite sottoscrizione dell'atto giuridico da parte dei presidenti del Parlamento europeo e del Consiglio dell'UE. Gli sviluppi dell'acquis di Schengen sono stati notificati alla Svizzera il 21 maggio 2019.

2.3 Procedura di recepimento degli sviluppi dell'acquis di Schengen

L'articolo 2 paragrafo 3 AAS obbliga la Svizzera a recepire e, se necessario, a trasporre nel diritto svizzero tutti gli atti adottati dall'UE quale sviluppo dell'acquis di Schengen sin dalla firma dell'accordo avvenuta il 26 ottobre 2004.

L'articolo 7 AAS prevede una procedura speciale per il recepimento e la trasposizione di uno sviluppo dell'acquis di Schengen: in un primo momento l'UE notifica «immediatamente» alla Svizzera l'avvenuta adozione di un atto che costituisce uno sviluppo dell'acquis di Schengen. Successivamente il Consiglio federale dispone di un termine di 30 giorni per comunicare al competente organo dell'UE (Consiglio dell'UE o Commissione europea) se e, all'occorrenza, entro quale termine intende recepire lo sviluppo notificatole. Il termine di 30 giorni inizia a decorrere dalla data dell'adozione dell'atto da parte dell'UE (art. 7 par. 2 lett. a AAS).

Se lo sviluppo da recepire è giuridicamente vincolante, la notifica di un atto da parte dell'UE e la nota di risposta della Svizzera costituiscono uno scambio di note che, dal punto di vista svizzero, è considerato alla stregua di un trattato internazionale. Conformemente ai requisiti costituzionali, l'approvazione formale di questo trattato incombe al Consiglio federale o al Parlamento e, nel quadro di un referendum, al popolo.

I due regolamenti UE da recepire sono giuridicamente vincolanti. Il recepimento dei presenti regolamenti UE deve pertanto avere luogo mediante scambio di note.

Nel presente caso, l'approvazione dello scambio di note compete all'Assemblea federale (cfr. n. 10.1 del presente messaggio). Il 19 giugno 2019 la Svizzera ha informato l'UE nelle sue note di risposte che il recepimento dello sviluppo potrà essere vincolante «soltanto previo soddisfacimento dei suoi requisiti costituzionali» (art. 7 par. 2 lett. b AAS). La Svizzera dispone, per recepire e trasporre gli sviluppi

di Schengen, di un termine massimo di due anni a decorrere dalla notifica degli atti da parte dell'UE. Entro tale termine deve inoltre aver luogo l'eventuale referendum.

Non appena la procedura nazionale è completata e tutti i requisiti costituzionali in vista del recepimento e della trasposizione dei regolamenti UE sono stati soddisfatti, la Svizzera ne informa per iscritto immediatamente il Consiglio dell'UE e la Commissione europea. Se non è indetto alcun referendum contro il recepimento e la trasposizione dei regolamenti UE, la comunicazione ha luogo immediatamente dopo la scadenza del termine referendario. Tale comunicazione equivale alla ratifica dello scambio di note.

La mancata trasposizione entro i termini prestabiliti di uno sviluppo dell'acquis di Schengen da parte della Svizzera può implicare la cessazione della cooperazione Schengen e pertanto anche della cooperazione Dublino (art. 7 par. 4 AAS in combinato disposto con l'art. 14 par. 2 AAD[6]).

In base alla data di notifica da parte dell'UE (21 maggio 2019), il termine di al massimo due anni per recepire e trasporre i regolamenti UE scade dunque il 21 maggio 2021. Poiché l'entrata in funzione delle componenti centrali e dunque l'attuazione delle pertinenti disposizioni dei regolamenti UE avverrà in modo scaglionato in una data successiva (per i dettagli cfr. n. 4.2) e considerato che l'interoperabilità sarà pertanto completamente realizzata non prima del 2023, di fatto dovrebbe sussistere un certo margine di flessibilità che consenta eventualmente di prorogare di poco il termine in modo pragmatico.

2.4 Rapporto con il programma di legislatura, la pianificazione finanziaria e la strategia del Consiglio federale

L'approvazione del presente messaggio è un nostro obiettivo annuale per il 2020. Il progetto è annunciato nel messaggio del 29 gennaio 2020 sul programma di legislatura 2019-2023[7].

Grazie all'utilizzo ottimale e interoperabile dei diversi sistemi d'informazione dell'UE, la Svizzera rinnova e sviluppa le proprie relazioni politiche ed economiche con l'UE. La condivisione tempestiva e completa delle informazioni rilevanti con le autorità competenti contribuisce alla gestione della migrazione e alla prevenzione della migrazione irregolare. La Svizzera deve prevenire la violenza, la criminalità e il terrorismo e combatterli efficacemente. Deve essere al corrente delle minacce alla propria sicurezza e disporre degli strumenti necessari per fronteggiarle in modo efficace. L'interoperabilità contribuisce a raggiungere tali obiettivi poiché consente di utilizzare in modo più efficiente i sistemi d'informazione dell'UE.

Nel preventivo 2020 con piano integrato dei compiti e delle finanze 2021-2023 è prevista una prima tranche per la realizzazione dell'interoperabilità dei sistemi

6 Accordo del 26 ottobre 2004 tra la Confederazione Svizzera e la Comunità europea relativo ai criteri e ai meccanismi che permettono di determinare lo Stato competente per l'esame di una domanda di asilo introdotta in uno degli Stati membri o in Svizzera; RS **0.142.392.68.**

7 FF **2020** 1565, in particolare 1684.

d'informazione dell'UE. Non appena saranno disponibili i piani di gestione aggiornati dei progetti e un rapporto sui rischi e sulla qualità relativo ai progetti in questione, libereremo la seconda tranche del credito d'impegno per il «Perfezionamento Schengen/Dublino». La liberazione di tutti i crediti potrà avvenire soltanto una volta che l'Assemblea federale avrà adottato le basi legali.

Il recepimento e la trasposizione dei regolamenti UE sull'interoperabilità non sono in contrasto con nessuna strategia del Consiglio federale e permettono alla Svizzera di adempiere ai propri obblighi derivanti dall'AAS.

3 Procedura di consultazione

3.1 Panoramica

Dal 9 ottobre 2019 al 9 gennaio 2020, è stata svolta una procedura di consultazione conformemente all'articolo 3 capoverso 1 lettera c della legge federale del 18 marzo 2005[8] sulla procedura di consultazione (LCo).

Sono pervenute 44 risposte. In totale hanno espresso un parere scritto tutti i Cantoni, tre partiti politici, cinque associazioni mantello, il Tribunale amministrativo federale e nove cerchie interessate. Di questi, hanno espressamente rinunciato a prendere posizione sette partecipanti.

32 partecipanti alla consultazione accolgono con favore il progetto. Di questi ultimi, 11 non hanno ulteriori osservazioni, mentre tre chiedono di apportare miglioramenti in fase di attuazione. I risultati della consultazione figurano nel rapporto sui risultati della procedura di consultazione[9].

Numerosi Cantoni (AI, FR, GE, JU, LU, NE, OW, SH, SO, TI, VS, ZG) e l'Associazione dei servizi cantonali di migrazione (ASM) sottolineano i costi supplementari e gli oneri aggiuntivi collegati al progetto, sebbene alcuni di loro (AI, LU, VS, ASM) ritengano che il valore aggiunto dell'interoperabilità per la sicurezza sia preponderante. JU e TI chiedono al Consiglio federale di fornire informazioni chiare ai Cantoni sull'entità dei costi e sui potenziali oneri aggiuntivi. OW e GE chiedono alla Confederazione sostegno finanziario oppure il versamento di indennità ai Cantoni. Il PLR e l'UDC si aspettano che durante i dibattiti parlamentari vengano fornite informazioni più precise in merito alla fattibilità, all'attuazione e al finanziamento dell'interoperabilità.

Diverse organizzazioni (Organizzazione svizzera di aiuto ai rifugiati [OSAR], Unione sindacale svizzera [USS], AsyLex, PSS), pur essendo favorevoli al recepimento di tali sviluppi dell'acquis di Schengen, che garantiscono la permanenza della Svizzera nell'associazione Schengen/Dublino, assumono una posizione critica nei confronti del progetto; una parte di esse si dichiara favorevole a un rafforzamento della tutela dei diritti fondamentali e della protezione dei dati. Alla luce dei pareri preva-

8 RS **172.061**

9 www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione concluse > 2019 > DFGP.

lentemente positivi, il decreto federale rimane pertanto invariato. Qui di seguito sono illustrate nel dettaglio le esigenze espresse dai partecipanti alla procedura di consultazione.

3.2 Argomentazioni dettagliate

Protezione dei dati

Diversi partecipanti alla consultazione criticano il fatto che la tutela dei diritti fondamentali e la protezione dei dati di cittadini di Stati terzi non siano sufficientemente garantite. Si temono inoltre attacchi da parte di pirati informatici. Per tale motivo, numerosi partecipanti chiedono l'introduzione e l'applicazione di obblighi di controllo a livello statale e di disposizioni in materia di protezione dei dati. A causa dei compiti supplementari derivanti per le autorità di vigilanza sulla protezione dei dati, alcuni partecipanti alla consultazione chiedono un aumento delle risorse del personale presso l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) e le autorità cantonali di vigilanza sulla protezione dei dati ed eventualmente anche uno sviluppo della loro struttura organizzativa.

Il Partito socialista svizzero (PSS) propone di introdurre l'articolo 111*k* D-LStrI, secondo il quale l'IFPDT, in qualità di autorità di vigilanza nazionale, dovrebbe pubblicare ogni anno il numero delle richieste di rettifica, cancellazione o limitazione del trattamento di dati personali nonché il numero effettivo di rettifiche e cancellazioni effettuate. L'articolo dovrebbe inoltre statuire che l'IFDPT è tenuto ad allestire un rapporto all'attenzione del Garante europeo della protezione dei dati, delle altre autorità di vigilanza nazionali e del Parlamento svizzero.

Il Consiglio federale dovrebbe inoltre provvedere a dotare l'IFPDT delle risorse sufficienti. A tale proposito osserviamo che entrambi i regolamenti UE sull'interoperabilità, elaborati con il coinvolgimento del Garante europeo della protezione dei dati, contengono un intero capo dedicato alla protezione dei dati e al relativo controllo (capo VII dei regolamenti UE sull'interoperabilità). È previsto inoltre anche il controllo da parte del Garante europeo della protezione dei dati. Si può inoltre rimandare al capitolo 14*c* D-LStrI contenente ora tutte le disposizioni riguardanti la protezione dei dati nell'ambito dell'AAS. Si applicano dunque i principi fondamentali del diritto in materia di protezione dei dati. L'accesso ai dati deve essere pertanto proporzionato agli obiettivi perseguiti e può essere concesso solo nella misura in cui i dati sono necessari per lo svolgimento dei compiti da parte delle autorità competenti. Un ulteriore elemento centrale nella valutazione della legislazione sulla protezione dei dati è costituito dal fatto che i diritti di accesso delle autorità ai sistemi d'informazione sottostanti all'interoperabilità non saranno ampliati. Tali diritti rimangono invariati e sono disciplinati nelle basi legali specifiche di tali sistemi d'informazione.

Nella misura in cui i dati sono consultati e trattati ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, si applicano

le norme della direttiva (UE) 2016/680[10], trasposta nel diritto svizzero con la legge del 28 settembre 2018[11] sulla protezione dei dati in ambito Schengen (LPDS). Se il trattamento dei dati avviene per altri scopi, i regolamenti UE sull'interoperabilità presuppongono l'applicazione del regolamento generale sulla protezione dei dati (regolamento [UE] 2016/679)[12]. Tale regolamento non è vincolante per la Svizzera, poiché l'UE non lo ha qualificato come sviluppo dell'acquis di Schengen e dunque non è stato trasposto dalla Svizzera in quanto tale. Tuttavia, le relative disposizioni per il trattamento di dati nel quadro della cooperazione prevista da Schengen sono *indirettamente* rilevanti. Di tali disposizioni si è tenuto conto nel quadro dell'attuale revisione totale della legge federale del 19 giugno 1992[13] sulla protezione dei dati (LPD). Lo scopo della revisione totale della LPD è quello di garantire in Svizzera un livello di protezione equivalente sia nel settore privato sia nel settore pubblico[14], motivo per cui una trasposizione specifica del regolamento generale sulla protezione dei dati risulta superflua nell'ambito del presente disegno.

Le registrazioni nelle componenti dell'interoperabilità sono soggette ai medesimi standard elevati di protezione dei dati valevoli per i sistemi d'informazione sottostanti all'interoperabilità. Sono competenti per il trattamento dei dati nell'sBMS e nel CIR, le autorità degli Stati Schengen/Dublino a loro volta responsabili per il trattamento dei dati nel SIS, nel VIS e nell'EES. Sono invece competenti per il trattamento dei dati nel MID, l'unità centrale ETIAS nonché le autorità degli Stati Schengen/Dublino che aggiungono o modificano i fascicoli di conferma dell'identità. La sicurezza delle componenti centrali e dell'infrastruttura di comunicazione incombe invece all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA). Per esempio, in caso di interruzione, eu-LISA garantisce il ripristino del normale funzionamento.

In relazione al nuovo articolo proposto 111*k* D-LStrI, il nostro Collegio constata che tali richieste trovano riscontro nell'articolo 51 paragrafi 2 e 4 e nell'articolo 37 paragrafo 5 delle direttive UE sull'interoperabilità. Con la trasposizione, tali direttive diventano vincolanti per la Svizzera. Il decreto federale riprende le disposizioni dei regolamenti UE soltanto nella misura in cui sia necessario in particolare in virtù della LPD. Occorre ad esempio disciplinare a livello di legge formale gli scopi del trattamento dei dati, i diritti di accesso, la trasmissione dei dati nonché le sanzioni

10 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio; GU L 119 del 4.5.2016, pag. 89.

11 RS **235.3**

12 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, GU L 119 del 4.5.2016, pag. 1.

13 RS **235.1**

14 Cfr. messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF **2017** 5939.

previste in caso di trattamento abusivo dei dati. Non è, tuttavia, opportuno riprendere tutti gli articoli dei regolamenti UE sull'interoperabilità nella legislazione svizzera.

Per quanto concerne le esigenze poste alle autorità di controllo, i regolamenti UE sull'interoperabilità rimandano alla direttiva (UE) 2016/680 e al regolamento (UE) 2016/679. Laddove si fa riferimento alla direttiva (UE) 2016/680, all'autorità di controllo sono state accordate le competenze previste dalla direttiva (cfr. art. 21-25 LPDS).

In relazione ai meccanismi di controllo, occorre evidenziare che in Svizzera esistono strutture già consolidate che continuano a essere sviluppate costantemente anche nell'ambito dei sistemi d'informazione Schengen/Dublino. L'IFPDT e le autorità cantonali di protezione dei dati collaborano attivamente nell'ambito delle rispettive competenze e provvedono a una vigilanza coordinata sul trattamento dei dati personali. L'IFPDT coordina l'attività di vigilanza con le autorità cantonali di protezione dei dati e funge da referente nazionale per il Garante europeo della protezione dei dati. L'IFPDT è stato consultato nell'ambito del presente progetto in relazione alla propria funzione e non ha espresso alcuna obiezione in merito. Le norme relative ai diritti delle persone interessate (diritto di accesso ai dati personali, di rettifica e di cancellazione degli stessi), la sicurezza dei dati e la vigilanza sul trattamento dei dati dovranno essere disciplinate a livello di ordinanza esecutiva.

In base ai regolamenti UE sull'interoperabilità, gli Stati Schengen/Dublino sono infine tenuti a prevedere nel diritto nazionale sanzioni per il trattamento o lo scambio di dati illeciti. La relativa disposizione sanzionatoria è già prevista dall'attuale articolo 120*d* D-LStrI. Tale disposizione era già stata introdotta in attuazione del regolamento VIS[15] dell'UE e successivamente completata con il sistema di ingressi/uscite (EES), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e ora anche col MID e col CIR. Non si ravvisano pertanto motivi che giustifichino un adeguamento dell'entità della sanzione penale.

Stigmatizzazione e discriminazione di cittadini di Stati terzi

Alcuni partecipanti alla consultazione (AsyLex, USS, OSAR, PSS) vedono nel progetto un ulteriore passo verso la discriminazione, la disparità di trattamento e la stigmatizzazione di cittadini di Stati terzi rispetto ai cittadini UE/AELS. Lo testimonierebbe in particolare l'uso sistematico di dati biometrici. È inoltre oggetto di critica la tendenza di fondo del progetto a considerare la migrazione principalmente nell'ottica della sicurezza interna.

Il nostro Collegio prende atto di tali riserve e sottolinea che l'interoperabilità non implica la raccolta di dati supplementari o svantaggi per i cittadini di Stati terzi, bensì agevola l'identificazione univoca di persone in base a dati biometrici e dunque

15 Regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS), GU L 218 del 13.8.2008, pag. 60; modificato da ultimo dal regolamento (UE) 2019/817, GU L 135 del 22.5.2019, pag. 27.

anche la mobilità di cittadini di Stati terzi che viaggiano all'interno dello spazio Schengen in modo lecito.

Notifica allo Stato segnalante in caso di consultazione delle banche dati di Interpol

Alcuni partecipanti alla consultazione (AsyLex, USS, OSAR) criticano il fatto che in caso di consultazione delle banche dati di Interpol tramite l'ESP, l'autorità segnalante, e dunque eventualmente anche uno Stato terzo, venga informata in caso di riscontro positivo in merito alla data e al luogo della consultazione. Ciò potrebbe portare a casi di abuso.

A tale riguardo, il nostro Consiglio osserva che, conformemente ai regolamenti UE sull'interoperabilità, i riscontri positivi non sono condivisi con lo Stato segnalante. Sono attualmente in corso colloqui tra l'UE e Interpol concernenti il collegamento di banche dati di Interpol all'interoperabilità, affinché tale condizione possa essere soddisfatta.

Costituzionalità

Il PSS critica l'insufficienza della base costituzionale materiale. La trasposizione dell'interoperabilità va infatti ben oltre la politica estera dato che si ripercuote anche su settori quali l'asilo, la migrazione e la sicurezza.

Rileviamo che la trasposizione dell'interoperabilità dispone di una base costituzionale (art. 54 cpv. 1 della Costituzione federale [Cost.][16]). L'interoperabilità riguarda infatti lo spazio Schengen, al quale la Svizzera partecipa, rientrando pertanto nell'ambito della politica estera. Tale cooperazione riguarda aspetti legati alla sicurezza e alla migrazione. Poiché si tratta della trasposizione di trattati internazionali, la disposizione della Costituzione federale è rilevante.

Constatiamo che l'interoperabilità ha ripercussioni rilevanti dato che riguarda tutti i cittadini di Stati terzi e interferisce con diversi diritti fondamentali, tra cui il diritto alla libertà di movimento (art. 10 cpv. 2 Cost.). Quest'ultima non risulta tuttavia essere limitata in maniera eccessiva dall'interoperabilità. Va inoltre tenuto conto del diritto alla protezione da un impiego abusivo dei dati personali (art. 13 cpv. 2 Cost.). Sottolineiamo in tale contesto il ruolo di controllo svolto dall'IFPDT e dalle autorità cantonali di protezione dei dati. Occorre inoltre affermare che l'interoperabilità non riguarda direttamente il settore dell'asilo. Le condizioni di entrata e di soggiorno non subiscono alcuna modifica con l'introduzione dell'interoperabilità.

Indipendentemente da quanto illustrato poc'anzi, la Svizzera s'impegna a vari livelli in favore delle persone bisognose di protezione. Nel 2019, il nostro Collegio ha approvato il programma di reinsediamento, nell'ambito del quale ha deciso di accogliere per un periodo di due anni rifugiati particolarmente bisognosi di protezione. La Svizzera può inoltre rilasciare un visto per motivi umanitari se in un caso concreto si può ritenere che la vita o l'integrità fisica di una persona sia direttamente, seriamente e concretamente minacciata nel Paese d'origine o di provenienza (art. 4

16 RS **101**

cpv. 2 dell'ordinanza del 15 agosto 2018[17] concernente l'entrata e il rilascio del visto; OEV).

4 Punti essenziali dei regolamenti UE

4.1 Panoramica

L'interoperabilità è disciplinata nell'UE all'interno di due regolamenti distinti e ciò è riconducibile al diverso grado di partecipazione alla cooperazione Schengen da parte degli Stati associati. Il primo regolamento riguarda il settore delle frontiere e dei visti (regolamento «IOP frontiere»), mentre il secondo riguarda il settore della cooperazione di polizia e giudiziaria, asilo e migrazione (regolamento «IOP polizia»). Salvo poche disposizioni, entrambi i regolamenti UE coincidono. L'interoperabilità non implica la creazione di alcuna banca dati aggiuntiva, bensì l'integrazione di nuove funzioni nei sistemi d'informazione attuali e futuri.

Con entrambi i regolamenti UE sull'interoperabilità saranno create quattro nuove componenti centrali per i sistemi d'informazione dell'UE, ovvero:

- il portale di ricerca europeo (*European Search Portal*, di seguito: «ESP») che permette alle autorità competenti di consultare contemporaneamente più sistemi d'informazione dell'UE tramite un'unica interrogazione;
- il servizio comune di confronto biometrico (*shared Biometric Matching Service*, di seguito «sBMS») che permette l'interrogazione di diversi sistemi d'informazione dell'UE tramite dati biometrici;
- un archivio comune di dati di identità (*Common Identity Repository*, di seguito «CIR») che contiene i dati d'identità (p. es. nome e data di nascita), dei documenti di viaggio o biometrici di cittadini di Stati terzi agevolandone così l'identificazione; e
- il rilevatore di identità multiple (*Multiple Identity Detector*, di seguito «MID») il quale evidenzia le correlazioni esistenti tra i dati esistenti e quelli nuovi contenuti nei diversi sistemi d'informazione dell'UE, contribuendo al contrasto della frode d'identità.

I regolamenti UE sull'interoperabilità riguardano i sistemi d'informazione e le banche dati dell'UE seguenti:

- il Sistema d'informazione Schengen (SIS) dove sono registrate segnalazioni di persone ricercate o scomparse nonché di veicoli e oggetti ricercati. Nel SIS sono inoltre registrati i divieti d'entrata e in futuro anche le decisioni di rimpatrio;
- il sistema d'informazione visti (C-VIS) dove sono contenuti i dati relativi ai visti Schengen;
- l'Eurodac, ovvero la banca dati centrale delle impronte digitali dei richiedenti l'asilo e delle persone fermate nel tentativo di entrare illegalmente;

17 RS **142.204**

- il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di Paesi terzi (ECRIS-TCN), un sistema elettronico volto allo scambio di informazioni registrate sul casellario giudiziale tra i Paesi dell'UE;
- il sistema di ingressi/uscite (EES), nel quale saranno registrati in futuro i dati relativi agli ingressi e alle uscite di cittadini di Stati terzi che soggiornano nello spazio Schengen per al massimo 90 giorni su un periodo di 180 giorni nonché i rifiuti d'entrata;
- il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), tramite il quale in futuro i cittadini di Paesi terzi esentati dall'obbligo del visto dovranno chiedere e ricevere l'autorizzazione ai viaggi prima di entrare nello spazio Schengen;
- i dati Europol (*Europol Information System*); e
- le banche dati di Interpol sui documenti di viaggio rubati o smarriti (Stolen and Lost Travel Documents, di seguito «SLTD») e sui documenti di viaggio associati a segnalazioni (Travel Documents Associated with Notices, di seguito «TDAWN»).

La Svizzera partecipa già ai sistemi d'informazione SIS, VIS ed Eurodac. È altrettanto prevista una partecipazione ai nuovi sistemi EES ed ETIAS, facenti ugualmente parte dell'acquis di Schengen. Nel giugno 2019[18] il Parlamento ha approvato il recepimento e l'attuazione del regolamento EES. Il messaggio relativo al recepimento e all'attuazione del regolamento ETIAS è stato adottato dal nostro Consiglio il 6 marzo 2020[19]. Il progetto si trova attualmente in fase di dibattito parlamentare. La Svizzera ha inoltre tempo fino a novembre 2020 per recepire gli sviluppi del SIS che prevedono nuove possibilità di cooperazione di polizia e nel settore della migrazione, tra l'altro tramite l'introduzione di una nuova categoria di segnalazione concernente le decisioni di rimpatrio. Il 6 marzo 2020[20] abbiamo adottato il messaggio relativo al recepimento e all'attuazione dei regolamenti SIS. Il progetto si trova attualmente in fase di dibattito parlamentare.

L'ECRIS-TCN non rappresenta invece uno sviluppo dell'acquis di Schengen, motivo per cui la Svizzera non vi ha accesso. La Svizzera sta attualmente valutando se parteciparvi. Nei regolamenti UE si parla pertanto di interoperabilità dei «sistemi d'informazione dell'UE». Tale espressione è utilizzata anche nel presente messaggio, salvo nel numero 7. Per quanto concerne la trasposizione nel diritto svizzero, è utilizzata invece l'espressione «sistemi d'informazione Schengen/Dublino», poiché la trasposizione riguarda soltanto tali sistemi.

La Svizzera non ha inoltre accesso diretto ai dati di Europol. In base agli articoli 8 e 9 dell'accordo del 24 settembre 2004[21] tra la Confederazione svizzera e l'Ufficio europeo di polizia, la Svizzera può richiedere a Europol di trasmetterle dati registrati nel sistema d'informazione di Europol (EIS). La Svizzera si impegna al fine di ottenere un accesso diretto ai dati di Europol. Sono in corso discussioni

18 FF **2019** 3819
19 FF **2020** 2577
20 FF **2020** 3173
21 RS **0.362.2**

sull'eventualità che l'UE possa concedere in futuro agli Stati associati a Schengen l'accesso diretto a questi dati tramite il portale ESP. Le modalità con cui le componenti centrali potranno accedere ai dati di Europol sono ancora oggetto di chiarimenti. Il diritto di consultazione dovrà, tuttavia, inserirsi nel quadro giuridico attuale (accordo di cooperazione tra la Svizzera ed Europol). Appare dunque opportuno sancire all'interno della legge federale del 16 dicembre 2005[22] sugli stranieri e la loro integrazione (LStrI) e nella legge federale del 13 giugno 2008[23] sui sistemi d'informazione di polizia della Confederazione (LSIP) la possibilità di accedere ai dati di Europol tramite il portale ESP. La Svizzera dispone inoltre, quale Paese membro di Interpol, di un accesso alle banche dati di Interpol menzionate qui sopra.

4.2 Applicabilità progressiva dei regolamenti UE sull'interoperabilità

Entrambi i regolamenti UE sull'interoperabilità sono entrati in vigore nell'UE l'11 giugno 2019. La maggior parte delle disposizioni materiali saranno, tuttavia, applicabili soltanto in un momento successivo. Spetta pertanto alla Commissione europea decidere in merito all'entrata in funzione progressiva delle singole componenti centrali, ragion per cui le pertinenti disposizioni diventeranno applicabili soltanto a partire dalla data di tale decisione (cfr. art. 79 del regolamento «IOP frontiere» e art. 75 del regolamento «IOP polizia»). Il presupposto per l'entrata in funzione delle singole componenti centrali è ad esempio l'avvenuto completamento del collaudo generale delle relative componenti centrali in collaborazione con gli Stati Schengen e le agenzie dell'UE. Devono inoltre essere state adottate le disposizioni tecniche e giuridiche per la raccolta e la trasmissione di dati (art. 72 del regolamento «IOP frontiere» e art. 68 del regolamento «IOP polizia»). Le singole componenti centrali diventeranno pertanto operative in momenti diversi. Secondo l'agenda attuale della Commissione europea, l'sBMS sarà operativo entro la fine del 2021, il CIR entro la metà del 2022 e l'ESP così come il MID, rispettivamente entro la metà e la fine del 2023. Sono inoltre previste diverse fasi transitorie prima che le singole componenti centrali possano effettivamente entrare in funzione. L'articolo 79 del regolamento «IOP frontiere» e l'articolo 75 del regolamento «IOP polizia» sanciscono infine che i regolamenti si applicano in relazione all'Eurodac a decorrere dalla data in cui la rifusione del regolamento (UE) n. 603/2013[24] diventa applicabile. L'integrazione dell'Eurodac nel quadro dell'interoperabilità è, tuttavia, prevista. Per tale motivo si fa menzione dell'Eurodac

22 RS **142.20**
23 RS **361**
24 Regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, GU L 180 del 26.9.2013, pag. 1.

anche nel numero 5. Non sono, tuttavia, ancora disponibili disposizioni concrete. La trasposizione nel diritto svizzero avverrà pertanto soltanto con il recepimento del regolamento Eurodac rivisto.

5 Contenuto dei regolamenti UE

Il presente numero fornisce una panoramica sul contenuto dei due regolamenti UE. Il numero 5.1 si concentra in particolare sulle quattro componenti centrali. Le ulteriori novità che hanno implicazioni anche per la Svizzera sono illustrate nel numero 5.2. Tali novità riguardano ad esempio disposizioni concernenti l'obbligo di informazione, i requisiti in materia di qualità dei dati nonché le modifiche apportate ad altri atti.

Poiché i due regolamenti sono sostanzialmente identici ad eccezione di poche disposizioni, nel numero 5 si è rinunciato a trattarli separatamente optando per una presentazione globale dei rispettivi contenuti. I numeri degli articoli e dei capi indicati coincidono quasi del tutto in entrambi i testi. I due regolamenti UE presentano alcune differenze soltanto a partire dalla fine del capo VIII che saranno di volta in volta segnalate tramite esplicito rimando.

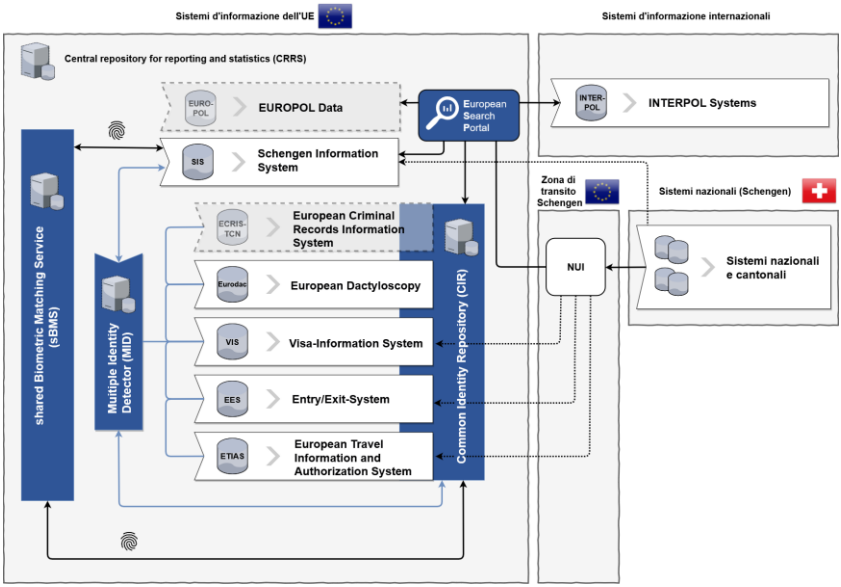
5.1 Le quattro nuove componenti centrali

Le quattro nuove componenti centrali rappresentano il fulcro dell'interoperabilità. Grazie ad esse i diversi sistemi d'informazione dell'UE comunicheranno tra loro in modo mirato. Lo scambio di informazioni diventerà dunque più efficiente e sarà possibile colmare le attuali lacune in materia di sicurezza. Le diverse componenti centrali sono sviluppate in modo tale da fornirsi sostegno e integrarsi reciprocamente. Soltanto la combinazione di tutte le componenti centrali permette di raggiungere pienamente gli obiettivi dell'interoperabilità.

Il portale ESP consentirà in futuro l'interrogazione simultanea di più sistemi d'informazione dell'UE. Tramite l'ESP è possibile consultare direttamente i dati contenuti nei singoli sistemi (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN, banche dati di Europol e Interpol; cfr. n. 4.1), ma anche i dati contenuti nel CIR. Il MID è destinato a rilevare le identità multiple registrate nei diversi sistemi. A tale scopo, il MID confronta i dati registrati nel CIR con quelli contenuti nel SIS. Per il confronto dei dati biometrici, il MID si serve dell'sBMS, mentre il confronto con i dati concernenti l'identità e i dati sui documenti di viaggio è eseguito tramite l'ESP. Le quattro componenti centrali insieme, non solo facilitano lo scambio di informazioni e la corretta identificazione delle persone, ma permettono anche di rilevare le identità multiple e le frodi di identità.

Il grafico sottostante mostra in che modo sono collegate le componenti centrali e quali sono i sistemi interessati. La NUI (National Uniform Interface) è l'interfaccia tramite la quale viene allestito un collegamento standard tra i sistemi nazionali degli Stati Schengen e le componenti centrali dell'UE. Per l'ETIAS, l'EES e il VIS sarà stabilito ugualmente un collegamento tra le rispettive componenti dell'UE e le

componenti nazionali tramite la NUI. Nei numeri seguenti è illustrata ciascuna componente centrale dell'interoperabilità.



5.1.1 Portale di ricerca europeo (ESP) (capo II)

La creazione dell'ESP rappresenta una funzione centrale dell'interoperabilità. L'ESP è istituito al fine di agevolare l'accesso rapido, continuato, efficace, sistematico e controllato delle autorità competenti ai sistemi di informazione dell'UE, ai dati Europol e alle banche dati Interpol conformemente ai rispettivi diritti di accesso (art. 6). Grazie all'ESP, in futuro le autorità competenti potranno accedere tramite un'unica interrogazione alle informazioni per esse rilevanti e avere in tal modo un quadro globale della persona oggetto del controllo.

Uso del portale di ricerca europeo (art. 7)

L'uso dell'ESP è riservato alle autorità nazionali e alle agenzie dell'UE che hanno accesso ad almeno uno dei sistemi di informazione dell'UE (EES, ETIAS, VIS, SIS, Eurodac, banche dati di Europol oppure ECRIS-TCN), al CIR, al MID oppure alle banche dati Interpol. In futuro le autorità competenti degli Stati Schengen useranno l'ESP per consultare l'EES, il VIS, l'ETIAS, l'Eurodac o l'ECRIS-TCN nonché il CIR ai fini degli articoli 20-22 (per le interrogazioni del CIR si veda la spiegazione dettagliata al n. 5.1.3). Potranno ugualmente impiegare l'ESP per consultare il SIS centrale nonché i dati Europol e le banche dati Interpol. Per contro, i diritti di accesso delle autorità ai singoli sistemi restano immutati.

Profili per gli utenti del portale di ricerca europeo (art. 8)

In cooperazione con gli Stati Schengen, l'agenzia eu-LISA crea profili basati su tutte le categorie di utenti dell'ESP. Ogni profilo comprende in particolare le informazioni concernenti i sistemi d'informazione dell'UE, i dati Europol e le banche dati Interpol che possono essere interrogati. Le basi legali che disciplinano tali sistemi definiscono le autorità che possono accedere ai rispettivi sistemi d'informazione e per quali scopi. I profili sono riesaminati da eu-LISA in cooperazione con gli Stati Schengen, almeno una volta all'anno e, se necessario, aggiornati.

Interrogazioni (art. 9)

Un'interrogazione tramite l'ESP può essere effettuata tramite i dati di identità, dei documenti di viaggio o biometrici. In funzione del profilo dell'utente, l'ESP interroga simultaneamente tutti i sistemi d'informazione rilevanti (EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, CIR nonché i dati Europol e le banche dati Interpol). Non appena i dati sono disponibili in uno dei sistemi d'informazione dell'UE, l'ESP li mette a disposizione degli utenti nel quadro dei rispettivi diritti di accesso. In tale contesto, la risposta fornita dall'ESP indica il sistema d'informazione dell'UE cui appartengono i dati, salvo il caso in cui si tratti di un'interrogazione del CIR ai fini di identificazione ai sensi dell'articolo 20. Infatti, nel caso di tali interrogazioni, si tratta unicamente di identificare una persona, senza che le competenti autorità di polizia siano tenute a sapere in quale sistema è registrata la persona in questione (cfr. n. 5.1.3 in merito all'art. 20). In caso di interrogazioni del CIR ai sensi dell'articolo 22 ai fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi, le autorità di perseguimento penale possono visualizzare unicamente se i dati sono presenti in un sistema d'informazione. I rispettivi dati non sono, tuttavia, visualizzati. L'accesso a tali dati deve essere richiesto separatamente (cfr. n. 5.1.3 in merito all'art. 22). Le interrogazioni delle banche dati Interpol lanciate attraverso l'ESP sono effettuate in modo tale che nessuna informazione è comunicata allo Stato che ha effettuato la segnalazione.

Registrazioni (art. 10)

L'eu-LISA e gli Stati Schengen sono tenuti a conservare le registrazioni delle interrogazioni effettuate tramite l'ESP. Gli Stati Schengen conservano le registrazioni relative all'uso dell'ESP fino al livello di collaboratore. Le registrazioni possono essere utilizzate unicamente per il monitoraggio ai fini della protezione dei dati. Tali registrazioni devono essere protette dall'accesso non autorizzato e cancellate un anno dopo la loro creazione, tranne il caso in cui siano necessarie per procedure di monitoraggio già avviate.

Procedure sostitutive in caso di impossibilità tecnica dell'uso del portale di ricerca europeo (art. 11)

L'articolo 11 disciplina la procedura da adottare nel caso in cui l'ESP non possa essere utilizzato per motivi tecnici. Se ciò non è possibile a causa di un guasto dell'ESP, l'eu-LISA ne informa i relativi utenti in modo automatizzato. Qualora vi

fosse un problema all'infrastruttura nazionale di uno Stato Schengen, quest'ultimo ne informa eu-LISA e la Commissione europea in modo automatizzato. Fintantoché il guasto tecnico non è riparato, i sistemi di informazione dell'UE o il CIR possono essere consultati direttamente.

Periodo transitorio per l'uso del portale di ricerca europeo

L'articolo 67 del regolamento «IOP frontiere» e l'articolo 63 del regolamento «IOP polizia» sanciscono che l'uso del portale ESP è facoltativo per un periodo di due anni a decorrere dall'entrata in funzione delle componenti centrali. Tale termine può essere prorogato una volta di un ulteriore anno.

5.1.2 Servizio comune di confronto biometrico (sBMS) (capo III)

L'sBMS consente di effettuare interrogazioni con dati biometrici trasversalmente in più sistemi di informazione dell'UE (art. 12). Nei regolamenti UE è utilizzata la sigla «BMS»: poiché tale sigla è già in uso nel diritto svizzero e ha un significato diverso, si è deciso di utilizzare la sigla «sBMS» al fine di evitare confusioni.

Conservazione di template biometrici nel servizio comune di confronto biometrico (art. 13)

L'sBMS conserva i template biometrici, che ottiene dai dati biometrici provenienti dall'EES, dal VIS, dal SIS e dall'ECRIS-TCN nonché in futuro dall'Eurodac. I template sono rappresentazioni matematiche ottenute estraendo elementi dai dati biometrici, limitatamente alle caratteristiche necessarie per effettuare identificazioni e verifiche (art. 4 par. 12). L'ETIAS non è interessato poiché non contiene dati biometrici. Ciascun template contiene un riferimento ai sistemi di informazione dell'UE in cui sono conservati i corrispondenti dati biometrici e un riferimento alle registrazioni contenute in tali sistemi. Soltanto i template contenenti dati biometrici che rispettano le norme minime di qualità dei dati possono essere inseriti nell'sBMS.

Ricerca di dati biometrici tramite il servizio comune di confronto biometrico (art. 14)

Le interrogazioni con dati biometrici nel CIR e nel SIS sono effettuate tramite i template biometrici conservati nell'sBMS e soltanto per le finalità previste.

Periodo di conservazione dei dati nel servizio comune di confronto biometrico (art. 15)

I template e i riferimenti ai sistemi d'informazione dell'UE da cui provengono sono conservati nell'sBMS per il tempo in cui i corrispondenti dati biometrici sono conservati nel CIR (provenienti dal VIS, dall'EES, dall'ETIAS, dall'Eurodac e dall'ECRIS-TCN) o nel SIS. I dati sono in seguito cancellati in modo automatizzato.

Registrazioni (art. 16)

Sia eu-LISA sia gli Stati Schengen sono tenuti a conservare le registrazioni di tutte le operazioni di trattamento dei dati. Le disposizioni concernenti l'utilizzo delle registrazioni e le misure di sicurezza da adottare illustrate nel numero 5.1.1 in merito all'articolo 10 si applicano per analogia.

5.1.3 Archivio comune di dati di identità (CIR) (capo IV)

Nell'archivio comune di dati di identità («CIR») è creato un fascicolo individuale per ciascuna persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nell'ECRIS-TCN. Il CIR costituisce dunque una parte integrante di questi sistemi. I dati rimangono, tuttavia, registrati nel sistema corrispondente. Tale accesso faciliterà la corretta identificazione delle persone registrate in uno dei sistemi d'informazione dell'UE summenzionati. Tramite il CIR sarà inoltre possibile agevolare e semplificare alle autorità di perseguimento penale l'accesso ai sistemi d'informazione dell'UE non dedicati al perseguimento penale ai fini di prevenzione, accertamento o indagine di reati di terrorismo o di altri reati gravi (art. 17 con rimando all'art. 22). Per via dell'architettura tecnica complessa del SIS, i dati del SIS non sono inclusi nel CIR.

Dati dell'archivio comune di dati di identità (art. 18)

Il CIR conserva i dati d'identità e, ove disponibili, i dati sui documenti di viaggio nonché i dati biometrici provenienti dall'EES, dal VIS, dall'ETIAS, dall'ECRIS-TCN e dall'Eurodac. La conservazione dei dati è effettuata tramite separazione per logica in base al sistema d'informazione di provenienza dei dati. Per ciascuna serie di dati conservati nel CIR, è inoltre inserito un riferimento ai sistemi di informazione dell'UE cui appartengono i dati («effettive registrazioni» in base alla terminologia dell'UE). I diritti di accesso delle autorità al CIR dipendono dalle basi giuridiche che disciplinano i singoli sistemi di informazione dell'UE e dai rispettivi diritti di accesso previsti dai regolamenti UE sull'interoperabilità ai fini degli articoli 20-22.

Aggiunta, modifica e cancellazione di dati nell'archivio comune di dati di identità (art. 19)

I dati conservati nel CIR sono adeguati in modo automatizzato non appena nell'EES, nel VIS, nell'ETIAS o nell'ECRIS-TCN e in futuro nell'Eurodac sono aggiunti, modificati o cancellati dati. Quando è creato un collegamento bianco o rosso nel MID (per i dettagli si veda il n. 5.1.4) che riguarda dati che compongono il CIR, non sono creati nuovi fascicoli, bensì aggiunti nuovi dati al fascicolo individuale dei dati oggetto del collegamento.

Accesso all'archivio comune di dati di identità a fini di identificazione (art. 20)

Il CIR ha lo scopo di agevolare l'identificazione di cittadini di Stati terzi. Per tale motivo, l'articolo 20 prevede che, in caso di controlli all'interno di un Paese e a determinate condizioni, gli agenti di polizia siano autorizzati a consultare il CIR

tramite un'interrogazione nell'ESP ai fini di identificazione. Il paragrafo 1 elenca i casi in cui è consentito: a) se una persona non può essere identificata in ragione dell'assenza di un documento di viaggio o di un altro documento credibile che ne provi l'identità; b) se sussistono dubbi quanto ai dati di identità forniti dall'interessato; c) se sussistono dubbi quanto all'autenticità del documento di viaggio o di un altro documento fornito dall'interessato; d) se sussistono dubbi quanto all'identità del titolare del documento di viaggio o di un altro documento; e) se l'interessato non è in grado o rifiuta di cooperare. Tali interrogazioni non sono autorizzate nel caso di minori di età inferiore a 12 anni, a meno che ciò non sia nell'interesse superiore del minore.

Di norma l'interrogazione del CIR è effettuata con i dati biometrici dell'interessato acquisiti sul posto durante una verifica dell'identità (par. 2). Se non possono essere usati i dati biometrici dell'interessato o se l'interrogazione con tali dati non dà esito positivo, l'interrogazione è effettuata con i dati di identità dell'interessato combinati con i dati del documento di viaggio. Se nel CIR sono conservati dati dell'interessato, l'autorità di polizia può consultarli senza che sia, tuttavia, visibile da quale sistema d'informazione dell'UE provengono tali dati. Il paragrafo 4 prevede la possibilità di interrogare i dati nel CIR al fine di identificare le vittime di catastrofe naturale, incidente o attacco terroristico e resti umani non identificati. Gli Stati Schengen che intendono avvalersi di entrambe le nuove possibilità adeguano le proprie legislazioni nazionali e definiscono le autorità autorizzate a effettuare l'interrogazione.

Accesso all'archivio comune di dati di identità a fini di individuazione di identità multiple (art. 21)

L'accesso al CIR è previsto anche in relazione ai collegamenti MID (per i dettagli cfr. n. 5.1.4). Nell'ambito della verifica di identità diverse in caso di collegamenti gialli e nell'ambito della lotta alla frode di identità in caso di collegamenti rossi, le autorità responsabili hanno accesso ai dati collegati che sono conservati nel CIR.

Interrogazione dell'archivio comune di dati di identità a fini di prevenzione, accertamento o indagine di reati di terrorismo o altri reati gravi (art. 22)

Le autorità competenti per la prevenzione, l'accertamento o l'indagine di reati di terrorismo o di altri reati gravi (le cosiddette «autorità designate»), definite da ciascun Paese conformemente alle basi giuridiche relative ai singoli sistemi, non hanno necessariamente un accesso diretto ai dati nell'EES, nel VIS, nell'ETIAS o nell'Eurodac, ma devono presentare richiesta di accesso presso un punto di accesso centrale, anch'esso definito nel diritto nazionale.

Con l'interoperabilità l'accesso delle autorità designate ai dati conservati in tali sistemi viene nuovamente regolamentato. Nello specifico, è prevista una procedura a due fasi tramite interrogazione nel CIR. Se vi sono fondati motivi per ritenere che la consultazione dei sistemi di informazione dell'UE possa servire alla prevenzione, all'accertamento o all'indagine di reati di terrorismo o di altri reati gravi, in particolare laddove sussista il sospetto che una persona è registrata in uno dei sistemi, le autorità designate ed Europol possono consultare il CIR. Questa prima fase avviene tramite la procedura «hit/no hit». Se vi è un hit (ovvero se i dati relativi a una perso-

na sono presenti in uno dei sistemi quali EES, ETIAS, VIS o Eurodac), il CIR segnala all'autorità che ha effettuato l'interrogazione in quale sistema d'informazione dell'UE sono conservati i dati. L'autorità in questione ha in seguito la possibilità, come finora, di richiedere il pieno accesso ad almeno uno dei sistemi di informazione dai quali è emerso un riscontro positivo. Il pieno accesso ai dati contenuti nell'EES, nel VIS o nell'ETIAS o nell'Eurodac resta soggetto alle condizioni e procedure previste negli strumenti giuridici che disciplinano i sistemi d'informazione sottostanti. Ove, in via eccezionale, tale accesso non sia richiesto, le autorità designate registrano la rispettiva motivazione scritta nel pertinente fascicolo.

Periodo di conservazione dei dati nell'archivio comune di dati di identità (art. 23)

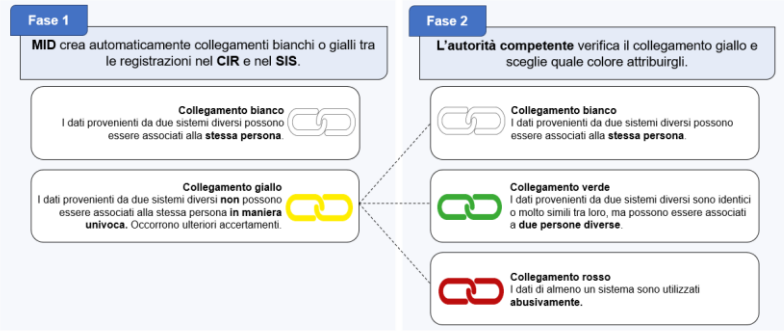
I dati conservati nel CIR sono cancellati in modo automatizzato conformemente alle disposizioni in materia di conservazione dei dati dei rispettivi sistemi d'informazione dell'UE dai quali provengono. I fascicoli individuali sono conservati nel CIR soltanto per il tempo in cui i dati corrispondenti sono conservati in almeno uno dei sistemi d'informazione dell'UE.

Registrazioni (art. 24)

eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati e le interrogazioni effettuate nel CIR. Gli Stati Schengen devono conservare le registrazioni relative alle interrogazioni del CIR ai sensi degli articoli 20-22; Europol deve invece conservare le registrazioni relative agli accessi ai sensi degli articoli 21 e 22. Le disposizioni concernenti l'utilizzo delle registrazioni e le misure di sicurezza da adottare illustrate nel numero 5.1.1 in merito all'articolo 10 si applicano per analogia.

5.1.4 Rilevatore di identità multiple (MID) (capo V)

Il MID è la quarta componente centrale. Esso contribuirà a individuare persone che utilizzano più identità o identità false e persegue il duplice obiettivo di agevolare le verifiche delle identità e contrastare le frodi di identità. A tale scopo nel MID sono creati e conservati fascicoli di conferma dell'identità contenenti collegamenti tra i dati dei diversi sistemi d'informazione dell'UE (art. 25). In sostanza, il MID verifica se i dati personali, dei documenti d'identità o biometrici registrati in un sistema sono registrati anche in altri sistemi. A seconda delle circostanze, il MID crea automaticamente collegamenti bianchi o gialli. Tutti i collegamenti gialli devono essere verificati manualmente dalle autorità competenti. Queste ultime sono tenute a verificare le diverse identità e, a seconda che si tratti della stessa persona o di una persona diversa, aggiornano il rispettivo status del collegamento come rosso, verde o bianco. Il grafico sottostante fornisce una panoramica di tali processi. Le procedure specifiche e il significato dei collegamenti saranno descritti dettagliatamente qui di seguito e illustrati, sulla base di tre esempi concreti, alla fine del presente numero.



Accesso al rilevatore di identità multiple (art. 26)

L'articolo 26 specifica gli scopi per i quali è consentito accedere ai dati conservati nel MID. Da un lato è concesso l'accesso alle autorità competenti per la verifica manuale delle identità diverse di cui all'articolo 29. Si tratta delle autorità che registrano o aggiornano i dati nell'EES, nel VIS, nell'ETIAS, nell'ECRIS-TCN, nel SIS e in futuro anche nell'Eurodac. Tali autorità sono definite nelle rispettive basi legali dei sistemi d'informazione. Dall'altro lato le autorità degli Stati Schengen e le agenzie dell'UE (in tale contesto Europol e guardia di frontiera e costiera europea) hanno accesso ai collegamenti rossi tramite il MID se hanno accesso almeno a uno dei sistemi d'informazione dell'UE interessati. L'accesso ai collegamenti bianchi o verdi è possibile se le autorità hanno accesso ai due sistemi d'informazione dell'UE che contengono i dati tra i quali è stato creato il rispettivo collegamento.

Rilevazione di identità multiple (art. 27)

L'articolo 27 illustra la procedura di rilevazione di identità multiple. La rilevazione di identità multiple è avviata quando sono registrati o aggiornati dati in uno dei sistemi d'informazione dell'UE (VIS, SIS, ETIAS, EES). A tale scopo, sono di volta in volta confrontati i nuovi dati con i dati già presenti nel SIS e nel CIR. L'sBMS funge da strumento di confronto dei dati biometrici, mentre l'ESP per il confronto dei dati di identità e dei dati sui documenti d'identità. La rilevazione di identità multiple è effettuata unicamente allo scopo di confrontare i dati tra i vari sistemi d'informazione dell'UE.

Esito della procedura di rilevazione di identità multiple (art. 28)

I possibili esiti di una procedura di rilevazione di identità multiple e i processi che ne conseguono sono descritti nell'articolo 28. Qualora dalla procedura di rilevazione di identità multiple non risulti alcuna corrispondenza con i dati presenti in altri sistemi d'informazione dell'UE, si procede con la registrazione dei dati come previsto dalle rispettive basi giuridiche. Qualora dalla procedura di rilevazione risultino una o più corrispondenze, sono creati collegamenti tra i dati, nuovi o aggiornati, usati per avviare l'interrogazione e i dati già presenti in un altro sistema d'informazione

dell'UE. Qualora risultino più corrispondenze è creato un collegamento tra tutti i dati in questione. Se i dati sono già oggetto di un collegamento, questo è esteso ai nuovi dati.

Qualora i dati di identità dei fascicoli oggetti del collegamento siano identici o simili, è creato automaticamente un collegamento bianco. Qualora invece i dati di identità non possano essere considerati simili, è creato automaticamente un collegamento giallo ed è necessaria una verifica manuale da parte delle autorità competenti. La Commissione europea stabilisce i casi in cui è possibile considerare i dati di identità identici o simili e adotta a tal fine atti delegati che la Svizzera è tenuta a recepire in quanto sviluppo dell'acquis di Schengen. Tutti i collegamenti sono conservati nel fascicolo di conferma dell'identità di cui all'articolo 34.

Verifica manuale delle identità diverse e autorità responsabili (art. 29)

Se durante la rilevazione di identità multiple tramite il MID è creato un collegamento giallo, le identità diverse devono essere verificate manualmente. La verifica è effettuata dall'autorità che ha registrato o aggiornato i dati in uno dei sistemi d'informazione dell'UE.

Il paragrafo 2 stabilisce un'eccezione a tale norma generale. Qualora sia creato un collegamento con una segnalazione ai sensi degli articoli 26, 32, 34 o 36 del regolamento (UE) 2018/1862[25], l'autorità responsabile della verifica manuale è l'ufficio SIRENE dello Stato Schengen che ha creato la segnalazione. Si tratta delle seguenti categorie di segnalazioni: segnalazione per l'arresto ai fini di estradizione (art. 26); persone scomparse (art. 32); ricerca del luogo di soggiorno (art. 34); controlli discreti, controlli di indagine o controlli specifici (art. 36). Ad eccezione dei divieti d'entrata e le decisioni di rimpatrio, l'ufficio SIRENE è competente per tutte le ricerche di persone. Il MID indica l'autorità responsabile nel fascicolo di conferma dell'identità.

La verifica deve avvenire tempestivamente. Una volta completata tale valutazione, l'autorità responsabile aggiorna il collegamento conformemente agli articoli 31-33 classificandolo come verde, rosso o bianco. Il collegamento risulta dunque come verificato. Il paragrafo 4 del regolamento «IOP frontiere» contiene ulteriori disposizioni concernenti la verifica necessaria in virtù della creazione o dell'aggiornamento di un fascicolo individuale nell'EES. Tale verifica deve essere avviata in presenza dell'interessato, al quale è offerta la possibilità di esprimersi in merito alle circostanze. Nel caso in cui la verifica manuale sia svolta alla frontiera esterna di Schengen, l'intera procedura deve avvenire, ove possibile, entro 12 ore.

25 Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione, GU L 312 del 7.12.2018, pag. 56; modificato da ultimo dal regolamento (UE) n. 2019/817, GU L 135 del 22.5.2019, pag. 27.

Qualora sia creato più di un collegamento, va esaminato ogni collegamento separatamente. Nel valutare la necessità di creare nuovi collegamenti, le autorità responsabili verificano se i dati per i quali risulta una corrispondenza sono stati già oggetto di un collegamento.

Collegamento giallo (art. 30)

I collegamenti gialli sono quei collegamenti per i quali non è stata ancora svolta alcuna verifica manuale delle identità diverse. È il caso ad esempio in cui i dati collegati contengono i medesimi dati di identità ma dati biometrici diversi o, viceversa, gli stessi dati biometrici ma dati di identità differenti. Quest'ultima circostanza si verifica ad esempio nel caso di un matrimonio con cambiamento del nome. Quando un collegamento è classificato come giallo, le rispettive autorità responsabili sono tenute a effettuare in ogni caso la verifica manuale ai sensi dell'articolo 29.

Collegamento verde (art. 31)

Il collegamento verde è creato sempre dopo l'esecuzione della verifica manuale. Tale collegamento evidenzia che i dati di identità relativi ai dati oggetto del collegamento si riferiscono a due persone diverse. È il caso ad esempio in cui i dati oggetto del collegamento evidenziano dati biometrici differenti ma gli stessi dati di identità perché due persone hanno casualmente lo stesso nome e la stessa data di nascita. In questo modo si faciliterà il controllo dell'identità di persone che viaggiano in modo lecito.

Se un'autorità di uno Stato Schengen dispone di prove indicanti che un collegamento verde è stato registrato incorrettamente, che non è aggiornato o che i dati sono stati trattati in violazione dei regolamenti UE sull'interoperabilità, essa controlla i dati pertinenti e, se necessario, rettifica o cancella senza indugio il collegamento. L'autorità responsabile della verifica manuale delle identità diverse deve essere informata senza indugio.

Collegamento rosso (art. 32)

Il collegamento rosso è creato sempre dopo l'esecuzione della verifica manuale. Tale collegamento evidenzia identità multiple usate in maniera ingiustificata oppure le frodi di identità. Sono diversi i casi in cui si può arrivare a un collegamento rosso:

- una persona utilizza più identità differenti: in questo caso sono registrati in diversi sistemi d'informazione dell'UE gli stessi dati biometrici o gli stessi dati relativi ai documenti di viaggio, ma con dati di identità differenti; i dati oggetto del collegamento si riferiscono quindi alla medesima persona;

- una persona utilizza il documento di viaggio di un'altra persona: i dati oggetto del collegamento evidenziano dati biometrici differenti, ma gli stessi dati relativi ai documenti di viaggio; i dati oggetto del collegamento si riferiscono dunque a due persone diverse;

– una persona fa finta di essere qualcun'altro: in questo caso sono registrati in diversi sistemi d'informazione dell'UE dati biometrici differenti con i medesimi dati di identità. I dati oggetto del collegamento si riferiscono quindi a due persone diverse.

Un collegamento rosso non ha conseguenze per la persona in questione. Gli eventuali provvedimenti possono essere adottati unicamente in conformità con il diritto dell'UE e con il diritto nazionale. Qualora sia creato un collegamento rosso tra dati dell'EES, dell'ETIAS, del VIS, dell'Eurodac o dell'ECRIS-TCN, il fascicolo individuale conservato nel CIR è aggiornato di conseguenza.

Qualora sia creato un collegamento rosso, l'autorità responsabile della verifica manuale delle identità diverse informa la persona interessata tramite modulo standard della presenza di dati di identità multipli illeciti e le indica come reperire informazioni sui dati, fornendole un numero di identificazione unico e l'indirizzo del sito web del portale (cfr. n. 5.2 in merito alla protezione dei dati). L'autorità può rinunciare a informare la persona se ciò è necessario ai fini del rispetto delle disposizioni relative al trattamento delle segnalazioni nel SIS, alla protezione della sicurezza e dell'ordine pubblico, alla prevenzione della criminalità o a garantire che non siano compromesse indagini nazionali (par. 4 e 5). Ogniqualvolta viene creato un collegamento rosso, il MID informa in modo automatizzato le autorità responsabili dei dati oggetto del collegamento.

Se un'autorità di uno Stato Schengen ha prove che suggeriscono che un collegamento rosso è stato registrato incorrettamente o che i dati sono stati trattati in violazione dei regolamenti UE sull'interoperabilità, nella maggior parte dei casi è tenuta a verificare i dati pertinenti e, ove necessario, a rettificare o cancellare il collegamento. Laddove, invece, il collegamento si riferisca a una segnalazione nel SIS di cui agli articoli 26, 32, 34 o 36 del regolamento (UE) 2018/1862, l'autorità informa immediatamente il competente ufficio SIRENE dello Stato Schengen che ha creato la segnalazione. In questo caso, l'ufficio SIRENE assume la responsabilità della verifica e, se del caso, rettifica o cancella il collegamento. L'autorità che ottiene le prove di un collegamento inesatto, informa senza indugio l'autorità competente per la verifica manuale delle identità diverse di ogni eventuale rettifica o cancellazione di un collegamento rosso.

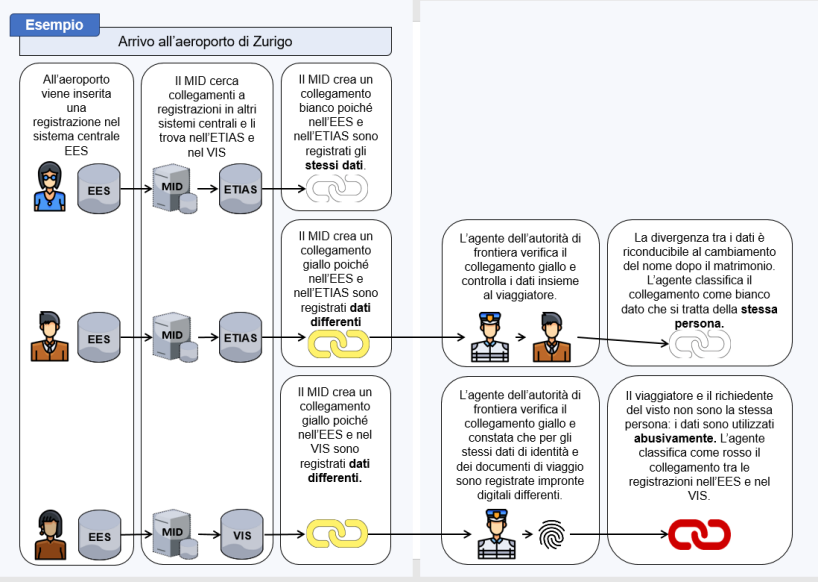
Collegamento bianco (art. 33)

Un collegamento bianco è creato automaticamente dal MID in occasione della verifica delle identità multiple ai sensi dell'articolo 27 (p. es. quando il collegamento evidenzia gli stessi dati di identità e gli stessi dati biometrici) oppure come risultato di una verifica manuale ai sensi dell'articolo 29 (se i dati biometrici sono identici, ma i dati di identità sono simili o differenti e l'autorità responsabile della verifica conclude che si tratta della stessa persona). Un collegamento bianco evidenzia dunque che i dati oggetto del collegamento si riferiscono alla stessa persona, la quale è già registrata almeno in un altro sistema d'informazione dell'UE. In questo modo si agevola la mobilità delle persone che sono ad esempio legittimamente in possesso di più documenti di viaggio validi. Qualora sia creato un collegamento bianco tra dati nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nell'ECRIS-TCN, il fascicolo individuale conservato nel CIR è aggiornato di conseguenza.

Qualora sia creato un collegamento bianco a seguito di una verifica da parte dell'autorità responsabile, quest'ultima informa la persona interessata tramite modulo standard della presenza di dati di identità simili o diversi e le fornisce indicazioni su come reperire informazioni sui dati. Come nel caso del collegamento rosso, l'autorità può rinunciare a informare la persona se ciò è necessario per motivi di sicurezza.

Se un'autorità di uno Stato Schengen dispone di prove indicanti che un collegamento bianco è stato registrato incorrettamente, non è aggiornato o che i dati sono stati trattati in violazione dei regolamenti UE sull'interoperabilità, essa controlla i dati pertinenti conservati e, se necessario, rettifica o cancella il collegamento. L'autorità responsabile della verifica manuale delle identità diverse deve essere informata senza indugio.

I tre esempi che figurano qui di seguito illustrano il funzionamento del MID e il significato dei diversi collegamenti.



I risultati della verifica manuale sono salvati nel fascicolo di conferma dell'identità.

Fascicolo di conferma dell'identità (art. 34)

Nel MID sono salvati unicamente i fascicoli di conferma dell'identità. Oltre alla tipologia di collegamento (art. 30-33), vi è inoltre indicato in quale sistema d'informazione dell'UE sono conservati i dati oggetto del collegamento. Ciascun fascicolo di conferma dell'identità contiene un numero di identificazione unico che permette di estrarre i dati oggetto del collegamento dai corrispondenti sistemi

d'informazione dell'UE. Vi sono inoltre indicati l'autorità responsabile della verifica manuale e la data della creazione del link o di un suo aggiornamento.

Conservazione dei dati nel rilevatore di identità multiple (art. 35)

I fascicoli di conferma dell'identità e i relativi dati, compresi i collegamenti, sono conservati nel MID solo per il tempo in cui i dati oggetto del collegamento sono conservati in più sistemi di informazione dell'UE. Essi sono successivamente cancellati in maniera automatizzata.

Registrazioni (art. 36)

Sia eu-LISA sia gli Stati Schengen sono tenuti a conservare le registrazioni di tutte le operazioni di trattamento dei dati e le interrogazioni nel MID. Le disposizioni concernenti l'utilizzo delle registrazioni e le misure di sicurezza da adottare illustrate al numero 5.1.1 in merito all'articolo 10 si applicano per analogia.

Periodo transitorio per il rilevatore di identità multiple

L'articolo 69 del regolamento «IOP frontiere» e l'articolo 65 del regolamento «IOP polizia» disciplinano il periodo transitorio per il rilevatore di identità multiple. Una volta che il MID sarà stato sviluppato e testato con successo e prima della sua entrata in funzione, tutti i dati conservati nell'EES, nel VIS, nell'Eurodac e nel SIS dovranno essere verificati al fine di rilevare eventuali identità multiple. Tale verifica avviene esclusivamente sulla base di dati biometrici. L'unità centrale ETIAS è competente per effettuare tali verifiche. Qualora sia creato un collegamento giallo con una segnalazione nel SIS ai sensi degli articoli 26, 32, 34 o 36 del regolamento (UE) 2018/1862, l'ufficio SIRENE competente è coinvolto nella verifica. Solo dopo che tutti i collegamenti gialli sono stati verificati e aggiornati, l'unità centrale ETIAS informa la Commissione europea la quale decide in seguito in merito all'effettiva entrata in funzione del MID. La verifica deve essere conclusa entro un anno. È consentito prorogare tale termine.

5.2 Ulteriori disposizioni

I due regolamenti dell'UE contengono, oltre alle disposizioni concernenti le quattro nuove componenti centrali, numerose altre disposizioni. Il relativo contenuto è sintetizzato qui di seguito. A tale proposito, occorre evidenziare che alcune delle disposizioni menzionate saranno da trasporre in Svizzera soltanto a livello di ordinanza, mentre altre non renderanno necessaria alcuna trasposizione nel diritto svizzero.

Misure a sostegno dell'interoperabilità (capo VI)

Per consentire l'interoperabilità dei diversi sistemi d'informazione dell'UE, sono in programma le seguenti misure di sostegno:

L'articolo 37 elenca le disposizioni concernenti i criteri di qualità dei dati. Da un lato sono previste procedure automatizzate per il controllo della qualità dei dati, dall'altro sono introdotte norme minime di qualità per l'inserimento dei dati nei sistemi d'informazione dell'UE e nelle componenti centrali. Con il formato universale dei messaggi (*Universal Message Format*), è istituito uno standard comune per lo scambio di informazioni transfrontaliero (art. 38). Tale standard deve essere utilizzato nell'EES, nell'ETIAS, nell'Eurodac, nell'ECRIS-TCN, nell'ESP, nel CIR e nel MID e potrebbe essere impiegato anche nei futuri sistemi d'informazione. Per scopi di analisi e per fini statistici, è istituito un archivio centrale di relazioni e statistiche (*Central Repository for Reporting and Statistics*; art. 39). Tale archivio fornisce dati statistici intersistemici. I dati sono anonimizzati al fine di impedire l'identificazione delle persone fisiche.

Protezione dei dati (capo VII)

Il capo VII è dedicato alla protezione dei dati. Nell'articolo 40 sono elencati i servizi responsabili del trattamento dei dati, mentre l'articolo 42 indica i servizi responsabili della sicurezza del trattamento dei dati. eu-LISA assume un'importanza particolare alla luce della sua responsabilità per le componenti centrali e l'infrastruttura di comunicazione. In caso di interruzione, eu-LISA garantisce ad esempio il ripristino del normale funzionamento.

L'articolo 44 sancisce che gli Stati Schengen sono tenuti ad adottare le misure necessarie per verificare la conformità ai regolamenti UE sull'interoperabilità. In base all'articolo 45, gli Stati Schengen sono tenuti a prevedere sanzioni per l'uso improprio di dati nonché il trattamento o lo scambio di dati illeciti. Le sanzioni devono essere effettive, proporzionate e dissuasive. Nell'articolo 46 è disciplinata la responsabilità in caso di danni. Di norma ha diritto al risarcimento ogni persona che abbia subito danni in conseguenza di un trattamento illecito di dati o di qualsiasi atto incompatibile con il regolamento. Il servizio interessato è esonerato dalla responsabilità se prova che l'evento dannoso non è a lui imputabile. Uno Stato Schengen è responsabile di ogni eventuale danno arrecato alle componenti dell'interoperabilità conseguente all'inosservanza degli obblighi previsti, nella misura in cui eu-LISA o un altro Stato Schengen abbia adottato provvedimenti ragionevolmente idonei a prevenire il danno o ridurne al minimo l'impatto.

Il diritto di informazione in relazione ai dati conservati nell'sBMS, nel CIR o nel MID è disciplinato nell'articolo 47. Se sono conservati dati personali nell'sBMS, nel CIR o nel MID, la persona interessata deve esserne informata con un linguaggio semplice e chiaro.

L'articolo 48 disciplina il diritto di accesso ai dati personali, di rettifica e di cancellazione degli stessi conservati nel MID. Qualora una persona domandi se sono trattati dati che la concernono o ne richieda la rettifica, la cancellazione o la limitazione del loro trattamento, ha il diritto di rivolgersi all'autorità competente di qualsiasi Stato Schengen, la quale a sua volta esamina la richiesta e vi risponde. Qualora la richiesta sia presentata a uno Stato diverso da quello competente, lo Stato al quale è stata presentata contatta ai fini di verifica dei dati lo Stato Schengen responsabile o l'unità centrale ETIAS, nel caso in cui quest'ultima sia competente per la verifica. La verifica deve essere effettuata di norma entro 45 giorni dalla ricezione della

richiesta, ma è comunque possibile una proroga. La persona è informata per iscritto in merito all'esito della verifica o a un'eventuale rettifica o cancellazione. Qualora lo Stato competente per la verifica non ritenga che i dati siano stati trattati o registrati illecitamente, informa l'interessato e gli fornisce istruzioni su come, se del caso, intentare un'azione o presentare un reclamo. Occorre infine conservare una registrazione scritta dell'intero processo. Un nuovo portale web intende facilitare alle persone interessate l'esercizio dei diritti di accesso, rettifica, cancellazione o limitazione del trattamento dei dati personali e il contatto con le autorità competenti (art. 49). La persona interessata può richiedere informazioni all'autorità competente inserendo il numero di identificazione unico di cui all'articolo 34 lettera c. Nel portale web è contenuto inoltre un modello di e-mail per facilitare la comunicazione nonché informazioni sui diritti e sulle procedure.

L'articolo 50 sancisce che i dati personali conservati nelle componenti centrali o da queste trattati non sono comunicati o messi a disposizione di Paesi terzi, organizzazioni internazionali, soggetti privati o persone fisiche. Sono fatte salve le pertinenti disposizioni sulla protezione dei dati relative alla comunicazione di dati sancite nelle basi giuridiche dei sistemi d'informazione dell'UE nonché la consultazione delle banche dati Interpol tramite il portale ESP in conformità con i regolamenti UE sull'interoperabilità.

Gli articoli 51 e 52 disciplinano il controllo da parte delle autorità competenti in tale ambito nonché l'audit del Garante europeo della protezione dei dati. Gli Stati Schengen assicurano che le autorità di controllo monitorino indipendentemente la legittimità del trattamento dei dati. Essi provvedono affinché le proprie autorità di controllo dispongano delle risorse e delle competenze sufficienti e ricevano le informazioni necessarie all'esecuzione dei controlli. Le autorità di controllo sono tenute a pubblicare ogni anno il numero delle richieste di rettifica, cancellazione o limitazione del trattamento dei dati personali nonché le conseguenti azioni intraprese. Esse provvedono affinché, almeno ogni quattro anni, sia svolto un audit dei trattamenti di dati personali conformemente ai pertinenti principi internazionali. Il Garante europeo della protezione dei dati è competente per la sorveglianza delle operazioni di trattamento dei dati effettuate da eu-LISA, dall'unità centrale ETIAS e da Europol. L'articolo 53 statuisce che le autorità di controllo nazionali e il Garante europeo della protezione dei dati sono tenuti a cooperare attivamente e ad assicurare il controllo coordinato dell'uso delle componenti centrali e dell'applicazione delle altre disposizioni dei regolamenti UE sull'interoperabilità. Ogni due anni, il Garante europeo della protezione dei dati allestisce una relazione congiunta su tali attività. Tale relazione comprende un capitolo su ciascuno Stato Schengen redatto dall'autorità di controllo dello Stato interessato.

Responsabilità (capo VIII)

Fino all'articolo 57, la numerazione degli articoli nei testi dei due regolamenti sull'interoperabilità corrisponde. Negli articoli 54 e 55 sono illustrate le responsabilità di eu-LISA in fase di sviluppo e dopo l'entrata in funzione. eu-LISA è responsabile dello sviluppo delle componenti centrali, di ogni adattamento necessario per realizzare l'interoperabilità tra i sistemi centrali dell'EES, del VIS, dell'ETIAS, del SIS, dell'Eurodac, dell'ECRIS-TCN nonché dell'infrastruttura di comunicazione.

Dopo l'entrata in funzione, eu-LISA è responsabile della gestione tecnica e della manutenzione dei sistemi. In tale contesto, eu-LISA non ha accesso a nessuno dei dati personali trattati. L'articolo 56 elenca le responsabilità degli Stati Schengen, tra cui figurano la connessione dei sistemi nazionali alle nuove componenti centrali o la gestione e il disciplinamento delle modalità di accesso da parte delle autorità nazionali competenti all'ESP, al CIR e al MID. Il regolamento «IOP polizia» elenca inoltre nell'articolo 57 le responsabilità di Europol. Le responsabilità dell'unità centrale ETIAS (art. 57 del regolamento «IOP frontiere» e art. 58 del regolamento «IOP polizia») corrispondono in entrambi i regolamenti.

Modifiche di altri strumenti dell'Unione (capo IX)

I regolamenti UE sull'interoperabilità comportano modifiche di altri atti in vigore. Si tratta di atti normativi che la Svizzera ha già trasposto tramite scambio di note o per i quali è attualmente in corso la procedura di recepimento, ovvero: il regolamento (CE) n. 767/2008 sul VIS, il regolamento (UE) 2016/399[26] sul codice frontiere Schengen, il regolamento (UE) 2017/2226[27] sull'EES, il regolamento (UE) 2018/1240[28] sull'ETIAS, il regolamento (UE) 2018/1726[29] sull'eu-LISA, il regolamento (UE) 2018/1861[30] sul SIS, la decisione 2004/512/CE[31] che istituisce il VIS e la decisione 2008/633/GAI[32] relativa all'accesso per la consultazione al VIS da parte delle autorità di perseguimento penale. Le modifiche di tali atti sono disciplinate

26 Regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio, del 9 marzo 2016, che istituisce un codice unionale relativo al regime di attraversamento delle frontiere da parte delle persone (codice frontiere Schengen), GU L 77 del 23.3.2016, pag. 1.

27 Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011, GU L 327 del 9.12.2017, pag. 20; modificato da ultimo dal regolamento (UE) 2019/817, GU L 135 del 22.5.2019, pag. 27.

28 Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226, GU L 236 del 19.9.2018, pag. 1; modificato da ultimo dal regolamento (UE) 2019/817, GU L 135 del 22.5.2019, pag. 27.

29 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), che modifica il regolamento (CE) n. 1987/2006 e la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (UE) n. 1077/2011, GU L 295 del 21.11.2018, pag. 99.

30 Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006, GU L 312 del 7 dicembre 2018, pag. 14.

31 Decisione del Consiglio, dell'8 giugno 2004, che istituisce il sistema di informazione visti (VIS), GU L 213 del 15.6.2004, pag. 5.

32 Decisione 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate dagli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi, GU L 218 del 13.8.2008, pag. 129.

negli articoli 58-65 del regolamento «IOP frontiere». Il regolamento «IOP polizia» illustra negli articoli 59-62 le modifiche al regolamento (UE) 2018/1726 sull'eu-LISA, al regolamento (UE) 2018/1862 sul SIS e al regolamento (UE) 2019/816[33] sull'ECRIS-TCN. La Svizzera non è, tuttavia, collegata a quest'ultimo.

Tali modifiche sono necessarie al fine di poter sfruttare a pieno le nuove possibilità offerte dall'interoperabilità. In particolare si tratta di definire le categorie dei dati che saranno registrati o trattati nelle nuove componenti centrali e di prevedere il collegamento dei singoli sistemi alle nuove componenti centrali.

Disposizioni finali (capo X)

Nell'ultimo capo sono contenute le disposizioni finali concernenti le fasi transitorie per l'uso delle singole componenti centrali nonché i compiti che le diverse autorità sono tenute ad assolvere in tale ambito (art. 67-69 del regolamento «IOP frontiere» nonché art. 63-65 del regolamento «IOP polizia»). Sono inoltre disciplinati l'inizio delle attività (art. 72 del regolamento «IOP frontiere» e art. 68 del regolamento «IOP polizia»), la formazione delle autorità responsabili (art. 76 del regolamento «IOP frontiere» e art. 72 del regolamento «IOP polizia»), il monitoraggio e la valutazione delle componenti centrali (art. 78 del regolamento «IOP frontiere» e art. 74 del regolamento «IOP polizia») nonché l'entrata in vigore (art. 79 del regolamento «IOP frontiere» e art. 75 del regolamento «IOP polizia»).

6 Punti essenziali del testo di attuazione

6.1 La normativa proposta

Il progetto costituisce un recepimento di sviluppi dell'acquis di Schengen. Per garantirne la trasposizione in Svizzera occorre apportare adeguamenti a leggi federali e, in una seconda fase, anche alle rispettive ordinanze (cfr. n. 6.2).

6.2 Adeguamenti giuridici necessari

I regolamenti UE «IOP frontiere» e «IOP polizia» contengono, da un lato, disposizioni direttamente applicabili e, dall'altro, disposizioni da concretizzare nel diritto nazionale. Il decreto federale riprende le disposizioni dei regolamenti UE soltanto nella misura in cui ciò si rende necessario in virtù della LPD. Occorre dunque disciplinare a livello di legge formale le finalità del trattamento dei dati, i diritti di accesso, la comunicazione dei dati e le sanzioni in caso di trattamento abusivo dei dati.

33 Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726, GU L 135 del 22.5.2019, pag. 1.

Sono inoltre riprese singole disposizioni necessarie alla comprensione del contesto, per quanto riguarda ad esempio la definizione delle componenti dell'interoperabilità.

Le novità che implicano un adeguamento di leggi federali sono illustrate nel presente numero. Molti adeguamenti riguardano invece solo le ordinanze che saranno emanate successivamente e non saranno pertanto trattati in questa sede. I regolamenti UE sull'interoperabilità non determinano né un ampliamento dei diritti di accesso delle singole autorità ai sistemi sottostanti né una modifica delle finalità di accesso. La creazione, ad esempio, del portale web contribuisce, tuttavia, ad agevolare la comunicazione tra le competenti autorità nazionali in merito alle persone registrate. In generale, va dunque evidenziato che l'accesso ai dati personali sensibili resta disciplinato in modo chiaro anche in seguito al recepimento di entrambi i regolamenti UE.

Le componenti centrali collegano i sistemi d'informazione disciplinati dalla LStrI e le banche dati di polizia regolamentate dalla LSIP. Per motivi di trasparenza, le componenti centrali riguardanti i sistemi d'informazione che hanno attualmente la propria base legale formale nella LStrI e nella LSIP devono essere pertanto disciplinate all'interno di queste due leggi. Tali componenti sono regolamentate in entrambe le leggi secondo l'ordine cronologico della loro entrata in funzione (sBMS, seguito in successione da CIR, ESP e MID).

L'introduzione delle componenti nella LStrI e nella LSIP impone una modifica della struttura dei due testi legislativi.

La necessità concreta di adeguamenti nelle singole leggi è riassunta qui di seguito (cfr. n. 7 per i commenti ai singoli articoli).

Legge federale sugli stranieri e la loro integrazione

Poiché alcuni sistemi d'informazione disciplinati dalla LStrI sono regolamentati dall'AAD e anche per evitare confusione con il «Sistema d'informazione Schengen N-SIS», viene introdotto il termine «sistemi d'informazione Schengen/Dublino».

L'introduzione delle componenti centrali dei sistemi d'informazione Schengen/Dublino rende necessario apportare modifiche alla struttura dei capitoli 14–14*c* LStrI, che disciplineranno, rispettivamente, le disposizioni generali sulla protezione dei dati, tutti i sistemi d'informazione, l'interoperabilità tra i sistemi d'informazione Schengen/Dublino e la protezione dei dati nell'ambito Schengen/Dublino.

Poiché con l'introduzione dell'interoperabilità è stato necessario adeguare nove regolamenti UE, è opportuno modificare le corrispondenti disposizioni della LStrI che disciplinano o disciplineranno questi sistemi d'informazione Schengen/Dublino.

Il CIR diventa parte integrante dei sistemi EES, ETIAS, VIS (e, in un secondo tempo, dell'Eurodac). Le corrispondenti disposizioni della LStrI devono essere adattate, essendo previsto che il CIR sostituisca parte del sistema centrale dei vari sistemi dell'UE, quali VIS, Eurodac, EES ed ETIAS, e che determinati dati alfanumerici (dati di identità e dati dei documenti di viaggio) e biometrici dei singoli sistemi siano memorizzati nel CIR. Pertanto, la LStrI deve stabilire quali dati restano nel sistema centrale del rispettivo sistema d'informazione e quali sono invece conservati nel CIR.

Inoltre, devono essere regolamentate anche le singole componenti centrali dell'interoperabilità; in particolare, ne vanno definiti il contenuto e l'accesso (l'sBMS nell'art. 110, il CIR nell'art. 110*a*-110*d* e il MID nell'art. 110*f*). Ciò corrisponde alla disposizione dell'articolo 17 capoverso 1 LPD, secondo cui gli organi federali possono trattare dati personali soltanto se esiste una pertinente base legale.

Nel caso del CIR, le diverse modalità di accesso devono essere regolamentate in funzione del loro scopo: identificazione delle persone (art. 110*b*), verifica delle identità multiple (art. 110*c*) e accertamento dei reati (art. 110*d*). In quest'ultimo caso, tutte le autorità designate, in particolare il Servizio delle attività informative della Confederazione (SIC), dovrebbero poter verificare nel CIR se nei sistemi d'informazione Schengen/Dublino non di polizia (EES, ETIAS, VIS) ci sono dati disponibili (meccanismo «hit/no hit» ai sensi dell'articolo 22 dei regolamenti UE sull'interoperabilità). Devono inoltre essere designate le autorità di polizia competenti per l'identificazione delle persone e occorre definire quale autorità è responsabile della verifica delle identità multiple e in quali casi.

Vanno inoltre disciplinati la consultazione dei dati tramite l'ESP (art. 110*e*) e i diversi diritti di accesso al MID (art. 110*g*) da parte delle autorità competenti.

Anche la comunicazione dei dati a organismi autorizzati (art. 110*h*), la responsabilità per il trattamento dei dati nell'sBMS, nel CIR e nel MID e le sanzioni per l'uso improprio dei dati devono essere disciplinate a livello legislativo (art. 120*d*). A tal fine, saranno adeguate anche le attuali disposizioni concernenti il sistema d'informazione visti (C-VIS), l'EES e l'ETIAS.

Inoltre, si prevedono ulteriori spiegazioni e chiarimenti negli atti di esecuzione e negli atti delegati dell'UE, che saranno notificati a tempo debito anche alla Svizzera e che dovranno probabilmente essere attuati a livello di ordinanza.

Infine, è necessario aggiornare i rimandi ai regolamenti UE nella legge.

Legge federale sul sistema d'informazione per il settore degli stranieri e dell'asilo

Nella legge federale del 20 giugno 2003[34] sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA) devono essere adattati singoli rimandi alle disposizioni della LStrI, che saranno modificate nell'ambito della presente revisione. Tali adeguamenti non comportano modifiche materiali della LSISA.

Legge sulla responsabilità

La legge federale del 14 marzo 1958[35] sulla responsabilità (LResp) disciplina attualmente la responsabilità per danni derivanti dall'utilizzazione del SIS, all'interno degli articoli 19*a* e 19*b*. Le basi giuridiche dell'UE relative all'EES, al VIS, all'ETIAS e alle componenti centrali conoscono disposizioni analoghe a quelle già valide per il SIS in materia di responsabilità per danni causati da un trattamento illecito di dati. Appare pertanto opportuno disciplinare nella LResp tutti i sistemi

34 RS **142.51**
35 RS **170.32**

d'informazione Schengen/Dublino e le rispettive componenti oggetto di disposizioni in materia di responsabilità. L'sBMS e l'ESP non costituiscono una compilazione di dati ai sensi dell'articolo 3 lettera d LPD, poiché al loro interno non vi è registrato alcun dato personale. Per tale ragione, al termine «sistema d'informazione» verrà ora affiancato anche quello di «componente».

Legge federale sui sistemi d'informazione di polizia della Confederazione

Oltre alla LStrI occorre adeguare anche la LSIP. Quest'ultima disciplina le basi giuridiche degli attuali sistemi d'informazione di polizia della Confederazione. Anche in questo caso la maggior parte delle disposizioni dei due regolamenti UE sull'interoperabilità sono direttamente applicabili e non necessitano pertanto di alcuna trasposizione nel diritto svizzero. Tuttavia, conformemente all'articolo 17 LPD, il trattamento di dati personali degni di particolare protezione da parte delle autorità federali è autorizzato soltanto in presenza di una pertinente base legale formale. Per tale ragione le componenti centrali che riguardano i sistemi d'informazione Schengen/Dublino oggetto della LSIP vanno ora disciplinati in quest'ultima. Nello specifico si tratta delle componenti centrali che includono il SIS.

Nella LSIP sono pertanto inserite disposizioni relative all'sBMS, al ESP e al MID dal tenore pressoché analogo a quello delle pertinenti disposizioni introdotte nella LStrI.

I sistemi d'informazione Schengen/Dublino o le rispettive componenti come pure il relativo trattamento dei dati e la responsabilità per quest'ultimo, devono essere ora disciplinati in articoli consecutivi (16-16*f* LSIP), rispecchiando l'ordine cronologico della loro entrata in funzione prevista (l'sBMS nell'art. 16*a*, l'ESP nell'art. 16*b* e il MID nell'art. 16*c*). Si è inoltre rinunciato a introdurre una struttura completamente nuova poiché la LSIP sarà modificata nell'ambito di diversi progetti legislativi attualmente in fase di dibattito parlamentare (legge federale sulle misure di polizia per la lotta al terrorismo[36] e decreto federale che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento delle basi legali sull'istituzione, l'esercizio e l'uso del Sistema d'informazione Schengen [SIS][37]). Al momento anche l'ordine di entrata in vigore dei progetti summenzionati è ancora da definire. Poiché nel prossimo futuro la LSIP sarà oggetto di revisione totale, si è rinunciato per il momento ad adeguare la sistematica.

In seguito all'attuazione della direttiva (UE) 2016/680 entrata in vigore il 1° marzo 2019, l'articolo 349*c* del Codice penale svizzero (CP)[38] disciplina la comunicazione di dati personali a uno Stato terzo o a un organo internazionale.[39] L'articolo 13 capoverso 2 della legge federale del 7 ottobre 1994[40] sugli Uffici centrali di polizia giudiziaria della Confederazione e i centri comuni di cooperazione di polizia e doganale con altri Stati (LUC), entrato anch'esso in vigore il 1° marzo 2019, statuisce che la comunicazione di dati personali nel quadro della

36 FF **2019** 4033
37 FF **2020** ....
38 RS **311.0**
39 RU **2019** 625
40 RS **360**

cooperazione di polizia con le autorità straniere preposte al perseguimento penale è retta dagli articoli 349*a*–349*h* CP[41]. La LSIP disciplina, per contro, in via generale l'utilizzo dei sistemi d'informazione di polizia della Confederazione; per giunta con la trasposizione dei regolamenti UE sull'interoperabilità il suo campo d'applicazione verrà ulteriormente ampliato. Per tale ragione, è necessario definire in una disposizione separata la comunicazione di dati a terzi e agli organi internazionali nel quadro dell'interoperabilità (art. 16*e*). Occorre infine anche disciplinare la responsabilità per il trattamento dei dati nei sistemi d'informazione Schengen/Dublino o nelle rispettive componenti (art. 16*f*).

6.3 Particolare necessità di coordinamento

L'interoperabilità necessita di un coordinamento particolare per quanto riguarda il recepimento e la trasposizione delle basi legali che istituiscono un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS). Poiché il progetto concernente il sistema ETIAS[42] è attualmente all'esame del Parlamento, nell'ambito del presente disegno di decreto federale non è possibile fare alcun riferimento a tale sistema d'informazione, sebbene rappresenti una parte integrante dell'interoperabilità. L'interoperabilità richiede un coordinamento anche con il recepimento delle basi legali concernenti l'istituzione, l'esercizio e l'uso del Sistema d'informazione Schengen (SIS); il progetto relativo al SIS[43] si trova ugualmente ancora all'esame del Parlamento. Dopo la votazione finale, i pertinenti articoli del presente disegno di decreto federale dovranno essere completati o adeguati di conseguenza. Vi è inoltre la necessità di coordinare il presente progetto con l'entrata in vigore delle basi legali per l'istituzione e l'uso del sistema di ingressi e uscite (EES)[44]. Un'eventuale necessità di coordinamento sussiste infine con la modifica della LStrI del 14 dicembre 2018 relativa alle ordinanze di esecuzione delle norme procedurali e dei sistemi d'informazione.[45] La necessità di coordinamento tra i diversi progetti sarà illustrata nel dettaglio nel numero 8.

41 RU **2019** 625

42 Messaggio del 6 marzo 2020 relativo all'approvazione e alla trasposizione nel diritto svizzero dello scambio di note tra la Svizzera e l'UE concernente il recepimento del regolamento (UE) 2018/1240 sul sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (Sviluppo dell'acquis di Schengen) e alla modifica della legge federale sugli stranieri e la loro integrazione (Assoggettamento del Servizio delle attività informative della Confederazione alla legge sulla protezione dei dati in ambito Schengen), 20.027, FF **2020** 2577.

43 Messaggio del 6 marzo 2020 relativo all'approvazione e alla trasposizione nel diritto svizzero degli scambi di note tra la Svizzera e l'UE concernenti il recepimento delle basi legali sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) (Sviluppi dell'acquis di Schengen) e alla modifica della legge federale sul sistema d'informazione per il settore degli stranieri e dell'asilo 20.025, FF **2020** 3117.

44 Decreto federale che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento delle basi legali per l'istituzione e l'uso del sistema di ingressi e uscite (EES) (regolamenti [UE] 2017/2226 e 2017/2225) (Sviluppi dell'acquis di Schengen); FF **2019** 3819.

45 RU **2019** 1413

7 Commento ai singoli articoli del testo di attuazione

7.1 Legge federale del 16 dicembre 2005 sugli stranieri e la loro integrazione (LStrI)

Art. 7 cpv. 3, primo periodo, nota a piè di pagina

Poiché il regolamento (UE) 2016/399 sul codice frontiere Schengen è modificato dal regolamento «IOP frontiere», la nota a piè di pagina dell'articolo 7 capoverso 3 va adattata di conseguenza.

Art. 9a

L'articolo 9*a* riprende senza modifiche materiali il contenuto dell'attuale articolo 103 LStrI che tratta la sorveglianza dell'arrivo all'aeroporto. A seguito di tale modifica, i rimandi nell'articolo 1 capoverso 2 LSISA devono essere adattati.

Art. 92a

L'articolo 92*a* riprende senza modifiche materiali il contenuto dell'attuale articolo 104 LStrI che tratta l'obbligo di comunicazione delle imprese di trasporto aereo. A seguito di tale modifica, i rimandi negli articoli 104*a* capoversi 1bis, 2, 3, 3bis, 4 e 5, 104*b* capoverso 1, 122*b* capoverso 2 e 122*c* capoverso 3 lettera b devono essere adattati.

Capitolo 14: Trattamento e protezione dei dati

In seguito all'introduzione delle nuove componenti centrali, che influiscono su tutti i sistemi d'informazione Schengen/Dublino, occorre modificare la struttura dei capitoli 14–14*c* come segue:

- il capitolo 14 conterrà tutte le disposizioni relative alla protezione e al trattamento dei dati in generale;
- il capitolo 14*a* disciplinerà tutti i sistemi d'informazione (sistemi nazionali e sistemi d'informazione Schengen/Dublino);
- il capitolo 14*b*, che finora conteneva le disposizioni sulla protezione dei dati nell'ambito degli accordi di associazione a Schengen, conterrà le disposizioni in materia di «interoperabilità tra i sistemi d'informazione Schengen/Dublino»;
- il capitolo 14*c*, che finora conteneva le disposizioni sull'Eurodac, disciplinerà la protezione dei dati nell'ambito degli accordi di associazione a Schengen. Le disposizioni relative all'Eurodac sono incluse nel capitolo 14*a*, in una sezione separata.

Il titolo del capitolo 14 è modificato. Questo capitolo disciplinerà infatti solo il trattamento e la protezione dei dati, mentre ai sistemi d'informazione sarà dedicato un capitolo a parte (14*a*).

Oltre agli articoli 101 LStrI (Trattamento dei dati), 102 LStrI (Rilevamento di dati per stabilire l'identità e l'età), 102*a* LStrI (Dati biometrici per carte di soggiorno) e 102*b* LStrI (Controllo dell'identità del titolare di una carta di soggiorno biometrica), il capitolo 14 comprenderà i seguenti articoli:

– 102*c* (Comunicazione di dati personali all'estero);
– 102*d* (Comunicazione di dati personali allo Stato d'origine o di provenienza);
– 102*e* (Comunicazione di dati personali nel contesto degli accordi di transito e di riammissione).

La suddivisione in sezioni sarà soppressa.

Art. 102c Comunicazione di dati personali all'estero

L'articolo 102*c* riprende senza modifiche materiali il contenuto dell'attuale articolo 105 LStrI che tratta la comunicazione dei dati personali all'estero.

Art. 102d Comunicazione di dati personali allo Stato d'origine o di provenienza

L'articolo 102*d* riprende senza modifiche materiali il contenuto dell'attuale articolo 106 LStrI che tratta la comunicazione di dati personali allo Stato d'origine o di provenienza.

Art. 102e Comunicazione di dati personali nel contesto degli accordi di transito e di riammissione

L'articolo 102*e* riprende senza modifiche materiali il contenuto dell'attuale articolo 107 LStrI che tratta la comunicazione dei dati personali nel contesto degli accordi di riammissione e di transito.

Art. 103

Cfr. commento all'articolo 9*a*.

Capitolo 14a: Sistemi d'informazione

Il capitolo 14*a* inizia ora prima dell'articolo 103*a* LStrI (Sistema d'informazione sulle entrate rifiutate) e riguarda i seguenti sistemi d'informazione:

– sezione 1 (Sistema d'informazione sulle entrate rifiutate [sistema INAD]: art. 103*a* LStrI[46];
– sezione 2 (Sistema di ingressi/uscite [EES] e controllo di confine automatizzato): art. 103*b*–103*g* LStrI[47];
– sezione 3 (Sistema d'informazione sui passeggeri [sistema API]): art. 104*a* – 104*c* e 108 LStrI (l'art. 108 LStrI è già abrogato);

46 FF **2019** 3819
47 FF **2019** 3819

- sezione 4 (Sistema centrale d'informazione visti [C-VIS] e sistema nazionale visti [ORBIS]): art. 109*a*–109*e* LStrI*;*
- sezione 5 (Sistema d'informazione per l'attuazione del ritorno): art. 109*f*–109*j* LStrI;
- sezione 6 (Eurodac): art. 109*k* e 109*l* D-LStrI;
- sezione 7 (Sistema di gestione dei fascicoli personali e della documentazione): art. 109*m* D-LStrI.

Sezione 1: Sistema d'informazione sulle entrate rifiutate (sistema INAD)

Prima dell'articolo 103*a* è ora inserita una nuova sezione intitolata «Sistema d'informazione sulle entrate rifiutate» (sistema INAD)».

Art. 103a[48]

Poiché la sezione 1 comprende un solo articolo, la rubrica dell'articolo 103*a* può essere soppressa.

Sezione 2: Sistema di ingressi/uscite (EES) e controllo di confine automatizzato

Prima dell'articolo 103*b* è inserita una nuova sezione contenente disposizioni riguardanti l'EES e il controllo di confine automatizzato.

Art. 103b cpv. 1, nota a piè di pagina, cpv. 2 lett. a e b^{bis} *e cpv. 4*[49]

Cpv. 1, nota a piè di pagina

Poiché il regolamento (UE) 2017/2226 sul sistema di ingressi/uscite EES è modificato dal regolamento «IOP frontiere», la nota a piè di pagina dell'articolo 103*b* capoverso 1 va adattata di conseguenza.

Cpv. 2 lett. a e b^{bis}

L'articolo 103*b* capoverso 2 lettera a non riporta più i dati sui visti rilasciati, i quali sono ora infatti trattati separatamente alla lettera b^{bis}. Ciò consente un rimando preciso, nel capoverso 4, ai dati ora registrati nel CIR. L'espressione «dati alfanumerici» è sostituita da «i dati di identità e i dati dei documenti di viaggio».

Cpv. 4

Il capoverso 4 specifica quali dati sono trasmessi e memorizzati nel CIR (cfr. commenti ad art. 110*a*). I dati di identità e i dati dei documenti di viaggio (art. 103*b* cpv. 2 lett. a LStrI), nonché l'immagine del volto e, se del caso, le impronte digitali (art. 103*b* cpv. 2 lett. b e cpv. 3 LStrI) sono registrati nel CIR. Le informa-

48 FF **2019** 3819
49 FF **2019** 3819

zioni riguardanti il momento dell'ingresso nello spazio Schengen e dell'uscita dallo stesso, il valico di frontiera e l'autorità responsabile del controllo di confine nonché i dati relativi al rifiuto di entrata non sono registrati nel CIR, ma continuano a essere memorizzati soltanto nell'EES.

Art. 103d, rubrica (concerne soltanto il testo francese) e cpv. 3[50]

La rubrica nella versione francese è adeguata al tenore delle disposizioni. Per quanto riguarda la comunicazione dei dati EES registrati nel CIR, il capoverso 3 rimanda all'articolo 110*h*, che si riferisce a sua volta all'articolo 40 dei regolamenti UE sull'interoperabilità (cfr. commenti all'art. 110*h* e n. 3.2, Protezione dei dati). In linea di principio, ai dati di base dell'EES registrati nel CIR si applicano le disposizioni contenute nel capo VII dei regolamenti UE sull'interoperabilità.

Art. 104

Si veda il commento all'articolo 92*a*.

Sezione 3: Sistema d'informazione sui passeggeri (sistema API) e accesso ai dati sui passeggeri nel singolo caso

Prima dell'articolo 104*a* è inserita una nuova sezione contenente norme sul sistema d'informazione sui passeggeri API (art. 104*a*–104*c*). Alcune disposizioni della presente sezione richiedono adattamenti formali. Non ci sono tuttavia modifiche materiali.

Art. 104a, rubrica, nonché cpv. 1bis*–4 e 5, frase introduttiva*

Poiché l'articolo 104*a* è ora una delle numerose disposizioni della sezione relativa al sistema d'informazione sui passeggeri, è necessario adattarne la rubrica. Inoltre, vanno adeguati i rimandi nei capoversi menzionati (cfr. commento ad art. 92*a*).

Art. 104b cpv. 1

Si veda il commento all'articolo 92*a*.

Capitolo 14 sezione 3 (art. 105–107)

Abrogata

La sezione 3 del capitolo 14 è abrogata. Il capitolo non contiene più una suddivisione in sezioni. Gli articoli 105–107 sono trasposti negli articoli 102*c*–102*e* senza modifiche materiali.

50 FF **2019** 3819

Sezione 4: Sistema centrale d'informazione visti (C-VIS) e sistema nazionale visti (ORBIS)

Prima dell'articolo 109*a* è inserita una nuova sezione contenente norme relative al C-VIS e a ORBIS (art. 109*a*–109*e* e art. 109*f*–109*j*).

Art. 109a, rubrica, nonché cpv. 1 e cpv. 1bis

Cpv. 1

Poiché il regolamento (CE) n. 767/2008 concernente il VIS è modificato dal regolamento (UE) n. 2019/817 («IOP frontiere»), la nota a piè di pagina dell'articolo 109*a* capoverso 1 va adattata di conseguenza.

Cpv. 1bis

Il capoverso 1bis specifica quali dati sono memorizzati nel C-VIS e quali dati sono registrati nel CIR (cfr. commenti all'art. 110*a*). I dati di identità, i dati dei documenti di viaggio e i dati biometrici sono registrati nel CIR. Le restanti informazioni sulla procedura di visto non sono invece registrate nel CIR e restano memorizzate soltanto nel C-VIS.

Art. 109b, cpv. 1, 2, frase introduttiva, 2bis–4

Il capoverso 1 introduce nella LStrI il termine «ORBIS» per il sistema nazionale dei visti. Di conseguenza, il termine ORBIS sostituisce l'espressione «sistema nazionale visti» nelle disposizioni successive. Alcune disposizioni sono adeguate sul piano formale e redazionale, senza tuttavia subire modifiche materiali.

Art. 109c, rubrica e frase introduttiva

Si veda il commento all'articolo 109*b*.

Art. 109d, nota a piè di pagina

La nota a piè di pagina deve essere aggiornata.

Sezione 5: Sistema d'informazione per l'attuazione del ritorno

Prima dell'articolo 109*f* LStrI è inserita una nuova sezione contenente norme sul sistema d'informazione per l'attuazione del ritorno. Queste disposizioni sono state introdotte con la modifica del 14 dicembre 2018 della LStrI (Norme procedurali e sistemi d'informazione) e sono entrate in vigore il 1° aprile 2020.[51] Non sono state apportate modifiche materiali alle disposizioni.

51 RU **2019** 1413, **2020** 881

Sezione 6: Eurodac

Prima dell'articolo 109*k* è inserita una nuova sezione contenente norme sull'Eurodac.

Art. 109k Rilevamento e trasmissione dei dati nell'Eurodac

L'articolo 109*k* riprende il contenuto del vigente articolo 111*i* LStrI senza subire modifiche materiali. È adeguata soltanto la rubrica. Il presente articolo riguarda l'Eurodac.

Le componenti centrali dovrebbero coprire anche l'Eurodac. Il CIR dovrebbe offrire infatti un contenitore comune per i dati di identità, i dati dei documenti di viaggio e i dati biometrici delle persone registrate nell'Eurodac. Tuttavia, il regolamento «IOP polizia» si applica all'Eurodac soltanto a partire dalla data di applicazione della nuova versione del regolamento (UE) n. 603/2013 (art. 75 del regolamento «IOP polizia»).

Art. 109l Comunicazione di dati Eurodac

Questo articolo riprende l'attuale articolo 111*d* capoverso 5, senza modifiche materiali, ma con adeguamenti redazionali. La disposizione disciplina la comunicazione dei dati Eurodac e appartiene tematicamente alla sezione 7.

Sezione 7: Sistema di gestione dei fascicoli personali e della documentazione

La vigente sezione 3 diventa la sezione 7. La sezione contiene una disposizione sul sistema di gestione dei fascicoli personali e della documentazione della Segreteria di Stato della migrazione (SEM).

Art. 109m

Questo articolo riprende l'attuale articolo 110 senza modifiche materiali.

Capitolo 14b: Interoperabilità tra i sistemi d'informazione Schengen/Dublino

Sezione 1: Servizio comune di confronto biometrico (sBMS)

Art. 110

L'articolo 110 disciplina ora il servizio comune di confronto biometrico (sBMS). La norma dell'attuale articolo 110 LStrI (sistema di gestione automatizzata dei fascicoli personali e della documentazione) non è più necessaria ed è pertanto abrogata.

Cpv. 1 e 3

Con l'ausilio dei cosiddetti «template biometrici» (dati relativi alle caratteristiche biometriche ricavati dai dati personali biometrici contenuti nei sistemi d'informazione Schengen/Dublino), l'sBMS permette la consultazione trasversale

dei sistemi d'informazione Schengen/Dublino interoperabili. Non è possibile dedurre i dati biometrici effettivi dal template.

A differenza del CIR (art. 110*a*–110*d* D-LStrI) o del MID (art. 110*g* D-LStrI), l'sBMS non costituisce una raccolta di dati o una «banca dati» ai sensi dell'articolo 3 lettera g LPD. I template biometrici contenuti nell'sBMS non sono dati personali biometrici, né vengono memorizzati in questo sistema altri dati personali (cfr. n. 5.2.1). Sebbene le disposizioni relative all'sBMS contenute nei due regolamenti UE sull'interoperabilità siano direttamente applicabili, nella LStrI va inclusa per completezza una disposizione sull'sBMS. Anche altre disposizioni nuove della LStrI rimandano all'sBMS.

Cpv. 2

Il riferimento nell'sBMS al rispettivo sistema d'informazione serve a determinare da quale sistema d'informazione Schengen/Dublino (EES, VIS, Eurodac, SIS) e da quali registrazioni effettive in questi sistemi provengono i dati personali biometrici, sulla base dei quali sono stati generati i template biometrici.

Le disposizioni dettagliate sull'sBMS sono contenute nel capo III dei due regolamenti UE sull'interoperabilità. Per informazioni dettagliate sull'sBMS si veda il numero 5.1.2.

Sezione 2: Archivio comune di dati di identità (CIR)

Art. 110a Contenuto dell'archivio comune di dati di identità

Cpv. 1

Il CIR contiene, per ogni persona registrata nell'EES, nel VIS, nell'ETIAS o, in una fase successiva, nell'Eurodac, un fascicolo individuale contenente i dati di identità, i dati dei documenti di viaggio o i dati biometrici provenienti da questi sistemi d'informazione Schengen/Dublino. I dati alfanumerici comprendono i dati di identità dell'interessato e i dati dei suoi documenti di viaggio. L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

Il CIR è inteso a facilitare l'identificazione delle persone i cui dati sono contenuti nei sistemi d'informazione Schengen/Dublino di cui sopra e a contribuire all'individuazione di identità multiple. Dovrebbe inoltre facilitare e armonizzare l'accesso a tali sistemi d'informazione da parte delle autorità designate a fini di prevenzione, individuazione o investigazione di reati di terrorismo o di altri reati gravi. I corrispondenti diritti di accesso al CIR sono disciplinati dagli articoli 110*b*–110*d* LStrI. È previsto che la consultazione del CIR sia attivata tramite l'ESP (cfr. art. 110*e* D-LStrI). Il CIR dovrebbe entrare in funzione a metà del 2022, mentre l'ESP sarà operativo soltanto dalla metà del 2023. Resta pertanto da chiarire se il CIR potrà essere consultato anche senza l'ESP durante il periodo transitorio, ossia fino a quando le componenti centrali non saranno entrate entrambe in funzione. Per informazioni dettagliate sul CIR si veda il numero 5.1.

Cpv. 2

Per ciascuna serie di dati di identità, di dati dei documenti di viaggio e biometrici memorizzati, il CIR contiene un riferimento al sistema d'informazione Schengen/Dublino sottostante da cui provengono i dati corrispondenti e un riferimento alla registrazione effettiva nel sistema d'informazione Schengen/Dublino.

Disposizioni dettagliate sul CIR sono contenute nel capo IV dei due regolamenti UE sull'interoperabilità.

Art. 110b Consultazione del CIR a fini di identificazione

Cpv. 1 e 2

Ai sensi dell'articolo 20 paragrafo 1 dei regolamenti UE sull'interoperabilità per una richiesta di identificazione deve essere soddisfatta una delle seguenti condizioni (cpv. 1 lett. a e cpv. 2):

- l'autorità di polizia non è in grado di identificare una persona in ragione dell'assenza di un documento di viaggio o di un altro documento credibile che ne provi l'identità;
- sussistono dubbi quanto ai dati di identità forniti da una persona;
- sussistono dubbi quanto all'autenticità del documento di viaggio o di un altro documento credibile fornito da una persona;
- sussistono dubbi quanto all'identità del titolare del documento di viaggio o di un altro documento credibile;
- una persona non è in grado o rifiuta di cooperare.

In caso di calamità naturali, incidenti o attacchi terroristici, le autorità autorizzate alla consultazione ai sensi dell'articolo 110*b* capoverso 3 D-LStrI possono consultare il CIR sulla base dei dati biometrici della persona interessata solo per identificare persone sconosciute che non possono provare la loro identità o resti umani non identificati (cpv. 1 lett. b).

Cpv. 3

Il capoverso 3 elenca le autorità che possono consultare il CIR in singoli casi concreti per identificare i cittadini stranieri (cittadini di Stati terzi). Una consultazione può essere effettuata solo per i seguenti scopi: combattere l'immigrazione illegale, proteggere l'ordine e la sicurezza pubblici e salvaguardare la sicurezza interna.

Le autorità competenti sono l'Ufficio federale di polizia (fedpol), le autorità di polizia dei Cantoni e dei Comuni e l'Amministrazione federale delle dogane (AFD) ai fini della protezione della popolazione e della salvaguardia della sicurezza interna. fedpol ottiene l'accesso per condurre sul territorio nazionale identificazioni nell'ambito dei suoi compiti di mantenimento dell'ordine e della sicurezza pubblici. Le autorità di polizia cantonali e comunali dispongono ugualmente di un accesso al CIR per verificare la legalità del soggiorno di persone. L'AFD ha accesso al sistema

per l'adempimento dei compiti che le sono assegnati, in particolare per garantire il traffico regolare di merci e persone attraverso il confine doganale e per contribuire alla sicurezza interna del Paese e alla protezione della popolazione. In particolare, ha la facoltà di controllare la circolazione delle persone. Questo controllo comprende la verifica dell'identità, del diritto di attraversare le frontiere e del diritto di soggiorno in Svizzera.

Cpv. 4 e 5

La consultazione del CIR è generalmente effettuata sulla base dei dati biometrici aggiornati dello straniero acquisiti direttamente sul posto. Di regola, la procedura di identificazione deve essere avviata in presenza dell'interessato, sebbene la sua presenza non sia necessaria durante l'intera procedura. Se la consultazione per mezzo di dati biometrici non è possibile o non ha esito positivo, la ricerca deve essere effettuata sulla base dei dati dei documenti di viaggio o dei dati di identità disponibili.

Art. 110c Consultazione del CIR ai fini dell'individuazione di identità multiple

Cpv. 1

Se durante la consultazione del CIR compare un collegamento giallo (cfr. n. 5.1.4), le autorità di cui al presente capoverso possono accedere per la verifica manuale di identità multiple soltanto ai dati personali biometrici contenuti nel CIR, ai dati di identità, ai dati del documento di viaggio e al riferimento al sistema d'informazione Schengen/Dublino da cui provengono i dati. L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

Cpv. 2

Se durante la consultazione del CIR compare un collegamento rosso (cfr. n. 5.1.4), le autorità che hanno accesso al CIR, all'EES, all'ETIAS, al C-VIS, all'Eurodac o al SIS in virtù della LStrI o della LSIP possono, per combattere le frodi di identità, accedere ai dati contenuti nel CIR (cfr. commento al cpv. 1) e al riferimento al sistema d'informazione Schengen/Dublino. L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

Art. 110d Consultazione del CIR ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo o altri reati gravi

Cpv. 1 e 2

Se, in un caso specifico, vi è motivo di ritenere che la consultazione di un sistema d'informazione Schengen/Dublino possa contribuire alla prevenzione, all'individuazione o all'investigazione di reati terroristici o altri reati gravi, fedpol, il SIC, il Ministero pubblico della Confederazione e le autorità cantonali di polizia e di perseguimento penale nonché le autorità di polizia delle città di Zurigo, Winterthur, Losanna, Chiasso e Lugano possono consultare il CIR per appurare se nei sistemi

EES, VIS, ETIAS o Eurodac sono disponibili dati relativi alla persona interessata. Le autorità di polizia comunali elencate in questo capoverso (Zurigo, Lugano, ecc.) hanno il diritto di consultare i dati in quanto, come le forze di polizia cantonali, svolgono funzioni di polizia giudiziaria nell'ambito della prevenzione, dell'individuazione e dell'investigazione di reati gravi (cfr. anche la disposizione nell'art. 109*a* cpv. 3 LStrI). Nel messaggio del Consiglio federale del 22 maggio 2019[52] concernente la legge federale sulle misure di polizia per la lotta al terrorismo la nozione di «reato grave» viene definita con maggiore precisione. Rientrano in questa definizione in particolare i reati di cui all'articolo 286 capoverso 2 del Codice di procedura penale[53]. Nel quadro delle modifiche di legge inerenti alla lotta al terrorismo, viene anche precisata all'interno del CP la nozione di «reati terroristici».

Cpv. 3 e 4

L'accesso al CIR da parte delle autorità competenti avviene tramite una procedura a due tappe. In una prima fase, l'autorità competente può soltanto appurare se nei sistemi d'informazione in questione sono contenute informazioni su di una persona. Se una consultazione del CIR rivela che i dati relativi alla persona interessata sono contenuti in uno dei sistemi d'informazione Schengen/Dublino di cui sopra, il CIR notifica alle autorità designate di cui al capoverso 2 il corrispondente riferimento ai sistemi EES, VIS, ETIAS o Eurodac. In una seconda fase, l'autorità dovrà richiedere un accesso ai dati in questione alla Centrale operativa di fedpol.

Se un'autorità di cui al capoverso 2 rinuncia a presentare una domanda nonostante un'indicazione pertinente, i motivi della rinuncia vanno registrati in modo tracciabile in un fascicolo nazionale.

Sezione 3: Portale di ricerca europeo (ESP)

Art. 110e

L'ESP deve rendere possibile la consultazione trasversale e parallela di tutti i pertinenti sistemi d'informazione Schengen/Dublino, delle banche dati Interpol e dei dati Europol. L'obiettivo è avere un'interfaccia unica per poter consultare agevolmente le informazioni necessarie nei diversi sistemi d'informazione, nel pieno rispetto dei diritti di accesso e dei requisiti in materia di protezione dei dati.

Sulla base dei dati di identità, di quelli dei documenti di viaggio e dei dati biometrici personali, l'ESP può essere usato per consultare simultaneamente i sistemi EES, VIS, ETIAS, Eurodac, SIS, le banche dati di Interpol SLTD e TDAWN e i dati Europol (art. 6 e 7 dei regolamenti UE sull'interoperabilità). L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

Una ricerca tramite ESP viene avviata quando:

– vengono inseriti dati in una delle banche dati di cui sopra;

52 FF **2019** 3935
53 RS **312.0**

– vengono eseguiti controlli di confine alle frontiere esterne di Schengen o controlli d'identità.

Una ricerca può anche essere avviata per verificare la legittimità del soggiorno di cittadini di Paesi terzi in Svizzera.

Tuttavia, la ricerca mediante l'ESP è possibile solo per le autorità già autorizzate ad accedere a una delle suddette banche dati (art. 7 dei regolamenti UE sull'interoperabilità). Per consentire l'uso dell'ESP, l'eu-LISA crea categorie di profili utente ESP che tengono conto dei diritti di accesso (art. 8 dei regolamenti UE sull'interoperabilità).

All'utente verranno mostrati solo i dati a cui ha diritto di accesso e i riferimenti di cui agli articoli 30–33 dei regolamenti UE sull'interoperabilità. Non vengono fornite informazioni su dati cui l'utente non è autorizzato ad accedere (art. 9 dei regolamenti UE sull'interoperabilità).

Ciascuno Stato Schengen tiene un registro delle consultazioni dell'ESP effettuate dalle autorità autorizzate o dal loro personale.

Le interfacce nazionali con i vari sistemi d'informazione devono essere mantenute per disporre di un'alternativa tecnica.

Sezione 4: Rilevatore di identità multiple (MID)

Art. 110f Contenuto del rilevatore di identità multiple (MID)

Il MID è al tempo stesso un rilevatore e una nuova banca dati alla quale alcune autorità hanno accesso. Questa banca dati contiene fascicoli di conferma dell'identità ai sensi dell'articolo 34 dei regolamenti UE sull'interoperabilità. Il loro contenuto è memorizzato per il tempo in cui i dati oggetto del collegamento sono conservati in almeno due sistemi d'informazione Schengen/Dublino (art. 35 dei regolamenti UE sull'interoperabilità).

Cpv. 1

Il capoverso 1 stabilisce gli obiettivi del MID, ossia facilitare i controlli d'identità e combattere le frodi d'identità.

Cpv. 2

Il capoverso 2 stabilisce, conformemente ai regolamenti UE, che è automaticamente avviata una procedura di rilevazione di identità multiple nel CIR e nel SIS quando sono creati o aggiornati un fascicolo nell'EES, nel VIS, nell'ETIAS oppure una segnalazione nel SIS. L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

Cpv. 3

Questo capoverso stabilisce la procedura per la verifica di identità multiple nel contesto dell'interoperabilità dei diversi sistemi d'informazione Schengen. Come il SIS, il CIR, l'ETIAS, il VIS, l'EES e, in una fase successiva, l'Eurodac utilizzano l'sBMS (art. 110) e l'ESP (art. 110*e*) per rilevare le identità multiple. L'sBMS consente un confronto biometrico (art. 27 par. 2 dei regolamenti UE sull'interoperabilità), mentre la consultazione nell'ESP è effettuata sulla base dei dati di identità e dei dati dei documenti di viaggio (art. 27 par. 3 e 4 dei regolamenti UE sull'interoperabilità) La verifica avviene dopo la registrazione o l'aggiornamento di un fascicolo in uno dei diversi sistemi (cfr. art. 110*f* cpv. 2).

Cpv. 4

Questo capoverso specifica le condizioni per la creazione nel MID di un fascicolo di conferma dell'identità secondo l'articolo 34 dei regolamenti UE sull'interoperabilità. Tali fascicoli sono creati quando la procedura di rilevazione delle identità multiple evidenzia collegamenti tra i dati dei diversi sistemi d'informazione che sono legati alla stessa persona e che potrebbero eventualmente appartenere a quest'ultima. Questi collegamenti si riferiscono in particolare a identità multiple riconducibili alla stessa persona in maniera giustificata o ingiustificata. Il MID contiene anche un riferimento ai sistemi d'informazione interessati, segnatamente un numero di identificazione univoco, che consente di estrarre i dati associati dai rispettivi sistemi. Infine, nel MID sono elencati anche la data di creazione del collegamento, il suo aggiornamento e l'autorità responsabile della verifica dei collegamenti.

Art. 110g Verifica manuale delle identità diverse nel MID

Cpv. 1

La verifica manuale deve essere effettuata ogni volta che vi sono collegamenti tra dati di sistemi diversi e le identità non corrispondono o non si somigliano (collegamento giallo, art. 28 par. 4 dei regolamenti UE sull'interoperabilità). Per effettuare la verifica manuale, le autorità competenti (art. 110*c*) hanno accesso al MID. Le autorità competenti sono quelle che hanno accesso al CIR per individuare eventuali identità multiple. Per questo motivo, è opportuno un rimando all'articolo 110*c* capoverso 1 che designa le autorità che hanno accesso al CIR.

Cpv. 2

Questo capoverso stabilisce quali autorità sono responsabili della verifica dei collegamenti gialli nel MID. In linea di principio, si tratta dell'autorità che avvia una consultazione creando un fascicolo o aggiornando i dati nel C-VIS, nell'EES o nell'ETIAS (una volta che il recepimento di tale sviluppo sarà stato approvato). Per contro, nei casi in cui esiste un collegamento con segnalazioni di polizia, la verifica compete all'Ufficio SIRENE di fedpol.

Per sostenere la verifica manuale dei collegamenti del MID, è prevista la creazione di un servizio centrale di esperti («zentrale MID-Expertenstelle», di seguito: MES)

composto di collaboratori degli uffici federali abilitati a verificare i collegamenti. Il MES intende fornire sostegno alle autorità in casi particolarmente complessi o laddove un'autorità non disponga delle competenze necessarie per procedere alla verifica di un collegamento.

Cpv. 3

La verifica di identità multiple è effettuata in presenza della persona interessata (art. 29 del regolamento «IOP frontiere»), in particolare laddove la verifica avvenga nell'ambito di un controllo di confine o se occorre verificare collegamenti sul territorio svizzero. Nel caso di collegamenti relativi a una domanda di autorizzazione ai viaggi ETIAS, la verifica può essere effettuata in assenza della persona interessata.

Cpv. 4

Se viene scoperta un'identità multipla illecita (collegamento rosso, art. 32 dei regolamenti UE sull'interoperabilità) o se i dati di una persona figurano legittimamente in diversi sistemi d'informazione Schengen (collegamento bianco, art. 33 dei regolamenti UE sull'interoperabilità), la persona interessata deve esserne informata. L'autorità responsabile della verifica manuale trasmette tali informazioni mediante un modulo standard. Inoltre, se viene creato un collegamento rosso, il MID informa automaticamente le autorità responsabili dei dati collegati (art. 32 par. 6 dei regolamenti UE sull'interoperabilità).

Sezione 5: Comunicazione dei dati e responsabilità per il trattamento di dati

Art. 110h Comunicazione di dati dell'sBMS, del CIR e del MID

In linea di massima, i dati delle componenti dell'interoperabilità non possono essere comunicati a Stati terzi, organizzazioni internazionali e soggetti privati. Restano valide le prescrizioni in materia di comunicazione dei dati previste per ogni singolo sistema (art. 50 dei regolamenti UE sull'interoperabilità). Si tratta dell'articolo generale 111*d* LStrI e degli articoli 103*d*[54] e 108*f* LStrI che disciplinano la comunicazione dei dati nei sistemi informativi EES ed ETIAS. I dati provenienti da tali sistemi potranno essere comunicati in qualsiasi momento in conformità con le disposizioni vigenti o che saranno in vigore in futuro. Tali disposizioni prevedono che i dati dei vari sistemi, compreso il contenuto del CIR, possono essere trasmessi in alcuni casi specifici.

Art. 110i Responsabilità per il trattamento di dati dell'sBMS, del CIR e del MID

Questa disposizione rimanda all'articolo 40 dei regolamenti UE sull'interoperabilità per quanto riguarda la responsabilità del trattamento dei dati nelle tre componenti di interoperabilità sBMS, CIR e MID (cfr. n. 3.2, Protezione dei dati).

54 FF **2019** 3819

Capitolo 14c: Protezione dei dati nell'ambito degli Accordi di associazione alla normativa di Schengen

L'attuale capitolo 14*b* diventa il capitolo 14*c*; tutte le disposizioni relative alla protezione dei dati nell'ambito degli Accordi di associazione a Schengen figurano pertanto dopo il nuovo capitolo 14*b* che riguarda l'interoperabilità.

Le disposizioni del presente capitolo rimangono materialmente invariate.

L'articolo 111*c* capoverso 3 rimanda ai nuovi articoli 109*l*, 111*a* e 111*d*. Non subisce alcuna modifica materiale.

L'articolo 111*d* capoverso 5 è abrogato e diventa il nuovo articolo 109*l* D-LStrI.

Il diritto di accesso di cui all'articolo 111*f* si riferisce in particolare alla LPD e alle leggi cantonali in materia di protezione dei dati. Questa disposizione si applica anche alle informazioni contenute nei vari sistemi d'informazione Schengen/Dublino. Poiché tale articolo riprende l'articolo 8 LPD, se ne propone l'abrogazione.

Analogamente, il diritto di modificare o cancellare i dati nonché il diritto all'informazione sono disciplinati dalla LPD. Alcuni aspetti della protezione dei dati in relazione ai vari sistemi Schengen/Dublino e all'interoperabilità sono o saranno specificati nelle ordinanze esecutive. Pertanto, i vari diritti di protezione dei dati non sono elencati in questo capitolo.

L'attuale capitolo 14c sull'Eurodac è spostato e inserito prima del capitolo sull'interoperabilità. Il capitolo vigente è pertanto abrogato.

Art. 120d Trattamento indebito di dati personali nei sistemi d'informazione

Conformemente all'articolo 45 dei regolamenti UE sull'interoperabilità, gli Stati Schengen sono tenuti a prevedere sanzioni per l'uso improprio di dati nonché il trattamento o lo scambio di dati illeciti. Le sanzioni devono essere effettive, proporzionate e dissuasive. Disposizioni simili figurano nel regolamento (CE) n. 767/2008 concernente il VIS (art. 36) e nel regolamento (UE) 2017/2226 (art. 48).

L'articolo 120*d*, modificato nel quadro dei progetti riguardanti l'EES, deve essere nuovamente adattato ai fini dell'interoperabilità.

Il progetto ETIAS implica ugualmente una modifica della presente disposizione. Tale progetto è attualmente discusso dal Parlamento.

Innanzitutto la rubrica della disposizione viene adeguata. Viene infatti eliminato il riferimento alla SEM, poiché alcuni di questi sistemi sono sistemi d'informazione Schengen/Dublino (CIR e MID), che non rientrano esclusivamente nelle competenze della SEM. Per contro il VIS, l'EES e in futuro l'ETIAS sono sistemi d'informazione Schengen/Dublino di competenza della SEM.

Il capoverso 1 che era stato inserito nel quadro del progetto EES e che non è entrato ancora in vigore, col presente disegno è trasposto, senza modifiche materiali, nell'articolo 101 capoverso 2.

In virtù di tale trasposizione, l'articolo 120*d* (stato: adozione del progetto EES da parte del Parlamento) non sarà più suddiviso in capoversi e andrà pertanto modificato sul piano della struttura.

Il capoverso 2 lettera a che era stato introdotto nel quadro del progetto EES e che non è entrato ancora in vigore è trasposto nella lettera a (senza capoverso). Esso punisce con la multa il trattamento indebito dei dati nel C-VIS.

La lettera b del capoverso 2 che era stata ugualmente introdotta nel quadro del progetto EES e che non è ancora entrata in vigore diventa la lettera b (senza capoverso) e prevede la stessa sanzione per il trattamento indebito nell'EES.

In futuro si prevede di menzionare anche l'ETIAS. Quest'ultimo è tuttavia oggetto di un progetto separato che è attualmente trattato dal Parlamento.

È inoltre opportuno introdurre due lettere che stabiliscano le disposizioni relative al CIR (lett. d) e al MID (lett. e). Qualsiasi trattamento di dati contrario agli articoli 110*a*–110*d*, 110*f* e 110*g* D-LStrI va punito con una multa che, secondo l'articolo 106 capoverso 1 CP, può arrivare fino a 10 000 franchi se i collaboratori delle autorità competenti trattano deliberatamente i dati personali in contrasto con lo scopo previsto.

Ai sensi dell'attuale articolo 120*e* LStrI, il perseguimento penale è di competenza dei Cantoni.

Art. 122b cpv. 2

Si veda il commento all'articolo 92*a*.

Art. 122c cpv. 3 lett. b

Si veda il commento all'articolo 92*a*.

Art. 126 cpv. 5

Si veda il commento all'articolo 102*e*.

7.2 Legge federale del 20 giugno 2003 sul sistema d'informazione per il settore degli stranieri e dell'asilo

Art. 1 cpv. 2

Si veda il commento all'articolo 92*a* D-LStrI.

Art. 15 Comunicazione all'estero

Gli articoli 105–107 LStrI sono sostituiti dagli articoli 102*c*–102*e* D-LStrI. Il corrispondente rimando nell'articolo 15 LSISA deve essere adattato di conseguenza.

L'attuale rimando agli articoli 111*d* capoverso 5 e 111*i* LStrI è sostituito da un rimando agli articoli 109*k* e 109*l* D-LStrI.

7.3 Legge del 14 marzo 1958 sulla responsabilità (LResp)

Titolo del capo Va

Nella legge sulla responsabilità occorre estendere la responsabilità per danni causati dal trattamento illecito dei dati da parte di una persona al servizio della Confederazione o di un Cantone a tutti i sistemi d'informazione Schengen/Dublino e alle rispettive componenti. Il titolo del capo V*a* deve essere pertanto modificato come segue: *Capo Va: Responsabilità per danni derivanti dall'esercizio o dall'uso dei sistemi d'informazione Schengen/Dublino o delle loro componenti*.

Art. 19a

L'articolo 19*a* LResp disciplina attualmente la responsabilità in relazione al SIS. Esso statuisce infatti che la Confederazione risponde del danno causato illecitamente a terzi da una persona al servizio della Confederazione o di un Cantone in seguito all'esercizio del SIS. Il capoverso 2 stabilisce inoltre che la Confederazione, ove abbia risarcito il danno, ha diritto di regresso contro il Cantone al cui servizio si trova la persona che ha causato il danno.

Il campo d'applicazione del presente articolo va esteso a tutti i sistemi d'informazione Schengen/Dublino nonché alle loro componenti. Le diverse basi giuridiche pertinenti dell'UE prevedono infatti che una persona che abbia subito danni materiali o immateriali in conseguenza di un trattamento illecito di dati personali ha diritto al risarcimento da parte dello Stato Schengen responsabile del danno subito. Tali disposizioni sulla responsabilità si trovano nello specifico all'articolo 45 del regolamento (UE) 2017/2226 per quanto concerne l'EES, all'articolo 33 del regolamento (CE) n. 767/2008 per quanto riguarda il VIS, all'articolo 63 del regolamento (UE) 2018/1240 per quanto attiene all'ETIAS, all'articolo 37 del regolamento (UE) n. 603/2013 in relazione all'Eurodac e, infine, all'articolo 46 dei regolamenti UE sull'interoperabilità per quanto concerne le componenti centrali.

Per tale ragione, nell'articolo 19*a* sono ora integrati l'EES (lett. b), il C-VIS (lett. c), il CIR (lett. d), l'ESP (lett. e), il MID (lett. f) e l'Eurodac (lett. g). L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

È inoltre apportata una piccola modifica formale alla disposizione: per motivi di chiarezza, l'espressione «utilizzazione» è sostituita da «esercizio e uso». Occorre inoltre sottolineare che anche nella versione francese, specificamente all'articolo 19*b*, l'espressione «utilisation» è già utilizzata nella versione in vigore.

Art. 19b

Anche il presente articolo necessita di essere adeguato. Esso è ora suddiviso in due capoversi. Alla lettera a, il rinvio al SIS deve essere sostituito dall'espressione «uno

dei sistemi d'informazione Schengen/Dublino o una delle sue componenti». Anche la lettera b deve essere adeguata. La versione in vigore si riferisce infatti esclusivamente a una segnalazione nel SIS che abbia causato un danno. Pertanto, occorre ora includere tutti i sistemi d'informazione Schengen/Dublino, parlando più generalmente di «trattamento dei dati».

Infine, gli Accordi di associazione alla normativa di Schengen e Dublino vanno elencati all'interno di un allegato (cfr. cpv. 2).

7.4 Legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione (LSIP)

Adeguamento della struttura

Nella LSIP occorre integrare diversi articoli relativi ai sistemi d'informazione Schengen/Dublino o alle rispettive componenti. A tal fine si rende necessario adeguare o introdurre diversi titoli.

Art. 2

Il presente articolo elenca i sistemi d'informazione disciplinati dalla LSIP. Come illustrato al numero 6.2, le componenti centrali che concernono il SIS vanno regolamentate anche nella LSIP. Esse sono pertanto integrate nell'articolo 2.

Nell'articolo 2 viene ora operata una distinzione tra i sistemi d'informazione di polizia (lett. a), da un lato, e i sistemi d'informazione Schengen/Dublino e le loro componenti (lett. b), dall'altro.

Nella lettera a sono quindi ora menzionati al numero 1, la rete dei sistemi d'informazione di polizia (art. 9–14), al numero 2, il sistema di ricerca informatizzato di polizia (art. 15), al numero 3, il registro nazionale di polizia (art. 17) e, al numero 4, il sistema di gestione delle pratiche e degli atti di fedpol (art. 18).

Quale sistema d'informazione Schengen/Dublino, al numero 1 della lettera b è invece menzionata la parte nazionale del Sistema d'informazione Schengen (N-SIS; art. 16). Nei numeri 2-4 sono inoltre inseriti, secondo un ordine che rispecchia la loro presumibile entrata in funzione, le componenti centrali sBMS, ESP e MID, disciplinate rispettivamente dagli articoli 16*a*, 16*b* e 16*c*.

Art. 16a Servizio comune di confronto biometrico (sBMS)

Poiché è collegato anche al SIS, l'sBMS deve essere regolamentato anche dalla LSIP, e più precisamente nel presente articolo, analogamente all'articolo 110 D-LStrI. Nonostante l'applicabilità diretta dei regolamenti UE sull'interoperabilità, l'sBMS è integrato per ragioni di completezza e per permettere di effettuare rinvii. L'sBMS non è una collezione di dati ai sensi dell'articolo 3 lettera g LPD, in quanto non permette di ricercare i template biometrici secondo le persone interessate.

Cpv. 1

Nell'sBMS sono registrati i template biometrici ottenuti dalle immagini del volto e dalle impronte digitali registrate nel SIS e nel CIR. Il capoverso 1 specifica che i dati pertinenti del CIR provengono dall'EES, dal C-VIS e dall'Eurodac.

Cpv. 2

Il riferimento di cui al capoverso 2 riguarda il sistema d'informazione Schengen/Dublino dal quale sono stati originariamente ricavati i template biometrici nonché l'effettiva registrazione in tale sistema. I dati sono registrati separatamente in base al sistema d'informazione da cui provengono.

Cpv. 3

L'sBMS serve a effettuare una consultazione trasversale sulla base di dati biometrici. Ogni qualvolta sono create o aggiornate nuove registrazioni, ha luogo un confronto automatizzato dei dati riguardanti le persone contenuti nel CIR e nel SIS.

La cancellazione dei rispettivi dati nel CIR o nel SIS determina la cancellazione automatica dei dati nell'sBMS.

Art. 16b Portale di ricerca europeo (ESP)

Poiché è collegato al SIS, l'ESP deve essere disciplinato, oltre che nella LStrI (art. 110*e*), anche nella LSIP.

Cpv. 1

Come illustrato in merito all'articolo 110*e* D-LStrI, l'ESP consentirà di consultare, mediante un'unica ricerca, tutti i pertinenti sistemi d'informazione Schengen/Dublino e le loro componenti (SIS, EES, VIS, ETIAS, Eurodac e CIR) nonché le banche dati di Interpol e i dati Europol. L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

Cpv. 2

L'accesso online all'ESP è limitato alle autorità che sono autorizzate ad accedere ad almeno uno dei sistemi d'informazione Schengen/Dublino e alle loro componenti (SIS, EES, VIS, ETIAS, Eurodac e CIR) o alle banche dati di Interpol e ai dati Europol.

Cpv. 3

Le autorità autorizzate all'accesso possono effettuare consultazioni sulla base dei dati di identità, dei dati dei documenti di viaggio o biometrici. Le ricerche possono riguardare persone o documenti di viaggio.

Cpv. 4

Il risultato delle consultazioni è limitato ai sistemi d'informazione Schengen/Dublino, alle banche dati Interpol e ai dati Europol per i quali l'autorità interessata dispone di un diritto d'accesso. Le risposte indicano inoltre da quali sistemi sottostanti provengono i dati in questione nonché i collegamenti esistenti.

In cooperazione con gli Stati Schengen, eu-LISA definirà all'interno di un atto di esecuzione i campi di dati da usare per l'interrogazione, i dati specifici che possono essere interrogati e le categorie di dati che possono essere forniti in ciascuna risposta. Questi elementi andranno in parte disciplinati all'interno di ordinanze di esecuzione.

Art. 16c Rilevatore di identità multiple

Il MID concerne anch'esso il SIS e va pertanto disciplinato, oltre che nella LStrI (art. 110*f*), anche nella LSIP.

Cpv. 1

Il capoverso 1 disciplina gli scopi del MID. Il MID deve servire a svolgere le verifiche di identità e a contrastare la frode di identità.

Cpv. 2

In determinati casi viene automaticamente avviata una procedura di rilevazione delle identità multiple nel SIS e nel CIR. È quanto avviene quando nel SIS, nell'EES, nell'ETIAS, nel C-VIS e, in futuro anche nell'Eurodac, sono registrati o aggiornati dei dati. L'ETIAS non può essere ancora menzionato nel testo di legge, poiché il Parlamento non ha ancora approvato il recepimento di tale sviluppo (cfr. n. 8.1).

Cpv. 3

Il presente capoverso illustra come si svolge concretamente la procedura di rilevazione automatica delle identità multiple. Per verificare se nel SIS o nel CIR sono già registrati dati su una persona, i dati appena registrati o aggiornati sono confrontati con i template biometrici contenuti nell'sBMS. A sua volta, l'ESP confronta i dati di identità e quelli dei documenti di viaggio con i dati alfanumerici già registrati.

Se risultano una o più corrispondenze, il SIS e il CIR creano un collegamento tra i dati usati per avviare la consultazione e i dati per i quali è emersa la corrispondenza.

Cpv. 4

In caso di collegamento viene creato un fascicolo di conferma dell'identità (cfr. art. 34 dei regolamenti [UE] 2019/817 e [UE] 2019/818). Il fascicolo contiene i seguenti dati: il tipo di collegamento tra i dati, a condizione che sussista una corrispondenza, un riferimento ai sistemi d'informazione Schengen/Dublino in cui sono conservati i dati oggetto del collegamento, un numero di identificazione unico che permette di estrarre i dati oggetto del collegamento dai corrispondenti sistemi d'informazione Schengen/Dublino, l'autorità responsabile della verifica manuale delle identità diverse nonché la data della creazione del collegamento o del suo aggiornamento.

Art. 16d Verifica manuale di collegamenti nel MID

Il presente articolo definisce le autorità competenti per la verifica manuale dei collegamenti esistenti tra i sistemi d'informazione Schengen/Dublino (cfr. art. 110 cpv. 1 D-LStrI).

Cpv. 1

Il diritto d'accesso serve alla verifica manuale dei collegamenti gialli.

Cpv. 2

In linea di principio, la verifica manuale deve essere eseguita dall'autorità che ha effettuato una registrazione o una modifica a un fascicolo contenuto all'interno di uno dei sistemi d'informazione Schengen/Dublino.

Se il collegamento concerne una segnalazione nel SIS, tranne laddove quest'ultima si riferisca a un rifiuto d'entrata, la verifica manuale compete all'Ufficio SIRENE. Se la verifica riguarda l'EES, la competenza è affidata all'Amministrazione federale delle dogane (AFD) o alla polizia cantonale. La SEM e le altre autorità competenti in materia di visti sono chiamate a effettuare verifiche manuali se il collegamento concerne il C-VIS. Se il collegamento riguarda invece l'ETIAS, la verifica manuale è eseguita dalla SEM.

L'autorità competente per la verifica manuale ha accesso a tutti i dati di cui ha bisogno per procedere alla verifica dell'identità. Si tratta dei dati oggetto del collegamento contenuti nel pertinente fascicolo di conferma dell'identità nonché dei dati di identità oggetto del collegamento nel CIR e nel SIS. La verifica delle identità diverse deve essere effettuata senza indugio. In tale contesto occorre classificare il collegamento come verde (i dati di identità nei fascicoli oggetto del collegamento non si riferiscono alla stessa persona), rosso (in caso di identità multipla illecita o di frode di identità) o bianco (si tratta della stessa persona) e integrare il fascicolo di conferma dell'identità. Ogni collegamento deve essere verificato singolarmente.

Cpv. 4

Se dalla verifica manuale emerge un'identità multipla illecita (collegamento rosso) o che una persona è registrata in più sistemi d'informazione Schengen/Dublino (collegamento bianco), la persona in questione deve essere informata mediante un modulo standard. È possibile rinunciare a procedere a una tale informazione se ciò potrebbe pregiudicare una segnalazione nel SIS o se è necessario per motivi di sicurezza e ordine pubblico, per prevenire la criminalità e garantire che non siano compromesse indagini nazionali.

Il MID informa automaticamente le autorità competenti per i dati oggetto di un collegamento rosso.

La verifica manuale deve avvenire, nella misura del possibile, in presenza della persona in questione. È il caso in particolare dei controlli all'ingresso nel territorio svizzero, laddove la Svizzera valga come primo Stato Schengen.

Art. 16e Comunicazione di dati dell'sBMS, del CIR e del MID

Il presente articolo stabilisce che i dati personali registrati nelle componenti dell'interoperabilità o da queste trattati o consultati non possono essere in linea di principio trasferiti o messi a disposizione di Paesi terzi, organizzazioni internazionali o soggetti privati. Restano valide le prescrizioni in materia di comunicazione dei dati previste per ogni singolo sistema.

Art. 16f Responsabilità per il trattamento di dati dell'sBMS, del CIR e del MID

Occorre infine disciplinare la responsabilità per il trattamento dei dati, retta dall'articolo 40 dei regolamenti UE sull'interoperabilità.

8 Necessità di coordinamento

8.1 Coordinamento con il progetto ETIAS

I rinvii all'interoperabilità contenuti negli articoli 110*a* capoverso 1, 110*c*, 110*e* capoverso 1 e 110*f* capoverso 2 LStrI del presente disegno dovrebbero menzionare anche il sistema ETIAS. Tuttavia, il progetto ETIAS[55] dovrebbe essere approvato dal Parlamento soltanto in occasione della sessione autunnale del 2020, motivo per cui non è possibile rinviare all'ETIAS prima di tale data. Dopo la votazione finale, detti articoli potranno essere modificati all'interno del presente disegno, inserendo un rinvio all'ETIAS. Anche l'articolo 19*a* capoverso 1bis LResp che disciplina attualmente la responsabilità in relazione ai sistemi UE dovrà menzionare l'ETIAS. Lo stesso vale anche per gli articoli 16*b* capoverso 1 e 16*c* capoverso 2 LSIP relativi all'ESP e al MID.

55 Decreto federale che approva e traspone nel diritto svizzero lo scambio di note tra la Svizzera e l'UE concernente il recepimento del regolamento (UE) 2018/1240 che istituisce il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (Sviluppo dell'acquis di Schengen), FF **2020** 2645.

Nel quadro dei dibattiti parlamentari concernenti il presente disegno, il Dipartimento federale di giustizia e polizia (DFGP) proporrà al Parlamento tali adeguamenti.

Alcune disposizioni del progetto ETIAS che sono attualmente oggetto di dibattito parlamentare dovranno essere ugualmente adeguate in virtù dell'interoperabilità. Si tratta nello specifico degli articoli 5 capoverso 1 lettera a^{bis}, 108*a*, 108*f* e 120*d* LStrI. Tali disposizioni saranno adeguate come segue:

La nota a piè di pagina di cui all'articolo 5 capoverso 1 lettera a^{bis} LStrI del progetto ETIAS andrà aggiornata, in quanto il regolamento (UE) 2018/1240 è modificato dal regolamento «IOP frontiere».

La sezione contenente le disposizioni relative a ETIAS (art. 108*a*–108*g*) deve essere adeguata alla nuova struttura prevista dal presente progetto (cfr. n. 7, commento al capitolo 14*a*). Di conseguenza, il titolo della sezione che precede l'articolo 108*a* come pure tutti i titoli delle sezioni seguenti dovranno essere rinumerati.

L'articolo 108*a* LStrI nel progetto ETIAS disciplina i dati contenuti in ETIAS. Alcuni di questi dati saranno ora registrati nel CIR. Un nuovo capoverso 3 dovrà pertanto precisare quali dati di identità e dei documenti di viaggio (art. 108*a* cpv. 1 lett. a nella versione del progetto ETIAS) sono registrati nel CIR. Le informazioni relative alle domande di autorizzazione ai viaggi ETIAS accolte o respinte e i dati dell'elenco di controllo saranno esclusi dai dati da registrare nel CIR e continueranno a essere memorizzati solo nell'ETIAS.

L'articolo 108*f* LStrI contenuto nella versione del progetto ETIAS che è attualmente al vaglio del Parlamento andrà anch'esso adeguato in virtù dell'interoperabilità. Questo articolo disciplina la comunicazione di dati ETIAS. Sarà aggiunto un nuovo capoverso 3. Infatti, poiché il CIR diventerà parte integrante dell'ETIAS, le disposizioni sulla comunicazione dei dati ETIAS si applicheranno anche ai dati ETIAS registrati nel CIR (dati di identità, dati dei documenti di viaggio e dati biometrici). Per la comunicazione dei dati ETIAS registrati nel CIR, il nuovo capoverso 3 conterrà pertanto un rinvio all'articolo 110*h*, che rimanda a sua volta all'articolo 40 dei regolamenti (UE) sull'interoperabilità. Tale disposizione è analoga a quella applicabile all'EES (art. 103*d* cpv. 3 LStrI del presente disegno).

Infine, il contenuto dell'articolo 120*d* capoverso 2 LStrI, nella versione sottoposta al Parlamento nel quadro del progetto ETIAS, dovrà essere integrato nel tenore dell'articolo 120*d* del presente disegno. In conclusione, tali articoli dovranno essere pertanto ancora adeguati in seguito alla votazione finale in merito al progetto ETIAS.

8.2 Coordinamento con la modifica della LStrI del 14 dicembre 2018 relativa all'attuazione delle norme procedurali e dei sistemi d'informazione

Un'eventuale necessità di coordinamento sussiste inoltre in relazione all'articolo 111 LStrI (Sistemi d'informazione per documenti di viaggio). Tale disposizione deve essere abrogata nell'ambito del progetto «Norme procedurali e sistemi

d'informazione»[56]. Diversamente da tutte le altre disposizioni di questo progetto, l'abrogazione dell'articolo 111 LStrI non è ancora entrata in vigore. La SEM infatti per un periodo transitorio dovrà ancora ricorrere necessariamente all'attuale sistema di rilascio di documenti di viaggio. Qualora l'articolo 111 LStrI non dovesse essere ancora abrogato al momento dell'entrata in vigore del decreto federale relativo all'interoperabilità, dovrà essere rinumerato dato che non ha motivo di figurare all'interno della nuova sezione «Comunicazione dei dati e responsabilità per il trattamento di dati».

8.3 Coordinamento con il progetto SIS

L'interoperabilità deve essere coordinata con la revisione in corso della LStrI e della LSIP nel quadro del progetto SIS. Attualmente il Parlamento sta esaminando il decreto federale concernente il SIS. Quest'ultimo dovrebbe essere adottato dal Parlamento in occasione della sessione autunnale o invernale del 2020. A prescindere che la presente modifica della LSIP entri in vigore successivamente o contestualmente al decreto federale concernente il SIS, l'articolo 16 LSIP, e nella fattispecie il capoverso 1 primo periodo, della versione francese deve essere adeguato conformemente alla versione contenuta nel presente disegno. Il capoverso 2 lettera b del presente disegno dovrà essere ripreso come lettera c nella versione del progetto SIS.

Infine, poiché il regolamento (UE) 2018/1861 è modificato dal regolamento «IOP frontiere», la nota a piè di pagina dell'articolo 68*a* capoverso 2 LStrI nella versione del progetto SIS è modificata di conseguenza.

8.4 Coordinamento con il progetto EES

Il decreto federale concernente l'EES[57] è stato approvato dal Parlamento il 21 giugno 2019. Il progetto contiene una modifica della LStrI in cui sono state introdotte nuove disposizioni relative al sistema d'informazione EES.

Le modifiche della LStrI previste dal presente progetto si basano sulle disposizioni della LStrI contenute nel decreto federale concernente l'EES, vista la loro forma definitiva in seguito all'approvazione del Parlamento.

Il decreto federale concernente l'interoperabilità riprende il contenuto del decreto federale concernente l'EES, aggiungendovi elementi fondamentali ai fini dell'interoperabilità (Sezione 2: Sistema di ingressi/uscite [EES] e controllo di confine automatizzato). Qualora il decreto federale concernente l'EES dovesse entrare in vigore simultaneamente a quello concernente l'interoperabilità, saranno le disposizioni di quest'ultimo a prevalere.

56 RU **2019** 1413

57 Decreto federale che approva e traspone nel diritto svizzero gli scambi di note tra la Svizzera e l'UE concernenti il recepimento delle basi legali per l'istituzione e l'uso del sistema di ingressi e uscite (EES) (regolamenti [UE] 2017/2226 e 2017/2225) (Sviluppo dell'acquis di Schengen), FF **2019** 3819.

9 Ripercussioni

9.1 Ripercussioni sulle finanze e sul personale della Confederazione

Per la Confederazione, il progetto avrà delle ripercussioni sulle finanze e sul personale sia nella fase di progettazione sia nell'applicazione dei regolamenti UE sull'interoperabilità a partire dall'entrata in funzione dell'interoperabilità. L'interoperabilità comporterà vantaggi considerevoli per la Confederazione e i Cantoni.

9.1.1 Ripercussioni sulle finanze e sul personale: fase di progettazione

I costi complessivi per la Confederazione derivanti dai progetti in materia di interoperabilità sono stimati a 21 milioni di franchi per l'intero periodo che va dal 2020 al 2025.

Costi dei progetti in materia di interoperabilità (in mio.)	Totale	2020	2021	2022	2023	2024	2025
Interoperabilità fedpol	**11,3**	2,9	3,1	1,4	1,5	1,2	1,2
Interoperabilità SEM	**7,7**	2,1	2,2	2,4	1,0		
Sviluppo IOP (SEM)	**2,0**					1,0	1,0
Totale	**21,0**	**5,0**	**5,3**	**3,8**	**2,5**	**2,2**	**2,2**

I progetti di fedpol e della SEM s'inseriscono all'interno di un credito d'impegno per lo sviluppo dell'acquis di Schengen/Dublino, che fa parte di un programma della Segreteria generale del DFGP (SG-DFGP). Il programma è gestito come progetto chiave TIC. Il decreto federale concernente il credito d'impegno[58] è stato approvato dal Consiglio nazionale il 21 dicembre 2019 e dal Consiglio degli Stati l'11 giugno 2020. Il fabbisogno di mezzi finanziari per questi progetti relativamente al periodo 2020–2022 ammonta complessivamente a 14,1 milioni di franchi. Di questa somma, 9,8 milioni rientrano nella prima tranche del credito d'impegno e sono coperti dai mezzi centrali TIC assegnati dalla Confederazione e da risorse proprie del DFGP. A partire dal 2023, il finanziamento di questi progetti dovrebbe essere garantito nel quadro della liberazione della seconda tranche del credito d'impegno.

Il recepimento e la trasposizione dell'interoperabilità determineranno anche ripercussioni sul piano tecnico. Un'ulteriore componente tecnica nazionale dovrebbe garantire il collegamento dei sistemi svizzeri all'ESP. Un client MID nazionale è inoltre indispensabile per procedere alla verifica dei collegamenti del MID (cfr. 5.1). Queste componenti sono messe a disposizione dal Centro Servizi informatici del DFGP (CSI-DFGP). I costi di sviluppo sono compresi nei costi di progetto elencati

58 Decreto federale dell'11 giugno 2020 concernente un credito d'impegno per lo sviluppo dell'acquis di Schengen/Dublino, FF **2020** 5745.

qui sopra. I requisiti tecnici sono specificati da eu-LISA. Alla luce degli sviluppi delle componenti dell'UE, è inoltre lecito attendersi che le componenti nazionali dovranno anch'esse subire adeguamenti. Tali modifiche saranno apportate dopo l'entrata in funzione dell'interoperabilità, prevista nel 2023, nell'ambito del progetto «Sviluppo IOP» della SEM. Per quest'ultimo progetto sono previsti costi pari a un milione di franchi rispettivamente per il 2024 e il 2025.

L'attuazione della fase di progettazione dovrebbe comportare per fedpol nel periodo tra il 2020 e il 2023 oneri in termini di personale pari a 2800 giorni/persona. La SEM stima invece tali oneri a 3960 giorni/persona. Le risorse di personale in questione saranno compensate internamente.

Per l'AFD, gli oneri supplementari per la direzione di progetto e i costi di sviluppo per l'adeguamento delle soluzioni per i controlli mobili e stazionari alle frontiere dovrebbero aggirarsi attorno a qualche milione di franchi. Allo stato attuale delle conoscenze, i costi si iscriveranno nel programma DaziT dell'AFD. Gli obblighi finanziari che ne derivano saranno computati sul credito globale del programma.

9.1.2 Ripercussioni sulle finanze e sul personale: entrata in funzione

Costi d'esercizio

Nel 2023 dovrebbero sorgere costi d'esercizio pari a 0,2 milioni di franchi e a partire dal 2024 due milioni di franchi ogni anno per la gestione delle due componenti di interoperabilità nazionali. Quest'ultimo importo è necessario per garantire l'estensione dell'interoperabilità ai sistemi nazionali e per la verifica dei collegamenti del MID. Sul piano nazionale, l'interoperabilità rappresenta un progetto che riguarda non solo aspetti organizzativi, ma implica anche la creazione e la gestione di componenti tecniche nazionali. Al momento della redazione del messaggio[59] concernente un credito d'impegno per l'attuazione dello sviluppo dell'acquis di Schengen/Dublino, la portata del progetto non era ancora nota, in quanto l'UE non aveva ancora fornito le pertinenti informazioni. Per tale ragione, i costi d'esercizio ricorrenti (annuali) derivanti dalle componenti di interoperabilità a partire dall'entrata in funzione di quest'ultima sono stimati a circa 2 milioni di franchi all'anno, in luogo degli 0,2 milioni di franchi menzionati nel messaggio concernente il credito d'impegno. Questa cifra si ricava dal confronto con il progetto EES, nell'ambito del quale il CSI-DFGP dovrà ugualmente mettere a disposizione e gestire due componenti nazionali, sostenendo costi d'esercizio di entità analoga. I mezzi finanziari necessari al funzionamento del sistema saranno precisati nella fase di progettazione e saranno richiesti nella misura desiderata nel quadro dell'allestimento del preventivo 2024.

Ripercussioni sul personale derivanti dalla verifica dei collegamenti del MID

[59] Messaggio del 4 settembre 2019 concernente un credito d'impegno per lo sviluppo dell'acquis di Schengen/Dublino, FF **2019** 5095.

L'entrata in funzione dell'interoperabilità nel 2023 determinerà un aumento dei riscontri positivi, rendendo così necessaria una loro successiva verifica manuale. I collegamenti del MID che presentano dati divergenti (contrassegnati in giallo) devono essere sempre verificati manualmente. I due regolamenti UE sull'interoperabilità stabiliscono che la verifica manuale dei collegamenti del MID debba essere eseguita dall'autorità che ha creato o aggiornato i dati che hanno generato un collegamento MID. Per la Svizzera tale compito incombe a fedpol, alla SEM, all'AFD, alle rappresentanze all'estero del Dipartimento federale degli affari esteri (DFAE) nonché alle autorità cantonali di polizia e migratorie. Un collegamento giallo MID è creato ad esempio quando un cittadino di uno Stato terzo segnalato nel SIS ai fini di un divieto d'entrata richiede un visto Schengen utilizzando un passaporto contraffatto. Le sue impronte digitali nel SIS e nel VIS risulteranno identiche, ma non i suoi dati di identità. Il rispettivo collegamento MID andrà pertanto verificato manualmente. A tal fine saranno necessari ulteriori accertamenti al fine di stabilire con esattezza l'identità della persona. Questa procedura consente, da un lato, di agevolare la mobilità di persone che viaggiano legalmente e, dall'altro, di individuare e prevenire, con l'ausilio della verifica manuale, le frodi d'identità. Per poter far fronte a questo nuovo compito supplementare, le autorità competenti necessitano di risorse di personale aggiuntive. Allo stato attuale delle conoscenze, si stima che le autorità svizzere saranno chiamate in futuro a verificare manualmente ogni anno circa 10 000 collegamenti gialli del MID. All'incirca il 60 per cento di questi collegamenti dovrebbero riguardare dati del SIS. Questi ultimi saranno verificati dall'Ufficio SIRENE di fedpol per conto dei Cantoni e di altre autorità. Circa il 40 per cento dei collegamenti gialli sarà invece trattato dalla SEM, dall'AFD, dal DFAE e dalle autorità cantonali di polizia e migratorie.

Dalla valutazione di diverse varianti organizzative è emerso che le autorità competenti in materia di migrazione dovrebbero essere sostenute nella verifica dei collegamenti del MID da un servizio centrale di esperti del MID (MES) gestito e finanziato dalla Confederazione. Il MES dovrebbe essere accorpato alla SEM. Quest'organo permetterà alle autorità competenti di ricevere sostegno nei casi complessi, evitando in tal modo che possano insorgere oneri supplementari nell'adempimento delle loro attività quotidiane. Al contempo, il MES intende fornire sostegno anche a quelle autorità che sono chiamate solo raramente a dover verificare un collegamento del MID e che non dispongono quindi delle pertinenti conoscenze specialistiche (p. es. le ambasciate svizzere all'estero). Questa forma di centralizzazione limitata consentirà di sfruttare le sinergie e di conseguire una riduzione dei costi. In qualità di centro di competenza, il MES garantirà sinergie sul piano della qualità raggruppando le conoscenze di diversi settori, il che permetterà di migliorare la qualità delle verifiche e rendere più fluidi i canali di comunicazione. All'interno del MES dovrebbe operare il personale dei diversi uffici federali competenti. L'organizzazione e la composizione dettagliata del MES saranno definite nella fase di progettazione. Il MES non sarà tuttavia autorizzato a verificare i collegamenti in modo autonomo. Dopo un primo esame del collegamento del MID, sarà infatti tenuto a trasmetterne i risultati all'autorità competente. Quest'ultima deciderà in seguito se le divergenze sono legittime o se si è dinanzi a una frode d'identità. I collegamenti del MID contenenti dati SIS dovranno essere sempre verificati

dall'Ufficio SIRENE Svizzera. Il fabbisogno supplementare in termini di personale è riportato nella tabella qui sotto.

Al momento dell'entrata in funzione dell'interoperabilità nel 2023, bisognerà disporre di personale appositamente formato. Il DFGP valuterà fino alla metà del 2021 quanti posti supplementari saranno necessari a partire dal 2023 tenendo conto della verifica in corso dei compiti all'interno del DFGP e delle derivanti compensazioni interne. Un eventuale fabbisogno supplementare in termini di personale sarà richiesto al Parlamento nel quadro del messaggio concernente il preventivo 2022 con piano integrato dei compiti e delle finanze.

Secondo una stima preliminare del DFGP, il fabbisogno supplementare di personale è ripartito nel modo seguente e sarà illustrato in modo dettagliato nei numeri seguenti:

Fabbisogno supplementare di personale (stima)

	A partire dal 2023
Equivalenti a tempo pieno (FTE)	
fedpol	11
SEM	6
AFD	1
DFAE	0,9
Cantoni (polizie cantonali e autorità migratorie)	1,1
Totale	**20**

Ripercussioni sul personale per fedpol

I collegamenti del MID concernenti le segnalazioni SIS devono essere verificati dall'Ufficio SIRENE. Questo tipo di verifica richiede talvolta accertamenti e consultazioni approfondite in Svizzera e con altri Stati Schengen. Lo sviluppo del SIS implica già attualmente per l'Ufficio SIRENE un termine per il trattamento di 12 ore e nuove categorie di segnalazioni. Per lo scambio di informazioni l'Ufficio SIRENE dovrà garantire un servizio a turni 24 ore su 24, sette giorni su sette. A tal fine, dovrà incrementare i propri effettivi nei turni di notte, nei fine settimana e nei giorni festivi.

La verifica dei collegamenti del MID concernenti segnalazioni SIS implica anche il controllo della corrispondenza dei dati biometrici. Il confronto dei dati biometrici sarà garantito 24 ore su 24, sette giorni su sette, dalla divisione Identificazione biometrica.

L'interoperabilità consentirà un confronto automatizzato tra i dati di polizia e i dati provenienti da altri sistemi d'informazione dell'UE. Le autorità di polizia disporranno pertanto sempre più spesso di informazioni rilevanti ai fini di polizia suscettibili

di sfociare in indagini. L'interoperabilità comporterà pertanto un incremento degli oneri in materia di coordinamento e preparazione per la Polizia giudiziaria federale.

Tutti i compiti descritti qui sopra genereranno nei settori interessati oneri supplementari cui non sarà possibile far fronte in assenza di risorse aggiuntive. Fedpol stima che con l'entrata in funzione dell'interoperabilità, il fabbisogno supplementare in termini di personale ammonterà a 11 FTE.

Ripercussioni sul personale per la SEM

Presso la SEM la verifica dei collegamenti del MID sarà di competenza dell'ambito direzionale Immigrazione e integrazione, all'interno del quale sono collocate le autorità della SEM competenti conformemente ai regolamenti UE. La verifica dei collegamenti del MID comporterà complessivamente per la SEM un fabbisogno supplementare in termini di personale pari a 5 FTE. Una parte di questi posti sarà destinata al MES che tratterà i collegamenti del MID complessi concernenti il settore della migrazione.

I compiti di gestione e sostegno sono già inclusi nei 5 FTE. Inoltre, la SEM dovrà inoltre assolvere compiti legati alla responsabilità in materia di applicazioni e prodotti concernenti le componenti tecniche nazionali.

Complessivamente, il fabbisogno supplementare di personale per il SEM ammonterà a 6 FTE.

Ripercussioni sul personale per l'AFD

Il presente sviluppo comporta per l'AFD ripercussioni sul piano finanziario, procedurale nonché in termini di personale. Occorre infatti, da un lato, apportare modifiche alle interfacce dei sistemi già esistenti e, dall'altro, realizzare diversi nuovi sistemi come l'ESP, obbligatorio per i controlli delle persone alle frontiere esterne di Schengen. Bisogna infine tener conto anche di eventuali modifiche collegate alla creazione di una piattaforma nazionale di consultazione (cfr. n. 9.2.2).

L'ESP determinerà modifiche ai processi operativi, in particolare per quanto riguarda l'individuazione di identità multiple e fittizie. Allo stato attuale si stima che l'incremento in materia di efficienza derivante da una maggiore automatizzazione e gli oneri risultanti dall'individuazione di identità fittizie si compenseranno. La verifica dei collegamenti del MID, comprese le misure di formazione e formazione continua, determineranno per l'AFD un modesto fabbisogno supplementare, che sarà compensato internamente.

Ripercussioni personali per la Direzione consolare e le rappresentanze svizzere all'estero (DFAE)

La Direzione consolare del DFAE supporta le rappresentanze all'estero nella fornitura di servizi consolari. Mette a loro disposizione strumenti di lavoro adatti allo scopo e coordina la collaborazione con i partner nazionali e internazionali. Le rappresentanze all'estero saranno responsabili della verifica dei collegamenti del MID, laddove i dati concernenti una domanda di visto presentata presso le loro sedi con-

ducano a un collegamento MID con i dati registrati in un altro sistema d'informazione dell'UE. Allo stato attuale delle conoscenze si stima che il fabbisogno supplementare di personale per la Direzione consolare e le rappresentanze all'estero possa essere compensato in seno al dipartimento. Il sostegno offerto dal MES permetterà di sgravare le rappresentanze all'estero nei casi complessi che necessitano di accertamenti più approfonditi.

9.2 Ripercussioni per i Cantoni

I regolamenti UE sull'interoperabilità permetteranno anche alle autorità cantonali di polizia e migratorie di disporre in qualsiasi momento di informazioni per loro rilevanti. I benefici previsti sono notevoli; tuttavia, non è escluso che possano insorgere determinati oneri supplementari per i Cantoni.

9.2.1 Ripercussioni sulle finanze e sul personale

L'interoperabilità consentirà anche alle autorità cantonali di polizia e migratorie di utilizzare in modo più efficace e mirato le informazioni a loro disposizione. Il rischio che le identità multiple non vengano individuate sarà ridotto, mentre aumenterà la probabilità di ottenere un riscontro positivo. È previsto che le autorità di polizia dei Cantoni e dei Comuni possano accedere ai dati contenuti nel CIR al fine di identificare le persone che si trovano nello spazio Schengen. Nel quadro della loro attività di prevenzione, indagine, accertamento e perseguimento del terrorismo o di altri reati gravi, le polizie cantonali potranno beneficiare dell'accesso concesso alle autorità di perseguimento penale. Tramite una consultazione nel CIR potranno infatti verificare se in uno dei sistemi d'informazione dell'UE sono registrati dati concernenti una determinata persona. Quale punto d'accesso centrale per le consultazioni da parte delle autorità di perseguimento penale in sistemi d'informazione non di polizia, fedpol è responsabile per la concessione, in un secondo momento, a tali autorità dell'accesso ai dati richiesti. Tale competenza, già prevista per il VIS, è ora estesa anche all'EES.

L'utilizzo dell'ESP durante i controlli alle frontiere esterne dello spazio Schengen diverrà obbligatorio. Oltre all'AFD, anche le autorità di polizia cantonali incaricate del controllo alle frontiere esterne di Schengen saranno interessate da tale misura. Nello specifico dovranno verificare i collegamenti del MID che concernono dati dell'EES. Questo nuovo compito genererà oneri supplementari. Il sostegno offerto dal MES permetterà di sgravare le autorità cantonali di polizia e migratorie nei casi complessi che necessitano di accertamenti più approfonditi.

Per la verifica dei collegamenti del MID, la Confederazione metterà a disposizione un client (componente nazionale). L'integrazione di questo client nei rispettivi sistemi cantonali sarà competenza dei Cantoni. Il collegamento dei sistemi nazionali di consultazione all'ESP richiederà anche modifiche tecniche ai sistemi cantonali di consultazione. Tali modifiche sono anch'esse di competenza cantonale. Altre modifiche sono ipotizzabili, sebbene al momento non possano essere ancora definite con precisione. I Cantoni saranno coinvolti per tempo nei gruppi di lavoro al fine di garantire una stretta collaborazione nella fase di realizzazione.

9.2.2 Piattaforma nazionale di consultazione

L'interoperabilità a livello dell'UE e la mozione Eichenberger[60] hanno sollecitato la Svizzera a rendere i sistemi d'informazione cantonali interoperabili tra loro nonché con quelli della Confederazione. La piattaforma nazionale di consultazione è un progetto condotto dai Cantoni separatamente dal recepimento dei regolamenti UE sull'interoperabilità. In linea di massima, i Cantoni sono responsabili della tutela della sicurezza e dell'ordine pubblici nei rispettivi territori. È a essi quindi che è affidata in via prioritaria la competenza in materia di polizia. La Confederazione assolve invece determinati compiti di polizia in ambiti specifici. La piattaforma nazionale di consultazione dovrebbe pertanto consentire di sfruttare le sinergie tra i sistemi d'informazione nazionali e cantonali e di presentare agli utenti i risultati delle ricerche in maniera più chiara e uniforme. Visti gli evidenti benefici e la fattibilità di una piattaforma nazionale di consultazione, nel quadro dell'armonizzazione dell'informatica di polizia svizzera (Centro di competenze per le tecniche di polizia e informatiche) è stato avviato un progetto sul tema. Il progetto prevede una gestione centralizzata della piattaforma di consultazione; la gestione dei dati e dei sistemi d'informazione dovrebbe invece restare di competenza delle rispettive autorità. I diritti di accesso delle autorità resterebbero immutati (cfr. commento all'art. 16*b* cpv. 5 D-LSIP). Poiché il progetto concernente la realizzazione tecnica della piattaforma nazionale di consultazione è stato appena avviato, le specificazioni tecniche sono attualmente ancora troppo vaghe per poterne dedurre una necessità d'intervento legislativo. La base giuridica relativa alla piattaforma sarà presentata in un secondo momento nel quadro di un progetto separato.

9.3 Ripercussioni in altri settori

Nei settori dell'economia, della società e dell'ambiente non sono attese ripercussioni dirette. L'interoperabilità contribuirà ad accrescere la sicurezza nello spazio Schengen, con ripercussioni positive anche per l'economia e la società.

10 Aspetti giuridici

10.1 Costituzionalità

Gli scambi di note tra la Svizzera e l'UE concernenti il recepimento dei regolamenti UE sull'interoperabilità si basano sull'articolo 54 capoverso 1 Cost., secondo cui la Confederazione è competente per gli affari esteri. L'articolo 184 capoverso 2 Cost. conferisce al Consiglio federale la facoltà di firmare e ratificare trattati internazionali. Secondo l'articolo 166 capoverso 2 Cost., l'Assemblea federale approva i trattati internazionali, esclusi quelli la cui conclusione è di competenza del Consiglio federale in virtù della legge o di un trattato internazionale. Nel presente caso il Consiglio federale non può invocare tale competenza (cfr. art. 7*a* cpv. 1 e 2 della legge del 21 marzo 1997[61] sull'organizzazione del Governo e dell'Amministrazione [LOGA]

60 Mozione 18.3592, Scambio di dati di polizia su scala nazionale.
61 RS **172.010**

nonché art. 24 cpv. 2 della legge del 13 dicembre 2002[62] sul Parlamento [LParl]). Ne deriva che l'Assemblea federale è competente per l'approvazione di entrambi gli scambi di note.

10.2 Compatibilità con altri impegni internazionali della Svizzera

Con il recepimento dei due sviluppi dell'acquis di Schengen, la Svizzera adempie i propri impegni derivanti dall'AAS. Contribuisce inoltre all'applicazione uniforme dei sistemi d'informazione Schengen/Dublino. Il recepimento dei due regolamenti UE e le modifiche legislative che ne derivano sono pertanto compatibili con gli impegni internazionali della Svizzera.

10.3 Forma dell'atto

Il recepimento dei due regolamenti UE non implica l'adesione della Svizzera a un'organizzazione di sicurezza collettiva o a una comunità sopranazionale. Il decreto federale concernente l'approvazione dei pertinenti scambi di note non sottostà pertanto al referendum obbligatorio di cui all'articolo 140 capoverso 1 lettera b Cost.

Secondo l'articolo 141 capoverso 1 lettera d numero 3 Cost., i trattati internazionali sottostanno a referendum facoltativo se comprendono disposizioni importanti che contengono norme di diritto o per l'attuazione dei quali è necessaria l'emanazione di leggi federali. Secondo l'articolo 22 capoverso 4 LParl, contengono norme di diritto le disposizioni che, in forma direttamente vincolante e in termini generali ed astratti, impongono obblighi, conferiscono diritti o determinano competenze. Sono considerate importanti le disposizioni che, nella legislazione nazionale in base all'articolo 164 capoverso 1 Cost. sono emanate sotto forma di legge federale.

I presenti regolamenti UE recepiti mediante scambio di note comprendono disposizioni importanti che contengono norme di diritto quali i diritti di consultazione e di accesso ai sistemi d'informazione. Il recepimento richiede inoltre modifiche a livello di legge (cfr. n. 6.2). Il presente decreto federale sottostà pertanto a referendum facoltativo secondo l'articolo 141 capoverso 1 lettera d numero 3 Cost.

L'Assemblea federale approva mediante decreto federale i trattati internazionali sottostanti al referendum (art. 24 cpv. 3 LParl).

In virtù dell'articolo 141*a* capoverso 2 Cost., se il decreto di approvazione di un trattato internazionale sottostà a referendum facoltativo, l'Assemblea federale può includere nel decreto le modifiche legislative necessarie per l'attuazione del trattato.

Le disposizioni legali proposte dal disegno traspongono nel diritto svizzero le basi legali concernenti l'interoperabilità tra i sistemi d'informazione dell'UE e derivano direttamente dagli obblighi ivi contenuti. Il disegno dell'atto normativo può dunque essere incluso nel decreto di approvazione.

62 RS **171.10**

10.4 Subordinazione al freno alle spese

Il presente progetto non prevede nuovi crediti d'impegno o limiti di spesa implicanti spese uniche di oltre 20 milioni di franchi. Il progetto non è pertanto subordinato al freno alle spese (art. 159 cpv. 3 lett. b Cost.).

Abbreviazioni

AAD	Accordo del 26 ottobre 2004 tra la Confederazione Svizzera e la Comunità europea relativo ai criteri e ai meccanismi che permettono di determinare lo Stato competente per l'esame di una domanda di asilo introdotta in uno degli Stati membri o in Svizzera; RS *0.142.392.68*
AAS	Accordo del 26 ottobre 2004 tra la Confederazione svizzera, l'Unione europea e la Comunità europea, riguardante l'associazione della Svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen, RS *0.362.31*
AFD	Amministrazione federale delle dogane
ASM	Associazione dei servizi cantonali di migrazione
CIR	Archivio comune di dati di identità
Commissione LIBE	Commissione del Parlamento europeo che si occupa di questioni correlate a temi quali le libertà civili, la giustizia e gli affari interni
COREPER	Comitato dei rappresentanti permanenti dei governi degli Stati membri dell'UE
Cost.	Costituzione federale, RS *101*
CP	Codice penale svizzero, RS *311.0*
CSI-DFGP	Centro servizi informatici del DFGP
C-VIS	Sistema centrale d'informazione visti
DFAE	Dipartimento federale degli affari esteri
DFGP	Dipartimento federale di giustizia e polizia
ECRIS-TCN	Sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di Paesi terzi (*European Criminal Records Information System on Third-Country Nationals*).
EES	Sistema europeo di ingressi/uscite
ESP	Portale di ricerca europeo

ETIAS	Sistema europeo di informazione e autorizzazione ai viaggi
eu-LISA	Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia
Eurodac	Banca dati centrale dell'UE contenente le impronte digitali delle persone che hanno presentato una domanda d'asilo in uno Stato Dublino o che sono state arrestate nel tentativo di entrare illegalmente
Europol	Ufficio europeo di polizia
fedpol	Ufficio federale di polizia
FTE	Equivalenti a tempo pieno (*Full time equivalent*)
IFPDT	Incaricato federale della protezione dei dati e della trasparenza
Interpol	Organizzazione internazionale di polizia criminale (*International Criminal Police Organization*)
LParl	Legge del 13 dicembre 2002 sul Parlamento, RS *171.10*
LPD	Legge federale del 19 giugno 1992 sulla protezione dei dati, RS *235.1*
LPDS	Legge del 28 settembre 2018 sulla protezione dei dati in ambito Schengen, RS *235.3*
LResp	Legge del 14 marzo 1958 sulla responsabilità, RS *170.32*
LSIP	Legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione, RS *361*
LSISA	Legge federale del 20 giugno 2003 sul sistema d'informazione per il settore degli stranieri e dell'asilo, RS *142.51*
LStrI	Legge federale del 16 dicembre 2005 sugli stranieri e la loro integrazione, RS *142.20*
MES	Servizio centrale di esperti
MID	Rilevatore di identità multiple
NUI	Interfaccia nazionale di collegamento tra i sistemi nazionali degli Stati Schengen e le componenti centrali dell'UE (*National Uniform Interface*)
ORBIS	Sistema nazionale visti
OSAR	Organizzazione svizzera di aiuto ai rifugiati
PSS	Partito socialista svizzero
Regolamenti UE	Regolamento (UE) 2019/817 (regolamento «IOP

sull'interoperabilità	frontiere») e regolamento (UE) 2019/818 (regolamento «IOP polizia»)
Regolamento «IOP frontiere»	Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, GU L 135 del 22.5.2019, pag. 27
Regolamento «IOP polizia»	Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816, GU L 135 del 22.5.2019, pag. 85
sBMS	Servizio comune di confronto biometrico
SEM	Segreteria di Stato della migrazione
SIC	Servizio delle attività informative della Confederazione
SIS	Sistema d'informazione Schengen
SLTD	Banca dati di Interpol sui documenti di viaggio rubati e smarriti (*Stolen and Lost Travel Documents Database*)
TDAWN	Banca dati di Interpol sui documenti di viaggio associati a segnalazioni (*Travel Documents Associated with Notices Database*)
Ufficio SIRENE	Servizio nazionale di contatto per tutte le ricerche compiute con l'ausilio del SIS (SIRENE = *Supplementary Information Request at the National Entries*)
USS	Unione sindacale svizzera
VIS	Sistema di informazione visti