Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
Ufficio federale di polizia fedpol

Gennaio 2020

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 (Sviluppi dell'acquis di Schengen)

Rapporto sui risultati della procedura di consultazione

Indice

1 Situazione iniziale

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'UE. 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 consultando un determinato sistema d'informazione, le autorità non vengano a conoscenza di 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 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 d'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.

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 poter sempre disporre di tutte le informazioni essenziali affinché, come nel caso illustrato poc'anzi, non venga ad esempio rilasciato un visto a un criminale. A

---

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.

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. Entrambi i regolamenti UE permetteranno infine di rilevare con maggiore efficacia le identità multiple e le frodi di identità. Tramite l'interoperabilità non sono registrati nuovi dati, bensì sono semplicemente 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 relativi sistemi di base.

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 rafforzare la 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. Lo scambio di dati agevolato 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 da parte del Parlamento. Le rispettive note di risposta sono state trasmesse all'UE il 19 giugno 2019. L'obiettivo del progetto è di recepire entro i termini prestabiliti gli sviluppi dell'acquis di Schengen e di creare le necessarie basi giuridiche per la loro trasposizione.

2 Svolgimento della procedura di consultazione e panoramica dei risultati

2.1 Osservazioni preliminari

Conformemente all'articolo 3 capoverso 1 lettere c–e della legge federale del 18 marzo 2005[4] sulla procedura di consultazione (LCo), è stata indetta una procedura di consultazione, avviata il 9 ottobre 2019 e conclusasi il 9 gennaio 2020.

Il rapporto sui risultati presenta le disposizioni accolte positivamente così come quelle che hanno sollevato dubbi o critiche, e indica eventuali proposte di modifica. Per quanto riguarda i partecipanti alla consultazione che si sono espressi a favore del progetto, si parte dal presupposto che approvino tutte le disposizioni, ad eccezione di quelle respinte in modo esplicito. Per quanto concerne i partecipanti contrari al progetto in generale, si parte dal presupposto che respingano tutte le disposizioni, salvo quelle approvate esplicitamente.

Il presente rapporto riassume i risultati della procedura di consultazione. I partecipanti che hanno espresso il proprio parere sono elencati al numero 3. Per quanto attiene alle motivazioni dettagliate si rimanda alla versione originale dei pareri[5].

4 RS **172.061**

5 Il rapporto sui risultati della procedura di consultazione è disponibile all'indirizzo www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione concluse > 2019 > DFGP.

2.2 Sintesi dei risultati della procedura di consultazione

Sono pervenute **44** risposte. In totale hanno espresso un parere scritto 26 Cantoni, tre partiti politici, cinque associazioni mantello, il TAF e nove cerchie interessate. Di questi, hanno espressamente rinunciato a prendere posizione sette partecipanti (**USI, SSDP, ACS, Associazione svizzera dei magistrati, SZ, AUSL, TAF**). Il **TAF** chiede esplicitamente di considerare la propria risposta come astensione e non come consenso. In seno all'**ASM** soltanto due autorità migratorie a livello di città e alcune autorità migratorie cantonali si sono espresse su singoli punti.
AG, AR, BE, BS, GL, GR, CDDGP, CCPCS, SG, UR e **ZH** accolgono il progetto e non hanno ulteriori osservazioni. La **CDDGP** rimanda ai pareri della **CCPCS** e dell'**ASM**.

AI, BL, FR, GE, JU, LU, NE, NW, SH, SO, TG, TI, OW, VD, VS, ZG, ASM, PLR, PSS, OSAR e **USS** giudicano positivamente il progetto e hanno alcune osservazioni. **PSS, OSAR** e **USS** chiedono di apportare miglioramenti in fase di attuazione.

AI, FR, GE, JU, LU, NE, OW, SH, SO, TI, VS, ZG e **ASM** sottolineano i costi supplementari e gli oneri aggiuntivi che incomberebbero alle autorità cantonali. **AI, LU, VS** e **ASM** ritengono, tuttavia, che il valore aggiunto dell'interoperabilità per la sicurezza sia superiore.

OSAR, USS, AsyL e **PSS** si esprimono a favore di un rafforzamento della tutela dei diritti fondamentali e della protezione dei dati.

OSAR e **USS** approvano il recepimento degli sviluppi dell'acquis di Schengen a condizione che vi sia una prosecuzione dell'associazione a Schengen e Dublino. **OSAR**, **USS** e **AsyL** esprimono, tuttavia, le proprie riserve nei confronti del progetto. L'**USS** è in linea con il parere dell'**OSAR.**

BL, SO e **UDC** ribadiscono la necessità di creare una piattaforma nazionale di ricerca alla quale sono collegati i sistemi d'informazione di polizia della Confederazione e dei Cantoni.

2.3 Pareri generali sull'interoperabilità

2.3.1 Importanza per la Svizzera

BL, PLR, FR, JU, NE, NW, SO, TI e **ASM** sottolineano nei rispettivi pareri che l'interoperabilità rappresenterà un valore aggiunto per il lavoro delle autorità interessate. **NW** ribadisce il fatto che l'interoperabilità avrà ripercussioni positive in termini di efficienza poiché diminuirà il rischio di non venire a conoscenza di informazioni rilevanti su persone.
FER, JU, GE, NW, OW, SH, SO, UR e **ZG** ritengono che l'interoperabilità avrà effetti positivi sulla sicurezza nello spazio Schengen e anche sulla sicurezza interna della Svizzera. Secondo **SO**, l'interoperabilità permetterà alle autorità di evitare decisioni errate per via di accertamenti incompleti dei fatti. **UDC** e **ZH** si aspettano che l'interoperabilità contribuirà a incrementare l'efficacia dei controlli presso gli aeroporti svizzeri.

2.3.2 Ripercussioni per i Cantoni

Coinvolgimento dei Cantoni

SO chiede che i Cantoni vengano coinvolti tempestivamente nei lavori di adeguamento tecnico e operativo. **NE** evidenzia che sia la polizia cantonale sia l'ufficio cantonale della migrazione auspicano che l'Amministrazione federale sviluppi una piattaforma facile da utilizzare, intuitiva e pronta a essere impiegata sul campo. **SH** invita la Confederazione a mettere a disposizione dei Cantoni le piattaforme tecniche necessarie ad adeguare le applicazioni cantonali nonché a predisporre i processi e le interfacce correlati all'interoperabilità in modo tale da limitare per quanto possibile gli oneri tecnici, amministrativi e finanziari per i Cantoni. **GE** chiede che

nell'ordinanza di esecuzione degli atti delegati venga definita una ripartizione chiara dei ruoli e delle sfere di competenza. **VD** auspica che gli uffici cantonali della migrazione possano beneficiare di un accesso integrale alle nuove componenti introdotte con l'interoperabilità.

Risorse

AI, FR, GE, JU, LU, NE, OW, SH, SO, TI, VS, ZG e **ASM** rimarcano i costi supplementari e gli oneri aggiuntivi per le autorità cantonali. **JU, OW** e **TI** esprimono le proprie perplessità in merito. **AI, LU, VS** e **ASM** partono dal presupposto che il valore aggiunto dell'interoperabilità per la sicurezza sia comunque superiore. **JU** e **TI** esortano il Consiglio federale a fornire informazioni chiare ai Cantoni sull'entità dei costi e sui potenziali oneri aggiuntivi. **OW** e **GE** chiedono alla Confederazione sostegno finanziario oppure il versamento di indennità ai Cantoni.

TI e **FR** presumono che i costi per i Cantoni si limiteranno agli adeguamenti tecnici. **FR** ricorda che i Cantoni dovranno provvedere anche alla formazione del personale competente. **GE** evidenzia che con le informazioni disponibili attualmente non è ancora possibile effettuare una stima delle ripercussioni finanziarie e tecniche. **SH** osserva che i costi e gli oneri aggiuntivi per i Cantoni dovranno essere per quanto possibile limitati.

PLR e **UDC** auspicano che per i dibattiti parlamentari vengano fornite informazioni più precise in merito a fattibilità, attuazione e finanziamento dell'interoperabilità. L'**UDC** critica il fatto che nell'ambito della sua adesione a Schengen, la Svizzera recepisca una normativa senza che sia possibile stimare in maniera adeguata le ripercussioni finanziarie. Chiede pertanto di documentare costantemente gli oneri aggiuntivi degli sviluppi in modo tale che, in caso di ritardi del progetto, sia eventualmente possibile effettuare una nuova valutazione.

Il **PSS** critica la mancata distinzione tra diritti e doveri della Confederazione e dei Cantoni e il fatto che, in base alla pianificazione attuale, il Consiglio federale preveda il trasferimento unilaterale degli elevati costi di investimento alla Confederazione, sebbene i Cantoni dispongano di competenze importanti in materia di migrazione e sicurezza pubblica.

Attuazione giuridica

BL e **SO** evidenziano l'esigenza di intervenire sul piano legislativo cantonale così come la conseguente necessità di coordinamento e armonizzazione. Per la creazione delle basi giuridiche a livello cantonale, **BL** propone di utilizzare come base il modello del concordato di polizia della Svizzera nordoccidentale per lo scambio di dati di polizia tra i Cantoni. Con lettera del 6 novembre 2019 la **CCPCS** ha sottoposto alla **CDDGP** la medesima proposta. Anche **NW** appoggia la proposta.

OW rammenta che occorre tenere conto dei costi aggiuntivi che scaturirebbero per i Cantoni in seguito alle modifiche previste a livello di ordinanza.

VD parte dal presupposto che lo sviluppo dell'acquis di Schengen non avrà ripercussioni di alcun tipo sulla legislazione cantonale.

Piattaforma nazionale di ricerca

BL e **SO** evidenziano la necessità di creare una piattaforma nazionale di ricerca per agevolare lo scambio dei dati di polizia provenienti dai sistemi cantonali e nazionali. L'**UDC** accoglie la creazione di uno strumento nazionale di ricerca e rimanda alla mozione Eichenberger[6] adottata da entrambe le Camere federali. Secondo **SO,** la necessità di legiferare a livello cantonale vale anche per il progetto di introdurre una piattaforma nazionale di ricerca. Anche in questo caso si potrebbe utilizzare il modello di concordato di polizia della Svizzera nordoccidentale proposto per l'interoperabilità.

[6] Mozione 18.3592 «Scambio di dati di polizia su scala nazionale»

2.3.3 Tutela dei diritti fondamentali e protezione dei dati

OSAR, USS, **AsyL** e **PSS** si esprimono a favore di un rafforzamento della tutela dei diritti fondamentali e della protezione dei dati personali. **OSAR** e **PSS** si appellano al parere[7] del Garante europeo della protezione dei dati in merito all'interoperabilità e ne condividono i timori secondo cui l'interoperabilità «potrebbe diventare uno strumento pericoloso per i diritti fondamentali».

OSAR e **USS** chiedono che vengano introdotti soltanto i regolamenti verificati, valutati e approvati dall'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

OSAR disapprova il fatto che nel progetto non si menzioni il diritto di cittadini di Stati terzi di accedere ai propri dati o al relativo trattamento.

SO evidenzia che con l'interoperabilità possono insorgere nuovi rischi per la protezione dei dati e che occorre dunque attuare in modo coerente le disposizioni in materia di protezione dei dati. **TG** chiede che vengano disciplinati in maniera dettagliata gli obblighi dello Stato in materia di controlli affinché si possa conferire la giusta importanza alla protezione e alla sicurezza dei dati. **SO** e **PLR** sottolineano la necessità di rispettare in modo coerente le norme relative alle competenze e le disposizioni concernenti la protezione dei dati.

L'**UDC** ritiene che il progetto non sollevi particolari problemi per quanto riguarda la protezione dei dati poiché non sono raccolti dati supplementari e i diritti di accesso ai singoli sistemi rimangono invariati.

Nel suo parere, **TI** evidenzia una divergenza con l'Incaricato cantonale della protezione dei dati il quale esprime i propri dubbi per quanto riguarda la protezione dei dati personali nel quadro dell'interoperabilità.

SO ritiene che i diritti delle persone oggetto di controlli siano garantiti.

Legge sulla protezione dei dati in ambito Schengen

PLR ritiene che la protezione dei dati personali sensibili debba essere garantita tramite la legge sulla protezione dei dati in ambito Schengen.

Piattaforma di collegamento con il Garante europeo della protezione dei dati (GEPD)

OSAR, USS e **PSS** criticano la mancanza di chiarezza giuridica per quanto riguarda la piattaforma di collegamento con il GEDP e l'autorità di controllo nazionale. **OSAR** e **USS** contestano il mancato collegamento con la nuova legge sulla protezione dei dati in ambito Schengen. Tali interfacce dovrebbero essere chiarite e disciplinate a livello di legge. Il **PSS** chiede che venga chiarito a chi compete la responsabilità di collaborare con il GEDP in qualità di autorità nazionale di controllo. Secondo il **PSS** tale competenza spetta all'IFPDT, il quale dovrebbe essere rivalutato in un'autorità di controllo indipendente. Sarebbe inoltre necessario chiarire a chi spetta redigere il capitolo sulla Svizzera destinato a integrare la relazione periodica sulle attività in seno all'UE e a quale istanza in Svizzera debba essere trasmessa per conoscenza la relazione globale e in quale forma.

Notifica all'autorità segnalante in caso di consultazione delle banche dati di Interpol

AsyL, **USS** e **OSAR** criticano il fatto che in caso di consultazione delle banche dati di Interpol tramite l'ESP, l'autorità segnalante venga informata in caso di riscontro positivo in merito alla data e al luogo della consultazione. L'**AsyL** chiede che il proprietario dei dati non riceva in nessun caso informazioni sul fatto che le sue banche dati sono state consultate tramite l'ESP.

[7] Sintesi del parere del Garante europeo della protezione dei dati sulle proposte di due regolamenti che istituiscono un quadro per l'interoperabilità tra i sistemi di informazione su larga scala dell'UE (GU C 233 del 4.7.2018, pag. 12).

L'**OSAR** chiede, tenendo conto del fatto che tale richiesta renderebbe necessario attuare modifiche delle norme presso Interpol, che al momento di trasporre l'interoperabilità nel diritto nazionale venga previsto per lo meno un attento controllo.

Abuso di dati da parte di terzi

AsyL, PSS e **TG** temono che vi sia un rischio maggiore di abuso di dati da parte di terzi (privati o Stati terzi, p. es. tramite attacchi di hacking). L'**AsyL** chiede di allestire chiari scenari di emergenza.

Margine d'errore

L'**OSAR** fa notare che potrebbero diffondersi informazioni errate a livello nazionale e internazionale per via della dimensione dei sistemi d'informazione collegati, del grado di utilizzo e del numero di Stati collegati. Ciò condurrebbe a un aumento notevole di falsi riscontri positivi compromettendo gravemente la tutela dei diritti fondamentali.

L'**AsyL** ritiene che il MID sollevi questioni piuttosto delicate. Nei regolamenti UE sull'interoperabilità non risulta chiaro come gestire le persone che dispongono legittimamente di più identità. L'**AsyL** prevede che il MID presenterà una percentuale di errore talmente elevata da non poter soddisfare le esigenze in materia di protezione dei dati e ritiene dunque che tale margine di errore è da considerarsi sproporzionato. L'**OSAR** chiede di inserire esplicitamente una clausola di salvaguardia per le persone che dispongono di più identità legittime. I soggetti particolarmente a rischio sono secondo l'**OSAR** le donne che cambiano il proprio cognome in seguito al matrimonio, persone con doppia nazionalità o persone con nomi molto comuni. Tali problemi potrebbero accentuarsi in particolare nel caso di cittadini di Stati terzi, specialmente per le persone provenienti da Paesi in cui la lingua ufficiale non è scritta con l'alfabeto latino e i cui nomi devono essere traslitterati nelle banche dati dell'UE.

Limitazione delle finalità

AsyL e **OSAR** criticano il fatto che con il collegamento delle banche dati viene meno il principio della limitazione delle finalità dei diversi sistemi. L'interoperabilità consentirebbe di utilizzare i dati per nuovi scopi per i quali non erano stati previsti originariamente.

Secondo il **PSS,** i criteri vaghi menzionati nell'articolo 20 dei regolamenti UE sull'interoperabilità potrebbero condurre a consultazioni di routine, il che andrebbe contro il principio della limitazione delle finalità.

Sanzioni

L'**AsyL** ritiene che le multe previste in caso di violazioni della protezione dei dati siano sanzioni troppo poco severe rispetto alla gravità della violazione. Occorrerebbe dunque sancire per legge la possibilità di comminare una pena più severa.

Dotazione di risorse alle autorità di controllo sulla protezione dei dati

Privatim, OSAR, USS e **SO** evidenziano che le autorità di controllo nazionali e cantonali sulla protezione dei dati dovranno assumere compiti supplementari e che pertanto la Confederazione e i Cantoni dovranno fare in modo che vengano fornite loro le risorse necessarie. **Privatim** chiede che le risorse necessarie siano indicate al numero 6.3 del rapporto esplicativo.

2.3.4 Stigmatizzazione e discriminazione di cittadini di Stati terzi

AsyL, OSAR, **USS** e **PSS** vedono nel progetto un ulteriore passo verso la discriminazione, la disparità di trattamento e la stigmatizzazione di cittadini di Stati terzi rispetto ai cittadini UE/AELS, in particolare attraverso l'uso sistematico di dati biometrici. Il **PSS** chiede di presentare le cifre che quantifichino l'entità della frode di identità da parte di cittadini di Stati terzi.

OSAR, **USS** e **PSS** ritengono peraltro assai problematica la tendenza soggiacente al progetto a considerare la migrazione principalmente nell'ottica della sicurezza interna.
L'**OSAR** sottolinea che le autorità di controllo devono garantire che nella prassi il CIR venga consultato ai fini di identificazione tramite dati biometrici soltanto come ultima opzione al fine di impedire la stigmatizzazione e la discriminazione di persone in base al loro aspetto o alla loro presunta origine etnica o nazionalità.

2.3.5 Base costituzionale, basi giuridiche

Il **PSS** critica l'insufficienza della base costituzionale materiale (cfr. n. 7.1 del rapporto esplicativo) poiché la trasposizione dei regolamenti UE va ben oltre i confini della politica estera.
Il **PSS** lamenta inoltre il fatto che non risulta chiaro quali norme dei regolamenti UE sono riprese nelle disposizioni di legge e quali invece sono considerate direttamente applicabili. Di conseguenza non sono riprese disposizioni importanti in materia di diritti fondamentali, protezione dei dati e autorità di controllo e nemmeno le misure di valutazione e di qualità dei dati.

Delega al Consiglio federale

Il **PSS** ritiene problematico il fatto che in più punti è prevista la competenza di delega al Consiglio federale. L'**OSAR** critica il fatto che nel progetto posto in consultazione manchi un riferimento alla delega al Consiglio federale delle disposizioni di attuazione sulla protezione dei dati.

2.4 Pareri sui singoli articoli del decreto federale

2.4.1 Legge sugli stranieri e la loro integrazione (LStrI)[8]

Art. 101 segg. AP-LStrI: l'**ASM** parte dal presupposto che le modifiche previste alla LStrI, in particolare agli articoli 101 e seguenti, oltre a VIS, ORBIS, SIS ed Eurodac, riguardino anche il SIMIC, sebbene non sia menzionato esplicitamente.

Art. 101 AP-LstrI: Trattamento dei dati

Art. 101 cpv. 2 AP-LStrI: **OSAR** e **USS** criticano il fatto che l'articolo 20 paragrafo 5 dei regolamenti UE sull'interoperabilità che impone di adottare misure legislative nazionali volte a evitare qualsiasi discriminazione nei confronti di cittadini di Stati terzi non sia stato trasposto nell'avamprogetto. L'**OSAR** propone di introdurre la seguente integrazione alla fine dell'articolo: «*È garantita la dignità umana e l'integrità delle persone di cui sono trattati i dati e sono adottate le misure necessarie al fine di evitare qualsiasi discriminazione».*

Art. 101 cpv. 3 e 4 AP-LStrI (nuovi): il **PSS** propone la seguente integrazione:

«[3] *L'autorità competente per il trattamento dei dati impiega un servizio di controllo interno. Quest'ultimo vigila:*

a. sul rispetto di elevati standard di qualità;

b. su una gestione completa dei rischi in materia di sicurezza delle informazioni;

c. sulla legalità, l'adeguatezza, l'efficacia e la correttezza dei trattamenti dei dati e controlla a campione i verbali di utilizzo dei sistemi d'informazione Schengen/Dublino e il rispetto della legge sulla protezione dei dati.

[8] RS **142.20**

[4] *Il servizio di controllo interno allestisce annualmente un rapporto all'attenzione dell'Incaricato federale per la protezione dei dati e della trasparenza (IFPDT).*»

Art. 110: Servizio comune di confronto biometrico (sBMS)

Art. 110 cpv. 2 AP-LStrI: **OSAR** e **USS** propongono di chiarire all'interno di un periodo supplementare che un'autorità che avvia una consultazione nell'sBMS, vede soltanto i riferimenti a quei sistemi d'informazione dell'UE cui ha accesso (cfr. commento all'art. 18*a* cpv. 1 LSIP).

Art. 110*b* AP-LStrI: Consultazione del CIR a fini di identificazione

Art. 110*b* cpv. 1 AP-LStrI: **OSAR** e **USS** ritengono che l'articolo sia formulato in modo troppo vago e incompleto in quanto indebolisce il principio di esclusività previsto dall'articolo 20 paragrafo 2 dei regolamenti UE sull'interoperabilità. La nuova formulazione proposta è pertanto la seguente: «*Il CIR può essere consultato soltanto da un'autorità ai sensi del capoverso 3 e unicamente ai fini dell'identificazione di una persona*».

Art. 110b cpv. 2 AP-LStrI: l'**OSAR** critica il fatto che gli scopi siano formulati in modo troppo ampio e vago contraddicendo quindi i requisiti posti dall'articolo 20 paragrafo 5 dei regolamenti UE sull'interoperabilità. Anche il **PSS** considera troppo ridotta la densità normativa e propone la seguente aggiunta:

«[2] *… e salvaguardare la sicurezza nazionale. La consultazione del CIR avviene di norma in presenza dell'interessato e se quest'ultimo:*

a. non è in grado di collaborare e non può esibire alcun documento dal quale si evince la sua identità; o

b. si rifiuta di collaborare; o

c. se vi è il sospetto fondato che il documento esibito sia falso o che l'interessato non stia dicendo la verità sulla propria identità.

[2bis] *È vietata la duplicazione dei dati personali contenuti nel CIR.*»

Art. 110*b* cpv. 4 AP-LStrI: l'**OSAR** chiede di aggiungere che la consultazione debba avvenire sul posto e *«in presenza dell'interessato»*, come previsto nell'articolo 20 paragrafo 2 dei regolamenti UE sull'interoperabilità.

Art. 110*c* AP-LStrI: Consultazione del CIR a fini di individuazione di identità multiple

L'**ASM** sottolinea che la cerchia di autorità che dispongono dei diritti di accesso dovrebbe essere sufficientemente ampia affinché si possa rispondere al modello dei quattro filtri previsto dal piano d'azione IBM.

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

OSAR e **USS** raccomandano di precisare che le autorità di perseguimento penale che hanno un riscontro positivo devono sempre rivolgersi all'autorità di controllo al fine di verificare se le condizioni per l'accesso al CIR erano soddisfatte. Inoltre chiedono di disciplinare in modo più chiaro a livello di legge che per «altri reati gravi» si intendono i reati per i quali è prevista una pena detentiva di almeno tre anni, in particolare alla luce del fatto che il SIC ha accesso a dati personali sensibili.

OSAR e **PSS** criticano l'accesso agevolato da parte delle autorità di perseguimento penale ai dati contenuti nei sistemi d'informazione sulla migrazione. Il **PSS** vi ravvisa uno stravolgimento dei principi dello Stato di diritto in materia di perseguimento penale. Secondo l'**OSAR** ricorrere a un sistema di riscontro positivo o negativo significherebbe eliminare il meccanismo a cascata.

L'**UDC** approva l'accesso da parte delle autorità di polizia e migratorie poiché in questo modo anche le persone che si trovano già nello spazio Schengen possono essere identificate in modo più efficace in relazione alla loro persona e al loro statuto di soggiorno.

Art. 111*k* AP-LStrI (nuovo): Autorità nazionale di controllo e rapporto

Il **PSS** propone di inserire il nuovo articolo seguente:

«[1] L'autorità nazionale di controllo ai sensi dell'articolo 51 paragrafo 1 del regolamento generale sulla protezione dei dati (regolamento [UE] 2016/679) è l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT).

[2] Nell'ambito delle sue competenze, l'IFDPT ha la facoltà di impartire istruzioni alle autorità responsabili per il trattamento dei dati contenuti nei sistemi d'informazione Schengen/Dublino.

[3] L'IFDPT pubblica ogni anno il numero delle richieste di rettifica, cancellazione o limitazione del trattamento di dati personali, le misure successive adottate e il numero delle rettifiche, cancellazioni e limitazioni del trattamento effettuate in seguito alle richieste degli interessati (art. 51 par. 2 dei regolamenti [UE] 2019/817 e [UE] 2019/818).

[4] *L'IFDPT collabora con il Garante europeo della protezione dei dati e le altre autorità nazionali di controllo. Riferisce a quest'ultimo nel caso accerti discrepanze rilevanti tra le procedure adottate dai Paesi membri o trasmissioni illecite tramite i canali di comunicazione delle componenti di interoperabilità e trae le conclusioni per la Svizzera dalla relazione di valutazione redatta annualmente dalla Commissione europea sull'attuazione dei requisiti in materia di qualità dei dati da parte degli Stati membri (art. 37 par. 5 dei regolamenti [UE] 2019/817 e [UE] 2019/818).*

[5] L'IFDPT allestisce ogni due anni un rapporto all'attenzione del Parlamento svizzero e del Garante europeo della protezione dei dati sul trattamento dei dati nei sistemi d'informazione Schengen/Dublino.

[6] L'IFDPT controlla nell'ambito delle sue competenze l'attuazione delle raccomandazioni dell'UE sulla trasposizione e sull'applicazione del diritto Schengen in Svizzera.

[7] Il Consiglio federale provvede affinché l'IFDPT, quale autorità nazionale di controllo, disponga delle risorse e delle conoscenze specialistiche sufficienti per assolvere i compiti assegnatigli (art. 51 par. 4 dei regolamenti [UE] 2019/817 e [UE] 2019/818).»

2.4.2 Legge federale sui sistemi d'informazione di polizia della Confederazione[9]

Art. 18*a* LSIP: Servizio comune di confronto biometrico (sBMS)

Art. 18*a* cpv. 2 LSIP: **OSAR** e **USS** propongono di chiarire in un periodo supplementare che un'autorità che avvia una consultazione nell'sBMS veda unicamente i riferimenti ai sistemi d'informazione dell'UE cui ha accesso (cfr. commento all'art. 110 cpv. 2 AP-LStrI).

Art. 18*d* LSIP: Verifica manuale di collegamenti nel MID

Art. 18*d* LSIP: Verifica manuale di collegamenti nel MID

Il **PSS** chiede di introdurre scadenze fisse con termini concreti e di definire una procedura chiara che permetta di verificare tempestivamente i collegamenti nel MID. Propone la seguente formulazione: «*[3bis] La verifica manuale delle identità diverse avviene, ove possibile, sempre entro 12 ore dall'accertamento e dalla comunicazione di un collegamento non verificato. L'interessato è informato senza indugio sempreché una tale comunicazione non pregiudichi interessi preponderanti in materia di sicurezza.»*

[9] RS **361**

2.4.3 Legge sulla responsabilità[10]

Art. 19*b* LResp

Art. 19*b* cpv. 1 LResp: **TG** evidenzia che il primo periodo statuisce che la Confederazione risponde del danno causato a terzi «*senza che sia necessario provare l'illiceità»,* tuttavia la lettera a prevede che affinché sussista una responsabilità occorre una memorizzazione «*indebita».* Non è quindi chiaro se questa disposizione sia una norma di responsabilità causale o se, affinché vi sia una responsabilità, debba tuttavia sussistere l'illiceità.

[10] RS **170.32**

3 Elenco dei partecipanti

Cantoni

Cantone di Argovia, Consiglio di Stato	**AG**
Cantone di Appenzello Interno, Consiglio di Stato	**AI**
Cantone di Appenzello Esterno, Consiglio di Stato	**AR**
Cantone di Berna, Consiglio di Stato	**BE**
Cantone di Basilea Campagna, Consiglio di Stato	**BL**
Cantone di Basilea Città, Consiglio di Stato	**BS**
Cantone di Friburgo, Consiglio di Stato	**FR**
Cantone di Ginevra, Consiglio di Stato	**GE**
Cantone di Glarona, Consiglio di Stato	**GL**
Cantone dei Grigioni, Consiglio di Stato	**GR**
Cancelleria dello Stato del Cantone del Giura	**JU**
Cantone di Lucerna, Consiglio di Stato	**LU**
Cantone di Neuchâtel, Consiglio di Stato	**NE**
Cantone di Nidvaldo, Consiglio di Stato	**NW**
Cantone di Obvaldo, Consiglio di Stato	**OW**
Cantone di San Gallo, Consiglio di Stato	**SG**
Cantone di Sciaffusa, Consiglio di Stato	**SH**
Cantone di Soletta, Consiglio di Stato	**SO**
Cantone di Svitto, Consiglio di Stato	**SZ**
Cantone di Turgovia, Consiglio di Stato	**TG**
Repubblica e Cantone Ticino, Consiglio di Stato	**TI**
Cantone di Uri, Consiglio di Stato	**UR**
Cantone di Vaud, Consiglio di Stato	**VD**
Cantone del Vallese, Consiglio di Stato	**VS**
Cantone di Zugo, Consiglio di Stato	**ZG**
Cantone di Zurigo, Consiglio di Stato	**ZH**

Partiti politici

PLR.I Liberali Radicali	PLR
Partito socialista svizzero	PSS
Unione Democratica di Centro	UDC

Tribunali federali

Tribunale amministrativo federale	TAF

Associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna

Associazione dei Comuni Svizzeri	ACS
Unione delle città svizzere	UCS

Associazioni mantello nazionali dell'economia

Unione svizzera degli imprenditori	USI
Associazione degli uffici svizzeri del lavoro	AUSL
Unione sindacale svizzera	USS

Le cerchie interessate

AsyLex	AsyL
Fédération des Entreprises Romandes	FER
Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia	CDDGP
Conferenza dei comandanti delle polizie cantonali	CCPCS
privatim Conferenza degli incaricati svizzeri per la protezione dei dati	privatim
Organizzazione svizzera di aiuto ai rifugiati (OSAR)	OSAR
Società Svizzera di diritto penale	SSDP

Associazione svizzera dei magistrati	
Associazione dei servizi cantonali di migrazione	ASM