Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2023
www.fedlex.admin.ch
La versione elettronica firmata
è quella determinante

23.073

Messaggio concernente la legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici

del 22 novembre 2023

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici nonché il disegno di decreto federale che stanzia crediti d'impegno per l'implementazione e la gestione dell'Id-e.

Nel contempo vi proponiamo di togliere dal ruolo i seguenti interventi parlamentari:

2021 M 21.3124	Identità elettronica statale affidabile (N 14.9.21; S 13.6.22)
2021 M 21.3125	Identità elettronica statale affidabile (N 14.9.21; S 13.6.22)
2021 M 21.3126	Identità elettronica statale affidabile (N 14.9.21; S 13.6.22)
2021 M 21.3127	Identità elettronica statale affidabile (N 14.9.21; S 13.6.22)
2021 M 21.3128	Identità elettronica statale affidabile (N 14.9.21; S 13.6.22)
2021 M 21.3129	Identità elettronica statale affidabile (N 14.9.21; S 13.6.22)

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

22 novembre 2023

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Alain Berset
Il cancelliere della Confederazione, Walter Thurnherr

Compendio

Un nuovo mezzo d'identificazione elettronico (Id-e), gratuito e facoltativo, permetterà di provare la propria identità per via elettronica in maniera semplice, sicura e rapida. Emesso dalla Confederazione, esso garantirà il livello più elevato possibile di protezione dei dati personali. I titolari avranno il massimo controllo possibile sui loro dati. L'infrastruttura di fiducia, implementata dalla Confederazione per gestire gli Id-e, potrà pure essere utilizzata da altre autorità nonché dagli attori del settore privato che intendono emettere e verificare mezzi di autenticazione elettronici.

Situazione iniziale

Dopo l'esito negativo della votazione popolare del 7 marzo 2021 sulla legge federale sui servizi d'identificazione elettronica, il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia di delineare, in collaborazione con la Cancelleria federale e il Dipartimento federale delle finanze , una soluzione per un mezzo d'identificazione elettronico statale. Nel frattempo, il Consiglio nazionale e il Consiglio degli Stati hanno accolto sei identiche mozioni, depositate da tutti i gruppi parlamentari, che chiedevano la messa a punto di un sistema gestito dallo Stato atto a provare la propria identità in rete.

Desiderando coinvolgere da subito le cerchie interessate nell'elaborazione della nuova legge, nell'autunno 2021 l'Ufficio federale di giustizia ha avviato una consultazione pubblica informale. Fondandosi sui pareri ricevuti, il 17 dicembre 2021 il Consiglio federale ha preso una decisione di principio in cui ha posto le fondamenta del futuro Id-e. L'avamprogetto di legge è stato posto in consultazione dal 29 giugno 2022 al 20 ottobre 2022.

Contenuto del progetto

Il nuovo Id-e permetterà di identificarsi elettronicamente in maniera semplice, sicura e rapida. Potrà farne richiesta chiunque sia titolare di una carta d'identità svizzera, di un passaporto svizzero o di una carta di soggiorno per stranieri rilasciata in Svizzera. La Confederazione fornirà un'applicazione per smartphone con la quale l'utente potrà gestire il suo Id-e in tutta sicurezza. L'Id-e potrà essere utilizzato sia in Internet (ad es. per ordinare online un estratto del casellario giudiziale) sia nel mondo reale (ad es. per provare la propria età al fine di acquistare alcolici). Contrariamente a quanto prevedeva la legge respinta in votazione, sarà la Confederazione a emettere gli Id-e e a gestire l'infrastruttura necessaria.

I titolari dell'Id-e avranno il massimo controllo possibile sui loro dati (identità autosovrana o autogestita o «self-sovereign identity»). La protezione dei dati sarà garantita dal sistema stesso (principio della protezione dei dati fin dalla progettazione e per impostazione predefinita), come richiesto dalle mozioni depositate, nonché dalla limitazione del flusso di dati necessari (principio della minimizzazione dei dati) e dal loro salvataggio decentralizzato. Inoltre, il Consiglio federale ha formulato il testo di legge in maniera il più possibile neutra sul piano tecnologico affinché il sistema possa adeguarsi costantemente al più recente stato della tecnica. Ad ogni modo il sistema

svizzero d'identificazione elettronica rispetterà le norme internazionali così che l'Id-e possa essere riconosciuto e utilizzato anche all'estero.

L'utilizzo dell'Id-e sarà gratuito e facoltativo. Accanto a quella elettronica, rimarrà comunque possibile anche l'identificazione fisica sul posto. D'altra parte tutte le autorità, comprese quelle cantonali e comunali, dovranno accettare l'Id-e quando ricorrono all'identificazione elettronica, ad esempio al momento di rilasciare un certificato di domicilio o un estratto del registro delle esecuzioni.

L'infrastruttura di fiducia implementata dalla Confederazione per gestire gli Id-e potrà essere utilizzata pure dalle autorità cantonali e comunali nonché da privati che intendono emettere mezzi di autenticazione elettronici. I documenti ufficiali come i certificati di domicilio o gli estratti del registro delle esecuzioni, nonché i diplomi, i biglietti di concerti o le tessere di membro potranno quindi essere emessi in forma elettronica con l'ausilio dell'infrastruttura di fiducia dello Stato e poi salvati e gestiti in tutta sicurezza nell'applicazione fornita dalla Confederazione o in un'applicazione di propria scelta.

Il Consiglio federale sottopone al Parlamento anche un decreto federale che stanzia crediti d'impegno per l'implementazione e la gestione dell'Id-e, con il quale propone un credito supplementare di 13,5 milioni di franchi nonché due altri crediti d'impegno per un importo totale di 85,1 milioni di franchi.

Indice

Compendio **2**

1 Situazione iniziale **6**

1.1 Rapporto con il programma di legislatura e il piano finanziario, nonché con le strategie del Consiglio federale 7

1.2 Stralcio di interventi parlamentari 8

2 Procedura preliminare, in particolare procedura di consultazione **8**

2.1 La prima legge federale sui servizi d'identificazione elettronica 8

2.2 Documento di discussione degli obiettivi dell'Id-e 9

2.3 Decisione di principio del Consiglio federale 10

2.4 Riassunto dei risultati della procedura di consultazione 10

2.4.1 Osservazioni generali 10

2.4.2 Osservazioni sulla nozione di identità elettronica autogestita e sul ruolo dello Stato 10

2.4.3 Singoli aspetti 11

2.5 Valutazione dei risultati della procedura di consultazione 11

3 Diritto comparato, in particolare rapporto con il diritto europeo **12**

4 Punti essenziali del progetto **13**

4.1 La normativa proposta 13

4.2 Compatibilità tra compiti e finanze 14

4.3 Attuazione 14

5 Commento ai singoli articoli **14**

6 Ripercussioni **48**

6.1 Ripercussioni per la Confederazione 48

6.2 Ripercussioni per i Cantoni e i Comuni, per le città, gli agglomerati e le regioni di montagna 51

6.3 Ripercussioni sull'economia 53

6.4 Ripercussioni sulla società 53

6.5 Ripercussioni sull'ambiente 54

7 Aspetti giuridici **54**

7.1 Costituzionalità 54

7.2 Compatibilità con gli impegni internazionali della Svizzera 54

7.3 Forma dell'atto 55

7.4 Subordinazione al freno alle spese 55

7.5 Rispetto del principio di sussidiarietà e del principio dell'equivalenza fiscale 55

7.6 Conformità alla legge sui sussidi 55

7.7 Delega di competenze legislative 56

7.8 Protezione dei dati 56

Legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (Legge sull'Id-e, LIdE) *(Disegno)* FF **2023** 2843

Decreto federale che stanzia crediti d'impegno per l'implementazione e la gestione dell'Id-e *(Disegno)* FF 2**023** 2844

Messaggio

1 Situazione iniziale

Il 7 marzo 2021, la legge federale sui servizi d'identificazione elettronica è stata respinta alle urne dal 64 per cento dei votanti. Il 10 marzo 2021, i rappresentanti di tutti i gruppi parlamentari hanno depositato sei mozioni dal medesimo tenore intitolate «Identità elettronica statale affidabile» (cfr. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 e 21.3129). Inoltre, nei tre mesi successivi alla votazione sono state depositate le interpellanze Andrey 21.3310 La carta d'identità come componente di una futura soluzione Ie e Graf-Litscher 21.3718 Identità elettroniche auto-sovrane. Le sei mozioni sono state accolte dal Consiglio nazionale il 14 settembre 2021 e dal Consiglio degli Stati il 13 giugno 2022. I dibattimenti relativi all'interpellanza Andrey 21.3310 sono stati rinviati e conclusi il 17 marzo 2023. Inoltre, il Consiglio nazionale ha deciso di liquidare l'interpellanza Graf-Litscher 21.3718.

In occasione della sua seduta del 26 maggio 2021, il Consiglio federale ha dichiarato che intendeva presentare in tempi rapidi una nuova soluzione per l'identificazione elettronica che tenesse conto delle preoccupazioni degli autori delle mozioni. Ha quindi incaricato il Dipartimento federale di giustizia e polizia (DFGP) di elaborare, in collaborazione con il Dipartimento federale delle finanze (DFF), la Cancelleria federale (CaF), i Cantoni e i due politecnici federali di Zurigo e Losanna, una bozza di testo entro fine 2021. Si trattava in particolare di esaminare le diverse possibilità tecniche per realizzare l'Id-e e di precisarne i corrispondenti costi.

In collaborazione con i Cantoni e alcuni esperti del mondo della scienza il DFGP ha preparato un documento di discussione degli obiettivi dell'Id-e[1] (qui di seguito «documento di discussione») che propone diverse definizioni dell'Id-e e della relativa infrastruttura di fiducia nonché tre soluzioni tecniche di realizzazione: l'identità autogestita («*self-sovereign identity*», SSI), l'infrastruttura a chiave pubblica («public key infrastructure», PKI) e il fornitore d'identità («identity provider», IdP) centrale dello Stato. In particolare, espone in dettaglio anche le modalità d'integrazione di ogni soluzione negli scambi economici e sociali nonché una serie di esempi di utilizzo di un Id-e statale.

Il documento di discussione è stato oggetto di una consultazione pubblica informale dal 2 settembre al 14 ottobre 2021. Sono pervenuti 60 pareri, inoltrati da amministrazioni cantonali nonché rappresentanti degli ambienti scientifici, delle organizzazioni economiche e delle imprese[2]. Per concludere la consultazione, il 14 ottobre 2021 il DFGP ha organizzato un dibattito pubblico sotto forma di conferenza che ha riunito 50 rappresentanti dei Cantoni, dei partiti, del mondo scientifico, della società civile e dell'economia nonché privati interessati. La consultazione pubblica informale mirava a raccogliere i pareri sulle principali esigenze cui dovrebbe rispondere l'Id-e, i suoi

1 www.bj.admin.ch > Stato & Cittadino > Progetti di legislazione in corso > Id-e statale > Documento di discussione degli obiettivi dell'Id-e

2 www.bj.admin.ch > Stato & Cittadino > Progetti di legislazione in corso > Id-e statale > Riassunto dei risultati della consultazione pubblica concernente gli obiettivi dell'Id-e

principali settori di utilizzo e i benefici attesi. Si trattava inoltre di conoscere l'opinione delle persone interessate sulla portata dell'ecosistema Id-e. Le informazioni acquisite hanno permesso al Consiglio federale di prendere una decisione di principio concernente il nuovo orientamento dell'Id-e.

I partecipanti alla consultazione si sono espressi a favore della soluzione SSI. Hanno parimenti sottolineato la necessità di un'infrastruttura di fiducia con un livello di ambizione 3 (cfr. documento di discussione, n. 4.2). Questa soluzione tiene conto delle domande poste dalle sei mozioni depositate in seguito alla votazione. Nel quadro dei futuri lavori occorrerà considerare questa volontà nonché i principi del rispetto della vita privata fin dalla progettazione («privacy by design»), della minimizzazione dei dati e del salvataggio decentralizzato dei dati. Il DFGP intende inoltre collaborare più strettamente con gli uffici e i Cantoni che svolgono progetti pilota in materia.

Fondandosi sui risultati della consultazione pubblica informale, il 17 dicembre 2021 il Consiglio federale ha preso una decisione di principio secondo cui il nuovo orientamento del progetto Id-e avrebbe seguito un approccio basato sui principi del rispetto della vita privata fin dalla progettazione, della minimizzazione dei dati e del salvataggio decentralizzato dei dati nonché su un'infrastruttura di fiducia statale che consenta di implementare un ecosistema di mezzi di autenticazione elettronici emessi da attori pubblici e privati. Ha delegato al DFGP la responsabilità di assicurare, in collaborazione con il DFF (Amministrazione digitale Svizzera, ADS) e la CaF (settore Trasformazione digitale e governance delle TIC, TDT), il flusso di informazioni e di coordinare le interazioni tra l'avamprogetto e i pertinenti progetti della Confederazione e dei Cantoni.

L'avamprogetto di legge è stato posto in consultazione dal 29 giugno al 20 ottobre 2022. Sono pervenuti 117 pareri, di cui la maggior parte positivi. Ha riscosso plauso, in particolare, la nuova distribuzione dei ruoli, con lo Stato come emittente del mezzo d'identificazione elettronico e gestore dell'infrastruttura di fiducia su cui si basa l'Id-e. Dai pareri emerge una chiara volontà di trovare una soluzione stabile, sicura e di facile utilizzo. Sulla base dei risultati della consultazione il Consiglio federale ha elaborato il presente disegno di legge.

1.1 Rapporto con il programma di legislatura e il piano finanziario, nonché con le strategie del Consiglio federale

Il disegno di legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'Id-e) è stato annunciato nel messaggio del 27 gennaio 2016[3] sul programma di legislatura 2015–2019 e nel decreto federale del 14 giugno 2016[4] sul programma di legislatura 2015–2019. In seguito all'esito negativo della votazione del 7 marzo 2021, il Consiglio federale ha deciso di rilanciare e reimpostare i lavori legislativi in materia d'identificazione elettronica. Il disegno non è stato annunciato né nel messaggio del

3 FF **2016** 909, in particolare 976 e 1026
4 FF **2016** 4605, in particolare 4607

29 gennaio 2020[5] sul programma di legislatura 2019–2023, né nel decreto federale del 21 settembre 2020[6] sul programma di legislatura 2019–2023.

1.2 Stralcio di interventi parlamentari

Il disegno di legge proposto attua gli interventi parlamentari seguenti:

– mozioni 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 e 21.3129 presentate da tutti i gruppi parlamentari e aventi tutte il titolo «Identità elettronica statale affidabile». Le mozioni chiedono al Consiglio federale di creare uno strumento d'identificazione elettronica statale, comparabile alla carta d'identità o al passaporto nel mondo reale e che consenta ai cittadini di comprovare la loro identità (autentificazione) nel mondo virtuale, osservando in particolare i principi della «privacy by design», della minimizzazione dei dati e della registrazione decentralizzata dei dati (come la registrazione dei dati dei documenti d'identità presso gli utenti). Le mozioni sono state accolte il 14 settembre 2021 dal Consiglio nazionale e il 13 giugno 2022 dal Consiglio degli Stati, secondo quanto proposto dal Consiglio federale.

Nel quadro dell'elaborazione del disegno sono stati presi in considerazione anche gli interventi parlamentari seguenti:

– interpellanza Andrey 21.3310 La carta d'identità come componente di una futura soluzione Ie. Il 26 maggio 2021 il Consiglio federale ha risposto alle domande poste nell'interpellanza. Il 17 marzo 2023 l'interpellanza è stata tolta dal ruolo poiché il Consiglio nazionale non ha concluso il suo esame entro il termine di due anni;

– interpellanza Graf-Litscher 21.3718 Identità elettroniche auto-sovrane. Il 18 agosto 2021 il Consiglio federale ha risposto alle domande, mentre il 1° ottobre 2021 il Consiglio nazionale ha deciso di liquidare l'interpellanza.

2 Procedura preliminare, in particolare procedura di consultazione

2.1 La prima legge federale sui servizi d'identificazione elettronica

I lavori legislativi relativi all'Id-e sono stati avviati nel 2013. Il 27 settembre 2019 il Parlamento ha adottato a larga maggioranza la legge federale sui servizi d'identificazione elettronica (Legge sull'Ie, LSIe), che prevedeva che l'Id-e fosse emessa da fornitori di identità privati sulla base dei dati identificativi messi loro a disposizione dall'Ufficio federale di polizia (fedpol). La Confederazione avrebbe attivamente assunto il ruolo di emittente di Id-e soltanto se non si fossero trovati dei fornitori di identità privati. Contro questo progetto è stato lanciato con successo il referendum e

5 FF **2020** 1565
6 FF **2020** 7365

la legge è stata nettamente respinta in occasione della votazione popolare del 7 marzo 2021. L'analisi Vox dei risultati della votazione ha tuttavia mostrato che la maggioranza dei votanti non si era espressa contro un'identificazione elettronica in sé ma contro il fatto che l'Id-e fosse emessa da fornitori privati.

2.2 Documento di discussione degli obiettivi dell'Id-e

Dopo il rifiuto della legge federale sui servizi d'identificazione elettronica, il 10 marzo 2021 sono state depositate sei mozioni di identico tenore (v. n. 1.2) che fissano gli obiettivi fondamentali del futuro mezzo d'identificazione elettronico senza tuttavia definire la strategia per conseguirli. Dato che la procedura di consultazione non è adatta a scegliere l'orientamento da dare al progetto, il 2 settembre 2021 la capodipartimento del DFGP ha avviato una consultazione pubblica informale sul documento di discussione degli obiettivi dell'Id-e in occasione dell'incontro del Comitato consultivo.

Il documento di discussione degli obiettivi dell'Id-e posto in consultazione fornisce una panoramica delle varie soluzioni, illustra e analizza possibili definizioni e dimensioni del futuro mezzo d'identificazione elettronico svizzero e dell'infrastruttura connessa e propone tre approcci tecnologici di realizzazione:

- identità autosovrana (SSI);
- infrastruttura a chiave pubblica (PKI);
- fornitore d'identità (IdP) centrale dello Stato.

La maggioranza dei partecipanti alla consultazione pubblica ha espresso preferenza per la SSI in quanto ritiene questa soluzione tecnica la più adatta per soddisfare i valori e le funzioni richiesti. Solo pochi hanno optato per le varianti PKI e IdP, principalmente poiché tali soluzioni sono conosciute da lungo tempo.

In merito alla questione se, per garantire la sicurezza, nell'attuazione si debba ricorrere a un *hard-token* (apparecchio/elemento fisico per la conservazione di chiavi digitali private), la maggioranza si è detta contraria per favorire la facilità d'uso. Per pochi partecipanti, invece, un'Id-e sicura non è possibile senza token fisico.

Oltre alla soluzione tecnica, il documento di discussione propone, in analogia alla discussione nell'UE, tre livelli di ambizione (ossia tre possibilità per il futuro utilizzo dell'Id-e):

- livello di ambizione 1: l'Id-e rimane l'unico mezzo d'identificazione elettronico disponibile;
- livello di ambizione 2: oltre all'Id-e, lo Stato può emettere anche altri mezzi di autenticazione elettronici
- livello di ambizione 3: non solo lo Stato, ma anche privati possono emettere mezzi di autenticazione elettronici.

Il livello di ambizione 3 è stato considerato l'obiettivo da conseguire da quasi tutti i partecipanti che si sono espressi in merito. Per alcuni di loro era tuttavia ipotizzabile un ampliamento graduale dal livello di ambizione 1 al livello 2 per arrivare infine

al livello 3. La consultazione è stata conclusa con una conferenza pubblica il 14 ottobre 2021.

2.3 Decisione di principio del Consiglio federale

Fondandosi sui risultati della consultazione informale condotta sul documento di discussione degli obiettivi dell'Id-e, il 17 dicembre 2021 il Consiglio federale ha stabilito i principi per la configurazione di un futuro mezzo d'identificazione elettronico statale: i titolari dell'Id-e devono avere il massimo controllo possibile sui loro dati («self-sovereign identity»); la protezione dei dati deve essere garantita tra l'altro dal sistema stesso («privacy by design»), ma anche mediante la limitazione dei flussi di dati necessari (principio della minimizzazione dei dati) e il salvataggio decentralizzato dei dati. L'Id-e deve fondarsi su un'infrastruttura gestita dallo Stato che potrebbe essere a disposizione di servizi statali e privati per l'emissione di diversi mezzi di autenticazione elettronici (ecosistema Id-e con livello di ambizione 3).

2.4 Riassunto dei risultati della procedura di consultazione

Il 29 giugno 2022 il Consiglio federale ha posto in consultazione l'avamprogetto della (seconda) legge sull'Id-e. La consultazione è durata fino al 20 ottobre 2022. In totale sono pervenuti 117 pareri.

2.4.1 Osservazioni generali

I pareri pervenuti sono per lo più positivi. È stata in particolare accolta con favore la nuova distribuzione dei ruoli, in cui lo Stato agisce da emittente del mezzo d'identificazione elettronico e da gestore della necessaria infrastruttura di fiducia. In generale è emerso chiaramente il desiderio che si trovi rapidamente una soluzione stabile, sicura e di facile utilizzo. Ha pure riscosso plauso la velocità con cui è stato elaborato l'avamprogetto di legge nonché la procedura partecipativa e trasparente.

Tre partecipanti respingono l'avamprogetto in generale. L'UDC ne mette in dubbio la costituzionalità. L'incaricato cantonale della protezione dei dati del Cantone Ticino e il Partito Pirata respingono il disegno per ragioni di protezione dei dati; il Partito Pirata fa inoltre valere ulteriori motivi.

2.4.2 Osservazioni sulla nozione di identità elettronica autogestita e sul ruolo dello Stato

Diversamente da quanto emerso nel quadro della respinta prima legge sull'eID con i privati in veste di emittenti dei mezzi d'identificazione elettronici, nei pareri concernenti il nuovo avamprogetto il ruolo dello Stato è stato tematizzato solo marginal-

mente. Nessuno ha contestato che lo Stato debba svolgere il ruolo principale nello sviluppo e nella gestione dell'infrastruttura di fiducia ed essere l'unico emittente del mezzo d'identificazione elettronico.

I pregi della soluzione di identità elettronica autogestita, che consente l'attuazione dei principi della «privacy by design», della minimizzazione dei dati e del salvataggio decentralizzato dei dati, sono stati riconosciuti. Al contempo è stato apprezzato che anche i privati possano utilizzare l'infrastruttura di fiducia.

2.4.3 Singoli aspetti

Nel quadro della consultazione sono risultati controversi soprattutto i seguenti aspetti:

- Diversi partecipanti hanno chiesto di estendere la cerchia degli aventi diritto a chiedere un Id-e, mentre altri hanno chiesto di restringerla al fine di garantire che l'Id-e sia rilasciato soltanto alle persone la cui identità può essere accertata in modo affidabile.
- Tra le numerose richieste riguardanti la procedura di emissione, una in particolare chiedeva di prevedere, oltre alla procedura di rilascio in linea, anche quella allo sportello.
- Ovviamente, il tema della protezione dei dati occupa un posto centrale nella maggior parte dei pareri. Numerosi partecipanti auspicano un livello di protezione più elevato, soprattutto per contrastare il rischio di un eccesso d'identificazione, ossia la richiesta di un Id-e senza un motivo legittimo oppure di un numero di componenti dell'Id-e maggiore di quello minimo necessario.
- L'avamprogetto di legge non si esprimeva in merito alla questione dell'accessibilità ai disabili in quanto lo Stato vi è comunque tenuto per legge. Ciò malgrado è stato a molte riprese chiesto di disciplinare espressamente questo aspetto nella legge sull'Id-e.
- L'avamprogetto prevede che i Cantoni designino i servizi tenuti a offrire assistenza in merito all'emissione e all'utilizzo dell'Id-e. Mentre la necessità di un sostegno è incontestata, numerosi partecipanti chiedono che la Confederazione assuma un ruolo più attivo e gestisca una helpdesk centrale. I Cantoni ritengono che a loro spetti soprattutto fornire assistenza in relazione all'utilizzo dell'Id-e nel quadro del Governo elettronico.

2.5 Valutazione dei risultati della procedura di consultazione

Contrariamente all'argomentazione dell'UDC, il Consiglio federale ritiene che la legge sull'Id-e poggi su una base costituzionale solida (v. n. 7.1). Le riserve sollevate dall'incaricato della protezione dei dati del Cantone Ticino e dal Partito Pirata in materia di protezione dei dati sono comprensibili ma non bastano a giustificare il rifiuto dell'avamprogetto di legge (v. n. 7.7).

Le seguenti proposte avanzate in sede di consultazione sono state integrate in particolare nel disegno di legge:

- sarà possibile ottenere l'Id-e non soltanto in linea ma anche allo sportello;
- saranno adottate restrizioni volte a impedire la richiesta di dati dell'Id-e non necessari all'ottenimento della prestazione desiderata e saranno previste sanzioni;
- l'accessibilità ai disabili sarà disciplinata esplicitamente;
- l'assistenza agli utenti per l'ottenimento dell'Id-e e l'utilizzo dell'infrastruttura di fiducia sarà fornita da fedpol e dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT), invece che dai servizi cantonali previsti nell'avamprogetto.

3 Diritto comparato, in particolare rapporto con il diritto europeo

L'Unione europea (UE) ha avviato una serie di riforme in materia d'identificazione elettronica. Il Consiglio federale ritiene necessario tener conto di questi sviluppi nella riflessione in proposito condotta a livello nazionale. Il 3 giugno 2021, la Commissione europea ha adottato una proposta[7] che modifica il regolamento (UE) n. 910/2014 (regolamento eIDAS) [8] e introduce un quadro giuridico per un'identità digitale europea. In base al nuovo regolamento, è previsto che nei dodici mesi successivi all'entrata in vigore delle nuove disposizioni, gli Stati membri offrano ai cittadini e alle imprese portafogli elettronici che collegano la loro identità elettronica nazionale ai mezzi di autenticazione di altri attributi personali (come la licenza di condurre, un diploma, un conto bancario). Questi portafogli potranno essere forniti dalle autorità pubbliche o da soggetti privati riconosciuti dagli Stati membri.

Il 6 dicembre 2022, il Consiglio ha adottato l'orientamento generale concernente il quadro per un'identità elettronica europea. In seno al Parlamento europeo l'affare è stato affidato alla Commissione per l'industria, la ricerca e l'energia (ITRE). Il Parlamento ha adottato la sua posizione il 16 marzo 2023 e in seguito sono stati avviati i negoziati. Affinché si concretizzi al più presto, la proposta è accompagnata da una raccomandazione. La Commissione ha invitato gli Stati membri a allestire un pacchetto comune di strumenti e ad avviare immediatamente i necessari lavori preparatori. Lo strumentario comprenderà l'architettura tecnica nonché norme e direttive relative alle buone prassi. Il 10 febbraio 2023 la Commissione ha pubblicato la prima versione del pacchetto comune di strumenti dell'UE per attuare il portafoglio europeo

7 Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea, COM (2021) 281 finale, 3 giugno 2021.

8 Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, GU L 257 del 28.8.2014, pag. 73.

di identità digitale (portafoglio EUDI)[9]. Il quadro definito dalla Commissione europea si fonda sui principi dell'identità autogestita (SSI), ma non fornisce indicazioni di carattere tecnico sulle esatte modalità di attuazione di tali principi. Da settembre 2021 gli Stati membri stanno negoziando direttamente tra loro le norme tecniche.

La Svizzera non è giuridicamente tenuta a recepire il regolamento eIDAS né i suoi sviluppi successivi. Tuttavia, visti gli stretti rapporti commerciali e sociali che intrattiene con la maggior parte dei Paesi membri dell'UE, ha tutto l'interesse a introdurre un sistema di identità elettronica interoperabile con quello dell'UE. Il disegno prevede che il Consiglio federale possa concludere accordi internazionali per il riconoscimento all'estero dell'Id-e svizzero e il riconoscimento in Svizzera degli Id-e stranieri (art. 31). In questo modo sarà possibile arrivare a un riconoscimento reciproco in particolare con l'UE. Il disegno è stato redatto in modo da essere compatibile con la pertinente legislazione europea.

4 Punti essenziali del progetto

4.1 La normativa proposta

Il disegno di legge prevede l'introduzione di un mezzo d'identificazione elettronico statale gratuito e volontario per i titolari di un documento d'identità emesso dalle autorità svizzere. In questo ambito lo Stato continua ad adempiere il suo compito principale, ossia verificare l'identità di una persona ed emettere il corrispondente mezzo d'identificazione elettronico. Come richiesto dalle mozioni depositate in Consiglio nazionale, il nuovo progetto segue un approccio fondato sui principi del rispetto della vita privata fin dalla progettazione e per impostazione predefinita, della minimizzazione dei dati e del salvataggio decentralizzato dei dati.

Inoltre, il disegno di legge mira a creare un'infrastruttura di fiducia statale che consenta agli attori dei settori pubblico e privato di emettere e utilizzare i mezzi di autenticazione elettronici. In questo quadro lo Stato gestirà i sistemi di base necessari (registro di base, registro di fiducia) e offrirà un portafoglio elettronico statale sotto forma di un'applicazione mobile che potrà contenere l'Id-e e altri mezzi di autenticazione elettronici. I titolari del portafoglio potranno presentare il loro Id-e e gli altri mezzi di autenticazione elettronici in maniera sicura e trasparente. Questa apertura del sistema permetterà di migliorare la diffusione dei mezzi di autenticazione elettronici e aumentarne l'utilizzo. Al contempo consentirà di rafforzare il livello di fiducia di cui beneficiano le procedure elettroniche in seno alla popolazione. Per la conservazione e la presentazione dei mezzi di autenticazione elettronici potranno essere utilizzate applicazioni alternative (portafogli elettronici), a condizione che siano compatibili dal punto di vista tecnico.

La messa a punto di un'infrastruttura elettronica di fiducia da parte dello Stato costituisce uno sviluppo importante e innovativo. Inoltre, questo progetto si basa su un'innovativa procedura partecipativa comprendente una consultazione informale, discus-

9 The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework: the Digital Identity Wallet Architecture and Reference Framework, gennaio 2023, versione 1.0.0 (disponibile solo in inglese).

sioni pubbliche e un forum di discussione specializzato in rete. Integra pure le esperienze raccolte nel quadro dei progetti pilota con altri uffici e degli scambi con altri Paesi.

La questione dell'utilizzo dell'Id-e in diversi ambiti è disciplinata soltanto a titolo indicativo nel disegno di legge (cfr. la modifica di altri atti normativi: legge federale dell'11 aprile 1889[10] sulla esecuzione e il fallimento [LEF] e legge federale del 19 giugno 2015[11] sulla cartella informatizzata del paziente [LCIP]). La questione è stata esaminata nel corso della consultazione. In considerazione della grande varietà dei possibili utilizzi, è opportuno disciplinare l'utilizzo dell'Id-e nelle leggi applicabili ai corrispondenti ambiti.

4.2 Compatibilità tra compiti e finanze

È stata realizzata una stima dei costi (v. n. 6.1 Ripercussioni per la Confederazione).

In totale, le risorse finanziarie necessarie per lo sviluppo e la gestione dell'infrastruttura di fiducia, l'emissione degli Id-e e i progetti pilota ammonteranno a circa 181,9 milioni di franchi per il periodo 2023–2028. A partire dal 2029, occorre prevedere costi annuali che si avvicineranno a 24,7 milioni di franchi.

I costi previsti possono essere considerati ragionevoli per un progetto di questa importanza, che servirà a far progredire la digitalizzazione in Svizzera.

4.3 Attuazione

Le disposizioni d'esecuzione necessarie per attuare la presente legge saranno disciplinate a livello di ordinanza (cfr. art. 28 e i relativi commenti).

5 Commento ai singoli articoli

Ingresso

Il disegno di legge si fonda sugli articoli 38 capoverso 1, 81 e 121 della Costituzione federale (Cost.)[12].

Dato che tratta l'identità elettronica statale, il disegno di legge si basa sugli articoli 38 capoverso 1 e 121 capoverso 1 Cost. L'articolo 38 capoverso 1 conferisce alla Confederazione la competenza di disciplinare l'acquisizione e la perdita della cittadinanza per origine, matrimonio e adozione, mentre l'articolo 121 capoverso 1 le attribuisce quella di legiferare sull'entrata, l'uscita, la dimora e il domicilio degli stranieri nonché sulla concessione dell'asilo. Sebbene i due articoli non si riferiscano esplicitamente ai documenti d'identità, da queste norme di delega è possibile dedurre che la Confede-

10 RS **281.1**
11 RS **816.1**
12 RS **101**

razione ha la competenza di disciplinare i documenti d'identità richiesti, anche se questi non sono utilizzati esclusivamente per dimostrare la cittadinanza dei cittadini svizzeri e lo statuto di soggiorno dei cittadini stranieri. Fondandosi su questi due articoli, la legge del 22 giugno 2001[13] sui documenti d'identità (LDI) e la legge federale del 16 dicembre 2005[14] sugli stranieri e la loro integrazione (LStrI) assegnano alla Confederazione la competenza di rilasciare rispettivamente i documenti d'identità ai cittadini svizzeri e i permessi di soggiorno ai cittadini stranieri. Dal momento che l'Id-e statale serve a dimostrare la propria identità nel mondo virtuale e il diritto di ottenere un Id-e è strettamente connesso al diritto di ottenere il corrispondente documento fisico, è giustificato fondare il disegno sulle stesse basi costituzionali su cui si basa la certificazione ufficiale dell'identità, della cittadinanza e dello statuto dei cittadini stranieri.

La competenza di creare un'infrastruttura di fiducia su cui fondare l'Id-e si rifà all'articolo 81 Cost., che permette alla Confederazione di realizzare e gestire opere pubbliche o sostenerne la realizzazione, nell'interesse del Paese o di una parte di esso. Viceversa, sostenere la realizzazione e la gestione di opere di terzi non può basarsi sull'articolo 81, ma eventualmente su un'altra competenza federale. Le «opere pubbliche», oggetto dell'articolo costituzionale, sono tradizionalmente di natura fisica (p. es. una galleria). Tuttavia, secondo il parere giuridico dell'Ufficio federale di giustizia (UFG) sulla cooperazione a livello di TIC tra la Confederazione e i Cantoni[15], sarebbe possibile, secondo un approccio sostenuto in parte anche dalla dottrina, far rientrare nel concetto di «opera» di cui all'art. 81 Cost. anche i grandi progetti informatici e altri elementi necessari alla costituzione di un panorama amministrativo elettronico uniforme[16]. In effetti, seguendo l'interpretazione evolutiva e teleologica di Lendi[17] e di Biaggini[18], le «opere pubbliche» possono essere anche immateriali o non tangibili, come un sistema informatico o un sistema di comunicazione realizzato nell'interesse della Svizzera. Il Consiglio federale concorda con questa interpretazione e ritiene pertanto ammissibile fondare sull'articolo 81 un disegno volto a introdurre un'infrastruttura di fiducia in grado di emettere, utilizzare e convalidare diversi mezzi di autenticazione elettronici (compreso l'Id-e). In tale contesto, va ricordato che l'articolo 81 Cost. non conferisce alla Confederazione la competenza di emanare e imporre norme tecniche e organizzative vincolanti per una collaborazione a livello di TIC tra la Confederazione e i Cantoni[19]. Per contro, la Confederazione può emanare

13 RS **143.1**
14 RS **142.20**
15 DFGP, Ufficio federale di giustizia, *Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten vom 22. Dezember 2011*, JAAC 2012.1 (pagg. 1–17), edizione del 1° maggio 2012 (disponibile solo in tedesco).
16 Ibid, pag. 8: «*Zusammengefasst wäre es nach einem in der Lehre teilweise befürworteten Ansatz möglich, grössere Informatikvorhaben und andere Elemente zur Schaffung einer einheitlichen elektronischen Verwaltungslandschaft unter dem Werkbegriff von Art. 81 BV zu subsumieren*».
17 Ibid; Lendi, Martin, in *St. Galler Kommentar*, 2ª ed. 2008, art. 81 n. 6; Vogel, Stefan, in *St. Galler Kommentar*, 4ª ed. 2023, art. 81 n. 5.
18 Ibid; Biaggini, Giovanni in *BV-Kommentar*, Zurigo 2007, art. 81 n. 2, criticato da Markus Kern in *Basler Kommentar*, n. 6 e 9.
19 Ibid; Biaggini, G., ibid, art. 81 n. 3

le disposizioni necessarie alla messa a disposizione e all'utilizzo sicuri, efficaci e uniformi dei lavori o delle opere pubbliche in questione.

Il disegno disciplina determinati aspetti di diritto civile relativi ai rapporti tra gli emittenti e i titolari di un Id-e nonché tra i verificatori e i titolari di un Id-e. Tuttavia, data l'importanza accessoria di tali rapporti, l'ingresso non cita l'articolo 122 capoverso 1 Cost. che stabilisce la competenza della Confederazione in materia di diritto civile.

Sezione 1 Oggetto e scopo

Art. 1

Cpv. 1

Lett. a

Il disegno disciplina i requisiti dell'infrastruttura di fiducia utilizzata per l'emissione, la revoca, la verifica, la conservazione e la presentazione dei mezzi di autenticazione elettronici.

Lett. b

Il disegno definisce i ruoli e le responsabilità relativi alla messa a disposizione dell'infrastruttura di fiducia.

Lett. c

Il disegno definisce il quadro giuridico dei mezzi di autenticazione elettronici in Svizzera e quindi anche dell'Id-e statale.

Cpv. 2

Lett. a

Il tenore della lettera a è stato rielaborato al fine di tenere conto dei risultati della consultazione. Diversi partecipanti hanno criticato il fatto che la disposizione riprendeva solo in parte il principio della protezione dei dati sin dalla progettazione e per impostazione predefinita di cui all'articolo 7 della legge federale del 25 settembre 2020[20] sulla protezione dei dati (LPD). La presente lettera è stata riformulata fondandosi sull'articolo 7 capoverso 2 LPD invece che sul principio più generale enunciato all'articolo 1 LPD. Il suo scopo è garantire che i provvedimenti tecnici e organizzativi previsti siano adeguati in particolare allo stato della tecnica, al tipo e all'entità del trattamento dei dati come pure ai rischi derivanti dal trattamento per la personalità o i diritti fondamentali delle persone interessate.

Questo obiettivo sarà raggiunto in particolare attuando le richieste delle sei mozioni dal medesimo tenore intitolate «Identità elettronica statale affidabile» (cfr. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 e 21.3129), depositate da parlamentari di tutti i gruppi in seguito al respingimento del primo progetto di legge in occasione della votazione del 7 marzo 2021. Secondo gli autori delle mozioni, il mezzo d'identificazione

20 RS **235.1**

elettronico statale deve rispettare i principi della «privacy by design», della minimizzazione dei dati e della registrazione decentralizzata dei dati (come la registrazione dei dati dei documenti d'identità presso gli utenti). La lettera a ribadisce questi requisiti come obiettivi specifici da raggiungere nel contesto della protezione dei dati personali.

La LPD si applica al trattamento dei dati personali effettuato nell'ambito dell'attuazione della legge. Per evitare ripetizioni e agevolare la leggibilità, le disposizioni del disegno non contengono rimandi ai pertinenti articoli della LPD (v. n. 7.8 Protezione dei dati).

Inoltre, il diritto cantonale sulla protezione dei dati si applica in linea di massima all'utilizzo dell'infrastruttura di fiducia da parte delle autorità cantonali nella misura in cui esse sono competenti per il trattamento dei dati. Ciò è in particolare il caso se emettono i loro propri mezzi di autenticazione elettronici o se verificano mezzi di autenticazione elettronici (compreso l'Id-e). Determinate disposizioni della presente legge intervengono tuttavia in singoli punti del diritto cantonale, che deve ad esempio rispettare gli standard minimi (più elevati) previsti dal disegno di legge come gli utenti privati dell'infrastruttura di fiducia.

Lett. b

La lettera b esplicita che la legge mira a consentire a un gruppo specifico di persone l'emissione e l'utilizzo dei mezzi di autenticazione elettronici. I mezzi di autenticazione saranno dunque emessi e utilizzati nelle relazioni tra privati nonché tra privati e autorità.

Il disegno di legge mira a garantire l'introduzione di procedure sicure nel quadro dell'infrastruttura di fiducia. I rischi connessi all'emissione, all'utilizzo e alla presentazione dei mezzi di autenticazione elettronici dovranno essere minimizzati mediante l'adozione di provvedimenti tecnici e organizzativi appropriati.

Lett. c

La lettera c mira a garantire che la configurazione dell'Id-e e dell'infrastruttura di fiducia corrisponda allo stato attuale della tecnica. Questa nozione si distingue concettualmente da altre nozioni simili quali le «regole riconosciute della tecnica» e lo «stato della scienza e della ricerca». In parole povere, l'espressione «stato attuale della tecnica» rinvia a tecnologie più innovative rispetto alla nozione di «regole riconosciute della tecnica» e a tecnologie più vecchie rispetto alla nozione di «stato della scienza e della ricerca». Questa distinzione costituisce la base sostanziale per determinare il livello di sicurezza richiesto. Anche l'articolo 7 capoverso 2 LPD esige l'adozione di provvedimenti adeguati allo stato della tecnica, senza però stabilire i criteri per determinare come questa nozione vada intesa. Ciò non permette tuttavia di concludere che quanto non è definito concretamente nella legge non possa essere verificato e quindi applicato.

Utilizzando questa espressione, il legislatore mira a un elevato livello di sicurezza e di protezione dei dati da conseguire mediante procedure avanzate. A tal fine è necessario promuovere la verifica regolare dei provvedimenti di sicurezza implementati per esaminarne l'efficacia rispetto agli obiettivi di protezione richiesti nonché il livello di

aggiornamento e di innovazione. Ciò significa che tali provvedimenti devono essere confrontati con i prodotti di sicurezza esistenti sul mercato. Ciò che oggi è considerato corrispondente allo «stato attuale della tecnica», domani può essere considerato una «regola riconosciuta della tecnica» a causa della discrepanza dovuta all'innovazione, ossia all'obsolescenza del provvedimento di sicurezza rispetto ad altri provvedimenti di sicurezza disponibili.

Lett. d

Il disegno mira inoltre a garantire la sicurezza dell'infrastruttura e delle procedure di emissione e di verifica degli altri mezzi di autenticazione elettronici. Tuttavia, per raggiungere questi obiettivi il progresso tecnico non deve essere limitato; il disegno prescrive dunque la scelta della soluzione tecnica soltanto quando strettamente necessario per raggiungere gli obiettivi legislativi. Prevede in particolare una gestione decentralizzata dei dati escludendo qualsiasi soluzione tecnica secondo la quale un fornitore di servizi d'identificazione si interpone tra il titolare e il verificatore di un mezzo di autenticazione elettronico. In tal modo il titolare ha un controllo maggiore sui suoi dati. La maggior parte degli aspetti legati alla scelta della tecnologia non è tuttavia disciplinata a livello di legge. Poiché il progresso tecnico è in rapida evoluzione, occorre garantire che il disegno possa essere attuato nel contesto tecnologico che si presenterà dopo la sua entrata in vigore e che è al momento ancora sconosciuto.

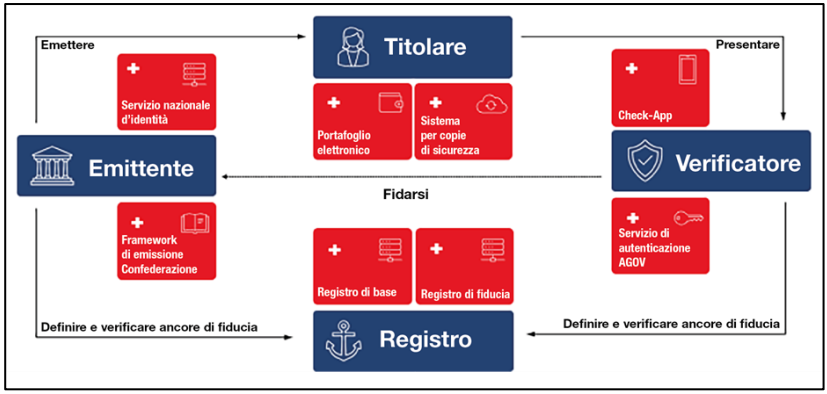
Vari aspetti da disciplinare a livello di ordinanza saranno, sotto il profilo tecnologico, molto più concreti e specifici. L'ordinanza dovrà garantire l'interoperabilità di tutti i sistemi coinvolti nella comunicazione; per farlo dovrà in particolare definire molto precisamente i formati dei dati e le interfacce. In tale contesto, sarà necessario rispettare il principio secondo cui devono essere prese solamente le decisioni tecnologiche assolutamente necessarie. Nella misura del possibile dovrebbe dunque essere lasciata ai diversi attori la scelta della tecnologia da utilizzare sul loro lato dell'interfaccia per formattare, memorizzare e trattare i dati.

Sezione 2 Infrastruttura di fiducia

Il disegno di legge attribuisce alla Confederazione la competenza di implementare, gestire e sviluppare un'infrastruttura informatica in grado di emettere, utilizzare, gestire, convalidare e revocare mezzi di autenticazione elettronici. L'infrastruttura di fiducia attua una serie di regolamenti, procedure, piani ed elementi infrastrutturali che assicurano la conformità del sistema e la fiducia in esso conformemente alle buone pratiche. Il suo obiettivo è permettere l'emissione, la revoca e l'utilizzo dell'Id-e e di altri mezzi di autenticazione elettronici.

L'infrastruttura di fiducia comprende tre tipi di attori: gli emittenti, i titolari e i verificatori. Le loro interazioni si fondano su standard di comunicazione definiti. L'infrastruttura di fiducia implementata dalla Confederazione si compone degli elementi seguenti: il registro di base (art. 2), il registro di fiducia (art. 3), l'applicazione per la conservazione e la presentazione dei mezzi di autenticazione elettronici (art. 7) e l'applicazione per la verifica degli stessi (art. 8). Il sistema d'informazione (art. 25) e il servizio di autenticazione della Cancelleria federale (modifica di altri atti normativi,

legge federale del 17 marzo 2023[21] concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità [LMeCA]) con l'Id-e integrano gli elementi centrali previsti dal presente disegno.



L'UFIT implementa e gestisce i diversi elementi dell'infrastruttura di fiducia. La responsabilità per gli eventuali danni causati utilizzando l'Id-e o l'infrastruttura di fiducia è retta dalle usuali disposizioni in materia di responsabilità del Codice delle obbligazioni[22] o della legge del 14 marzo 1958[23] sulla responsabilità (LResp).

Art. 2 Registro di base

Cpv. 1

L'UFIT mette a disposizione delle autorità e dei privati interessati un registro di base, che costituisce una componente essenziale dell'infrastruttura di fiducia e il primo elemento dell'ancora di fiducia del sistema (garante, «trust anchor»). Esso permette a un verificatore di assicurarsi che i mezzi di autenticazione elettronici non siano stati modificati successivamente e che provengano dall'emittente iscritto nel registro di base con il corrispondente identificativo.

Il registro di base può essere implementato in differenti forme. Tuttavia il disegno di legge, che è formulato in maniera più neutrale possibile dal punto di vista tecnologico, non prescrive la soluzione tecnica che deve essere scelta (v. commento all'art. 1 cpv. 2 lett. d). Non disciplina quindi in dettaglio le componenti tecniche del registro di base, ma prevede le funzioni che quest'ultimo deve assumere. A titolo esemplificativo, il registro di base potrà contenere i dati seguenti: gli identificativi degli emittenti e dei verificatori, le chiavi crittografiche richieste per controllare i loro identificativi e per verificare l'autenticità e l'integrità dei mezzi di autenticazione elettronici; i dati relativi alla revoca dei mezzi di autenticazione elettronici. Gli indirizzi postali, i numeri

21 FF **2023** 787
22 RS **220**
23 RS **170.32**

di telefono, gli indirizzi e-mail o altre coordinate degli emittenti e dei verificatori nonché i dati personali dei titolari non saranno registrati nel registro di base.

Cpv. 2

Gli emittenti possono iscrivere essi stessi i loro dati nel registro di base, consentendo in tal modo ai verificatori di controllare l'autenticità (unicamente per quanto riguarda i dati iscritti dagli emittenti) e l'integrità dei mezzi di autenticazione elettronici emessi da ciascuno di loro. Questi dati sono resi sicuri da un algoritmo crittografico al momento dell'iscrizione e sono considerati infalsificabili.

Gli emittenti e i verificatori che intendono annunciarsi nel registro di fiducia di cui all'articolo 3 devono iscrivere le loro informazioni nel registro di base. A questo stadio, la loro identità non è verificata. L'iscrizione nel registro di base permette unicamente di controllare se determinate informazioni, come una chiave pubblica, appartengono a un dato identificativo ma non significa che l'identità è stata verificata. È il registro di fiducia che consente di confermare l'appartenenza di un identificativo a un attore (v. commento all'art. 3)

Cpv. 3

Ad eccezione dei dati concernenti la revoca, il registro di base non contiene dati concernenti i mezzi di autenticazione elettronici come dati personali o indicazioni concernenti l'emissione dei mezzi di autenticazione elettronici.

Cpv. 4

I dati concernenti la revoca dei mezzi di autenticazione elettronici non consentono di risalire né all'identità del titolare né al contenuto del mezzo di autenticazione elettronico.

Cpv. 5

In sede di consultazione sono stati chiesti requisiti più precisi in merito all'utilizzo dei dati personali generati in occasione della consultazione del registro di base. Tali dati comprendono in particolare gli indirizzi IP e altri dati simili a seconda del protocollo utilizzato. Per quanto riguarda la registrazione dei dati e la loro analisi senza riferimento a persone, il capoverso 5 si allinea alle finalità di cui all'articolo 57*l* lettera b numeri 1–3 della legge del 21 marzo 1997[24] sull'organizzazione del Governo e dell'Amministrazione (LOGA). Il capoverso prevede inoltre che questi dati possano essere analizzati in riferimento a persone ma in maniera non nominale per le finalità di cui all'articolo 57*n* lettera a LOGA e in riferimento a persone e in maniera nominale per le finalità di cui all'articolo 57*o* capoverso 1 lettere a e b LOGA.

È opportuno precisare che l'UFIT non ha accesso al contenuto delle transazioni tra emittenti, titolari e verificatori.

24 RS **172.010**

Art. 3 Registro di fiducia

Cpv. 1

L'UFIT mette a disposizione un sistema accessibile al pubblico (registro di fiducia) contenente i dati per la verifica dell'identità degli emittenti e dei verificatori nonché per l'utilizzo sicuro dei mezzi di autenticazione elettronici. Questo sistema costituisce il secondo elemento dell'ancora di fiducia del sistema: permette ai titolari e ai verificatori di conoscere con chi hanno effettivamente a che fare. Oltre a quelle che permettono di verificare gli identificativi, il sistema mette a disposizione degli utenti anche parecchie altre informazioni. Ad esempio, consente di verificare se un emittente è autorizzato a emettere un determinato tipo di mezzo di autenticazione elettronico (p. es. fedpol è l'unico emittente dell'Id-e) o se un verificatore è autorizzato a esigere un mezzo di autenticazione elettronico particolare o certe informazioni ivi contenute (p. es. se un attore può chiedere il numero AVS contenuto nell'Id-e).

Ogni attore è libero di decidere quando consultare il registro di fiducia, che non è necessario per la verifica crittografica dei mezzi di autenticazione elettronici o la creazione di canali di comunicazione sicuri. Può tuttavia aumentare la fiducia di cui un attore beneficia presso il suo interlocutore nel caso in cui non ci sia alcun rapporto preesistente tra di loro, uno dei due desideri maggiori informazioni o sia richiesta una conferma dell'autenticità e dell'esattezza delle informazioni condivise.

Il registro di fiducia è concepito in modo da poter rispondere alle domande sia automatiche che manuali. Saranno principalmente le applicazioni per la conservazione e la presentazione (portafogli elettronici) e i sistemi utilizzati dai verificatori a fare ricorso a queste informazioni al fine di orientare meglio gli utenti e permettere loro di prendere decisioni con cognizione di causa.

Allo scopo di minimizzare il flusso di dati e di preservare il carattere decentralizzato dell'infrastruttura di fiducia, ogni conferma del sistema può essere emessa sotto forma di mezzo di autenticazione elettronico o di un altro mezzo simile a seconda dello stato della tecnica. Questi mezzi di autenticazione elettronici possono essere presentati da un emittente o da un verificatore a ogni attore interessato senza che questo debba consultare il registro di fiducia. Si tratta di un'opzione di applicazione del registro di fiducia in corso di valutazione.

Cpv. 2

L'UFIT è responsabile dell'esattezza delle informazioni che sono accessibili al pubblico nel registro di fiducia. È incaricato di implementare le procedure necessarie per garantire la qualità e l'esattezza delle informazioni e se del caso di rettificarle o aggiornarle.

Cpv. 3

Al fine di rafforzare la fiducia di cui beneficiano i servizi dell'Amministrazione digitale che ricorrono all'infrastruttura di fiducia, su loro domanda le autorità federali, cantonali e comunali sono iscritte nel registro di fiducia. Questa iscrizione conferma che un identificativo iscritto nel registro di base appartiene effettivamente a loro.

Cpv. 4

Il Consiglio federale può prevedere che la Confederazione confermi anche l'identificativo degli emittenti e dei verificatori del settore privato. Una misura di questo tipo può aumentare la fiducia di cui beneficia l'infrastruttura di fiducia nel contesto dell'identificazione elettronica. Sebbene gli emittenti e i verificatori del settore privato siano in linea di massima interessati a utilizzare il registro di fiducia, non è certo che lo faranno veramente una volta che questo sarà disponibile. Occorrerà attendere l'entrata in vigore della legge per vedere se queste intenzioni si concretizzeranno.

Sarà allora opportuno definire a livello di ordinanza i requisiti applicabili alla conferma dell'identificativo di questi attori. Dovranno inoltre essere previsti provvedimenti tecnici e organizzativi atti a garantire la qualità delle informazioni messe a disposizione dal registro di fiducia.

Infine, è possibile che gli attori del settore privato decidano di implementare, a loro spese e separatamente, registri di fiducia non statali (privati); il presente disegno di legge non impone loro dei limiti in questo ambito.

Cpv. 5

Il presente capoverso mira a permettere agli utenti di verificare nel registro di fiducia se l'identificativo di un emittente o di un verificatore è stato confermato dall'UFIT. Le conferme degli identificativi di cui ai capoversi 3 e 4 devono quindi figurare nel registro di fiducia.

Cpv. 6

In sede di consultazione è stato chiesto di precisare le finalità dell'utilizzo dei dati personali generati in occasione della consultazione del registro di fiducia. La disposizione rimanda semplicemente alle finalità di cui all'articolo 2 capoverso 5 senza elencarle, al fine di evitare ripetizioni e agevolare la lettura (v. commento all'art. 2 cpv. 5).

In sintesi, i dati personali generati in occasione della consultazione del registro di fiducia possono essere registrati per le finalità previste all'articolo 57*l* lettera b numeri 1–3 LOGA. Possono essere analizzati senza riferimento a persone per le finalità previste all'articolo 57*l* lettera b numeri 1–3 LOGA, in riferimento a persone ma in maniera non nominale per le finalità previste all'articolo 57*n* lettera a LOGA e in riferimento a persone e in maniera nominale per le finalità di cui all'articolo 57*o* capoverso 1 lettere a e b LOGA.

Cpv. 7

Il presente capoverso delega al Consiglio federale la competenza di prevedere disposizioni sulla fornitura di altre informazioni che garantiscano un utilizzo sicuro dei mezzi di autenticazione elettronici. Potrà in particolare trattarsi di dati sulle modalità di utilizzo dei mezzi di autenticazione elettronici o che consentono di stabilire se un emittente o un verificatore è autorizzato a emettere o verificare un determinato tipo di mezzo di autenticazione elettronico. Questa delega di competenze permetterà parimenti al registro di fiducia di evolvere e di soddisfare meglio le esigenze dell'ecosistema e dello sviluppo tecnico.

Art. 4 Emissione

Cpv. 1

Qualsiasi autorità pubblica e qualsiasi privato possono utilizzare l'infrastruttura di fiducia della Confederazione per emettere un mezzo di autenticazione elettronico (all'infuori dell'Id-e statale che sarà emesso unicamente da fedpol). Si tratta di una disposizione potestativa che non obbliga le autorità e i privati a servirsi dell'infrastruttura di fiducia. Inoltre, il capoverso non limita le tipologie di mezzi di autenticazione elettronici che possono essere emessi; mira a mettere a disposizione l'infrastruttura di fiducia a diversi attori e a consentire loro di emettere mezzi di autenticazione elettronici di tutti i tipi.

Questa disposizione è stata volutamente formulata in modo aperto al fine di non limitare a priori né la cerchia degli emittenti né il tipo di mezzi di autenticazioni elettronici. Per la medesima ragione si è rinunciato a prescrizioni concernenti le informazioni che gli emittenti devono conservare sui mezzi di autenticazione elettronici che hanno emesso. Queste decisioni devono essere prese caso per caso dagli emittenti stessi oppure, nel caso di un emittente pubblico, dal competente legislatore.

Il capoverso 1 non ha carattere potestativo per l'UFIT, che è incaricato di implementare le diverse componenti dell'infrastruttura di fiducia secondo gli articoli 2 e3.

Cpv. 2

I mezzi di autenticazione elettronici contengono diversi dati. Oltre ai dati di base stabiliti dall'emittente, devono comprendere quelli richiesti per la verifica dell'autenticità e dell'integrità, ad esempio una firma elettronica.

Art. 5 Revoca

Secondo il presente disegno di legge, gli emittenti hanno il diritto, ma non l'obbligo, di revocare dei mezzi di autenticazione elettronici utilizzando il registro di base. Possono decidere essi stessi quando un mezzo di autenticazione elettronico deve essere revocato e prevederlo in un contratto stipulato con il titolare. Inoltre, i terzi, autorità o privati, non sono competenti per revocare mezzi di autenticazione elettronici emessi da altri attori.

Il presente articolo non stabilisce requisiti minimi comuni per quanto concerne la revoca poiché i tipi e i casi di utilizzo dei mezzi di autenticazione elettronici sono molto vari e retti da leggi differenti. L'articolo mira unicamente a chiarire che i mezzi di autenticazione elettronici possono essere revocati dagli emittenti. Un mezzo di autenticazione elettronico revocato non può più essere riattivato: l'emittente può tuttavia sempre emetterne uno nuovo con il medesimo o un altro contenuto. Gli emittenti possono decidere di emettere mezzi di autenticazione elettronici non revocabili se una revoca è inutile o non è richiesta e la procedura di verifica dell'identità è onerosa e complicata.

Sebbene il disegno non preveda alcun obbligo di revoca, secondo l'articolo 6 capoverso 5 LPD gli emittenti devono prendere tutte le misure adeguate a rettificare, cancellare o distruggere i dati inesatti o incompleti rispetto allo scopo per il quale sono stati raccolti o trattati. È dunque possibile che in virtù di quest'obbligo legale gli emit-

tenti siano tenuti, in determinati casi, a revocare dei mezzi di autenticazione elettronici o a trovare altre misure tecniche per garantire il rispetto della LPD.

Art. 6 Forma e conservazione dei mezzi di autenticazione elettronici

Il titolare riceve il mezzo di autenticazione elettronica sotto forma di pacchetto di dati, che è conservato su un supporto tecnico scelto dal titolare. Il disegno di legge non prevede requisiti per quanto riguarda i dispositivi tecnici che devono essere utilizzati per conservare i mezzi di autenticazione elettronici. La Confederazione mette però a disposizione una pertinente applicazione strettamente concepita secondo i principi della protezione dei dati personali sin dalla progettazione e per impostazione predefinita (v. commento all'art. 7).

Art. 7 Applicazione per la conservazione e la presentazione dei mezzi di autenticazione elettronici

Cpv. 1

L'UFIT mette a disposizione un'applicazione, detta portafoglio elettronico statale, per conservare e presentare i mezzi di autenticazione elettronici. Si tratta di un'applicazione informatica che consente all'utente di richiedere, ottenere in modo sicuro, conservare, selezionare, combinare e condividere mezzi di autenticazione elettronici in maniera trasparente e tracciabile. Con tale applicazione l'utente può gestire l'Id-e e altri mezzi di autenticazione elettronici. Per quanto necessario, l'implementazione del portafoglio elettronico statale tiene conto delle norme elaborate dall'UE.

La legge non disciplina l'utilizzo dei portafogli elettronici emessi da altri attori. Oltre al portafoglio elettronico statale, gli utenti possono servirsi anche di altre applicazioni per conservare e presentare i loro mezzi di autenticazione elettronici.

Cpv. 2

Sempre più spesso chi perde il proprio smartphone o ne acquista uno nuovo ripristina le applicazioni a partire da un backup. In tal modo è possibile recuperare rapidamente le funzionalità del vecchio sistema. La medesima possibilità potrà essere offerta ai titolari del portafoglio elettronico statale.

Una delle previste funzionalità di base dell'applicazione permetterà di creare una copia di backup dei mezzi di autenticazione elettronici su un supporto di dati locale del titolare.

Il presente capoverso delega al Consiglio federale la competenza di prevedere che l'UFIT implementi un sistema informatico in cui i titolari possano salvare le copie dei loro mezzi di autenticazione elettronici. Dopo un cambio di supporto tecnico (smartphone, computer, ecc.), potranno in tal modo recuperare rapidamente i mezzi di autenticazione elettronici salvati.

L'utilizzo del sistema per le copie di sicurezza sarà volontario e possibile unicamente per gli utenti dell'applicazione di cui al presente articolo. Ogni titolare sarà libero di utilizzare l'opzione di backup dei suoi mezzi di autenticazione elettronici.

Solo i titolari avranno accesso alle loro copie di sicurezza. L'UFIT è tenuto a impostare il sistema in modo da impedire l'accesso a terzi.

Cpv. 3

Il presente capoverso delega al Consiglio federale la competenza di disciplinare le misure da adottare in caso di inattività prolungata nel sistema di conservazione, in particolare se le copie di sicurezza non sono state aggiornate o se non sono utilizzate dal titolare per un lungo periodo. Si tratta di una misura che consente di distruggere determinati dati per ridurne il volume accumulato nel corso del tempo. Con un'attuazione conforme ai requisiti della protezione e della minimizzazione dei dati non sarà possibile sapere chi è il titolare e consultarlo prima di un'eventuale distruzione dei dati. A livello di ordinanza saranno previsti termini compresi tra due e cinque anni.

Art. 8 Applicazione per la verifica dei mezzi di autenticazione elettronici

Cpv. 1

L'UFIT mette a disposizione un'applicazione che consente di verificare la validità dell'Id-e. Si tratta di una misura di sicurezza volta ad agevolare la verifica dell'Id-e e a garantirne la sicurezza nonché ad aumentare la fiducia di cui beneficia l'infrastruttura prevista dalla legge. L'utilizzo dell'applicazione è volontario: ogni verificatore è libero di ricorrervi per verificare l'Id-e emessa da fedpol.

Cpv. 2

Il Consiglio federale può decidere di permettere la verifica della validità anche di altri mezzi di autenticazione elettronici con l'applicazione di cui al capoverso 1. Quest'opzione potrebbe costituire una misura importante per agevolare l'utilizzo dell'infrastruttura di fiducia e dei mezzi di autenticazione elettronici. L'utilizzo dell'applicazione per verificare la validità degli altri mezzi di autenticazione elettronici sarà parimenti volontaria. Ogni verificatore sarà libero di decidere se ricorrere all'applicazione della Confederazione o a un'altra applicazione equivalente disponibile sul mercato.

Art. 9 Presentazione dei mezzi di autenticazione elettronici

Cpv. 1

Il titolare non è obbligato a presentare i suoi mezzi di autenticazione elettronici nella loro integralità, ma è libero di decidere quali parti di un mezzo di autenticazione elettronico o quali informazioni ivi contenute intende presentare al verificatore per conseguire l'obiettivo della verifica in un caso concreto. L'impostazione dei mezzi di autenticazione sarà definita per via d'ordinanza al fine di garantire che gli emittenti prevedano la possibilità di trasmettere alcuni o tutti gli elementi di un mezzo di autenticazione elettronico.

Il disegno di legge non prescrive quali dati devono essere trasmessi al momento della verifica del mezzo di autenticazione elettronico. L'attuazione tecnica deve inoltre per-

mettere che la verifica dell'autenticità e dell'integrità sia possibile anche se sono presentate solo singole parti di esso.

Spetta al verificatore definire i dati richiesti nel singolo caso. Il margine di manovra del titolare è quindi limitato dalle esigenze poste dal verificatore nel quadro della procedura di verifica. Se decide di non presentare gli elementi richiesti dal verificatore, il titolare potrebbe non essere in grado di accedere ai servizi offerti dal verificatore.

La LPD pone tuttavia dei limiti per quanto riguarda i dati che il verificatore può esigere dal titolare di un mezzo di autenticazione elettronico. L'articolo 6 capoverso 2 LPD prevede in particolare che il trattamento dei dati personali debba essere conforme ai principi della buona fede e della proporzionalità. Inoltre, i dati personali possono essere raccolti soltanto per uno scopo determinato e riconoscibile per la persona interessata e trattati ulteriormente soltanto in modo compatibile con tale scopo (art. 6 cpv. 3 LPD).

Cpv. 2

L'UFIT imposta l'infrastruttura di fiducia in modo che l'emittente di un mezzo di autenticazione elettronico non venga a conoscenza delle informazioni legate alla presentazione e alla verifica dello stesso.

Cpv. 3

Il registro di base e il registro di fiducia non permettono all'UFIT di accedere al contenuto dei mezzi di autenticazione elettronici presentati in quanto questi dati non sono salvati nei suddetti registri. Inoltre, l'UFIT non può trarne conclusioni sull'utilizzo di un mezzo di autenticazione elettronico e sulle autorità e persone private coinvolte. In veste di gestore dell'infrastruttura di fiducia può tuttavia accedere ai dati personali generati al momento della consultazione del registro di base di cui all'articolo 2 e del registro di fiducia di cui all'articolo 3, ad esempio agli indirizzi IP o ad altre informazioni simili a seconda del protocollo utilizzato.

Art. 10 Segnalazione di ciberattacchi agli emittenti e ai verificatori

La consultazione ha pure rivelato l'opportunità di prevedere un obbligo di segnalare gli attacchi informatici ai sistemi di emissione e di verifica. Non beneficiando dei necessari diritti di accesso, l'UFIT non è in grado di intercettare gli attacchi informatici ai sistemi che utilizzano l'infrastruttura di fiducia. L'obbligo di segnalazione è dunque essenziale per garantire una protezione efficace degli utenti dell'infrastruttura di fiducia della Confederazione.

È tuttavia opportuno coordinare il presente articolo con la prevista modifica della legge del 18 dicembre 2020[25] sulla sicurezza delle informazioni (LSIn), attualmente in esame presso il Parlamento[26]. L'articolo 74*b* prevede un nuovo obbligo di segnalare ciberattacchi a infrastrutture critiche. Nel caso in cui questa modifica dovesse essere

25 RS **128**

26 Messaggio del 2 dicembre 2022 concernente la modifica della legge sulla sicurezza delle informazioni (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), FF **2023** 84, 85; www.parlament.ch > Attività parlamentare > Ricerca Curia vista > 22.073.

approvata dal Parlamento ed entrasse quindi in vigore, il presente disegno includerebbe la disposizione di coordinamento seguente:

Art. 74b lett. v

1 L'obbligo di segnalare ciberattacchi si applica:

v. agli emittenti e ai verificatori di mezzi di autenticazione elettronici conformemente alla legge del … sull'Id-e.

Art. 11 Codice sorgente dell'infrastruttura di fiducia

Cpv. 1

La Confederazione pubblica su Internet il codice sorgente dei componenti dell'infrastruttura di fiducia di cui alle lettere a–d. Questa misura permette di aumentare la fiducia di cui beneficia questa infrastruttura in seno alla popolazione e di mantenere un livello di sicurezza elevato consentendo alle persone interessate di testare il codice pubblicato. Inoltre, il presente capoverso mira a preservare lo spirito di apertura che caratterizza l'approccio partecipativo del disegno.

Cpv. 2

L'UFIT può eccezionalmente decidere di non pubblicare il codice sorgente o una sua parte se vi è motivo di credere che la sua pubblicazione potrebbe compromettere la sicurezza informatica di uno dei componenti di cui al capoverso 1 lettere a–d. A titolo esemplificativo, sarebbe ipotizzabile non pubblicare il codice sorgente di componenti della procedura di verifica dell'identità in linea, se quest'ultima è effettuata mediante l'applicazione di cui all'articolo 7 (portafoglio elettronico statale).

Il disegno di legge non disciplina espressamente i provvedimenti tecnici e organizzativi da adottare nel quadro dell'infrastruttura di fiducia. Per evitare ripetizioni e agevolare la comprensione, il disegno non rimanda all'articolo 8 LPD, agli articoli 3 e 4 dell'ordinanza del 31 agosto 2022[27] sulla protezione dei dati (OPDa) o alle disposizioni della LSIn per quanto attiene ai provvedimenti tecnici e organizzativi appropriati che l'UFIT deve adottare per garantire un elevato livello di sicurezza adeguato ai rischi connessi alla gestione dell'infrastruttura di fiducia. Non prevede neppure espressamente che l'UFIT sia tenuto a controllare regolarmente gli elementi chiave dell'infrastruttura di fiducia fondandosi su norme nazionali e internazionali riconosciute in materia. Si tratta di una misura tecnica adottata tipicamente nella prassi al fine di garantire un livello di sicurezza elevato dell'infrastruttura informatica e non richiede una base legale formale.

27 RS **235.11**

Sezione 3 Id-e

Art. 12 Forma

L'UFIT mette a disposizione un'infrastruttura di fiducia (cfr. sezione 1) che consente ad attori pubblici e privati (cfr. limitazione all'art. 3 cpv. 4) di emettere diversi mezzi di autenticazione in forma elettronica, mezzi che possono essere utilizzati per dimostrare la propria identità, un fatto o un evento (mezzi di autenticazione elettronici). L'Id-e è emesso esclusivamente da fedpol mediante l'infrastruttura di fiducia statale e costituisce un mezzo di autenticazione elettronico che attesta l'identità del titolare. In particolare, l'Id-e costituisce un «documento probante» ai sensi dell'articolo 3 della legge del 10 ottobre 1997[28] sul riciclaggio di denaro (LRD).

Art. 13 Requisiti personali

Osservazione preliminare

Per richiedere un Id-e occorre disporre già di un documento d'identità rilasciato da un'autorità svizzera. Questo requisito ha il vantaggio di garantire che il richiedente sia stato identificato da un'autorità svizzera e che siano disponibili dati aggiornati che lo concernono.

Non vi è alcun obbligo di richiedere o utilizzare un Id-e. Tuttavia, se i requisiti personali sono soddisfatti, fedpol ha l'obbligo di rilasciare un Id-e al richiedente, che ne diventa titolare non appena l'ottiene.

Lett. a

N. 1

Per richiedere l'emissione di un Id-e, per i cittadini svizzeri è sufficiente disporre di un documento d'identità valido ai sensi della LDI. Questa disposizione include gli Svizzeri all'estero. Dato che agiscono sempre per il tramite del loro organo, ossia persone fisiche, le persone giuridiche non possono essere titolari di un Id-e e sono identificate mediante il numero d'identificazione univoco delle imprese (IDI)[29].

N. 2

Gli stranieri che possiedono una carta di soggiorno valida ai sensi della LStrI e dell'ordinanza del 24 ottobre 2007[30] sull'ammissione, il soggiorno e l'attività lucrativa (OASA) potranno ottenere un Id-e. Si tratta delle carte di soggiorno seguenti:

- permesso L: permesso di soggiorno di breve durata (art. 32 LStrI e 71 cpv. 1 OASA)
- permesso B: permesso di dimora (art. 33 LStrI e 71 cpv. 1 OASA)
- permesso C: permesso di domicilio (art. 34 LStrI e 71 cpv. 1 OASA)

28 RS **955.0**
29 Cfr. www.bfs.admin.ch/bfs > Registri > Registri delle imprese > Numero d'identificazione delle imprese IDI
30 RS **142.201**

- permesso Ci: permesso di dimora con attività lucrativa (art. 30 cpv. 1 lett. g, 98 cpv. 2 LStrI nonché 45 e 71*a* cpv. 1 lett. e OASA)
- permesso N: permesso per richiedente l'asilo (art. 42 LAsi e 71*a* cpv. 1 lett. b OASA)
- permesso F: permesso per stranieri ammessi provvisoriamente (art. 41 cpv. 2 LStrI e 71*a* cpv. 1 lett. c OASA)
- permesso S: permesso per persone bisognose di protezione (art. 74 LAsi e 71*a* cpv. 1 lett. d OASA)
- permesso G: permesso per frontalieri (art. 35 LStrI e 71*a* cpv. 1 lett. a OASA)

È innegabile che questa disposizione non autorizza tutti gli stranieri che sono in contatto con le autorità svizzere (p. es. gli stranieri che possiedono una casa di vacanza in Svizzera) a richiedere un Id-e. Poiché queste persone non sono mai state formalmente identificate da un'autorità svizzera, non può essere rilasciato loro un Id-e. Questa disposizione non esclude che le autorità che sono in stretto contatto con queste persone possano rilasciare loro un altro mezzo di autenticazione elettronico.

Gli Id-e emessi per i cittadini svizzeri e quelli per i cittadini stranieri sono equivalenti. Tuttavia, l'ottenimento di un Id-e non garantisce al titolare l'accesso a tutti i servizi connessi. Ad esempio non è certo che possa beneficiare di tutti i servizi offerti in linea. In effetti, alcuni fornitori di prestazioni potrebbero decidere, per ragioni di sicurezza legate all'affidabilità della verifica dell'identità degli stranieri, di limitare l'accesso ai loro servizi ai titolari di un determinato tipo di permesso di soggiorno. Il presente disegno di legge non introduce restrizioni d'accesso ai servizi in linea e lascia un margine di manovra ai fornitori di prestazioni in questione. Se giustificato e consentito dalla legislazione applicabile, è possibile limitare l'accesso a determinati servizi ai titolari di un permesso per stranieri la cui identità non ha potuto essere verificata in modo affidabile.

Per determinate categorie di permessi (p. es. N, F, S e Ci) non è a priori certo che l'identità abbia potuto essere verificata in modo affidabile. Numerosi richiedenti l'asilo non sono in grado di presentare un documento d'identità durante la procedura d'asilo e quindi non possono essere identificati con certezza. Il DFGP (la Segreteria di Stato della migrazione) riceve parecchie domande di cambiamento o di rettifica dei dati identificativi personali delle persone ammesse provvisoriamente, sovente senza che tali domande siano sostenute da documenti adeguati.

N. 3

Gli stranieri che possiedono una carta di legittimazione valida ai sensi dell'articolo 17 capoverso 1 dell'ordinanza del 7 dicembre 2007[31] sullo Stato ospite (OSOsp) in combinato disposto con l'articolo 71*a* capoverso 1 OASA possono ottenere un Id-e.

31 RS **192.121**

Lett. b

La presente lettera prevede la possibilità di emettere un Id-e per una persona interessata dopo la scadenza della durata di validità del suo documento d'identità o carta di soggiorno per stranieri o carta di legittimazione. L'Id-e potrà essere emesso a condizione che sia la richiesta di emissione di un documento d'identità ai sensi della LDI o di una carta di soggiorno ai sensi della legislazione federale sugli stranieri, l'integrazione e l'asilo (1), sia la richiesta di un Id-e (2) siano state presentate di persona. Le due domande possono essere presentate nel quadro di un unico appuntamento presso la competente autorità. Prima di emettere l'Id-e quest'ultima deve verificare l'identità del richiedente. La possibilità prevista alla lettera b soddisfa le esigenze della prassi e mira a garantire che l'emissione dell'Id-e sia di facile uso.

Art. 14 Contenuto

Cpv. 1

L'Id-e contiene i dati d'identificazione personale seguenti:

a. il cognome ufficiale;

b. i nomi;

c. la data di nascita;

d. il sesso;

e. il luogo d'origine; si tratta di una particolarità elvetica che è stata conservata per essere inclusa nell'Id-e e facilitare così determinate procedure amministrative in Svizzera;

f. il luogo di nascita; è richiesto sovente nel quadro delle transazioni internazionali ed è stato incluso nell'Id-e per questa ragione;

g. la cittadinanza; dato che anche gli stranieri che dispongono di una carta di soggiorno possono ottenere un Id-e, è opportuno menzionare la cittadinanza nel loro Id-e; questa informazione è richiesta sovente nel quadro delle transazioni nazionali e internazionali;

h. l'immagine del viso;

i. il numero AVS; in quanto numero univoco e costante per tutta la vita, il numero AVS è molto utile per le procedure amministrative. Può essere consultato soltanto dalle autorità autorizzate dalla legge.

Questi dati sono disponibili nei registri ufficiali statali a cui fedpol ha accesso conformemente all'articolo 25 capoverso 3 e sono ripresi nell'Id-e senza modifiche.

Cpv. 2

Oltre ai dati d'identificazione personale, l'Id-e contiene le informazioni supplementari seguenti: il suo numero, le date di emissione e di scadenza, informazioni sul documento d'identità utilizzato per la sua emissione, in particolare il tipo e la data di scadenza nonché informazioni relative alla procedura di emissione di tale documento.

Cpv. 3

Il presente capoverso è stato introdotto per tenere conto dei risultati della consultazione. Alcuni partecipanti hanno sottolineato che i documenti d'identità dei titolari dell'Id-e possono pure contenere dati supplementari quali il nome del rappresentante legale, il cognome d'affinità, il nome ricevuto in un ordine religioso, il nome d'arte o il nome dell'unione domestica registrata nonché la menzione di segni particolari. Questi dati possono essere utili o addirittura necessari nel quadro di transazioni che saranno svolte dal titolare dell'Id-e. Possono essere contenuti nell'Id-e a condizione che siano pure menzionati nel documento d'identità, nella carta di soggiorno per stranieri o nella carta di legittimazione del titolare.

Art. 15 Richiesta

Cpv. 1

Non vi è l'obbligo di richiedere un Id-e. La persona che vuole ottenerne uno deve richiederlo a fedpol. La richiesta deve provenire dal futuro titolare dell'Id-e (richiedente) e se del caso essere autorizzata dal suo rappresentante legale (cfr. cpv. 3 per i minorenni e le persone sotto curatela generale). Il richiedente o il rappresentante legale potrà richiedere l'emissione di un Id-e direttamente tramite il sistema d'informazione di fedpol o il portafoglio elettronico statale di cui all'articolo 7.

Cpv. 2

Al fine di tenere conto dei risultati della consultazione, il capoverso 2 prevede la possibilità di emettere simultaneamente diversi Id-e. Dalla consultazione è emersa un'esigenza in tal senso nella prassi. Ad esempio, un genitore potrebbe avere bisogno dell'Id-e di suo figlio per svolgere transazioni a suo nome. Per determinate persone potrebbe essere utile registrare il loro Id-e su diversi supporti tecnici, ad esempio uno smartphone privato, uno smartphone professionale, un tablet o un computer portatile. Per prevenire abusi, tuttavia, l'emissione di più Id-e deve essere simultanea. Una volta emessi il o gli Id-e, il titolare non potrà più richiederne uno supplementare per un altro supporto (senza che gli Id-e esistenti siano revocati, cfr. art. 18 lett. e). In tal caso dovrà presentare una nuova richiesta per tutti i supporti e i vecchi Id-e saranno revocati.

Cpv. 3

Secondo il presente capoverso, per ottenere l'Id-e i minorenni e le persone sotto curatela generale necessitano della dichiarazione di consenso del loro rappresentante legale. Questo requisito si allinea al limite d'età previsto per ottenere i documenti d'identità svizzeri (ossia 18 anni; cfr. art. 5 cpv. 1 LDI). Il rappresentante legale di un minore o di una persona sotto curatela generale può conservarne l'Id-e assieme al proprio nel portafoglio elettronico di cui all'articolo 7.

Art. 16 Verifica dell'identità

Cpv. 1

Il presente capoverso è stato introdotto per tenere conto dei risultati della consultazione. Numerosi partecipanti hanno chiesto che il disegno di legge preveda la possibilità di ottenere l'Id-e presentandosi di persona. Il capoverso 1 consente quindi al richiedente di far verificare la propria identità in linea da fedpol o di persona presso uno dei servizi o autorità competenti designati dai Cantoni in Svizzera o dal Consiglio federale all'estero. Sono state avviate consultazioni con i Cantoni allo scopo di valutare la possibilità di implementare procedure di verifica dell'identità, tra l'altro, presso gli uffici dei passaporti e gli uffici cantonali della migrazione.

Cpv. 2

Il presente capoverso attribuisce ai servizi e alle autorità di cui al capoverso 1 la competenza di verificare mediante un confronto se il viso del richiedente corrisponde all'immagine del viso contenuta nei registri federali ISA, SIMIC o Ordipro. Questa verifica può essere effettuata di persona o in linea. Le modalità della relativa procedura saranno definite dal Consiglio federale a livello di ordinanza (art. 19 lett. b).

Cpv. 3

Il presente capoverso costituisce una base legale in senso formale volta a permettere a fedpol di rilevare dati biometrici per effettuare il confronto di cui al capoverso 2, che sarà effettuato durante la procedura in linea. Il capoverso 3 soddisfa dunque i requisiti di cui all'articolo 34 capoverso 2 lettera a LPD, che esige una base legale figurante in una legge in senso formale per permettere agli organi federali di trattare dati personali degni di particolare protezione. L'articolo 5 lettera c n. 4 LPD definisce «i dati biometrici che identificano in modo univoco una persona fisica» come dati personali degni di particolare protezione. Per dati biometrici s'intendono «i dati relativi a caratteristiche fisiche, fisiologiche o comportamentali ottenuti grazie a un processo tecnico specifico e che permettono di identificare univocamente una persona o di confermarne l'identificazione»[32].

Alcuni partecipanti alla consultazione hanno chiesto che i dati biometrici rilevati durante la procedura di emissione dell'Id-e vengano immediatamente distrutti. Il disegno di legge non prevede un obbligo in tal senso bensì mira a consentire a fedpol di conservare i dati biometrici necessari a condurre un'inchiesta concernente il conseguimento fraudolento di un Id-e (art. 26 cpv. 1 lett. b). Di conseguenza, questi dati possono essere conservati fino a cinque anni dopo la scadenza dell'Id-e.

Art. 17 Emissione

fedpol si assicura che il richiedente soddisfi i requisiti definiti all'articolo 13. Se ciò è il caso, procede con la verifica della sua identità sulla base delle informazioni a tal scopo necessarie, confrontando le informazioni fornite dal richiedente con quelle con-

32 Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF **2017** 5939, in particolare 6012.

tenute nei registri federali di cui all'articolo 25 capoverso 3. Se l'identità del richiedente è verificata con successo, fedpol gli rilascia un Id-e con i dati definiti all'articolo 14.

Nella maggior parte dei casi la procedura di verifica dell'identità in linea sarà svolta in maniera automatizzata. In caso d'incertezza, fedpol potrà intervenire e riesaminare i dati generati durante la procedura di verifica. Il richiedente potrà pure presentare un reclamo presso il servizio di assistenza di fedpol. Le esigenze previste dall'articolo 21 capoverso 2 LPD dovranno essere rispettate nel quadro di questa procedura automatizzata.

Art. 18 Revoca

Occorre distinguere tra distruzione e revoca dell'Id-e.

La distruzione dell'Id-e costituisce una procedura irreversibile in cui il pacchetto di dati composto di attributi e materiale crittografico è soppresso. Dal punto di vista tecnico, l'emittente non può distruggere un Id-e a causa del carattere decentralizzato dell'infrastruttura di fiducia. Soltanto il titolare può distruggere il suo Id-e cancellandolo sul suo portafoglio elettronico o disinstallando quest'ultimo dal suo smartphone.

In caso di revoca, fedpol effettua un'iscrizione nel registro di base indicando che un Id-e specifico non è più valido. L'Id-e in questione rimane invariato nel portafoglio elettronico e può continuare a essere presentato. Tuttavia, non appena un verificatore verifica l'Id-e revocato, dall'iscrizione nel registro di base apprende che l'Id-e non è più valido.

Il disegno di legge prevede la possibilità di revocare un Id-e nei casi definiti alle lettere a-e. Il titolare o il rappresentante legale nel caso di un minorenne o di una persona sotto curatela generale può richiedere la revoca del suo Id-e o di quello della persona che rappresenta. Inoltre, fedpol revoca l'Id-e se vi è un sospetto fondato che sia utilizzato in maniera abusiva. Prima di procedere alla revoca, fedpol verifica le informazioni che gli sono state sottoposte. Revoca l'Id-e anche se apprende del decesso del titolare o della revoca del documento d'identità utilizzato per la procedura di emissione dell'Id-e. fedpol riceve le informazioni concernenti un sospetto di abuso sotto forma di notifiche push dai registri di cui all'articolo 25 capoverso 3. Il Consiglio federale disciplina per via d'ordinanza gli obblighi delle competenti autorità per quanto concerne l'invio delle notifiche.

Inoltre, l'Id-e è revocato se il titolare ne ottiene uno nuovo. Un Id-e revocato non può più essere riattivato: la persona in questione può tuttavia richiedere a fedpol l'emissione di un nuovo Id-e ai sensi dell'articolo 15 capoverso 1.

La revoca costituisce una misura tecnica che non può essere annullata. Inoltre, non può essere comunicata al titolare dell'Id-e in quanto non è sicuro che il canale di comunicazione con fedpol stabilito con la trasmissione dell'Id-e sia ancora attivo. Il titolare è infatti libero di sopprimerlo una volta ricevuto l'Id-e. Il disegno di legge prevede la revoca come misura tecnica volta a prevenire abusi. Si tratta di un compromesso tra l'utilizzo agevole dell'Id-e e la necessità di garantire un livello di sicurezza elevato. La revoca, d'altronde, non comporta il ritiro del diritto di ottenere un Id-e. Il titolare può presentare una nuova richiesta di emissione.

La revoca dell'Id-e costituisce un atto materiale e non è quindi oggetto di una decisione di fedpol. Il titolare può prenderne atto durante l'utilizzo dell'Id-e o del suo portafoglio elettronico. Inoltre, può contattare l'assistenza tecnica di fedpol per assicurarsi che il suo Id-e sia stato revocato oppure può chiedere che fedpol pronunci la revoca mediante decisione formale conformemente all'articolo 25*a* della legge del 20 dicembre 1968[33] sulla procedura amministrativa (PA). In tal caso dovrà fornire a fedpol i dati personali supplementari necessari per l'invio della decisione.

Art. 19 Procedure

Al Consiglio federale è delegata la competenza di disciplinare le procedure relative alla presentazione della richiesta di emissione dell'Id-e (art. 15), alla verifica dell'identità del richiedente (art. 16), nonché all'emissione (art. 17) e alla revoca (art. 18) dell'Id-e.

Art. 20 Durata di validità

Per ragioni di sicurezza, l'Id-e ha una durata di validità limitata. Il Consiglio federale disciplina in un'ordinanza le esigenze relative a tale durata. In questo quadro sarà opportuno chiarire se la durata di validità dell'Id-e deve corrispondere a quella del documento utilizzato per la sua emissione. La durata di validità sarà indicata nell'Id-e (art. 14 cpv. 2 lett. b e c). Se le autorità ritirano il documento d'identità utilizzato per l'emissione dell'Id-e, fedpol revocherà l'Id-e non appena ne sarà venuto a conoscenza (art. 18 lett. d n. 1).

Un Id-e non più valido rimane disponibile sul supporto elettronico del titolare in quanto mezzo di autenticazione elettronico autentico ma scaduto.

Art. 21 Obblighi di diligenza del titolare

Cpv. 1

Gli obblighi dei titolari di un Id-e emesso nel quadro del disegno di legge corrispondono in linea di massima agli obblighi di diligenza che devono abitualmente essere rispettati utilizzando i servizi bancari in linea. È ad esempio necessario e ragionevolmente esigibile che il titolare non riveli l'eventuale codice PIN e non lo conservi insieme al supporto dell'Id-e, nonché che attivi le funzioni di restrizione dell'accesso all'apparecchio mobile che serve da supporto dell'Id-e, ad esempio il riconoscimento delle impronte digitali o il codice PIN, oppure vi installi un programma antivirus. Pur prendendo tutte le precauzioni possibili, nessuno è totalmente al sicuro da un'usurpazione d'identità, che potrà però essere punita con una sanzione adeguata. In occasione della revisione della LPD, il Codice penale[34] è stato completato con l'articolo 179^{decies}, che punisce l'usurpazione d'identità con una pena detentiva sino a un anno o una pena pecuniaria. Al fine di evitare ridondanze, il presente disegno di legge non contiene disposizioni che sanzionano tale reato.

33 RS **172.021**
34 RS **311.0**

Cpv. 2

La perdita di un documento d'identità deve sempre essere notificata alla polizia (art. 8 LDI). Una disposizione analoga non ha senso per l'Id-e, che dovrebbe sempre beneficiare di una doppia protezione (salvaguardia dell'accesso all'apparecchio e salvaguardia dell'accesso al portafoglio elettronico). In altri termini, un apparecchio che cade in mano a persone non autorizzate non dovrebbe permettere di accedere all'Id-e in esso contenuto. Tuttavia, il titolare può sempre – dunque anche in caso di perdita – chiedere la revoca dell'Id-e (art. 18 lett. a).

Se sospetta un utilizzo abusivo del suo Id-e, il titolare deve segnalarlo immediatamente a fedpol e se del caso chiederne la revoca.

Art. 22 Obbligo di diligenza del verificatore

Il presente articolo è stato introdotto per tenere conto dei risultati della consultazione. L'assenza di disposizioni che limitano il trattamento dei dati da parte del verificatore è stata oggetto di numerose critiche e proposte. È stato principalmente criticato il fatto che il verificatore potesse decidere liberamente se e in quale misura vada presentato un mezzo di autenticazione elettronico. Secondo alcuni partecipanti, tale possibilità dovrebbe essere limitata dalla legge allo stretto necessario e assoggettata a un consenso informato ed esplicito. I partecipanti erano inoltre del parere che l'avamprogetto e la LPD non tutelino a sufficienza i titolari dei mezzi di autenticazione elettronici dal rischio di ricorso ingiustificato all'identificazione elettronica da parte dei verificatori.

Elaborando la presente disposizione si è constatato che sanzioni efficaci possono essere inflitte unicamente nel quadro dell'utilizzo dell'Id-e. I casi di utilizzo degli altri mezzi di autenticazione elettronici sono troppo diversificati e non abbastanza noti per consentire l'imposizione di sanzioni uniformi. Inoltre, è emerso che le sanzioni penali non costituiscono lo strumento migliore per prevenire le violazioni del capoverso 1. In considerazione delle sanzioni penali previste per la violazione delle diverse disposizioni della LPD, una violazione del capoverso 1 appare meno grave e non potrebbe essere punita con una sanzione paragonabile. Oltre a ciò, le esigenze del capoverso 1 lasciano un ampio margine di interpretazione e non sono idonee all'imposizione di una sanzione penale. Nella prassi, le sanzioni penali valutate darebbero luogo a importanti incoerenze e iniquità. Esigenze più precise, quali l'iscrizione obbligatoria nel registro di fiducia dei verificatori che ricorrono all'Id-e, permetterebbero di sanzionare i casi di inosservanza ma sarebbero diametralmente opposte ai principi fondamentali della SSI e genererebbero un notevole onere burocratico. Infine, la comunicazione delle violazioni agli altri utenti e l'esclusione del verificatore colpevole si sono rivelati strumenti più utili ed efficaci per sanzionare il comportamento scorretto.

La possibilità di disciplinare altri aspetti quali un obbligo esteso di informare il titolare, un diritto esteso del titolare di opporsi o il divieto di collegamento[35] (strumento volto a combattere l'eccesso d'identificazione), è stata esaminata per dare seguito alle

35 Ai sensi dell'art. 7 par. 4 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), GU L 119 del 4.5.2016, pag. 1.

critiche e agli argomenti formulati dai partecipanti alla consultazione. Alla luce delle difficoltà tecniche nell'attuazione di queste esigenze non è stato possibile definire nuove regole comuni in materia. Inoltre, il Consiglio federale non intende riaprire la discussione concernente i compromessi convenuti per quanto riguarda le sanzioni nel quadro della LPD.

Le disposizioni della LPD e il Codice civile (CC)[36] rimangono applicabili in materia. Va rammentato che il trattamento dei dati personali contenuti nell'Id-e deve essere proporzionato (adeguato, pertinente e non eccessivo) alle finalità determinate dal verificatore (art. 6 cpv. 2 LPD).

Cpv. 1

Al fine di dare seguito alle preoccupazioni espresse in sede di consultazione, il capoverso 1 mira a inasprire i requisiti della LPD e dell'avamprogetto per quanto concerne l'utilizzo dell'Id-e. Stabilisce le condizioni alle quali il verificatore può domandare ai titolari di trasmettere dati personali contenuti dell'Id-e ossia unicamente se la verifica dell'identità del titolare o di un elemento di essa è prevista dalla legge (lett. a) o necessaria per ragioni di affidabilità della transazione (lett. b). Il presente capoverso mira dunque a limitare la possibilità di richiedere dati personali non essenziali alla fornitura di una prestazione. Si tratta di prevenire i casi di ricorso ingiustificato all'identificazione elettronica da parte dei verificatori.

Lett. a

Un esempio di trasmissione di dati personali per la finalità di cui alla lettera a sarebbe una domanda di accesso secondo gli articoli 25 LPD e 16 capoverso 3 OPDa. La persona che chiede al responsabile del trattamento di accedere alle pertinenti informazioni riceve in particolare informazioni sulla sua identità. Potrebbe pure trattarsi dell'obbligo previsto all'articolo 20 dell'ordinanza del 15 novembre 2017[37] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT), secondo cui i fornitori di servizi di telecomunicazione (FST) e i rivenditori devono verificare l'identità degli utenti. Inoltre, l'articolo 17 dell'ordinanza dell'11 novembre 2015[38] sul riciclaggio di denaro (ORD), che prevede un obbligo d'identificazione della controparte da parte del commerciante al momento della conclusione di un contratto, soddisfa parimenti le esigenze della presente lettera. Anche l'obbligo di identificarsi nel quadro della richiesta di una cartella informatizzata del paziente costituirà un caso di applicazione della presente lettera conseguente alla modifica della legislazione relativa alla cartella informatizzata del paziente.

Lett. b

Un esempio di trasmissione di dati personali per la finalità di cui alla lettera b potrebbe essere la verifica dell'identità di una persona al fine di sostenere un esame organizzato da un'università o da un altro istituto formativo, oppure la necessità di verificare l'identità di una persona al momento della consegna di un pacco da parte del servizio di consegna. In questi casi la verifica dell'identità costituisce un elemento essenziale.

36 RS **210**
37 RS **780.11**
38 RS **955.01**

Viceversa, la verifica dell'identità di un consumatore in occasione di un acquisto contro fattura in Internet non soddisfa le esigenze della lettera b. Il venditore potrebbe volere assicurarsi mediante l'Id-e che il suo interlocutore sia maggiorenne e che sia una persona reale. Si tratta di un bisogno reale e importante ma non di una necessità legata all'affidabilità della transazione; in questo caso, infatti, il venditore dovrebbe verificare in particolare la solvibilità o l'indirizzo per assicurarsi che la persona che acquista senza pagare sia solvibile e che riceva l'acquisto. La verifica dell'identità per mezzo dell'Id-e non permette di ottenere né l'indirizzo né le informazioni relative alla solvibilità della persona in questione. La richiesta dei dati personali contenuti nell'Id-e non aumenta automaticamente il livello di affidabilità di un acquisto contro fattura.

Cpv. 2

In virtù del capoverso 2, l'UFIT pubblica nel registro di fiducia un elenco dei casi d'identificazione mediante l'Id-e che violano le esigenze di cui al capoverso 1. Si tratta di una misura di sicurezza essenziale volta a prevenire le violazioni e a informare gli utenti sulle violazioni commesse. Non avendo la competenza per individuare queste violazioni, l'UFIT agisce dopo aver preso conoscenza di una violazione; verifica la credibilità delle informazioni prima di pubblicarle. Se un verificatore è iscritto nel registro di fiducia e non rispetta le condizioni del capoverso 1, l'UFIT può anche decidere di escluderlo dal registro di fiducia.

Art. 23 Obbligo di accettare l'Id-e

Le autorità e gli altri organi che adempiono compiti pubblici devono accettare l'Id-e se ricorrono all'identificazione elettronica in esecuzione del diritto federale. La disposizione si applica anche alle autorità cantonali e comunali, ad esempio agli uffici d'esecuzione ai quali un privato richiede un estratto del registro delle esecuzioni per via elettronica e s'identifica con un Id-e (v. commento all'art. 33*a* cpv. 2bis LEF). Ciò è opportuno in quanto l'Id-e è concepito come mezzo d'identificazione elettronico statale che serve a provare la propria identità nel mondo virtuale; è dunque paragonabile alla carta d'identità e al passaporto nel mondo fisico, che sono pure accettati da tutte le autorità per l'identificazione. L'Id-e statale potrà essere utilizzato congiuntamente con i mezzi di accesso ai servizi amministrativi in linea. Questo obbligo si applica unicamente alle procedure d'identificazione che richiedono la presenza del titolare e la presentazione di un documento d'identità.

L'articolo 23 rispecchia l'importanza dell'Id-e ai sensi della presente legge e della sua accettazione da parte della popolazione, evidenziate dalla Strategia Svizzera digitale 2018–2022[39] e dalla Strategia di e-government Svizzera 2020–2023[40]. Non da ultimo si tratta in particolare di sostenere gli investimenti della Confederazione destinati all'attuazione dell'Id-e e di contribuire alla sua diffusione nell'amministrazione digitale, a beneficio non soltanto della Confederazione, dei Cantoni e dei Comuni, che potranno in tal modo conseguire dei risparmi a medio termine, ma anche della popolazione svizzera. Le questioni connesse all'utilizzo dell'Id-e e le relative ripercussioni

39 www.uvek.admin.ch > Comunicazione > Svizzera digitale > Strategia Svizzera digitale
40 www.bk.admin.ch > Trasformazione digitale e governance delle TIC > Direttive TIC > Strategie e strategie parziali > SN001 – Strategia di e-government Svizzera

giuridiche non sono disciplinate nel disegno ma devono essere regolamentate in maniera specifica per ogni settore. Il disegno di legge tiene in particolare conto della cartella informatizzata del paziente nonché del settore esecuzione e fallimento.

Art. 24 Alternative alla presentazione di un Id-e

Il presente articolo mira a garantire che i titolari non siano obbligati a presentare il loro Id-e nel quadro delle interazioni nel mondo reale. Malgrado i vantaggi dell'Id-e, non si intende escludere la possibilità di presentare dei documenti d'identità (fisici). Pertanto, se è possibile identificare una persona per mezzo di un documento d'identità nel quadro di una procedura che ne richiede la presenza, la presentazione dell'Id-e (o di elementi di esso) può essere offerta soltanto a titolo opzionale.

Art. 25 Sistema d'informazione per l'emissione e la revoca degli Id-e

Cpv. 1

fedpol gestirà un sistema d'informazione che tratterà i dati personali di cui all'articolo 14; tale sistema permetterà di ricevere le richieste di emissione e di eseguire i compiti di fedpol nel quadro dell'emissione e della revoca degli Id-e.

Cpv. 2

Il sistema d'informazione contiene i dati di cui all'articolo 14 capoverso 2 concernenti gli Id-e richiesti ed emessi nonché i dati relativi alla revoca di un Id-e. Vi sono inoltre conservati i dati relativi alla procedura di emissione necessari per fornire assistenza tecnica, allestire statistiche o condurre indagini in merito al conseguimento fraudolento o all'utilizzo abusivo di un Id-e.

Cpv. 3

Per emettere un Id-e il sistema d'informazione potrà accedere ai dati di cui all'articolo 14 capoverso 1, contenuti nei seguenti registri di persone gestiti a livello federale:

- il sistema d'informazione per i documenti d'identità (ISA) di cui all'articolo 11 LDI;
- il sistema d'informazione centrale sulla migrazione (SIMIC) di cui agli articoli 101 e seguenti LStrI e nell'ordinanza SIMIC del 12 aprile 2006[41];
- il registro elettronico dello stato civile (Infostar) di cui agli articoli 39 CC e 6*a* dell'ordinanza del 28 aprile 2004[42] sullo stato civile (OSC);
- il registro centrale degli assicurati dell'Ufficio centrale di compensazione dell'AVS (UCC-UPI) di cui all'articolo 71 capoverso 4 della legge del 20 dicembre 1946[43] su l'assicurazione per la vecchiaia e per i superstiti (LAVS); sarà accessibile solo la parte UPI del registro, responsabile della gestione del

41 RS **142.513**
42 RS **211.112.2**
43 RS **831.10**

numero AVS e dei dati menzionati all'articolo 133bis capoverso 4 dell'ordinanza del 31 ottobre 1947[44] sull'assicurazione per la vecchiaia e per i superstiti (OAVS);

– il sistema d'informazione Ordipro del Dipartimento federale degli affari esteri di cui agli articoli 5 della legge federale del 18 dicembre 2020[45] sul trattamento dei dati personali da parte del Dipartimento federale degli affari esteri e 2 dell'ordinanza Ordipro del 22 marzo 2019[46].

In tal modo fedpol potrà eseguire i compiti necessari per l'emissione dell'Id-e in maniera automatizzata e su questa base verificare l'identità del richiedente.

Cpv. 4

I dati ottenuti tramite interfacce non sono né duplicati né salvati nel sistema d'informazione di fedpol. Sono controllati direttamente nei registri federali. fedpol li tratta unicamente allo scopo di emettere o revocare un Id-e; qualsiasi altro scopo di trattamento di questi dati è escluso.

Art. 26 Conservazione e distruzione dei dati

Cpv. 1

Il presente articolo è stato introdotto per tenere conto dei risultati della consultazione. Alcuni partecipanti hanno lamentato il fatto che l'avamprogetto non disciplinasse la durata di conservazione e la distruzione dei dati. Conformemente all'articolo 6 capoverso 4 LPD, i dati personali sono distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento. Gli scopi di trattamento risultano dalle basi legali previste per il trattamento di dati agli articoli 14 e 25 del presente disegno di legge. L'articolo 26 prevede termini di conservazione diversi per tre categorie di dati in considerazione dei differenti scopi di trattamento.

Lett. a

I dati di cui alla lettera a saranno conservati per 20 anni al massimo a partire dalla data della richiesta o dell'emissione dell'Id-e. Malgrado i diversi termini di conservazione previsti per i dati contenuti in ISA, SIMIC e Ordipro, ai dati concernenti i cittadini svizzeri e stranieri contenuti nel sistema d'informazione di fedpol si applicano gli stessi termini. Al fine di semplificare la procedura di conservazione dei dati, la presente disposizione si allinea ai termini di conservazione previsti per i dati relativi ai documenti d'identità svizzeri di cui all'articolo 37 capoverso 1 dell'ordinanza del 20 settembre 2002[47] sui documenti d'identità (ODI). In tal modo è previsto un unico termine di conservazione per i dati di cittadini svizzeri e stranieri.

44 RS **831.101**
45 RS **235.2**
46 RS **235.21**
47 RS **143.11**

Lett. b

Il termine fissato per la conservazione dei dati relativi alla procedura di emissione necessari per condurre un'indagine in merito a un conseguimento fraudolento di un Id-e, ivi compresi i dati biometrici di cui all'articolo 16 capoverso 3, è giustificato per ragioni probatorie. Oltre questo termine non è sicuro che sia necessario conservare i dati.

Cpv. 2

Tutti gli altri dati sono distrutti 90 giorni dopo la loro registrazione nel sistema. Questo requisito mira a garantire che l'articolo preveda un termine di conservazione per tutti i dati. Quelli non contemplati dal capoverso 1 sono conservati secondo il capoverso 2.

Cpv. 3

Il capoverso 1 si applica a condizione che l'articolo 38 LPD e le disposizioni della legge del 26 giugno 1998[48] sull'archiviazione (LAr) siano rispettati. L'articolo 6 LAr dispone che i dati di cui non si ha più bisogno siano offerti all'Archivio federale, il quale distrugge quelli che giudica non abbiano valore archivistico.

Sezione 4 Accessibilità per disabili

Art. 27

Il presente articolo è stato introdotto per tenere conto dei risultati della consultazione. Numerosi partecipanti hanno lamentato l'assenza nell'avamprogetto di disposizioni concernenti l'accessibilità per i disabili e hanno formulato un certo numero di richieste al riguardo. I capoversi 1–3 mirano a chiarire e rafforzare i requisiti previsti dalla legge del 13 dicembre 2002[49] sui disabili (LDis) e dall'ordinanza del 19 novembre 2003[50] sui disabili (ODis).

Secondo l'articolo 14 capoverso 2 LDis, le prestazioni offerte dalle autorità su Internet devono essere accessibili senza difficoltà alle persone ipovedenti. Inoltre, l'articolo 10 capoverso 1 ODis prescrive che l'informazione, le possibilità di contatto e le operazioni proposte su Internet devono essere accessibili alle persone audiolese, ipovedenti, affette da disturbi del linguaggio o da disturbi motori.

L'articolo 27 capoversi 1–3 si allinea ai requisiti di cui all'articolo 10 capoverso 1 ODis specificando quali componenti dell'infrastruttura devono essere resi accessibili ai disabili. I requisiti dell'ODis non valgono per le applicazioni di cui agli articoli 7 e 8 in quanto non si tratta di prestazioni fornite su Internet. I capoversi 1–3 mirano a estendere il campo di applicazione delle esigenze dell'ODis e a fissarle nel contempo a livello di legge.

48 RS **152.1**
49 RS **151.3**
50 RS **151.31**

Cpv. 1–3

Il capoverso 1 mira a garantire che l'Id-e possa essere ottenuta dai disabili e impone a fedpol di assicurarsi che la procedura di ottenimento rispetti le norme applicabili in materia di accessibilità per i disabili.

Anche il capoverso 2 prevede l'attuazione dell'accessibilità per i disabili in relazione con le applicazioni messe a disposizione dalla Confederazione per agevolare l'utilizzo dell'Id-e e di altri mezzi di autenticazione elettronici, ossia l'applicazione per la conservazione e la presentazione dei mezzi di autenticazione elettronici (art. 7) e l'applicazione per la verifica degli stessi (art. 8).

Inoltre, le norme in materia di accessibilità per i disabili dovranno essere rispettate nel quadro dell'ottenimento e dell'utilizzo di altri mezzi di autenticazione elettronici (cpv. 3). Le autorità federali e cantonali che utilizzano l'infrastruttura di fiducia per emettere e verificare i mezzi di autenticazione elettronici sono tenute a rispettare le norme in materia di accessibilità per i disabili nel quadro di queste procedure.

Cpv. 4

Al Consiglio federale è delegata la competenza di disciplinare le misure che fedpol, l'UFIT e le autorità devono adottare per garantire l'accessibilità per i disabili nei casi di cui ai capoversi 1–3. Può in particolare prevedere misure di comunicazione specifiche e rendere vincolanti norme tecniche riconosciute nel settore. Inoltre può esigere, a intervalli regolari, controlli e aggiornamenti. Per elaborare le pertinenti disposizioni consulterà le organizzazioni specializzate e l'Ufficio federale per le pari opportunità delle persone con disabilità.

Sezione 5 Assistenza tecnica

Art. 28

I requisiti concernenti l'assistenza previsti nell'avamprogetto sono stati rielaborati al fine di tenere conto dei risultati della consultazione. Alcuni partecipanti hanno criticato il fatto che l'avamprogetto incaricherebbe i Cantoni di designare dei servizi tenuti a offrire assistenza sul posto. Numerosi partecipanti hanno ritenuto che l'Amministrazione federale dovrebbe offrire un'assistenza a tutti gli utenti dell'infrastruttura di fiducia. L'articolo 28 incarica dunque la Confederazione di offrire un servizio d'assistenza nel quadro dell'emissione dell'Id-e e dell'utilizzo dell'infrastruttura di fiducia. Si tratterà di mettere a disposizione un servizio di assistenza di primo livello nelle tre lingue ufficiali della Confederazione e in inglese destinato alle autorità federali, cantonali e comunali nonché alle persone fisiche.

Sezione 6 Evoluzione tecnica

Art. 29

Cpv. 1

L'evoluzione tecnica avanza a grandi passi e continuerà a farlo anche dopo l'entrata in vigore di questa legge. Per tener conto di questa evoluzione, il capoverso 1 delega

al Consiglio federale la competenza di emettere, per via d'ordinanza, disposizioni complementari che permettano di adeguare l'infrastruttura di fiducia all'evoluzione tecnica e di garantire che continui a raggiungere gli obiettivi definiti dalla presente legge.

Cpv. 2

Per diverse ragioni, le disposizioni complementari possono richiedere una base legale formale. Ad esempio, conformemente all'articolo 34 capoverso 2 lettera a LPD non è sufficiente disciplinare il trattamento di dati degni di particolare protezione in un'ordinanza ma è richiesta una base legale in senso formale. Nel quadro del presente disegno di legge, l'ordinanza del Consiglio federale decadrà in tre casi: se, entro un termine di due anni dopo la sua entrata in vigore, il Consiglio federale non ha sottoposto all'Assemblea federale un disegno di legge che stabilisca la base legale pertinente; se il disegno è respinto dall'Assemblea federale; se la base legale prevista entra in vigore.

Sezione 7 Emolumenti

Art. 30

Cpv. 1

Agli emittenti e ai verificatori sono applicati emolumenti per l'iscrizione dei dati nel registro di base e nel registro di fiducia.

Dato che la legge non lo fissa, l'importo degli emolumenti sarà definito per via d'ordinanza. Potrà ammontare ad alcune decine o centinaia di franchi.

Cpv. 2

Secondo una prassi consolidata, le autorità federali non applicano alcun emolumento alle autorità cantonali per l'utilizzo della loro infrastruttura (e viceversa). L'utilizzo dell'infrastruttura di fiducia sarà dunque gratuito per Cantoni e Comuni.

Cpv. 3

Il capoverso precisa che nessun emolumento sarà riscosso per l'emissione, l'utilizzo, la verifica e la revoca dell'Id-e nella misura in cui i servizi sono forniti in linea.

Anche l'utilizzo del portafoglio elettronico emesso dalla Confederazione nonché la consultazione del registro di base e del registro di fiducia sono gratuiti.

Esonerando in gran parte gli utenti dal pagamento di emolumenti, il capoverso 3 mira a incoraggiare l'utilizzo e la diffusione dell'Id-e. La Confederazione ha tutto l'interesse alla diffusione più estesa possibile dell'Id-e al fine di agevolare gli scambi con le autorità e i privati.

Cpv. 4

Questo capoverso è stato elaborato al fine di considerare i risultati della consultazione. I Cantoni hanno chiesto che il disegno di legge preveda la possibilità di riscuotere un emolumento per i servizi forniti sul posto. Per dare seguito a questa richiesta, il Con-

siglio federale prevedrà per via d'ordinanza che il competente servizio possa riscuotere degli emolumenti per le prestazioni fornite sul posto.

Cpv. 5

Il Consiglio federale disciplina per via d'ordinanza la riscossione degli emolumenti conformemente all'articolo 46*a* LOGA.

Sezione 8 Trattati internazionali

Art. 31

Considerati i suoi stretti rapporti commerciali e sociali con la maggior parte dei Paesi membri dell'UE, la Svizzera ha tutto l'interesse a garantirsi la possibilità di essere presto o tardi integrata nel sistema europeo per l'interoperabilità dei sistemi d'identificazione elettronici. A tal scopo sarà necessario un trattato internazionale. L'articolo 31 delega al Consiglio federale la competenza di concludere trattati internazionali destinati ad agevolare l'utilizzo e il riconoscimento dell'Id-e sul piano internazionale e di emanare le necessarie disposizioni d'esecuzione. Un tale trattato permetterebbe di garantire il riconoscimento reciproco del sistema d'identificazione svizzero e di quelli notificati secondo il regolamento eIDAS o implementati da alcuni Stati membri dell'UE o da Stati terzi.

Sezione 9 Disposizioni finali

Art. 32 Disposizioni d'esecuzione

Le disposizioni d'esecuzione della presente legge disciplinano l'attuazione degli aspetti tecnici e organizzativi connessi alla trasmissione dei mezzi di autenticazione elettronici nonché il funzionamento delle componenti dell'infrastruttura di fiducia. Si tratterà in particolare di disciplinare il formato dei mezzi di autenticazione elettronici; gli standard e i protocolli per le procedure di comunicazione dei dati durante l'emissione e la presentazione dei mezzi di autenticazione elettronici; le componenti e le modalità di funzionamento del registro di base, del registro di fiducia, del sistema di conferma degli identificativi, dell'applicazione per la conservazione e la presentazione dei mezzi di autenticazione elettronici e del sistema per le copie di sicurezza; i giustificativi da presentare per l'iscrizione nel sistema di conferma degli identificativi; i provvedimenti tecnici e organizzativi da adottare per garantire la protezione e la sicurezza dei dati nel quadro della gestione e dell'utilizzo dell'infrastruttura di fiducia nonché le interfacce, le componenti e le modalità di funzionamento del sistema d'informazione per l'emissione e la revoca degli Id-e.

Art. 33 Modifica di altri atti normativi

Il disegno propone la modifica di altri atti normativi, principalmente allo scopo di permettere a fedpol di accedere ai sistemi d'informazione ISA, Infostar e SIMIC. Gli adeguamenti disciplinano parimenti, a titolo indicativo, l'utilizzo dell'Id-e in determinati settori quali la cartella informatizzata del paziente e quello delle esecuzioni e dei fallimenti.

Art. 34 Disposizione transitoria

Cpv. 1

Secondo l'articolo 23, le autorità e gli organi che adempiono compiti pubblici devono accettare l'Id-e se ricorrono all'identificazione elettronica in esecuzione del diritto federale. Il presente capoverso prevede un termine di due anni a partire dall'entrata in vigore della legge per l'attuazione di tale obbligo.

Cpv. 2

Per garantire la sicurezza, la qualità del sistema e la disponibilità dell'assistenza tecnica al momento dell'introduzione, il Consiglio federale può prevedere una messa a disposizione scaglionata dell'infrastruttura di fiducia e dell'Id-e nell'arco di due anni al massimo dopo l'entrata in vigore della presente legge. L'introduzione scaglionata potrà interessare, in particolare, le diverse funzionalità connesse al portafoglio elettronico quali la registrazione di diversi Id-e su differenti supporti o la registrazione dell'Id-e sui portafogli di fornitori di prestazioni terzi. Il presente capoverso mira a garantire il perfezionamento del prodotto a ogni fase della sua attuazione.

Il Consiglio federale può parimenti adottare misure volte a garantire un'emissione in linea sicura e di qualità. Le esperienze di altri Paesi hanno dimostrato che durante i primi mesi la richiesta è molto forte, per cui l'assistenza e la gestione tecnica del sistema sono messe sotto pressione. Per garantire la qualità e la sicurezza del sistema nel corso dell'introduzione, nei primi mesi il numero di Id-e emessi giornalmente potrebbe essere monitorato, con un possibile conseguente termine di attesa per i richiedenti.

Il Consiglio federale può ugualmente prevedere uno scadenzario per permettere alle autorità preposte al controllo dell'identità sul posto (art. 16 cpv. 1 lett. b) di organizzarsi per assumere questo nuovo compito come chiesto dai Cantoni (v. n. 6.2).

Art. 35 Referendum ed entrata in vigore

Come tutte le leggi federali, questa legge sottostà a referendum facoltativo. Il Consiglio federale ne fisserà l'entrata in vigore.

Modifica di altri atti normativi

Osservazione preliminare

Le condizioni d'identificazione e di autenticazione per le applicazioni dell'amministrazione digitale sono disciplinate nel diritto applicabile e, per quanto necessario, per via d'ordinanza o di direttiva. Diverse ordinanze e direttive dovranno essere modificate in vista dell'attuazione della legge sull'Id-e ma ciò avverrà soltanto al momento dell'adozione delle disposizioni d'esecuzione della legge, ragion per cui in questa sede sono spiegate soltanto le modifiche di altre leggi federali.

Da una valutazione dei diversi ambiti del diritto federale è emerso che nel quadro del presente progetto devono essere modificate soltanto le leggi presentate qui di seguito. La valutazione ha tenuto conto di tutti i pertinenti ambiti del diritto federale. Inoltre,

sono stati condotti colloqui con i dipartimenti federali interessati a ricorrere all'Id-e. Sono pochi gli ambiti in cui il diritto federale prescrive un'identificazione delle persone. D'altra parte, la legge non mira a disciplinare tutti gli ambiti in cui i mezzi di autenticazione elettronici saranno utilizzati, ma serve a creare le basi legali necessarie per l'utilizzo dell'Id-e e dell'infrastruttura di fiducia. Spetterà alle competenti autorità prevedere, in caso di bisogno, le basi legali necessarie in leggi settoriali.

1. Legge federale del 20 giugno 2003[51] sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA)

Art. 9 cpv. 1 lett. c n. 7bis e 2 lett. c n. 3 (nuovo)

L'articolo 9 capoverso 1 elenca le autorità alle quali la SEM può permettere di accedere mediante procedura di richiamo ai dati del settore degli stranieri che ha trattato o fatto trattare nel sistema d'informazione retto dalla LSISA. La lettera c precisa gli scopi per i quali l'accesso può essere concesso alle autorità federali competenti in materia di sicurezza interna. Si tratta di aggiungere all'elenco un nuovo scopo, ossia l'adempimento dei compiti che incombono loro in virtù della presente legge.

L'articolo 9 capoverso 2 elenca le autorità alle quali la SEM può permettere di accedere mediante procedura di richiamo ai dati del settore dell'asilo che ha trattato o fatto trattare nel sistema d'informazione retto dalla LSISA. La lettera c elenca gli scopi per i quali l'accesso potrebbe essere dato alle autorità federali competenti in materia di sicurezza interna. Il disegno aggiunge all'elenco un nuovo scopo, ossia l'adempimento dei compiti che incombono loro in virtù della legge sull'Id-e.

2. Legge del 22 giugno 2001 sui documenti d'identità

Art. 1 cpv. 3 secondo periodo

In linea di massima, soltanto i cittadini svizzeri possono ottenere un passaporto diplomatico o di servizio svizzero. Per ragioni di sicurezza, può tuttavia essere necessario rilasciare un passaporto diplomatico o di servizio svizzero anche a cittadini stranieri per determinati Stati di residenza o in vista dell'esercizio di determinate missioni nell'interesse e su mandato della Svizzera. Si tratta di evitare che gli stranieri che accompagnano diplomatici svizzeri o altri impiegati di una rappresentanza all'estero siano esposti a gravi inconvenienti. In determinati casi, per essere ammessi nello Stato accreditatario e, se del caso, ottenere un visto è indispensabile possedere un passaporto diplomatico o di servizio svizzero. Gli sviluppi sociali in materia di unioni personali e in particolare il fatto che un numero sempre maggiore di diplomatici abbia un coniuge o un partner straniero ha acuito ulteriormente la problematica. In certi casi occorre inoltre facilitare ai collaboratori stranieri l'esercizio di determinate funzioni. Per certe missioni nelle zone di crisi o di guerra che implicano rischi maggiori per la vita e l'integrità fisica, il DFAE può essere costretto a ricorrere a specialisti che non possiedono la cittadinanza svizzera; in ogni caso la persona reclutata non acquisisce la cittadinanza svizzera. Sulla pagina del passaporto contenente i dati personali, il Paese

51 RS **142.51**

di origine del titolare è dunque ugualmente menzionato alla rubrica «cittadinanza» e il luogo di origine è sostituito con «***».

Art. 11 cpv. 2 secondo periodo

L'articolo 11 capoverso 2 elenca gli scopi per i quali fedpol può trattare i dati nel quadro della gestione dell'ISA. Si tratta di aggiungere un nuovo scopo di trattamento, ossia l'adempimento dei compiti indicati nel presente disegno di legge.

3. Codice civile

Art. 43a cpv. 4 n. 9

L'articolo 43*a* CC disciplina l'accesso mediante procedura di richiamo ai registri informatizzati dello stato civile. fedpol è aggiunto all'elenco dei servizi che hanno accesso a Infostar.

4. Legge federale dell'11 aprile 1889 sulla esecuzione e sul fallimento

Art. 33a cpv. 2bis

Conformemente all'articolo 33*a* capoverso 1 LEF, gli atti possono essere trasmessi per via elettronica agli uffici di esecuzione e agli uffici dei fallimenti nonché alle autorità di vigilanza. Devono essere muniti di una firma elettronica qualificata (art. 33*a* cpv. 2 LEF) che permette di attribuire chiaramente l'atto a una persona fisica. Dato che questa attribuzione univoca può anche essere garantita presentando un Id-e, si rinuncia all'apposizione di una firma elettronica qualificata nelle piattaforme della Confederazione in quanto ciò permette di semplificare il processo di registrazione per tutte le persone coinvolte.

Il Consiglio federale designerà le piattaforme che possono essere utilizzate. Si pensa innanzitutto alle piattaforme per la comunicazione elettronica nella giustizia previste dalla pertinente legge[52] e alla piattaforma EasyGov[53] gestita dalla Segreteria di Stato dell'economia.

5. Legge federale del 19 giugno 2015 sulla cartella informatizzata del paziente

Art. 7

Il disegno di legge sostituisce l'espressione «identità elettronica» di cui all'articolo 7 LCIP con «strumento d'identificazione elettronico», che corrisponde meglio alla nozione disciplinata in questo articolo. Si tratta inoltre di evitare qualsiasi confusione con il presente disegno di legge, che stabilisce il quadro giuridico del mezzo d'iden-

52 FF **2023** 679

53 Questa corrisponde alla piattaforma elettronica di cui alla sezione 4 del disegno di legge sullo sgravio delle imprese (LSgrI), FF **2023** 167; cfr. il messaggio del 9 dicembre 2022 concernente la legge federale sullo sgravio delle imprese dai costi della regolamentazione (Legge sullo sgravio delle imprese, LSgrI), FF **2023** 166, pagg. 34–35.

tificazione elettronico statale. Quest'ultimo costituisce un mezzo in forma elettronica che certifica l'identità di una persona e non uno strumento d'identificazione che permette di autenticarsi e accedere a un servizio o un'applicazione. Per ragioni di chiarezza è opportuno mantenere una distinzione terminologica tra le due leggi e modificare la LCIP.

Art. 11 lett. c

Secondo l'attuale sistema della LCIP, gli strumenti d'identificazione elettronici per l'accesso alla cartella informatizzata del paziente sono emessi da privati che devono essere certificati da un organismo riconosciuto. A lungo termine, pure questi strumenti d'identificazione saranno emessi dalla Confederazione. Pertanto, la volontà politica espressa dal Popolo in occasione della votazione popolare del 7 marzo 2021, secondo cui questo compito non doveva essere conferito al settore privato, sarà rispettata pure nel settore della LCIP.

Con le modifiche previste nella LMeCA (cfr. n. 7), la Confederazione pone le basi richieste. Dovrà soddisfare i requisiti previsti dalla legislazione sulla cartella informatizzata del paziente; comunque una certificazione dell'organismo federale competente non è richiesta a tal fine. Dato che durante un determinato periodo transitorio strumenti d'identificazione privati continueranno a essere utilizzati per accedere alla cartella informatizzata del paziente, l'articolo 11 lettera c stabilisce ora che gli emittenti privati di strumenti d'identificazione devono continuare a essere certificati.

6. Legge del 18 marzo 2016[54] sulla firma elettronica

Art. 9 cpv. 4 e 4bis

Il secondo periodo del capoverso 4 è abrogato. Chiunque richiede il rilascio di una firma elettronica deve presentarsi personalmente. In base al capoverso 4bis, non è soggetto a questo obbligo se può provare la sua identità mediante un mezzo d'identificazione elettronico ai sensi della presente legge. Il Consiglio federale può prevedere per via d'ordinanza che le persone che provano, con la necessaria affidabilità, la loro identità in altro modo non devono presentarsi personalmente.

7. Legge federale del 17 marzo 2023 concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità

Il presente disegno di legge stabilisce il quadro legale applicabile al mezzo d'identificazione elettronico statale, che consente al titolare di identificarsi, ma non di autenticarsi, per accedere a un servizio in linea o a un'applicazione. Per questa ragione la presente legge modifica la futura LMeCA e introduce un sistema di autenticazione in quanto «mezzo TIC» ai sensi dell'articolo 11 capoversi 1–3 LMeCA. Il sistema si basa sull'Id-e e consente di accedere a un servizio o a un'applicazione. Quando sarà utilizzato come mezzo di autenticazione, l'Id-e conseguirà un livello di sicurezza pa-

54 RS **943.03**

ragonabile a quello «significativo» secondo il regolamento eIDAS e a un livello di affidabilità 3 secondo la norma eCH-0170[55].

Il sistema di autenticazione delle persone fisiche (servizio di autenticazione delle autorità svizzere AGOV[56]) è pure a disposizione dei Cantoni e dei Comuni come mezzo TIC. Inoltre, può essere utilizzato da organizzazioni e persone del diritto pubblico o privato nella misura in cui sono incaricate di eseguire il diritto federale.

L'esempio della cartella informatizzata del paziente illustra il modo in cui in futuro l'Id-e potrà essere utilizzato in interazione con AGOV: dopo avere ricevuto un Id-e, il titolare potrà utilizzare AGOV per accedere alla propria cartella informatizzata. Concretamente, ciò significa che gli utenti della cartella informatizzata del paziente potranno presentare l'Id-e come mezzo d'identificazione elettronico e accedere alla cartella informatizzata tramite una procedura di login direttamente via AGOV.

Affinché ciò sia realizzabile, i fornitori della cartella informatizzata del paziente, denominati comunità di riferimento, devono potersi connettere ad AGOV quale applicazione di destinazione (p. es. mediante protocolli SAML [Security Assertion Markup Language] od OIDC [OpenID Connect]). La partecipazione ai costi di utilizzo di AGOV è disciplinata all'articolo 11 LMeCA e prevede un'assunzione dei costi proporzionale all'utilizzo.

6 Ripercussioni

6.1 Ripercussioni per la Confederazione

Affinché l'Id-e possa essere attuata il più rapidamente possibile, è necessario che i preparativi tecnici siano effettuati parallelamente all'iter legislativo. L'obiettivo atteso e comunicato finora alle cerchie politiche, alle imprese e alla popolazione è che la Confederazione sia in grado di proporre agli abitanti della Svizzera e agli Svizzeri all'estero un mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (p. es. l'estratto del casellario giudiziale) di elevata qualità dall'entrata in vigore della legge. L'Amministrazione federale non può attendere questo momento per iniziare a elaborare una soluzione tecnica. Il Consiglio federale ha chiesto al Parlamento un credito di 6,6 milioni di franchi nel quadro della prima aggiunta al preventivo 2023 per finanziare quest'anno i progetti pilota e lo sviluppo dell'infrastruttura di fiducia dell'Id-e nonché un credito d'impegno di 40,4 milioni di franchi destinati all'attuazione pilota e allo sviluppo di questa infrastruttura. I fondi per il 2023 e il credito d'impegno sono stati approvati dal Parlamento il 1° giugno 2023.

Il progetto Id-e è gestito come un programma con coordinamento di progetto secondo Hermes. Il mandante è l'UFG. Un comitato di programma Id-e, presieduto dal direttore dell'UFG, coordina e accompagna la pianificazione dei lavori informatici. L'attuazione in singoli progetti è realizzata secondo il metodo agile. Il progetto Id-e è stato

55 www.ech.ch > eCH-0170 Modèle de qualité pour l'authentification des sujets V2.0 (disponibile in francese e tedesco)
56 www.agov.ch

classificato come «progetto chiave TDT» dal Cancelliere della Confederazione il 17 aprile 2023[57].

Nel quadro del progetto Id-e occorre implementare, gestire e sviluppare un sistema d'informazione per l'emissione degli Id-e e un'infrastruttura di fiducia. In totale, i mezzi finanziari necessari per lo sviluppo e la gestione dell'infrastruttura di fiducia, l'emissione degli Id-e e i progetti pilota ammonteranno a circa 181,9 milioni di franchi per il periodo 2023–2028. Di questa somma, 58 milioni di franchi sono già coperti dai fondi disponibili. Il Parlamento ha approvato un credito d'impegno di 40,4 milioni nel quadro della prima aggiunta al preventivo 2023 per gli impegni pluriennali connessi alla fase pilota e all'implementazione dell'Id-e.

Il fabbisogno supplementare per finalizzare l'implementazione a partire da metà 2025 e per la gestione a partire da inizio 2026 ammonta a circa 123,9 milioni di franchi. Dal 2029 si prevedono costi pari a circa 24,7 milioni per anno.

Un credito aggiuntivo di 15,3 milioni di franchi è richiesto per completare il progetto (programma Id-e) durante gli anni 2025 e 2026. Tale credito è necessario, da un lato, perché i fondi richiesti nel quadro della prima aggiunta nella primavera 2023 erano volti a coprire solamente il periodo fino alla messa in esercizio dell'Id-e e non il periodo tra metà 2025 e fine 2026 (7,7 mio.). Dall'altro lato, le risorse destinate ad AGOV non sono state considerate interamente nel credito d'impegno richiesto nel quadro della prima aggiunta (7,6 mio.).

Programma Id-e in franchi	P 2025	PF 2026	**Totale**
Infrastruttura d'emissione Id-e fedpol	6 701 500	965 700	**7 667 200**
AGOV/fase pilota ePerso	5 600 000	2 000 000	**7 600 000**

I fondi per beni e servizi connessi all'informatica serviranno a fedpol per il bando di concorso pubblico per l'acquisizione della tecnologia e dell'infrastruttura necessarie alla verifica in linea dell'identità e per lo sviluppo del sistema d'informazione del servizio nazionale d'identità (SID).

Inoltre, a partire da metà 2025 e fino al 2028 occorreranno altri due crediti d'impegno per un totale di 85,1 milioni di franchi (64,9 mio. per l'UFG e 20,2 mio. per fedpol). Saranno necessari solo fintantoché i fornitori di prestazioni interni della Confederazione non saranno in grado di garantire autonomamente la gestione del sistema.

57 www.bk.admin.ch > Documentazione > Comunicati stampa > Definiti nuovi progetti chiave TDT

Nuovo credito d'impegno UFG	P 2025	PF 2026	PF 2027	PF 2028	Totale
Prestazioni di consulenza/di terzi (incl. comunicazione)	100 000	800 000	800 000	800 000	**2 500 000**
Audit/SGSI/certificazione di sicurezza	0	400 000	400 000	400 000	**1 200 000**
Gestione UFIT Infrastruttura cloud incl. costi di licenza	3 100 000	3 100 000	3 100 000	3 100 000	**12 400 000**
Collaboratori esterni per la gestione	7 286 400	6 652 800	5 385 600	5 385 600	**24 710 400**
Spese di assistenza esterna	2 595 000	2 880 000	810 000	810 000	**7 095 000**
Prestazioni esterne uniche	3 000 000	5 000 000	5 000 000	4 000 000	**17 000 000**
Totale	**16 081 400**	**18 832 800**	**15 495 600**	**14 495 600**	**64 905 400**

Un importo di 0,1 milioni di franchi a partire da metà 2025 e uno di 0,8 milioni per anno a partire dal 2026 sono previsti per le prestazioni di consulenza e altre prestazioni di terzi nonché per le spese del servizio specializzato Id-e, incluse diverse misure di comunicazione. Le spese esterne per l'audit, il sistema di gestione della sicurezza delle informazioni (SGSI) e la certificazione di sicurezza ammonteranno a 0,4 milioni di franchi per anno a partire dal 2026. Le spese per beni e servizi e i costi interni di gestione ammonteranno a 3 milioni di franchi per anno a partire dal 2025 per il cloud necessario alla gestione dell'infrastruttura di fiducia dell'Id-e. Non è necessario alcun investimento a carico degli attivi fissi dell'UFIT. A ciò si aggiungono 0,1 milioni per anno di spese di licenza per il portale di gestione dei servizi informatici.

Le spese di assistenza esterna di 2,6 milioni di franchi per il 2025, di 2,9 milioni per il 2026 e di 0,8 milioni per anno a partire dal 2027 nonché le spese per i collaboratori esterni incaricati della gestione, di 7,3 milioni per il 2025, di 6,7 milioni per il 2026 e di 5,4 milioni per anno a partire dal 2027, costituiscono l'ultima parte dei costi di gestione ricorrenti.

Per quanto riguarda le spese di beni e servizi e i costi di gestione esterni unici, sono previsti nel 2025 altri 3 milioni di franchi per le prestazioni di servizi esterne (escl. l'assistenza). A causa del numero crescente di partecipanti all'ecosistema e dell'evoluzione tecnica all'estero, occorre prevedere investimenti significativi nel 2026 e nel 2027, ragion per cui si devono stanziare 5 milioni di franchi per questi due anni e altri 4 milioni a partire dal 2028.

Nuovo credito d'impegno fedpol	P 2025	PF 2026	PF 2027	PF 2028	Totale
Costi di licenza	500 000	1 000 000	1 000 000	1 000 000	**3 500 000**
Spese di gestione	380 000	760 000	760 000	760 000	**2 660 000**
Manutenzione, assistenza e sviluppo	651 300	1 302 600	1 302 600	1 302 600	**4 559 100**
Spese di assistenza esterne	1 584 000	3 168 000	3 168 000	1 584 000	**9 504 000**
Totale	**3 115 300**	**6 230 600**	**6 230 600**	**4 646 600**	**20 223 100**

I costi di gestione connessi all'informatica per gli anni 2025–2028 sono suddivisi in costi di licenza per il sistema di verifica in linea dell'identità di un richiedente, stimati al 20 per cento del prezzo d'acquisto, ossia un milione di franchi per anno (la metà nel 2025). I costi di gestione del sistema d'informazione del SID ammonteranno a 0,76 milioni di franchi per anno (la metà nel 2025). Le spese di manutenzione, assistenza e sviluppo del sistema d'informazione, stimate al 15 per cento dei costi di sviluppo, corrispondono a 1,3 milioni di franchi all'anno (la metà nel 2025). Infine, i costi unici per il personale esterno incaricato dell'assistenza ammonteranno a circa 1,6 milioni per il 2025, a 3,2 milioni per il 2026 e il 2027 e a 1,6 milioni per il 2028. Questi posti esterni non saranno più necessari a partire dal 2029.

Dal 2025 i servizi che intenderanno collegarsi all'infrastruttura di fiducia dell'Id-e (p. es. finanziamento della licenza digitale per allievo conducente da parte dei Cantoni, che fa attualmente parte dei progetti pilota) dovranno disporre delle risorse necessarie per il collegamento e la gestione. La gestione di altri mezzi di autenticazione elettronici deve pure essere garantita dai rispettivi gestori.

Nel rapporto esplicativo[58] posto in consultazione con l'avamprogetto, una stima iniziale dei crediti necessari (basata sull'esperienza acquisita nel quadro dell'emissione del certificato COVID-19) indicava costi progettuali di 25–30 milioni di franchi e costi operativi di 10–15 milioni di franchi all'anno. Nel rapporto si indicava che una stima più precisa delle risorse necessarie sarebbe stata effettuata in occasione della stesura del messaggio. Inoltre, soltanto le esperienze maturate con i progetti pilota hanno permesso di determinare la forma e la portata dell'assistenza tecnica.

Le elevate spese di assistenza tecnica nel quadro dell'infrastruttura di fiducia e dell'emissione dell'Id-e spiegano il forte incremento dei costi globali. Queste spese non erano ancora state considerate nel rapporto esplicativo. I costi operativi devono essere rivalutati ed eventualmente adeguati in fase di allestimento del preventivo per i prossimi anni.

6.2 Ripercussioni per i Cantoni e i Comuni, per le città, gli agglomerati e le regioni di montagna

In occasione della consultazione, diversi partecipanti hanno chiesto che la procedura di verifica necessaria per l'emissione dell'Id-e non sia effettuata soltanto tramite un canale in linea ma anche tramite una procedura sul posto presso strutture esistenti come gli uffici dei passaporti o i servizi della migrazione. In tal caso, le persone interessate potrebbero recarsi presso l'autorità per richiedere l'Id-e insieme ai documenti fisici oppure prendere appuntamento sul posto unicamente per il rilascio dell'Id-e.

Fondandosi sulle esperienze internazionali e su stime di massima, l'analisi si basa sulla seguente struttura quantitativa: 50 per cento delle persone che si presentano all'autorità per rinnovare i documenti d'identità decidono di richiedere anche l'Id-e; ciò rappresenta circa 400 000 casi all'anno per gli uffici dei passaporti e circa 130 000

58 www.fedlex.admin.ch > Procedure di consultazione > Procedure di consultazione concluse >2022 > DFGP > Legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici (Legge sull'Id-e, LIdE).

casi per i servizi di migrazione. Si stima che la quota di persone che si recheranno presso l'autorità espressamente per l'Id-e ammonti all'uno per cento di tutti i potenziali utenti dell'Id-e. Se sarà disponibile da subito con l'introduzione dell'Id-e, questa possibilità produrrà circa 28 000 appuntamenti sul posto nel primo anno, dato che la percentuale sarà leggermente più elevata all'inizio, e in seguito circa 1000 casi all'anno a partire dal quarto anno.

Dalle stime attuali del tempo necessario per ogni caso risultano costi supplementari di 15 franchi per la verifica in vista dell'emissione di un Id-e in combinazione con la domanda di un documento d'identità. Si calcolano in media 7 minuti supplementari per caso sul posto presso l'autorità. I costi della verifica sul posto per ottenere soltanto l'Id-e ammontano a 29 franchi. In questo caso si contano in media 14 minuti per caso. Basandosi sul numero di casi stimato, risultano spese di circa 8 milioni di franchi per anno. A titolo di confronto, i costi del canale in linea sono stimati a qualche franco per caso. Si tratta di stime provvisorie soggette a cambiare in seguito alla consultazione dettagliata con i Cantoni. I costi secondari (adeguamento delle infrastrutture degli edifici e delle postazioni, gestione del personale) non sono considerati in questi calcoli. Neppure le questioni relative all'acquisto e al finanziamento degli adeguamenti infrastrutturali eventualmente necessari sono state analizzate in dettaglio.

Per le loro prestazioni i Cantoni saranno liberi di riscuotere degli emolumenti il cui importo sarà fissato dal Consiglio federale in modo uniforme per tutta la Svizzera. Non è previsto un indennizzo diretto da parte della Confederazione.

Dopo diverse riunioni di lavoro con rappresentanti degli uffici dei passaporti e dei servizi della migrazione, seguite da una consultazione dei membri dell'Associazione dei servizi cantonali dei passaporti (ASCP) e dell'Associazione dei servizi cantonali di migrazione (ASM), le principali preoccupazioni si concentrano sulla gestione delle capacità, delle risorse e delle infrastrutture necessarie. I costi secondari generati dalla gestione delle capacità (infrastruttura delle postazioni, edifici, gestione del personale) non sono stati considerati nei calcoli di cui sopra. Gli adeguamenti dell'infrastruttura non implicano questioni soltanto finanziarie ma anche relative all'attuazione temporale (ritmo e cicli di acquisizione dei crediti e delle infrastrutture). Inoltre, gli «anni di punta» storicamente determinati (2025 e 2026, gli anni di forte richiesta di rinnovo del passaporto), le modifiche dovute alla prevista introduzione delle carte d'identità con microchip, una domanda accresciuta dovuta a una maggiore disponibilità di caratteri speciali nonché l'introduzione di una licenza di condurre digitale, che causerebbe una forte richiesta di Id-e, potrebbero coincidere con la fase di lancio dell'Id-e.

Oltre a coordinare le suddette attività, potrebbero essere seguiti diversi approcci per meglio ripartire le domande nel tempo e a seconda dei periodi: l'emissione dell'Id-e sul posto non dovrebbe essere necessariamente possibile da subito; ogni autorità potrebbe limitare mediante una quota il numero di appuntamenti disponibili per le persone che desiderano esclusivamente l'Id-e; un buon coordinamento tra il canale in linea e i verificatori sul posto potrebbe scongiurare l'eventuale sovraccarico risultante dall'introduzione di una quota nella procedura di emissione in linea.

La procedura di emissione in linea costituirà il principale canale per ottenere un Id-e. Grazie a meccanismi di orientamento verso questa modalità di richiesta, la maggior parte degli interessati dovrebbe ottenere l'Id-e tramite questo canale. Se le persone

interessate dovessero pagare un emolumento per la verifica sul posto, ciò costituirebbe un elemento forte per stimolare l'utilizzo del canale in linea, gratuito. L'esperienza dimostra che si ricorre volentieri alle prestazioni delle autorità che sono gratuite.

Le spese connesse all'emissione sul posto potranno essere assunte dai Cantoni o dai richiedenti stessi. I Cantoni, in effetti, beneficiano direttamente dell'attuazione e dell'utilizzo diffuso dell'Id-e. Potranno tuttavia riscuotere degli emolumenti per questa prestazione. Il Consiglio federale li autorizzerà alla riscossione per via d'ordinanza.

6.3 Ripercussioni sull'economia

La transizione digitale procede a grandi passi. Un numero crescente di transazioni può oramai essere effettuato in linea; presentarsi di persona è sempre meno necessario. Ci si attende sempre più che sia possibile svolgere per via elettronica diverse operazioni, di preferenza su uno smartphone. Sebbene i mezzi di comunicazione per farlo non manchino, non è ancora possibile creare, gestire e presentare dei mezzi di autenticazione elettronici che siano sufficientemente funzionali e accettati dalla maggior parte dei fornitori di prestazioni. L'infrastruttura di fiducia della Confederazione mira a colmare questa lacuna implementando un ecosistema che consente di emettere, utilizzare e presentare in maniera sicura diversi mezzi di autenticazione elettronici. Si tratta di un insieme di norme, procedure, principi ed elementi infrastrutturali che instaurano la fiducia nelle procedure digitali, ne garantiscono la conformità, e che sono accettati e utilizzati da parte di un vasto pubblico. Le transazioni elettroniche nei settori pubblico e privato potranno essere effettuate in modo più efficace e sicuro nel rispetto delle esigenze della LPD. Una simile infrastruttura permette di aumentare l'interconnessione tra i diversi attori e il livello di fiducia nelle transazioni elettroniche.

Per quanto concerne l'Id-e, uno dei suoi principali vantaggi è la possibilità di presentare i propri dati a un interlocutore in Internet. Il titolare non ottiene soltanto un maggiore controllo sui suoi dati, ma anche più responsabilità, in particolare per quanto concerne gli obblighi di diligenza, nel quadro delle transazioni elettroniche. La portata di questa responsabilità e le sue conseguenze saranno definite con maggiore precisione per via d'ordinanza. Inoltre, il possesso di un Id-e richiede un determinato livello di conoscenze sul funzionamento del suo sistema. Il dibattito pubblico concernente il progetto di legge ha permesso di sviluppare una certa sensibilità in materia digitale in seno alla popolazione svizzera.

6.4 Ripercussioni sulla società

L'identificazione sicura dell'interlocutore in una transazione elettronica permette di ridurre o di impedire i casi di abuso, aumentando la fiducia in Internet. L'abuso in Internet si basa sovente sull'impossibilità di identificare il proprio interlocutore in modo sicuro. Attualmente non è possibile distinguere i mittenti di spam dai mittenti affidabili e neppure chiedere conto ai primi del loro operato. Nel caso del phishing, i mittenti di messaggi di posta elettronica si spacciano per qualcun altro, per esempio

la banca del destinatario, e possono in tal modo causare danni ingenti. I mezzi d'identificazione elettronici riconosciuti contribuiscono a proteggere l'identità dei loro titolari in una società globalizzata e ampiamente interconnessa rendendo molto più difficile usurpare l'identità di una persona e utilizzarla in maniera potenzialmente problematica.

Una serie di disposizioni tecniche consentirà al titolare di non trasmettere all'interlocutore, al momento di presentare l'Id-e o un altro mezzo d'identificazione elettronico, tutti i dati ivi contenuti e, ad esempio, di rinunciare alla loro trasmissione. Il titolare dell'Id-e dovrà essere libero di comunicare tutte o una parte delle informazioni ivi contenute. In tal modo la sfera privata sarà meglio protetta, dato che non sarà più assolutamente necessario comunicare determinate informazioni.

Inoltre, il disegno di legge prevede restrizioni per quanto concerne l'utilizzo dell'Id-e da parte dei verificatori, che potranno richiedere al titolare di un Id-e determinati dati personali unicamente a determinate condizioni. In tal modo il disegno mira a limitare il ricorso ingiustificato all'identificazione elettronica da parte del verificatore.

6.5 Ripercussioni sull'ambiente

Il presente disegno di legge non ha ripercussioni dirette sull'ambiente. Il passaggio dalle transazioni fisiche alle transazioni elettroniche consentirà di risparmiare risorse e avrà dunque ripercussioni positive sull'ambiente. Ad esempio, potrà essere evitato il sovraccarico delle infrastrutture di trasporto risultante dalla necessità di presentarsi personalmente.

Il consumo energetico dell'infrastruttura di fiducia sarà paragonabile a quello delle altre infrastrutture informatiche già implementate dalla Confederazione. Inoltre, nel caso in cui la soluzione tecnica di attuazione si basasse su una tecnologia blockchain, l'utilizzo del meccanismo di validazione dei blocchi denominato «prova di lavoro» («proof of work»), noto per il suo elevato consumo energetico, può essere escluso per la messa a disposizione dell'infrastruttura di fiducia.

7 Aspetti giuridici

7.1 Costituzionalità

La competenza di disciplinare l'Id-e e l'infrastruttura di fiducia è basata sugli articoli 38 capoverso 1, 81 e 121 capoverso 1 Cost. Per maggiori informazioni si veda il capitolo 5 (Ingresso).

7.2 Compatibilità con gli impegni internazionali della Svizzera

Il disegno di legge è compatibile con gli impegni internazionali vigenti. Nel corso della sua elaborazione, il Consiglio federale si è adoperato affinché l'interoperabilità

internazionale sia possibile. Se auspicato in un secondo momento, l'Id-e svizzero potrà ottenere il riconoscimento internazionale. A tale scopo sarà necessario concludere trattati internazionali.

7.3 Forma dell'atto

In considerazione dell'oggetto, del contenuto e della portata del progetto, è necessario, in virtù dell'articolo 164 capoverso 1 Cost., emanare le disposizioni relative ai mezzi di autenticazione elettronici sotto forma di legge federale.

Conformemente agli articoli 163 capoverso 2 Cost. e 25 capoverso 2 della legge del 13 dicembre 2002[59] sul Parlamento (LParl), per l'atto concernente i crediti d'impegno da adottare è prevista la forma del decreto federale semplice non sottoposto a referendum.

7.4 Subordinazione al freno alle spese

La legge non contiene disposizioni relative a sussidi, ragione per cui non è subordinata al freno delle spese.

Conformemente all'articolo 159 capoverso 3 lettera b Cost., l'articolo 1 capoverso 2 lettere a e b del decreto federale che stanzia crediti d'impegno per l'implementazione e la gestione dell'Id-e richiede l'approvazione della maggioranza dei membri di ciascuna Camera, in quanto implica nuove spese uniche di oltre 20 milioni di franchi.

Il credito aggiuntivo proposto all'articolo 1 capoverso 1 del decreto federale, che non supera la soglia dei 20 milioni di franchi, non è subordinato al freno alle spese in quanto lo è il credito d'impegno iniziale.

7.5 Rispetto del principio di sussidiarietà e del principio dell'equivalenza fiscale

La prevista ripartizione dei compiti e il loro adempimento non violano né il principio di sussidiarietà né quello dell'equivalenza fiscale. Le ripercussioni finanziarie del progetto per la Confederazione superano i 10 milioni di franchi, mentre quelle per i Cantoni non possono ancora essere quantificate.

7.6 Conformità alla legge sui sussidi

Il disegno di legge non prevede né aiuti finanziari né indennità.

59 RS **171.10**

7.7 Delega di competenze legislative

Il disegno di legge si situa deliberatamente a un elevato livello di astrazione; è formulato in modo sostanzialmente neutro sul piano tecnologico al fine di rimanere aperto all'evoluzione futura. Il disciplinamento di determinate questioni, a volte anche piuttosto importanti, concernenti l'impostazione dell'infrastruttura e la portata delle prestazioni delle differenti componenti dell'infrastruttura e dell'Id-e è delegato al Consiglio federale.

7.8 Protezione dei dati

Le disposizioni del diritto in materia di protezione dei dati (LPD e pertinenti ordinanze) si applicano a tutte le parti coinvolte. I privati, gli emittenti e i verificatori del settore privato sono sottoposti alle disposizioni applicabili ai privati; la Confederazione (fedpol e altre autorità), gli emittenti e i verificatori del settore pubblico sono sottoposti alle disposizioni applicabili agli organi federali. Per evitare ripetizioni e agevolare la leggibilità, il presente disegno non contiene rimandi alle pertinenti disposizioni della LPD.

La protezione dei dati è uno degli obiettivi della legge ed è esplicitamente citata nel campo di applicazione. L'articolo 1 capoverso 2 lettera a riprende inoltre il tenore dell'articolo 7 capoverso 2 LPD precisando, ai numeri 1–4, come tale obiettivo sarà attuato nel contesto dell'Id-e. Si tratta in particolare di integrare le richieste espresse dalle sei identiche mozioni intitolate «Identità elettronica statale affidabile» (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 e 21.3129), depositate da tutti i gruppi parlamentari dopo l'esito negativo della votazione del 7 marzo 2021 sulla legge sui servizi d'identificazione elettronica. Gli autori delle mozioni chiedevano che l'identità elettronica statale osservasse i principi della «privacy by design», della minimizzazione dei dati e della registrazione decentralizzata dei dati (come la registrazione dei dati dei documenti d'identità presso gli utenti). L'articolo 1 capoverso 2 lettera a riformula queste esigenze come obiettivi specifici da raggiungere nell'ambito della protezione dei dati personali.

Inoltre, l'articolo 1 capoverso 2 lettera c del disegno mira a garantire che l'Id-e e l'infrastruttura di fiducia corrispondano allo stato attuale della tecnica. Con questa nozione, il legislatore intende conseguire un livello elevato di sicurezza e di protezione dei dati con procedure avanzate. L'articolo 1 capoverso 2 lettera d precisa d'altronde che la legge ha lo scopo di garantire che l'evoluzione tecnica connessa ai mezzi di autenticazione elettronici non sia limitata inutilmente. Il disegno di legge è formulato in modo sostanzialmente neutro sul piano tecnologico e disciplina la scelta della soluzione tecnica soltanto se è assolutamente necessario per conseguire gli obiettivi legislativi.

L'infrastruttura di fiducia prevista dal disegno di legge si basa sui principi elencati all'articolo 1 capoverso 2. Le componenti principali dell'infrastruttura sono definite alla sezione 2: si tratta del registro di base (art. 2), del registro di fiducia (art. 3), dell'applicazione per la conservazione e la presentazione dei mezzi di autenticazione elettronici (art. 7) e dell'applicazione per la verifica dei mezzi di autenticazione elet-

tronici (art. 8). Il registro di base e il registro di fiducia non contengono alcun dato dei mezzi di autenticazione elettronici. Il registro di base contiene solamente informazioni sulla loro revoca. I dati del titolare dell'Id-e e dei mezzi di autenticazione elettronici sono trasmessi unicamente tra l'emittente, il titolare e il verificatore, senza intermediari. L'idea alla base dell'infrastruttura di fiducia mira a creare un sistema in cui i flussi di dati sono diretti e trasparenti per tutti gli utenti, in cui gli emittenti non ricevono informazioni sull'utilizzo dei mezzi di autenticazione elettronici emessi, pur senza perdere il diritto di revocarli, e in cui i titolari beneficiano di misure di sicurezza corrispondenti allo stato attuale della tecnica. Il disegno di legge prevede che i dati personali generati durante la consultazione dei registri di base e di fiducia possano essere analizzati soltanto per le finalità di cui all'articolo 57*l* lettera b numeri 1–3 LOGA. Possono essere analizzati senza riferimento a persone per le finalità di cui all'articolo 57*l* lettera b numeri 1–3 LOGA.

L'articolo 14 elenca i dati che saranno contenuti nell'Id-e: si tratta di dati concernenti la persona (cpv. 1) e di dati concernenti l'Id-e (cpv. 2). I dati concernenti il titolare sono i seguenti: il cognome ufficiale, i nomi, la data di nascita, il sesso, il luogo di origine, il luogo di nascita, la cittadinanza, l'immagine del viso e il numero AVS. Questi dati sono disponibili nei registri ufficiali dello Stato ai quali fedpol ha accesso in virtù dell'articolo 25 capoverso 3. Oltre ai dati sulla persona, l'Id-e contiene i dati creati da fedpol al momento della sua emissione: si tratta del numero dell'Id-e, della data di emissione, della data di scadenza, di informazioni sul documento utilizzato per la procedura di emissione, in particolare il tipo e la data di scadenza, e di informazioni sulla procedura di emissione. L'Id-e può inoltre contenere ulteriori indicazioni che figurano sul documento d'identità del titolare (ad es. il nome del rappresentante legale, il cognome di affinità o il nome d'arte).

Il disegno di legge contiene disposizioni precise che consentono a fedpol di gestire un sistema d'informazione per l'identificazione dei richiedenti. L'articolo 25 capoverso 1 definisce la natura, il contenuto e lo scopo di questo sistema. L'articolo 25 capoverso 2 elenca le tipologie di dati che vi sono contenuti: i dati concernenti l'Id-e di cui all'articolo 14 capoverso 2, i dati relativi alla procedura di emissione necessari per fornire assistenza tecnica, allestire statistiche o condurre indagini nonché le indicazioni relative alla revoca di un Id-e.

I dati concernenti la persona sono consultati direttamente nei registri federali e non sono conservati nel sistema d'informazione di fedpol (cfr. art. 25 cpv. 4). L'articolo 25 capoverso 3 elenca i registri federali ai quali fedpol avrà accesso per confrontare i dati personali. Il sistema previsto mira a permettere a fedpol di adempiere i suoi compiti nel quadro dell'emissione e della revoca dei mezzi di autenticazione elettronici.

L'articolo 16 capoverso 3 costituisce una base legale in senso formale che consente a fedpol di rilevare dati biometrici per confrontare il viso della persona con l'immagine del viso di cui all'articolo 14 capoverso 1 lettera h. Questa procedura è necessaria per garantire che l'immagine del viso registrata dal richiedente al momento della procedura di emissione corrisponda effettivamente a quella contenuta nei registri federali ISA, SIMIC o Ordipro.

L’articolo 22 introduce restrizioni importanti per quanto concerne il trattamento dei dati personali contenuti nell’Id-e da parte del verificatore. Quest’ultimo può chiedere al titolare di trasmettergli dei dati personali contenuti nell’Id-e al fine di verificare la sua identità o un aspetto della stessa per ragioni di affidabilità della transazione o perché prescritto dalla legge. L’UFIT segnala le violazioni a dette restrizioni nel registro di fiducia e può escluderne i verificatori colpevoli. L’articolo 26 prevede termini di conservazione differenti per tre tipi di dati contenuti nel sistema d’informazione di fedpol. I dati concernenti gli Id-e richiesti ed emessi e le indicazioni relative alla revoca degli Id-e sono conservati per 20 anni a partire dalla data della richiesta o dell’emissione dell’Id-e (cpv. 1 lett. a). I dati relativi alla procedura di emissione, compresi i dati biometrici, necessari per condurre un’indagine in merito a un conseguimento fraudolento di un Id-e sono conservati per cinque anni dopo la scadenza dell’Id-e (cpv. 1 lett. b). Tutti gli altri dati sono distrutti 90 giorni dopo la loro registrazione nel sistema (cpv. 2).

L’articolo 32 lettera e, infine, delega al Consiglio federale la competenza di emanare le disposizioni di esecuzione concernenti i provvedimenti tecnici e organizzativi da adottare per garantire la protezione e la sicurezza dei dati nell’ambito della gestione e dell’utilizzo dell’infrastruttura di fiducia.