19.xxx

Rapporto esplicativo

sul recepimento e la trasposizione nel diritto svizzero delle basi legali concernenti la realizzazione dell'interoperabilità tra i sistemi d'informazione dell'UE nel settore delle frontiere, della migrazione e della polizia (regolamenti [UE] 2019/817 e [UE] 2019/818)

«Sviluppi dell'acquis di Schengen»

del …

Compendio

L'interoperabilità renderà possibile lo scambio d'informazioni tra i diversi sistemi d'informazione UE. Con un'unica interrogazione, le autorità di controllo delle frontiere, migratorie e di perseguimento penale potranno ottenere in futuro ampie informazioni su una persona sottoposta a controllo. L'interoperabilità intende migliorare la sicurezza nello spazio Schengen, rendere più efficienti i controlli alle frontiere esterne e contribuire alla gestione della migrazione irregolare. Il presente rapporto illustra le misure giuridiche necessarie ai fini del recepimento e della trasposizione dei regolamenti UE sull'interoperabilità e fornisce una panoramica sulle 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 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 eventuali sinergie. Vi è pertanto il rischio che informazioni importanti possano essere ignorate. Con l'interoperabilità i sistemi d'informazione dell'UE sono collegati in modo tale da rendere più efficace ed efficiente l'utilizzo delle informazioni disponibili. In futuro sarà infatti possibile effettuare un'interrogazione simultanea di diversi sistemi d'informazione. L'interoperabilità consente in particolare di individuare i collegamenti tra i dati. Per contro, i diritti di accesso delle autorità ai singoli sistemi restano immutati.

Entrambi i regolamenti UE sull'interoperabilità sono stati notificati alla Svizzera il 21 maggio 2019 come sviluppi dell'acquis di Schengen. Con l'Accordo di associazione alla normativa di Schengen, la Svizzera si è impegnata a recepire tutti i nuovi sviluppi dell'acquis di Schengen. La Svizzera ha quindi due anni di tempo per creare le basi giuridiche per la trasposizione dei regolamenti UE sull'interoperabilità.

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 permette inoltre il confronto automatizzato di dati biometrici di una persona, la raccolta all'interno di un archivio comune di dati personali e biometrici di cittadini di Paesi terzi e introduce nuove possibilità per risalire alla vera identità di persone che sono registrate in diversi sistemi d'informazioni sotto falsa identità o con identità multiple.

In Svizzera la trasposizione di entrambi i regolamenti UE richiede un adeguamento a livello di leggi federali e del relativo diritto d'esecuzione. Tale trasposizione comporta oneri supplementari in termini finanziari e di personale per la Confederazione e i Cantoni. I sistemi e i processi esistenti in Svizzera devono essere inoltre adeguati per poter sfruttare a pieno le possibilità offerte dall'interoperabilità. Al contempo sarà messo a disposizione uno strumento di ricerca nazionale allo scopo di migliorare l'interoperabilità tra i sistemi d'informazione nazionali e cantonali e di collegare questi ultimi al portale di ricerca europeo.

Indice

Rapporto esplicativo

1 Situazione iniziale

1.1 Necessità di intervento e obiettivi

Con l'accordo del 26 ottobre 2004[1] 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 (AAS), la Svizzera si è impegnata a recepire di principio tutti i nuovi sviluppi dell'acquis di Schengen (art. 2 par. 3 e 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'Unione europea (UE) e la trasmissione di una nota di risposta da parte della Svizzera.

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

- il regolamento (UE) 2019/817[2] concernente il settore delle frontiere e dei visti (di seguito regolamento «IOP frontiere»); e

- il regolamento (UE) 2019/818[3] concernente il settore della cooperazione di polizia e giudiziaria, asilo e migrazione (di seguito regolamento «IOP polizia»).

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 eventuali sinergie non possono dunque essere sfruttate. Vi è pertanto il rischio che, non potendo consultare i singoli sistemi d'informazione, le autorità ignorino le informazioni importanti ivi contenute così come eventuali correlazioni. L'esempio qui di seguito evidenzia un'attuale lacuna in materia di sicurezza e illustra come potrà essere colmata in futuro grazie all'interoperabilità:

Un criminale è segnalato in Svizzera nel Sistema d'informazione Schengen (SIS) ai fini di un divieto d'entrata ed è stato allontanato nel suo Paese d'origine. La stessa persona richiede un visto presso l'ambasciata di un altro Stato Schengen servendosi di una falsa identità. Sebbene le sue impronte digitali siano registrate nel sistema

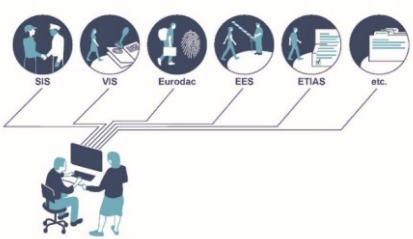
1 RS **0.362.31**

2 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.

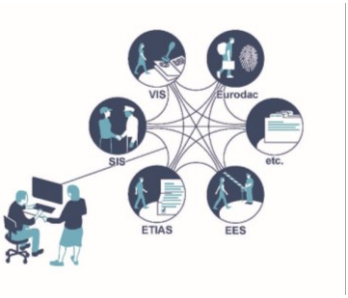
3 Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio del 20 maggio 2019 che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862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

d'informazione visti (VIS), queste ultime non sono 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) e di identificare i criminali che utilizzano false identità. Tramite il portale comune di ricerca europeo (ESP) potranno così essere consultati simultaneamente tutti i sistemi d'informazione (nel caso in questione il SIS e il VIS) effettuando un'unica interrogazione.



Senza interoperabilità ciascun sistema deve essere consultato separatamente.[4]



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

L'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. Tramite un'unica interrogazione, le autorità che hanno accesso ai sistemi interessati potranno 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 quello di permettere alle autorità di avere costantemente a disposizione tutte le informazioni essenziali affinché, come nel caso illustrato poc'anzi, non venga ad esempio rilasciato un visto a un criminale. A tal fine, l'UE ha approvato due regolamenti. Oltre alla creazione del portale ESP, con l'interoperabilità in futuro sarà possibile confrontare automaticamente anche i dati biometrici di una persona (impronte digitali e immagini del viso) con i dati registrati in altre banche dati. I dati d'identità e dei documenti di viaggio di cittadini di Stati terzi saranno inoltre registrati in una banca dati comune. Con entrambi i regolamenti UE sarà infine possibile rilevare con maggiore efficacia le identità multiple e le frodi di identità. Tramite l'interoperabilità non sono rilevati nuovi dati, bensì sono semplicemente

[4] Per «ecc.» s'intendono i sistemi d'informazione e le banche dati alle quali la Svizzera non ha attualmente accesso, ma per i quali sta attualmente valutando un eventuale accesso (ECRIS-TCN) o ai quali auspica accedere (dati Europol e banche dati Interpol).

aggiunte nuove funzioni agli attuali e futuri sistemi d'informazione. Per le autorità non vi sarà alcun cambiamento per quanto riguarda gli attuali diritti di accesso ai sistemi 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 essenziali 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 attuali lacune 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. Le informazioni disponibili potranno infatti essere utilizzate in modo più efficiente e mirato, apportando un importante valore aggiunto al lavoro delle autorità di controllo delle frontiere, migratorie e di perseguimento penale.

Il 21 maggio 2019 i due regolamenti UE sono stati notificati alla Svizzera come sviluppi dell'acquis di Schengen. Il 14 giugno 2019, il Consiglio federale ha approvato gli scambi di note concernenti il recepimento dei regolamenti UE, con riserva di approvazione parlamentare. Le rispettive note di risposta sono state trasmesse all'UE il 19 giugno 2019. L'obiettivo del presente avamprogetto è quello di recepire entro i termini prestabiliti gli sviluppi dell'acquis di Schengen e di creare le necessarie basi giuridiche per la relativa trasposizione.

1.2 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 giugno 2018. Le discussioni sono state particolarmente intense, soprattutto per quanto riguarda i temi seguenti:

- Attuazione: oltre alle ripercussioni finanziarie per gli Stati Schengen, sono state trattate le conseguenze dell'implementazione 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 alle frontiere esterne.
- 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[5].

5 SIRENE è l'acronimo di «Supplementary Information Request at the National Entries». Ciascuno Stato partecipante a Schengen dispone di un ufficio nazionale operativo 24 ore su 24, competente per lo scambio di informazioni e il coordinamento della procedura da adottare 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 da tale problematica sono soprattutto il Regno Unito e l'Irlanda, i quali essendo sprovvisti dell'accesso al SIS non possono usufruire della possibilità di rilevare le identità multiple, ma anche la Svizzera e altri Stati associati per via dell'accesso limitato ai dati Europol o del mancato accesso al sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di Paesi terzi (ECRIS-TCN).

Il 14 giugno 2018, il COREPER[6] ha definito le direttive negoziali per il trilogo con il Parlamento europeo. Sulla base degli adeguamenti apportati al testo di compromesso originario, il COREPER ha approvato nuovamente i testi modificati il 12 settembre 2018 e ha affidato il mandato negoziale per il trilogo. Il 15 ottobre 2018, la commissione LIBE[7] del Parlamento europeo ha approvato la sua relazione. Il trilogo si è protratto da ottobre 2018 a febbraio 2019 ed è stato accompagnato da incontri tecnici e riunioni dei relatori del Consiglio «Giustizia e affari interni» (GAI). I negoziati in sede di trilogo erano incentrati su altri temi rispetto a quelli affrontati a livello di esperti, ad esempio l'accesso a un archivio comune di dati di identità a scopo di identificazione o di perseguimento penale o l'obbligo di informazione degli Stati tramite portale web. La base giuridica che consenta l'interrogazione delle banche dati Interpol come parte dell'interoperabilità era ed è tuttora oggetto di discussioni. Le questioni ancora in sospeso saranno disciplinate in un accordo tra l'UE e Interpol. Gli esperti 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.

In occasione dell'ultimo trilogo del 5 febbraio 2019, la presidenza rumena del Consiglio e i rappresentanti del Parlamento europeo hanno raggiunto un accordo sulle due proposte di regolamento. Entrambi i testi sono stati approvati il 13 febbraio 2019 dal COREPER e il 19 febbraio 2019 dalla commissione LIBE del Parlamento europeo. 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.

1.3 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.

6 Comitato composto dai rappresentanti permanenti dei governi degli Stati membri dell'UE, responsabile della preparazione dei lavori del Consiglio dell'UE.
7 Commissione del Parlamento europeo che si occupa di questioni correlate a temi quali le libertà civili, la giustizia e gli affari interni.

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. 7.1 del presente rapporto esplicativo). 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[8]).

In base alla data di notifica da parte dell'UE (21 maggio 2019), il termine per recepire e trasporre i regolamenti UE scade dunque il 21 maggio 2021. Tuttavia il normale termine di due anni sarà prorogato in modo pragmatico se l'attuazione dell'atto nell'ambito dello spazio Schengen è prevista in una data successiva. È il caso di sin-

8 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.**

gole componenti centrali dei regolamenti UE sull'interoperabilità, la cui messa in funzione è prevista in un momento successivo e la cui completa trasposizione non avverrà prima del 2023.

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

Il presente avamprogetto non è annunciato esplicitamente né nel messaggio del 27 gennaio 2016[9] sul programma di legislatura 2015–2019 né nel decreto federale del 14 giugno 2016[10] sul programma di legislatura 2015–2019.

Il presente recepimento degli sviluppi dell'acquis di Schengen contribuisce, tuttavia, all'attuazione dell'obiettivo 4 nel quadro dell'indirizzo politico 1 così come degli obiettivi 13-15 nel quadro dell'indirizzo politico 3 della legislatura 2015-2019. Grazie all'utilizzo corretto 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 interne ed esterne alla propria sicurezza e disporre degli strumenti necessari per fronteggiarle in modo efficace. L'interoperabilità contribuisce a raggiungere tali obiettivi poiché colma le attuali lacune in materia di sicurezza e permette l'esecuzione di controlli più efficaci alle frontiere esterne.

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 d'informazione dell'UE. Non appena saranno disponibili i piani di gestione dei progetti e il rapporto sui rischi e sulla qualità relativo ai progetti in questione, il Consiglio federale libererà la seconda tranche del credito d'impegno per il «Perfezionamento Schengen/Dublino».

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

2 Punti essenziali dei regolamenti UE

2.1 Panoramica

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:

9 FF **2016** 909
10 FF **2016** 1039

- 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), i dei documenti di viaggio o biometrici di cittadini di Stati terzi agevolandone così l'identificazione;
- 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 (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 per entrata illegale;
- il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di Paesi terzi (ECRIS-TCN), un sistema elettronico volto allo scambio di informazioni 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 l'autorizzazione ai viaggi prima di entrare nello spazio Schengen;
- i dati Europol; 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 ai sistemi d'informazione SIS, VIS, Eurodac, EES ed ETIAS, i quali fanno tutti parte dell'acquis di Schengen. Il regolamento EES e il regolamento ETIAS sono stati notificati alla Svizzera nel 2018 come sviluppi dell'acquis di Schengen. La Svizzera ha inoltre tempo fino a novembre 2020 per recepire e trasporre gli sviluppi del Sistema d'informazione Schengen (SIS) che prevedono nuove possi-

bilità 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.

L'ECRIS-TCN non rappresenta invece uno sviluppo dell'acquis di Schengen, motivo per cui la Svizzera non vi ha per ora accesso[11]. Nei regolamenti UE si parla pertanto di interoperabilità dei «sistemi d'informazione dell'UE». Nel presente rapporto, tale formulazione è utilizzata per i numeri 1-3 nonché 6 e 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[12]. Sono in corso discussioni 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[13] sugli stranieri e la loro integrazione (LStrI) e nella legge federale del 13 giugno 2008[14] 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.

L'interoperabilità è disciplinata nell'UE all'interno di due regolamenti. 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»). Il motivo per cui è stato deciso di disciplinare l'interoperabilità in due regolamenti distinti è riconducibile al fatto che le disposizioni riguardano Paesi che presentano un grado diverso di partecipazione a Schengen. I sistemi VIS, EES ed ETIAS riguardano ad esempio componenti dell'acquis di Schengen ai quali l'Irlanda e il Regno Unito non partecipano. In virtù della sua partecipazione all'acquis di Schengen, la Svizzera è tenuta a recepire entrambi i regolamenti UE, i quali di fatto coincidono salvo poche disposizioni.

2.2 Entrata in vigore 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. La Commissione europea deciderà infatti 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

[11] La Svizzera sta attualmente valutando se partecipare all'ECRIS-TCN.
[12] In base agli articoli 8 e 9 dell'accordo del 24 settembre 2004 tra la Confederazione svizzera e l'Ufficio europeo di polizia (RS **0.362.2**), la Svizzera può richiedere a Europol di trasmettere dati registrati nel sistema d'informazione di Europol (EIS). La Svizzera si impegna al fine di ottenere un accesso diretto ai dati di Europol.
[13] RS **142.20**
[14] RS **361**

«IOP polizia»). Il presupposto per l'entrata in funzione delle singole componenti centrali è ad esempio l'avvenuto completamento del collaudo generale in collaborazione con gli Stati Schengen e le agenzie dell'UE responsabili delle componenti in questione. 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 il 2021, il CIR entro il 2022 e l'ESP così come il MID entro il 2023. Sono inoltre previste diverse fasi transitorie prima che le singole componenti centrali possano effettivamente entrare in funzione.

A prescindere da ciò, alcune disposizioni di entrambi i regolamenti UE sull'interoperabilità sono già applicabili dall'11 giugno 2019. Si tratta di norme rilevanti ai fini della fase di sviluppo. Esse sono destinate in primo luogo all'agenzia dell'UE eu-LISA, alla quale è affidata la responsabilità dello sviluppo delle diverse componenti centrali. Anche le basi giuridiche per l'adozione dei diversi atti di esecuzione tramite i quali la Commissione europea disciplinerà in maniera più precisa determinati aspetti, sono già entrate in vigore a giugno 2019. In tale contesto, la Svizzera ritiene che non vi sia una «particolare urgenza» che richieda l'applicazione provvisoria di entrambi gli scambi di note ai sensi dell'articolo 7*b* della legge del 21 marzo 1997[15] sull'organizzazione del Governo e dell'Amministrazione (LOGA).

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 diventa applicabile. L'integrazione di Eurodac nel quadro dell'interoperabilità è tuttavia prevista. Per tale motivo si fa menzione dell'Eurodac anche nel numero 3. Non sono, tuttavia, ancora disponibili disposizioni concrete. La trasposizione nel diritto svizzero avverrà pertanto soltanto con il recepimento del nuovo regolamento Eurodac.

3 Contenuto dei regolamenti UE

Qui di seguito si intende fornire una panoramica sul contenuto dei due regolamenti UE ponendo particolare enfasi sulle quattro componenti centrali. Le ulteriori novità che hanno implicazioni anche per la Svizzera sono illustrate nel numero 3.2. 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 3 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. Soltanto dalla fine del capo VIII, i due regolamenti UE presentano alcune differenze che saranno di volta in volta segnalate tramite esplicito rimando.

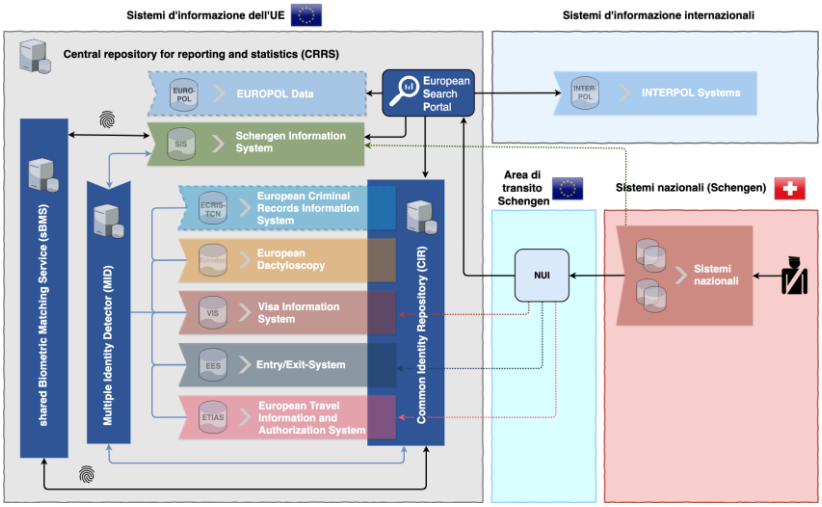
[15] RS **172.010**

3.1 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 più efficace. 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 reciproco. 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, ma anche i dati contenuti nel CIR, dove sono raccolti e archiviati i dati d'identità, dei documenti di viaggio o biometrici di tutti i cittadini di Stati terzi registrati in uno dei sistemi d'informazione dell'UE non di polizia. Poiché i dati registrati nel SIS non sono integrati nel CIR, occorre l'interfaccia MID destinata a rilevare le identità multiple nell'ambito del CIR nonché tra il CIR e il SIS. 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 tra loro 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 UE e le componenti nazionali tramite la NUI. Nei numeri seguenti è illustrata ciascuna componente centrale dell'interoperabilità.



3.1.1 Portale di ricerca europeo (capo II)

La creazione del portale di ricerca europeo («ESP») rappresenta un punto centrale dell'interoperabilità. Tale portale 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 oppure ECRIS-TCN), al CIR e al MID, ai dati Europol e alle banche dati Interpol se il diritto dell'UE o il diritto nazionale disciplinano i pertinenti diritti di accesso ai rispettivi sistemi e/o alle componenti centrali. 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, 21 e 22 (per le interrogazioni del CIR si veda la spiegazione dettagliata al n. 3.1.2). Potranno ugualmente impiegare l'ESP per consultare il SIS centrale (C-SIS)[16] nonché i dati Europol e le banche dati Interpol. Per le autorità degli Stati Schengen ciò non costituisce, tuttavia, un obbligo. I servizi dell'UE sono invece tenuti a effettuare le interrogazioni nel C-SIS tramite ESP.

16 Le interrogazioni tramite l'ESP riguardano sempre il SIS centrale, che si trova a Strasburgo. Non sono eseguite interrogazioni nelle parti nazionali.

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. I profili sono riesaminati da eu-LISA in cooperazione con gli Stati Schengen, almeno una volta all'anno, e aggiornati se necessario.

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 l'EES, l'ETIAS, il VIS, il SIS, l'Eurodac, l'ECRIS-TCN, il 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 di 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 (v. n. 3.1.3 in merito all'art. 20). In caso di interrogazioni del CIR ai sensi dell'articolo 22, le autorità di perseguimento penale possono visualizzare unicamente se i dati sono presenti in un sistema d'informazione. L'accesso deve essere richiesto separatamente (v. n. 3.1.3 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)

eu-LISA e gli Stati Schengen sono tenuti a conservare le registrazioni delle interrogazioni effettuate tramite l'ESP. 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, 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 UE «IOP frontiere» e l'articolo 63 «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.

3.1.2 Servizio comune di confronto biometrico (capo III)

Il servizio comune di confronto biometrico («sBMS»[17]) consente di effettuare interrogazioni con dati biometrici trasversalmente in più sistemi di informazione dell'UE (art. 12).

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

L'sBMS conserva i template biometrici[18], che ottiene dai dati biometrici provenienti dall'EES, dal VIS e dall'ECRIS-TCN nonché in futuro dall'Eurodac. 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 effettive registrazioni 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 di cui ai regolamenti UE sull'interoperabilità nonché ai regolamenti UE sui singoli sistemi.

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 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 al numero 3.1.1 in merito all'articolo 10 si applicano per analogia.

3.1.3 Archivio comune di dati di identità (capo IV)

È istituito un archivio comune di dati di identità («CIR») che, per ciascuna persona registrata nell'EES, nel VIS, nell'ETIAS, nell'Eurodac o nell'ECRIS-TCN, crea un

[17] Nei regolamenti UE è utilizzata la sigla «BMS»: poiché nel diritto svizzero è già in uso e ha un significato diverso, al fine di evitare confusioni si è deciso di utilizzare la sigla «sBMS».
[18] Si tratta di rappresentazioni matematiche ottenute estraendo elementi dai dati biometrici, limitatamente alle caratteristiche necessarie per effettuare identificazioni e verifiche (art. 4 par. 12).

fascicolo individuale, al fine di agevolare la corretta identificazione delle persone registrate in uno dei sistemi d'informazione dell'UE di cui sopra. 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 della sua architettura tecnica complessa, 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 in un secondo momento anche dall'Eurodac. La conservazione dei dati è effettuata tramite separazione per logica in base al sistema di 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. I diritti di accesso delle autorità al CIR si applicano conformemente al diritto nazionale, agli strumenti giuridici che disciplinano i sistemi di informazione dell'UE e ai rispettivi diritti di accesso previsti dai regolamenti UE sull'interoperabilità ai fini degli articoli 20, 21 e 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. 3.1.4) 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 i dati relativi all'identità nel CIR tramite un'interrogazione nell'ESP allo scopo di identificare la persona in questione. 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. Un'interrogazione nel CIR ai fini di identificazione non è autorizzata 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 consultare tali dati 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 v. n. 3.1.4). 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 designate da ciascun Paese conformemente alle basi giuridiche relative ai singoli sistemi, non hanno 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 da ciascun Paese.

Con l'interoperabilità l'accesso delle autorità di perseguimento penale 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 persona sono presenti in uno dei sistemi quali EES, ETIAS, VIS o Eurodac), il CIR segnala alle autorità competenti in quale sistema d'informazione dell'UE sono conservati i dati. Le autorità designate o Europol richiede in seguito il pieno accesso ad almeno uno dei sistemi di informazione dai quali è emerso un riscontro positivo. Ciò implica per le autorità designate la presentazione di una richiesta presso un punto di accesso centrale. Il pieno accesso ai dati contenuti nell'EES, nel VIS o nell'ETIAS o nell'Eurodac è 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 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

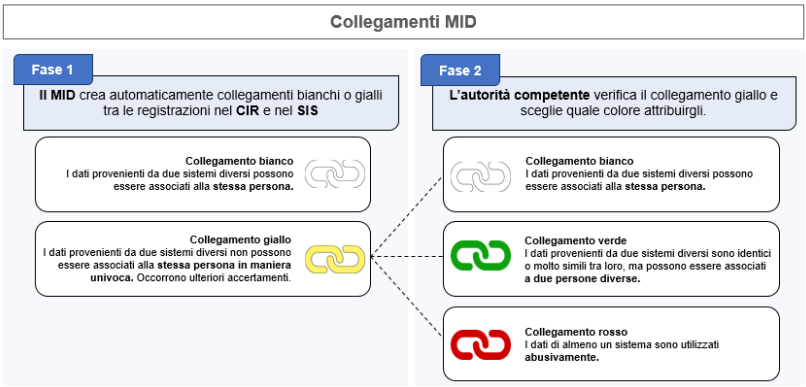
per il tempo in cui i dati corrispondenti sono conservati in almeno uno dei sistemi d'informazione dell'UE.

Registrazioni (art. 24)

eu-LISA conserva le registrazioni di tutte le operazioni di trattamento dei dati e le interrogazioni effettuate nel CIR. Ciascuno Stato Schengen deve conservare le registrazioni relative alle interrogazioni del CIR ai sensi degli articoli 20, 21 e 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 al numero 3.1.1 in merito all'articolo 10 si applicano per analogia.

3.1.4 Rilevatore di identità multiple (capo V)

Il rilevatore di identità multiple («MID») è la quarta componente centrale. Essa contribuirà a individuare persone che utilizzano più identità o identità false con 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 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. Ciò significa che queste ultime sono tenute a verificare le diverse identità e, a seconda che si tratti della stessa persona o di una persona diversa già registrata in uno dei sistemi d'informazione dell'UE, 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 all'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 hanno accesso ai collegamenti rossi se hanno accesso almeno a uno dei sistemi d'informazione dell'UE interessati, nonché ai collegamenti bianchi o verdi se 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. 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. È esclusa una simile ricerca nell'ambito dello stesso sistema.

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 per i quali è emersa una corrispondenza. 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 gli stessi o simili, è creato un collegamento bianco. Qualora invece i dati di identità non possano essere considerati simili, è creato 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. 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[19] ai sensi degli articoli 26, 32, 34 o 26 del regolamento (UE) 2018/1862[20], l'autorità responsabile della verifica manuale è l'ufficio SIRENE dello Stato Schengen che ha creato la segnalazione. 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, 32 e 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.

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 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, come 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 in base alla procedura di cui all'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

19 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.

20 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.

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.

Se l'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 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 dunque a due persone diverse.

Un collegamento rosso non ha alcuna ripercussione 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, del VIS, dell'ETIAS, 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 fornisce indicazioni su come reperire informazioni sui dati (tramite comunicazione di un numero di identificazione unico e dell'indirizzo del sito web del portale; v. n. 3.2). 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, della protezione della sicurezza e dell'ordine pubblico, della prevenzione della criminalità o per garantire che non siano compromesse indagini nazionali (par. 4 e 5). Qualora sia 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 tale autorità verifica

i dati pertinenti e, ove necessario, rettifica o cancella 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.

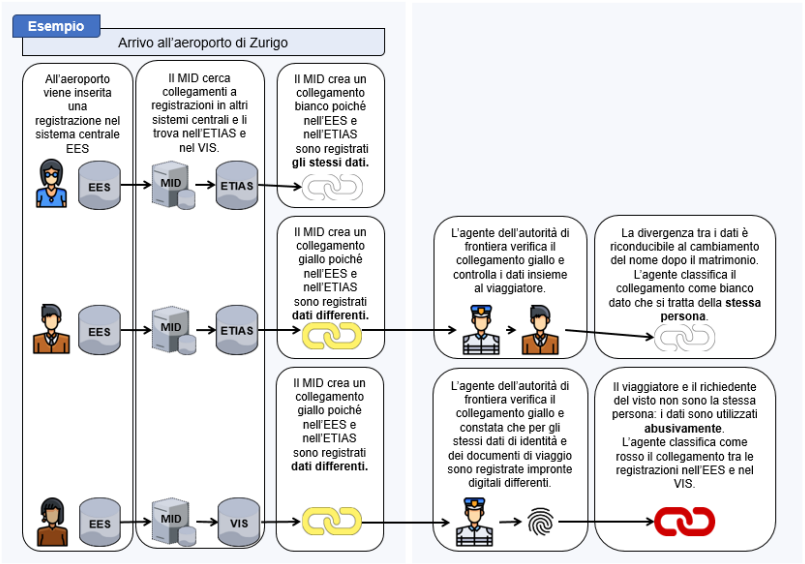
Collegamento bianco (art. 33)

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 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. 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 (tramite comunicazione di un numero di identificazione unico e dell'indirizzo del sito web del portale). 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 incorrettamente registrato, 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 senza indugio 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 due o più sistemi d'informazione dell'UE. Essi sono in seguito 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 3.1.1 in merito all'articolo 10 si applicano per analogia.

Periodo transitorio per il rilevatore di identità multiple

L'articolo 69 «IOP frontiere» e l'articolo 65 «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. 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. L'unità centrale ETIAS informa la Commissione europea, solo dopo che tutti i collegamenti gialli siano stati verificati manualmente e i loro status aggiornati in collegamenti verdi, bianchi o rossi. La Commissione europea 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.

3.2 Ulteriori disposizioni

I due regolamenti dell'UE contengono, oltre alle disposizioni concernenti le quattro nuove componenti centrali che rappresentano la parte principale dei regolamenti UE sull'interoperabilità, 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 interamente 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. Nell'articolo 48 è sancito 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 richiede 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 di rettifica o cancellazione dei dati personali sia presentata a uno Stato diverso da quello competente per la verifica manuale delle identità diverse, lo Stato al quale è stata presentata contatta le autorità dello Stato Schengen responsabile o l'unità centrale ETIAS, nel caso in cui sia competente per la verifica. La verifica deve essere effettuata di norma entro 45 giorni dalla ricezione della richiesta. Tale termine può essere prorogato. 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 o consultati 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 interessati dall'interoperabilità 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 istituire 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 regolamenti 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 sul codice frontiere Schengen, il regolamento (UE) 2017/2226 sull'EES, il regolamento (UE) 2018/1240 sull'ETIAS, il regolamento (UE) 2018/1726 sull'eu-LISA, il regolamento (UE) 2018/1861 sul SIS, la decisione 2004/512/CE che istituisce il VIS e la decisione 2008/633/GAI relativa all'accesso per la consultazione al VIS da parte delle autorità di perseguimento penale. Le modifiche di tali atti sono disciplinate 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 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[21] (art. 67-69 «IOP frontiere» nonché art. 63-65 «IOP polizia»). Vi sono inoltre disciplinati l'inizio delle attività (art. 72 «IOP frontiere» e art. 68 «IOP polizia»), la formazione delle autorità responsabili (art. 76 «IOP frontiere» e art. 72 «IOP polizia»), il monitoraggio e la valutazione delle componenti centrali (art. 78 «IOP frontiere» e art. 74 «IOP polizia») nonché l'entrata in vigore (art. 79 «IOP frontiere» e art. 75 «IOP polizia»).

4 Punti essenziali del testo di attuazione

4.1 La normativa proposta

Il progetto costituisce un recepimento dello sviluppo 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. 4.3.1).

4.2 Compatibilità tra compiti e finanze

La trasposizione dei regolamenti UE sull'interoperabilità comportano in Svizzera oneri finanziari e in termini di personale per l'Amministrazione federale e i Cantoni. Gli oneri menzionati al numero 6 vanno, tuttavia, considerati alla luce degli enormi benefici che dovrebbero scaturire dalle nuove possibilità previste da entrambi i regolamenti UE sull'interoperabilità. Le informazioni esistenti potranno essere infatti utilizzate in modo più efficiente e mirato, apportando così un importante valore aggiunto al lavoro delle autorità di controllo delle frontiere, migratorie e di perseguimento penale. L'interoperabilità contribuirà pertanto ad accrescere la sicurezza nello spazio Schengen.

21 Il rispettivo contenuto è illustrato nei numeri relativi alle singole componenti centrali (v. n. 3.1).

4.3 Attuazione

4.3.1 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. Le novità che implicano un adeguamento a livello di leggi federali sono illustrate nel presente numero. Molti adeguamenti riguardano invece solo ordinanze 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 norme relative alla finalità dei sistemi d'informazione dell'UE. 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[22] e le banche dati di polizia regolamentate dalla LSIP[23]. Per motivi di trasparenza, le componenti centrali riguardanti sistemi d'informazione che hanno attualmente la propria base legale formale nella LStrI e nella LSIP devono essere 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. 5 per i commenti ai singoli articoli).

Legge federale sugli stranieri e la loro integrazione

Alcune delle disposizioni da recepire nel diritto svizzero richiedono adeguamenti della LStrI.

Poiché i sistemi d'informazione disciplinati dalla LStrI sono regolamentati dall'accordo di associazione alla normativa di Dublino 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.

Con l'introduzione dell'interoperabilità è stato necessario adeguare nove regolamenti UE (su ETIAS, EES e SIS cfr. 3.2), ciò richiede la modifica anche delle corrispondenti

22 RS **142.20**
23 RS **361**

disposizioni della LStrI preposte a disciplinare oggi e in futuro 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 alcuni 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 (sBMS art. 110, CIR art. 110*a*-110*d* e MID art. 110*f*). Ciò corrisponde alla disposizione dell'articolo 17 capoverso 1 della legge federale del 19 giugno 1992[24] sulla protezione dei dati (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 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 nei diversi casi.

Vanno disciplinati pure 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 in materia di C-VIS, EES e 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[25] 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. Ciò non comporta modifiche materiali della LSISA.

24 RS **235.1**
25 RS **142.51**

Legge sulla responsabilità

La legge federale del 14 marzo 1958[26] sulla responsabilità (LResp) disciplina attualmente il SIS all'interno degli articoli 19*a* e 19*b*. Le basi giuridiche dell'UE relative a EES, VIS, 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 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

Come illustrato in precedenza, 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. 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 a sBMS, ESP e MID dal tenore pressoché analogo a quello delle pertinenti disposizioni introdotte nella LStrI.

La necessità di introdurre diversi articoli concernenti il trattamento dei dati nei sistemi d'informazione Schengen/Dublino impone un adeguamento della sistematica all'interno della LSIP. I sistemi d'informazione Schengen/Dublino o le rispettive componenti devono essere infatti ora disciplinati in una sezione separata (nuova sezione 4) rispecchiando l'ordine cronologico della loro entrata in funzione prevista (sBMS all'art. 18*a*, ESP all'art. 18*b* e MID all'art. 18*c*).

In seguito all'attuazione della direttiva (UE) 2016/680[27] entrata in vigore il 1° marzo 2019, l'articolo 349*c* CP disciplina la comunicazione di dati personali a uno Stato terzo o a un organo internazionale.[28] L'articolo 13 capoverso 2 della legge federale del 7 ottobre 1994[29] 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

26 RS **170.32**

27 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.

28 RU **2019** 625

29 RS **360**

personali nel quadro della cooperazione di polizia con le autorità straniere preposte al perseguimento penale è retta dagli articoli 349*a*–349*h* CP.[30] La LSIP disciplina, per contro, in via generale l'utilizzo del sistema d'informazione di polizia della Confederazione. Con la trasposizione dei regolamenti UE in questione il suo campo d'applicazione viene 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. 18*e*). Infine occorre anche disciplinare la responsabilità per il trattamento dei dati nei sistemi d'informazione Schengen/Dublino o nelle rispettive componenti (art. 18*f*).

4.3.2 Valutazione dell'esecuzione

Ogni Stato Schengen è sottoposto, almeno ogni cinque anni, a una valutazione volta a verificare la corretta applicazione del diritto Schengen. Finora la Svizzera è stata sottoposta a tre valutazioni: nel 2008, in vista dell'avvio della collaborazione operativa, nel 2014 e nel 2018. A essere valutati sono di volta in volta la cooperazione di polizia, SIS/SIRENE, le frontiere esterne, i rinvii, la protezione dei dati e i visti. La valutazione coinvolge sia la Confederazione sia i Cantoni. Al termine delle visite in loco, gli esperti competenti redigono i rapporti di valutazione in cui illustrano eventuali lacune. Il Consiglio dell'UE può emanare raccomandazioni concrete volte a colmare tali lacune. In seguito la Svizzera fornisce all'UE un rapporto in cui illustra le eventuali misure adottate in base alle raccomandazioni. In occasione delle prossime valutazioni verrà valutata anche la trasposizione dei regolamenti UE sull'interoperabilità.

5 Commento ai singoli articoli del testo di attuazione

5.1 Legge sugli stranieri e la loro integrazione

Art. 5 cpv. 1 lett. a^{bis}, nota a piè di pagina

Poiché il regolamento (UE) 2018/1240[31] sull'autorizzazione ai viaggi ETIAS è modificato dal regolamento (UE) 2019/817 («IOP frontiere»), la nota a piè di pagina dell'articolo 5 capoverso 1 lettera a^{bis} deve essere modificata di conseguenza.

Questa disposizione deve inoltre essere coordinata con il decreto federale sull'approvazione e la trasposizione dello scambio di note tra la Svizzera e l'Unione europea concernente il recepimento del regolamento (UE) n. 2018/1240 che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (Sviluppo dell'acquis di Schengen)[32].

30 RU **2019** 625

31 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.

32 Il progetto è stato posto in consultazione dal 13 febbraio 2019 al 20 maggio 2019.

Art. 7 cpv. 3, nota a piè di pagina

Poiché il codice frontiere Schengen (CFS)[33] è modificato dal regolamento (UE) 2019/817 («IOP frontiere»), la nota a piè di pagina dell'articolo 7 capoverso 3 va adattata di conseguenza.

Questa disposizione deve inoltre essere coordinata con il decreto federale sull'approvazione e la trasposizione dello scambio di note tra la Svizzera e l'Unione europea concernente il recepimento del regolamento (UE) n. 2018/1240 che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (Sviluppo dell'acquis di Schengen).

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. 68a cpv. 2, nota a piè di pagina

Poiché il regolamento (UE) 2018/1861[34] è modificato dal regolamento (UE) 2019/818 («IOP polizia»), la nota a piè di pagina dell'articolo 68*a* capoverso 2 deve essere adattata di conseguenza.

Questa disposizione deve inoltre essere coordinata con il 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) (regolamenti [UE] 2018/1862, 2018/1861 e 2018/1860) (Sviluppi dell'acquis di Schengen)[35].

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 nell'articolo 104*a* capoversi 1bis, 2, 3, 3bis, 4 e 5, nell'articolo 104*b* capoverso 1, nell'articolo 122*b* capoverso 2 e nell'articolo 122*c* capoverso 3 lettera b devono essere adattati.

33 Regolamento (UE) n. 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; modificato da ultimo dal regolamento (UE) n. 2019/817, GU L 135 del 22.5.2019, pag. 27.

34 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 7.12.2018, pag. 14; modificato da ultimo dal regolamento (UE) 2019/818, GU L 135 del 22.5.2019, pag. 85.

35 Il progetto è stato posto in consultazione dal 13 febbraio 2019 al 20 maggio 2019.

Protezione e trattamento dei dati

In seguito all'introduzione delle nuove componenti centrali, che influiscono su tutti i sistemi d'informazione Schengen/Dublino, l'avamprogetto prevede di 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 (SEM e Schengen);
- il capitolo 14*b,* che attualmente contiene 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».
- il capitolo 14*c*, che contiene le disposizioni sull'Eurodac, disciplinerà la protezione dei dati nel quadro degli accordi di associazione a Schengen. Le disposizioni relative all'Eurodac sono incluse nel capitolo 14*a* (sezione separata per Eurodac).

Capitolo 14: Trattamento e protezione dei dati

È modificato il titolo del capitolo 14 dal momento che secondo l'avamprogetto disciplinerà soltanto la protezione e il trattamento dei dati, mentre ai sistemi d'informazione sarà dedicato un capitolo a parte (14*a*).

Oltre agli articoli 101 LStrI (Trattamento dei dati), 102 (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* LStrI (Comunicazione di dati personali all'estero);
- 102*d* LStrI (Comunicazione di dati personali allo Stato d'origine o di provenienza);
- 102*e* LStrI (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 divulgazione 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

Si veda il commento all'articolo 9*a*.

Capitolo 14a: Sistemi d'informazione

Il capitolo 14*a* è ora inserito prima dell'articolo 103*a* LStrI (INAD) e riguarda i seguenti sistemi d'informazione:

- sezione 1 (Sistema d'informazione sulle entrate rifiutate, sistema INAD): articolo 103*a* LStrI;
- sezione 2 (Sistema di ingressi/uscite EES e controllo di confine automatizzato): articolo 103*b*–103*g* LStrI;
- sezione 3 (Sistema d'informazione sui passeggeri, sistema API): articoli 104*a*–104*c* e 108 LStrI (l'art. 108 LStrI è già abrogato);
- sezione 4 (Sistema europeo di informazione e autorizzazione ai viaggi ETIAS): articoli 108*a*–108*g* e 109 LStrI (l'art. 109 LStrI è già abrogato);
- sezione 5 (Sistema centrale d'informazione visti C-VIS e sistema nazionale visti ORBIS): articoli 109*a*–109*e* LStrI;
- sezione 6 (Sistema d'informazione per l'attuazione del ritorno[36]): articoli 109*f*–109*j* LStrI;
- sezione 7 (Eurodac): articoli 109*k* LStrI;
- sezione 8 (Sistema di gestione dei fascicoli personali e della documentazione): articoli 109*m* LStrI.

Sezione 1: Sistema d'informazione sulle entrate rifiutate

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

Art. 103a

Poiché la sezione 1 comprende un solo articolo, il titolo dell'articolo 103*a* può essere soppresso.

36 RU **2019** 1413

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 il sistema di ingressi/uscite 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

Cpv. 1, nota a piè di pagina

Poiché il regolamento (UE) 2017/2226[37] sul sistema di ingressi/uscite EES è modificato dal regolamento (UE) 2019/817 («IOP frontiere»), la nota a piè di pagina dell'articolo 103*b* capoverso 1 va adattata di conseguenza.

Questa disposizione deve inoltre essere coordinata con il decreto federale sull'approvazione e la trasposizione dello scambio di note tra la Svizzera e l'Unione europea concernente il recepimento del regolamento (UE) n. 2018/1240 che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (Sviluppo dell'acquis di Schengen).

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

L'articolo 103*b* capoverso 2 lettera a non riporta più i dati sui visti rilasciati che sono trattati separatamente alla lettera b^{bis}. Ciò consente un rimando preciso, al capoverso 4, ai dati ora conservati nel CIR. L'espressione «dati alfanumerici» è sostituita da «i dati d'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 d'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 conservati nel CIR. Le informazioni 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 trasmessi al CIR e continuano a essere conservati solo nell'EES.

Art. 103d, rubrica e cpv. 5

Dato che il CIR diventerà parte integrante dell'EES, le disposizioni sulla comunicazione dei dati dell'EES si applicheranno anche ai dati EES conservati nel CIR (dati di

37 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, pag. 27.

identità, dati dei documenti di viaggio e dati biometrici). La rubrica va pertanto integrata con «CIR». Per quanto riguarda la comunicazione dei dati EES conservati nel CIR, il capoverso 3 rimanda all'articolo 110*h*, che si riferisce a sua volta all'articolo 40 dei regolamenti (UE) 2019/817 e 2019/818 (cfr. commenti ad art. 110*h* e 3.2 Protezione dei dati).

Art. 104

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

Sezione 3: Sistema d'informazione sui passeggeri (sistema API)

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 e cpv. 1bis, 2, 3, 3bis, 4 e 5

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.

Sezione 4: Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS)

Prima dell'articolo 108*a* è inserita una nuova sezione contenente norme relative al sistema europeo di informazione e autorizzazione ai viaggi ETIAS (art. 108*a*–108*g*; l'art. 109 è già stato abrogato).

Art. 108a cpv. 1 lett. a e cpv. 3

Cpv. 1 lett. a

Il capoverso 1 lettera a precisa che i dati personali rappresentano i dati d'identità e i dati dei documenti di viaggio, ora conservati nel CIR.

Cpv. 3

Il capoverso 3 specifica quali dati sono trasmessi e conservati nel CIR (cfr. commenti ad art. 110*a*). I dati d'identità e i dati dei documenti di viaggio (art. 108*a* cpv. 1 lett. a) sono conservati nel CIR. Le informazioni relative alle domande di autorizzazione ai viaggi ETIAS accolte o respinte e i dati dell'elenco di controllo sono esclusi dalla trasmissione al CIR e continuano a essere memorizzati solo nell'ETIAS.

Art. 108f, rubrica e cpv. 3

Dato che il CIR diventerà parte integrante dell'ETIAS, le disposizioni sulla comunicazione dei dati ETIAS si applicheranno anche ai dati ETIAS conservati nel CIR (dati di identità, dati dei documenti di viaggio e dati biometrici). La rubrica va pertanto integrata con «CIR». Per quanto riguarda la comunicazione dei dati ETIAS conservati nel CIR, il capoverso 3 rimanda all'articolo 110*h*, che rimanda a sua volta all'articolo 40 dei regolamenti (UE) 2019/817 e 2019/818 (cfr. commenti ad art. 110*h* e 3.2 Protezione dei dati).

Sezione 5: 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 sistema centrale d'informazione visti e al sistema nazionale visti ORBIS (art. 109*a*–109*e* e 109*f*–109*j*; gli art. 109*f*–109*j* sono già stati abrogati).

Art. 109a rubrica, cpv. 1 nota a piè di pagina e cpv. 1bis

Cpv. 1, nota a piè di pagina

Poiché il regolamento (CE) n. 767/2008[38] concernente il sistema di informazione visti 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.

Questa disposizione deve inoltre essere coordinata con il decreto federale sull'approvazione e la trasposizione dello scambio di note tra la Svizzera e l'Unione europea concernente il recepimento del regolamento (UE) n. 2018/1240 che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (Sviluppo dell'acquis di Schengen).

Cpv. 1bis

Il capoverso 1bis specifica quali dati sono memorizzati nel C-VIS e quali dati sono trasmessi e conservati nel CIR (cfr. commenti ad art. 110*a*). I dati di identità, i dati

38 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) n. 2019/817, pag. 27.

dei documenti di viaggio e i dati biometrici sono conservati nel CIR. Le restanti informazioni sulla procedura di visto sono escluse dalla trasmissione al CIR e restano memorizzate soltanto nel C-VIS.

Art. 109b, rubrica, cpv. 1, cpv. 2, cpv. 2bis, cpv. 3 e nota a piè di pagina

La nuova sezione «Sistema centrale d'informazione visti (C-VIS) e sistema nazionale visti (ORBIS)» introduce nella LStrI il termine «ORBIS» per il sistema nazionale dei visti. Di conseguenza, il termine ORBIS sostituisce l'espressione «sistema nazionale visti» nelle seguenti disposizioni.

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 6: 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[39] della LStrI (Norme procedurali e sistemi d'informazione) ed entreranno in vigore all'inizio del 2020. Non vi sono modifiche materiali delle disposizioni.

Sezione 7: Eurodac

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

Art. 109k Rilevamento e trasmissione dei dati in 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 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 (UE) 2019/818 si applica a Eurodac a partire dalla data di applicazione della nuova versione del regolamento (UE) n. 603/2013[40] (art. 75 regolamento [UE] 2019/818).

39 RU **2019** 1413
40 GU L 180 del 29.6.2013, pag. 1.

Art. 109l

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 8: Sistema di gestione dei fascicoli personali e della documentazione

La vigente sezione 3 diventa sezione 8. La sezione contiene una disposizione sul sistema di gestione dei fascicoli personali e della documentazione della 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 111 è stato abrogato dalla modifica del 14 dicembre 2018[41] della LStrI (Norme procedurali e sistemi d'informazione). L'articolo 110 disciplina ora il servizio comune di confronto biometrico (sBMS). La norma dell'attuale articolo 110 LStrI 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 nel CIR e nel SIS), l'sBMS permette la consultazione trasversale dei sistemi d'informazione Schengen/Dublino interoperabili. Non è possibile dedurre i dati biometrici effettivi dal template.

L'sBMS è una delle quattro nuove componenti centrali dell'interoperabilità. A differenza del CIR (art. 110*a* segg. LStrI) o del MID (art. 110*g* LStrI), non si tratta tuttavia di una raccolta di dati o di 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. 3.2.1).

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. Altre disposizioni nuove della LStrI rimandano all'sBMS.

L'sBMS contiene template biometrici basati su dati personali biometrici provenienti dai sistemi EES, VIS, Eurodac e SIS. L'ETIAS non figura nell'elenco perché in questo sistema non sono memorizzati dati personali biometrici.

Cpv. 2

41 FF **2018** 6655

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

Disposizioni dettagliate sull'sBMS sono contenute nel capo III dei due regolamenti UE sull'interoperabilità (regolamento [UE] 2019/817 e regolamento [UE] 2019/818). Per informazioni dettagliate sull'sBMS si veda 3.1.2.

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

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

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 relativi ai suoi documenti di viaggio.

Il CIR è inteso a facilitare l'identificazione delle persone i cui dati sono contenuti nei sistemi d'informazione Schengen di cui sopra e a contribuire all'individuazione di identità multiple. Dovrebbe inoltre facilitare e armonizzare l'accesso delle autorità designate a tali sistemi di informazione a fini di prevenzione, individuazione o investigazione di reati di terrorismo o di altri reati gravi. I corrispondenti diritti di accesso sono disciplinati dagli articoli 110*b*- 110*d* LStrI. In linea di principio, in futuro un'interrogazione del CIR sarà sempre attivata tramite l'ESP (cfr. art. 110*e* LStrI). Secondo l'attuale pianificazione della Commissione europea, il CIR entrerà in funzione a metà del 2022, mentre l'ESP non sarà operativo fino a metà del 2023. Resta da chiarire se il CIR può essere consultato anche senza l'ESP durante il periodo transitorio fino a quando entrambe le componenti centrali non saranno operative. Per informazioni dettagliate sul CIR si veda 3.1.3.

Cpv. 2

Per ciascuna serie di dati d'identità, di documenti di viaggio e biometrici memorizzati, il CIR contiene un riferimento al sistema d'informazione Schengen/Dublino da cui provengono i dati corrispondenti e un riferimento all'insieme di dati effettivi del corrispondente sistema d'informazione Schengen/Dublino. I riferimenti sono utili in particolare alle autorità che non hanno accesso al sistema d'informazione Schengen da cui provengono i dati originali e devono chiedere la trasmissione dei dati necessari all'autorità centrale competente.

Disposizioni dettagliate sul CIR sono contenute nel capo IV dei due regolamenti UE sull'interoperabilità (regolamento [UE] 2019/817 e regolamento [UE] 2019/818).

Art. 110b Consultazione del CIR a fini di identificazione

Cpv. 1 e 2

Ai sensi dell'articolo 20 paragrafo 1 dei regolamenti (UE) 2019/817 e (UE) 2019/818, 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 LStrI possono interrogare il CIR con i 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 interrogare il CIR in singoli casi concreti per identificare i cittadini stranieri (cittadini di Stati terzi). Si tratta di fedpol, delle autorità di polizia dei Cantoni e dei Comuni e dell'Amministrazione federale delle dogane (AFD) per la protezione della popolazione e la salvaguardia della sicurezza interna. 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 il potere 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. Inoltre, una ricerca può essere effettuata solo per i seguenti scopi: combattere l'immigrazione clandestina, garantire e mantenere l'ordine e la sicurezza pubblici e proteggere la sicurezza interna.

Cpv. 4 e 5

L'interrogazione nel 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 un'interrogazione 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 a fini di individuazione di identità multiple

Cpv. 1

Se durante la consultazione del CIR compare un collegamento giallo (cfr. 3.1.4), 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 d'identità, ai dati del documento di viaggio e al riferimento al sistema d'informazione Schengen/Dublino da cui provengono i dati.

Cpv. 2

Se durante la consultazione del CIR compare un collegamento rosso (cfr. 3.1.4), le autorità che hanno accesso al CIR, all'EES, all'ETIAS, al C-VIS, all'Eurodac o al SIS sulla base della LStrI o della LSIP possono, per combattere le frodi di identità, accedere ai dati contenuti nel CIR (cfr. commento a cpv. 1) e al riferimento al sistema d'informazione Schengen/Dublino.

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 sapere se i dati relativi alla persona interessata sono disponibili nei sistemi EES, VIS, ETIAS o Eurodac. Le autorità di polizia locali elencate in questo capoverso (Zurigo, Lugano, ecc.) hanno il diritto di interrogare i dati in quanto, come le forze di polizia cantonali, svolgono funzioni di polizia criminale nell'ambito della prevenzione, dell'individuazione e dell'investigazione di reati gravi (cfr. anche la disposizione dell'art. 109*a* cpv. 3 LStrI).

Cpv. 3

Se un'interrogazione 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 1 il corrispondente riferimento ai sistemi EES, VIS, ETIAS o Eurodac. La risposta corrispondente può essere utilizzata solo per presentare una domanda di accesso al corrispondente sistema d'informazione Schengen/Dublino.

Cpv. 4

Le autorità di cui al capoverso 2 si mettono in contatto con la Centrale operativa di fedpol per chiedere il pieno accesso ai dati dell'interessato nel pertinente sistema d'in-

formazione Schengen/Dublino. 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 simultanea 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 una consultazione senza discontinuità delle 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 segg. regolamenti [UE] 2019/817[42] e [UE] 2019/818[43]).

Una ricerca tramite ESP viene avviata quando:

- sono inseriti dei dati in una delle banche dati di cui sopra;
- si eseguono 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 regolamenti [UE] 2019/817[44] e [UE] 2019/818[45]). Per consentire l'uso dell'ESP, l'eu-LISA crea categorie di profili utente ESP che tengono conto dei diritti di accesso (art. 8 regolamenti [UE] 2019/817[46] e [UE] 2019/818[47]).

All'utente verranno mostrati solo i dati a cui ha diritto di accesso e i riferimenti come da articoli 30–33 dei regolamenti [UE] 2019/817[48] e [UE] 2019/818[49]. Non vengono fornite informazioni su dati cui l'utente non è autorizzato ad accedere (art. 9 regolamenti (UE) 2019/817[50] e (UE) 2019/818[51]).

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

42 Cfr. nota 2.
43 Cfr. nota 3.
44 Cfr. nota 2.
45 Cfr. nota 3.
46 Cfr. nota 2.
47 Cfr. nota 3.
48 Cfr. nota 2.
49 Cfr. nota 3.
50 Cfr. nota 2.
51 Cfr. nota 3.

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. L'obiettivo del MID è facilitare i controlli d'identità e combattere le frodi d'identità.

Cpv. 1

Il capoverso 1 riprende il contenuto di questa banca dati come previsto dai regolamenti UE. Si tratta di 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 di informazione Schengen (art. 35 regolamenti IOP).

Cpv. 2

Il capoverso 2 stabilisce, conformemente alla normativa unionale, 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.

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 regolamenti [UE]), mentre la consultazione nell'ESP avviene sulla base dei dati di identità e dei dati dei documenti di viaggio (art. 27 par. 3 e 4 regolamenti [UE]). 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 il contenuto del MID. Si tratta di collegamenti tra i dati dei diversi sistemi d'informazione che sono legati alla stessa persona ed eventualmente riguardano la stessa persona. 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 recuperare 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.

Il fascicolo di conferma dell'identità del MID, ai sensi dell'articolo 34 dei regolamenti (UE) 2019/817 e (UE) 2019/818, contiene le seguenti informazioni:

- il tipo di collegamento tra i dati per i quali risulta una corrispondenza (art. 30–33 regolamenti [UE] 2019/817[52] e [UE] 2019/818[53]);
- il riferimento ai sistemi d'informazione Schengen/Dublino da cui provengono i dati di cui al capoverso 1;
- un numero di identificazione unico;
- l'autorità responsabile della verifica manuale delle identità diverse;
- la data della creazione del collegamento o del suo aggiornamento.

Art. 110g Verifica manuale di collegamenti 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 regolamenti [UE]). 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 AP-LStrI che specifica 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 ricerca creando un fascicolo o aggiornando i dati nel C-VIS, nell'EES o nell'ETIAS. Nei casi di segnalazioni di polizia, l'Ufficio SIRENE di fedpol è l'autorità responsabile della verifica.

Cpv. 3

La verifica di identità multiple è effettuata in presenza della persona interessata (art. 29 regolamento [UE] 2019/817). Ciò vale in particolare quando la verifica avviene 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.

52 Cfr. nota a piè di pagina relativa all'art. 110 cpv. 1.
53 Cfr. nota a piè di pagina relativa all'art. 110 cpv. 1.

Cpv. 4

Se viene scoperta un'identità multipla illecita (collegamento rosso, art. 32 regolamenti IOP) o se i dati di una persona sono legalmente disponibili in diversi sistemi d'informazione Schengen (collegamento bianco, art. 33 regolamenti IOP), 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 regolamenti IOP).

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 regolamenti [UE] 2019/817 e [UE] 2019/818). Si tratta dell'articolo generale 111*d* LStrI e degli articoli 103*d* 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 due regolamenti IOP ([UE] 2019/817 e [UE] 2019/818) per quanto riguarda la responsabilità del trattamento dei dati nelle tre componenti di interoperabilità sBMS, CIR e MID (cfr. 3.2 Protezione dei dati).

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* e tutte le disposizioni relative alla protezione dei dati nell'ambito degli Accordi di associazione a Schengen vanno a far parte del 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* AP-LStrI.

Il diritto di accesso di cui all'articolo 111*f* si riferisce in particolare alle leggi federali o cantonali in materia di protezione dei dati. Questa disposizione si applica anche alle informazioni contenute nei vari sistemi d'informazione Schengen. Si propone di abrogare questo articolo perché riprende l'articolo 8 LPD.

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 e all'interoperabilità sono o saranno specificati nelle ordinanze esecutive. Pertanto, i vari diritti di protezione dei dati non sono elencati in questo capitolo.

Capitolo 14c Eurodac (vigente)

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

L'articolo 120*d*, modificato nel quadro dei progetti riguardanti l'EES e l'ETIAS, deve essere nuovamente adattato ai fini dell'interoperabilità. Nella rubrica della disposizione viene eliminato il riferimento alla SEM, poiché alcuni di questi sistemi sono sistemi d'informazione Schengen/Dublino che non rientrano esclusivamente nelle competenze della SEM.

Il capoverso 1 è trasposto, senza modifiche materiali, nell'articolo 101 capoverso 2.

Il capoverso 2 punisce con la multa il trattamento indebito dei dati nei sistemi C-VIS (lett. a), EES (lett. b) ed ETIAS (lett. c). È opportuno prevedere 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* o *110g* AP-LStrI va punito con una multa che, secondo il Codice penale svizzero, può arrivare fino a CHF 10 000 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*.

5.2 Legge federale del 20 giugno 2003 sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA)

Art. 1 cpv. 2

Si veda il commento all'articolo 92a.

Art. 15 Comunicazione all'estero 111a-111d

Gli articoli 105–107 LStrI sono sostituiti dagli articoli 102*c*–102*e* AP-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* AP-LStrI.

5.3 Legge sulla responsabilità

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'utilizzazione 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'utilizzazione 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) 2019/817 e (UE) 2019/818 per quanto concerne le componenti centrali.

Per tale regione, nell'articolo 19*a* sono ora integrati l'EES (lett. b), il C-VIS (lett. c), l'ETIAS (lett. d), il CIR (lett. e), l'ESP (lett. f), il MID (lett. g) e l'Eurodac (lett. h).

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 (cpv. 2).

5.4 Legge federale sui sistemi d'informazione di polizia della Confederazione

Adeguamento della sistematica

Nella LSIP occorre integrare diversi articoli relativi ai sistemi d'informazione Schengen/Dublino o alle rispettive componenti. A tal fine si rende necessario adeguare la sistematica della legge. I sistemi d'informazione Schengen/Dublino vanno infatti ora regolamentati in una sezione separata (4) dopo i sistemi d'informazione di polizia «nazionali».

Art. 2

Il presente articolo elenca i sistemi d'informazione disciplinati dalla LSIP. Come illustrato al numero 4.3.1, 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 della Confederazione (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. 16) e, al numero 4, il sistema di gestione delle pratiche e degli atti dell'Ufficio federale di polizia (fedpol; art. 17).

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. 18). 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 18*a*, 18*b* e 18*c*.

Art. 16, 17

Come conseguenza dell'adeguamento della sistematica, il registro nazionale di polizia (attualmente disciplinato dall'art. 17) e il sistema di gestione delle pratiche e degli atti di fedpol (attualmente disciplinato dall'art. 18) hanno ora la propria base legale formale rispettivamente negli articoli 16 e 17 in modo da figurare all'interno della legge prima dei sistemi «internazionali».

Nuovo titolo: sezione 4: Sistemi d'informazione Schengen/Dublino e loro componenti

I sistemi d'informazione Schengen/Dublino e le loro componenti sono ora disciplinati separatamente nella sezione 4. Per tale ragione, occorre introdurre il pertinente titolo.

Il SIS, che è attualmente disciplinato dall'articolo 16, trova ora la sua base legale formale nell'articolo 18.

Art. 18a 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 LStrI. Nonostante l'applicabilità diretta dei regolamenti (UE) 2019/817 e 2019/818, 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 in base alle persone interessate.

Cpv. 1

Nell'sBMS sono conservati i template biometrici ottenuti dalle immagini del volto e dalle impronte digitali registrati 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. 18b 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* LStrI, l'ESP consentirà di consultare, mediante un'unica ricerca effettuata sulla base dei dati di identità o dei documenti di viaggio o biometrici, tutti i pertinenti sistemi d'informazione Schengen/Dublino (SIS, EES, VIS, ETIAS, Eurodac e CIR) nonché le banche dati di Interpol e i dati Europol.

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 (SIS, EES, VIS, ETIAS, Eurodac e CIR), alle banche dati di Interpol SLTD e TDAWN o ai dati Europol.

Cpv. 3

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

Cpv. 4

Il risultato delle interrogazioni 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 online. 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 disciplinati a livello di ordinanza.

Cpv. 5

Sul piano tecnico, si prevede di creare una «piattaforma nazionale di ricerca» per il collegamento all'ESP. A tale piattaforma saranno collegati anche i sistemi d'informazione di polizia cantonale, nella misura in cui ciò sia consentito dai regolamenti UE.

Tuttavia le informazioni tecniche attualmente disponibili sono troppo limitate per poter formulare una base legale formale dettagliata. Quest'ultima sarà pertanto integrata in un secondo momento.

Art. 18c Contenuto del rilevatore di identità multiple (MID)

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 e i suoi contenuti. 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.

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, l'sBMS confronta i dati appena registrati o aggiornati con i template biometrici in esso contenuti. 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 l'interrogazione e i dati per i quali è emersa la corrispondenza.

Cpv. 4

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

Art. 18d 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 LStrI).

Cpv. 1

Il diritto d'accesso serve alla verifica manuale dei collegamenti gialli (ovvero dei collegamenti per i quali non è stata ancora effettuata alcuna verifica manuale).

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 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.

Articolo 18e Comunicazione di dati dell'sBMS, del CIR e del MID

Il *presente articolo* disciplina la comunicazione di dati dei sistemi d'informazione Schengen/Dublino e delle loro componenti. In linea di massima, i dati 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.

Articolo 18f 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) 2019/817 e (UE) 2019/818.

6 Ripercussioni

6.1 Ripercussioni sulle finanze e sul personale della Confederazione

Sia la fase di progettazione sia l'applicazione dei regolamenti UE sull'interoperabilità comportano per fedpol e la SEM ripercussioni sulle finanze e sul personale. Tali ripercussioni sono illustrate separatamente qui di seguito.

6.1.1 Costi di progetto per fedpol e la SEM

Presso fedpol l'attuazione sul piano tecnico e organizzativo dei regolamenti UE sull'interoperabilità è coordinata nell'ambito del progetto «Interoperabilità TO». Il progetto si prefigge di allestire il collegamento della parte nazionale del sistema d'informazione Schengen N-SIS alle nuove componenti centrali CIR, MID e ESP. Data l'assenza di specifiche tecniche, attualmente non è noto in che modo le componenti dell'infrastruttura nazionale dovranno essere adeguate in virtù della verifica dei collegamenti MID.

Presso la SEM l'attuazione dei due regolamenti UE è realizzata nel quadro del progetto «Interoperabilità SEM». Il programma verte su temi trasversali quali l'utilizzo comune delle nuove componenti di sistema per le interfacce Schengen nonché sui cambiamenti di carattere organizzativo. L'introduzione delle nuove quattro componenti dovrebbe infatti generare nuovi processi, che dovranno essere a loro volta assegnati alle singole unità organizzative.

fedpol e la SEM coordinano dal punto di vista strategico e operativo i propri progetti volti ad attuare sul piano tecnico e organizzativo i regolamenti UE sull'interoperabilità. Per sfruttare le sinergie tra i progetti sul piano operativo, hanno luogo regolarmente riunioni di coordinamento tra i responsabili dei programmi e dei progetti. Lo scambio d'informazioni è garantito non solo tramite il contatto diretto ma anche mediante l'accesso reciproco alle piattaforme di progetto. L'interoperabilità è uno dei progetti riassunti nell'ambito del programma relativo allo sviluppo dell'acquis di Schengen/Dublino. Nel quadro di questo programma, i progetti vengono coordinati sotto il profilo del rispetto delle prescrizioni in materia di scadenze, costi e qualità. Le questioni strategiche di ordine superiore sono trattate all'interno del comitato direttivo che si riunisce periodicamente.

Attualmente i progetti si trovano nella fase di avvio o di progettazione. L'attuazione pratica del collegamento alle componenti centrali dipenderà dall'impostazione adottata dall'agenzia eu-LISA nonché dalle specifiche tecniche. Lo sviluppo avverrà analogamente alla messa in funzione scaglionata delle componenti centrali da parte dell'UE. Alla fine del 2019 sono attesi i primi atti di esecuzione dell'UE in materia di interoperabilità che permetteranno a fedpol e alla SEM di conoscere ulteriori dettagli inerenti all'attuazione. Le attuali stime sui costi di progetto si basano sugli oneri previsti.

Nella fase di progettazione sono attese le seguenti ripercussioni:

I costi per i progetti condotti da fedpol e dalla SEM in materia di interoperabilità ammontano, secondo le stime, a 21,6 milioni di franchi per l'intero periodo, il che corrisponde a 14,1 milioni di franchi per gli anni 2020-2022. Il finanziamento è reso possibile da un nuovo credito d'impegno per l'attuazione dello sviluppo di Schengen/Dublino, integrato nel programma della SG-DFGP. Il messaggio concernente il credito d'impegno è stato trasmesso al Parlamento dal Consiglio federale il 4 settembre 2019. Il programma è gestito come progetto chiave TIC. Il fabbisogno di mezzi finanziari per il periodo 2020-2022 pari a 14,1 milioni di franchi rientra nella prima parte del credito d'impegno ed è coperto dai mezzi centrali TIC assegnati dal Consiglio federale e dalle prestazioni proprie degli uffici interessati.

Costi dei progetti in materia di interoperabilità	**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	**8,3**	2,1	2,2	2,4	1,2	0,2	0,2
Sviluppo IOP (SEM)	**2,0**					1.0	1,0
Totale	**21,6**	**5,0**	**5,3**	**3,8**	**2,7**	**2,4**	**2,4**

Gli importi corrispondono ai costi riportati nel messaggio concernente un credito d'impegno per l'attuazione dello sviluppo dell'acquis di Schengen/Dublino che è stato trasmesso al Parlamento dal Consiglio federale il 4 settembre 2019.

La realizzazione 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 destinati a risorse specializzate. La SEM calcola per lo stesso periodo 3960 giorni/persona. Le risorse di personale in questione saranno compensate internamente. Le risorse necessarie derivanti da queste stime sono state comunicate al CSI nell'agosto del 2019. Dall'analisi approfondita dei requisiti da parte del CSI potrebbero risultare ulteriori adeguamenti.

6.1.2 Costi di applicazione, esercizio e sviluppo per fedpol e la SEM

Grazie all'interoperabilità, in futuro le autorità competenti potranno accedere a maggiori informazioni. Il numero di riscontri positivi aumenterà generando, a sua volta, un incremento del numero dei casi. Tutto ciò apporterà enormi benefici in termini di sicurezza per lo spazio Schengen. Il maggior numero di casi richiederà, tuttavia, anche maggiori oneri per il loro trattamento. Inoltre la verifica dei collegamenti del MID ai fini dell'identificazione corretta di persone rappresenterà un nuovo compito aggiuntivo per le autorità. L'applicazione dei regolamenti UE sull'interoperabilità comporterà pertanto un maggior fabbisogno di personale presso fedpol e presso la SEM. In particolare il controllo dei dati biometrici derivante dalla verifica dei collegamenti del MID determinerà un fabbisogno supplementare di personale presso l'ufficio SIRENE, BiomID e i servizi della SEM. Attualmente non è possibile quantificare in modo preciso il fabbisogno in termini di personale. Quest'ultimo verrà tuttavia illustrato dettagliatamente all'interno del messaggio.

I costi supplementari di esercizio pari a 0,2 milioni di franchi che sorgeranno con l'entrata in funzione dell'interoperabilità saranno compensati mediante la ridefinizione delle priorità sulla scorta dei mezzi disponibili. Un eventuale fabbisogno supplementare in termini finanziari e di personale sarà rilevato e documentato in occasione dell'elaborazione del messaggio relativo all'approvazione e trasposizione nel diritto svizzero dei regolamenti UE sull'interoperabilità. Con il messaggio verrà presentato un piano di finanziamento in tal senso.

Gli sviluppi tecnici previsti per le componenti centrali entro il 2025 dovrebbero causare costi annuali pari a circa un milione di franchi e saranno eseguiti dopo l'entrata in funzione nel 2023 di tali componenti nell'ambito del progetto «Sviluppo IOP» della SEM (p. es. in relazione ai nodi d'accesso). Non sono previsti ulteriori costi d'esercizio.

6.1.3 Costi per l'AFD

Il presente sviluppo comporta ripercussioni sul piano finanziario, procedurale nonché in termini di personale per l'Amministrazione federale delle dogane (AFD). 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 ricerca.

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 i risparmi derivanti da una maggiore automatizzazione e gli oneri risultanti dall'individuazione di identità fittizie si compenseranno. Le ripercussioni in termini di personale concernono le misure di formazione e formazione continua.

Gli oneri supplementari con incidenza sul finanziamento 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 derivanti saranno computati sul credito globale del programma.

6.2 Ripercussioni sul piano tecnico

Il recepimento e la trasposizione dei regolamenti UE sull'interoperabilità determineranno anche ripercussioni sul piano tecnico.

Un'ulteriore componente nazionale dovrebbe garantire il collegamento dei sistemi svizzeri all'ESP. Al contempo tale soluzione dovrebbe permettere di perfezionare l'interoperabilità dei sistemi nazionali e cantonali di polizia in Svizzera. L'obiettivo è di consentire di sfruttare le sinergie tra i sistemi d'informazione e fare in modo che gli utenti visualizzino i risultati delle ricerche con maggiore chiarezza e rapidità. fedpol e la SEM collaborano strettamente per verificare se tale obiettivo possa essere realizzato tramite una nuova piattaforma nazionale di ricerca a beneficio anche dei Cantoni. Nel quadro dell'armonizzazione dell'informatica di polizia svizzera (AiP) è stato realizzato uno studio preliminare sul tema. Lo studio giunge alla conclusione che i benefici e la fattibilità di una piattaforma nazionale di ricerca sono chiaramente evidenti. Lo studio raccomanda una gestione centralizzata della piattaforma di ricerca; la gestione dei dati e dei sistemi d'informazione dovrebbe invece restare di competenza delle rispettive autorità. I diritti d'accesso delle autorità restano immutati. Tale componente nazionale sarà finanziata tramite il credito d'impegno per l'attuazione dello sviluppo di Schengen/Dublino.

6.3 Ripercussioni per i Cantoni e i Comuni

I regolamenti UE sull'interoperabilità comportano ripercussioni non solo a livello federale, ma anche per le autorità cantonali di polizia e migratorie.

L'utilizzo dell'ESP durante i controlli alle frontiere esterne dello spazio Schengen diverrà obbligatorio. Tale obbligo dovrebbe generare maggiori oneri per le autorità di controllo alle frontiere, soprattutto per quelle operanti in seconda linea. La possibilità di consultare simultaneamente un numero maggiore di sistemi d'informazione rispetto a prima aumenta la probabilità di ottenere un riscontro positivo. L'AFD e le autorità cantonali incaricate del controllo alle frontiere esterne dello spazio Schengen sono inoltre chiamate a verificare i collegamenti del MID. Si tratta di un nuovo compito che, unitamente al seguito dei lavori, dovrebbe causare oneri aggiuntivi. L'ESP può, tuttavia, essere utilizzato anche da altre autorità quali le polizie cantonali e le autorità cantonali competenti in materia di migrazione. È previsto ad esempio 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. Tale accesso faciliterà la corretta identificazione delle persone. Nel quadro della loro attività di prevenzione, indagine, accertamento e perseguimento di reati gravi e del terrorismo, le polizie cantonali potranno beneficiare anche delle nuove procedure previste per l'accesso da parte delle autorità di perseguimento penale. Tramite un'interrogazione 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 interrogazioni da parte delle autorità di perseguimento penale in sistemi d'informazione

non di polizia, fedpol è responsabile per la concessione a tali autorità dell'accesso ai dati richiesti. Tale competenza, già prevista per il VIS, è ora estesa anche all'EES.

Alla luce delle novità in materia di interoperabilità, si prevedono adeguamenti a diverse applicazioni cantonali. Il collegamento dei sistemi svizzeri all'ESP richiederà ad esempio modifiche tecniche dei sistemi cantonali di interrogazione. Altre modifiche sono ipotizzabili, sebbene al momento non possano essere ancora illustrate con precisione.

Anche per quanto attiene ai processi operativi, sono prevedibili ulteriori modifiche. La verifica dei collegamenti del MID costituisce un nuovo compito per le autorità interessate. Tali collegamenti sono il risultato della rilevazione di identità multiple che viene eseguita in occasione di ogni nuova registrazione o della modifica di dati nei sistemi d'informazione dell'UE. L'accertamento dei dati biometrici, ove necessario, deve essere eseguito da fedpol (BiomID). Gli oneri supplementari risultanti da questo nuovo compito sono attualmente difficili da quantificare, poiché non esistono ancora dati precisi sul numero probabile di collegamenti. Inoltre, al momento risulta complicato valutare in quale misura i Cantoni saranno interessati da tali verifiche, dato che i processi concreti per la verifica dei collegamenti del MID devono ancora essere definiti.

I probabili oneri supplementari vanno visti alla luce dei grossi vantaggi che l'interoperabilità comporta. Anziché consultare singolarmente i sistemi d'informazione, le autorità di controllo delle frontiere, migratorie e di perseguimento penale potranno infatti ottenere, tramite un'unica interrogazione, una panoramica dei dati disponibili di una persona. I processi operativi sono pertanto resi più efficienti, in quanto non sarà più necessario interrogare ogni singolo sistema. Inoltre, mentre diminuisce il rischio che alcuni dati possano essere ignorati, aumenta la probabilità di ottenere un riscontro positivo. Le informazioni disponibili potranno infatti essere utilizzate in modo più efficiente e mirato, apportando un importante valore aggiunto al lavoro delle autorità di controllo delle frontiere, migratorie e di perseguimento penale.

6.4 Ripercussioni in altri settori

Nei settori dell'economia, della società e dell'ambiente non sono attese ripercussioni dirette. Le questioni che riguardano tali settori non sono pertanto approfondite in modo dettagliato. L'interoperabilità contribuirà ad accrescere la sicurezza nello spazio Schengen, con ripercussioni positive anche per l'economia e la società.

7 Aspetti giuridici

7.1 Costituzionalità

Il 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 2019/818 che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere, della migrazione e della polizia si basa sull'arti-

colo 54 capoverso 1 della Costituzione federale[54] (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. Orbene, nel presente caso il Consiglio federale non può invocare tale competenza (cfr. art. 7*a* cpv. 1 e 2 [LOGA] nonché art. 24 cpv. 2 della legge federale del 13 dicembre 2002[55] sull'Assemblea federale [LParl]). Ne deriva che l'Assemblea federale è competente per l'approvazione di entrambi gli scambi di note.

7.2 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'attuazione uniforme dei sistemi d'informazione Schengen/Dublino. Il recepimento dei due regolamenti UE e le modifiche legislative che ne derivano sono pertanto compatibili con il diritto internazionale.

7.3 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 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. 4). Il decreto federale che approva e traspone nel diritto svizzero le basi giuridiche europee per l'interoperabilità tra i sistemi di informazione dell'UE 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).

54 RS **101**
55 RS **171.10**

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 dall'avamprogetto traspongono nel diritto svizzero le basi legali concernenti l'interoperabilità tra i sistemi d'informazione dell'UE e derivano direttamente dagli obblighi ivi contenuti. L'avamprogetto dell'atto normativo può dunque essere incluso nel decreto di approvazione.

7.4 Aspetti giuridici del testo di attuazione

Competenza di delega al Consiglio federale ai sensi dell'articolo 110h LStrI e dell'articolo 22 LSIP

La delega di competenze a favore del Consiglio federale si fonda sull'articolo 182 capoverso 1 Cost., in virtù del quale il Consiglio federale può emanare norme di diritto sotto forma di ordinanza. Si tratta qui di norme di diritto necessarie in vista dell'attuazione delle prescrizioni di legge e dei regolamenti UE sull'interoperabilità.

Elenco delle abbreviazioni

AAS	Accordo di associazione a Schengen
CIR	Archivio comune di dati di identità (*Common Identity Repository*)
Commissione LIBE	Commissione del Parlamento europeo che si occupa di questioni concernenti le libertà civili, la giustizia e gli affari interni (*Civil Liberties, Justice and Home Affairs*)
COREPER	Comitato dei rappresentanti permanenti degli Stati membri (*Comité des représentants permanents*)
ECRIS-TCN	Sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di Paesi terzi *(European Criminal Records Information System for third Country Nationals)*
EES	Sistema di ingressi/uscite (*Entry-Exit System*)
ESP	Portale di ricerca europeo (*European Search Portal*)
ETIAS	Sistema europeo di informazione e autorizzazione ai viaggi *(European Travel Information and Authorisation System)*
eu-LISA	Agenzia europea per la gestione operativa dei sistemi IT su larga scala
Eurodac	Banca dati centralizzata delle impronte digitali di richiedenti l'asilo e persone fermate al momento dell'entrata illegale (*European Dactyloscopy*)
HPi	Armonizzazione dell'informatica di polizia svizzera
IOP	Interoperabilità
IOP frontiere	Regolamento (UE) 2019/817
IOP polizia	Regolamento (UE) 2019/818
MID	Rilevatore di identità multiple (*Multiple Identity Detector*)
sBMS	Servizio comune di confronto biometrico (*shared Biometric Matching Service*)
SIS	Sistema d'informazione Schengen *(Schengen Information System)*
SLTD	Banca dati Interpol sui documenti di viaggio rubati o smarriti (*Stolen and Lost Travel Documents Database*)

TDAWN	Banca dati Interpol sui documenti di viaggio associati a segnalazioni (*Travel Documents Associated with Notices*)
Ufficio SIRENE	Servizio centrale competente per il coordinamento e il trattamento di tutte le segnalazioni SIS (*Supplementary Information Request at the National Entry*)
VIS	Sistema di informazione visti (*Visa Information System*)