Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizio e polizia DFGP
Ufficio federale di giustizia UFG

Berna, giugno 2022

Legge federale sul mezzo d'identificazione elettronico e altri mezzi di autenticazione elettronici

(Legge sull'Id-e, LIdE)

Rapporto esplicativo per l'avvio della procedura di consultazione

Indice

Compendio

La digitalizzazione della società avanza rapidamente e la possibilità di identificarsi nel mondo virtuale è un caposaldo di questa grande trasformazione. Il presente avamprogetto di legge intende introdurre un mezzo d'identificazione elettronico, basato su un'infrastruttura gestita dalla Confederazione e rilasciato dallo Stato rilascia ai titolari di documenti d'identità emessi dalle autorità svizzere. Tale infrastruttura permetterà di creare e gestire vari mezzi di autenticazione elettronici potenziandone così la diffusione e l'impiego in linea con gli sviluppi europei e internazionali e nel rispetto dei requisiti in materia di protezione dei dati personali.

Contesto

Il 7 marzo 2021, la legge federale sui servizi d'identificazione elettronica (Legge sull'eID, LSIE)[1] è stata respinta da quasi il 65 per cento dei votanti. Il 10 marzo 2021 i rappresentati di tutti i gruppi parlamentari hanno depositato nella sessione primaverile delle Camere federali sei identiche mozioni che chiedevano un'identità elettronica statale affidabile (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 e 21.3129).

Il 26 maggio 2021, il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia (DFGP) di elaborare rapidamente, in collaborazione con il Dipartimento federale delle finanze (DFF) e con la Cancelleria federale (CaF), una soluzione per un Id-e* statale. In una prima fase il DFGP ha preparato un documento di lavoro insieme a specialisti dei Cantoni e a esperti scientifici. Oltre a illustrare tre soluzioni tecniche di realizzazione, questa prima analisi presentava anche le modalità d'integrazione di ciascuna di esse nel contesto economico e sociale nonché diverse possibilità d'impiego dell'Id-e.

Il documento di lavoro è stato sottoposto a una consultazione pubblica, tenutasi dal 2 settembre al 14 ottobre 2021, cui hanno partecipato cittadini privati, amministrazioni cantonali nonché rappresentanti degli ambienti scientifici, delle organizzazioni economiche e del mondo imprenditoriale, per un totale di 60 pareri. Il 14 ottobre 2021, a conclusione della consultazione, il DFGP ha organizzato un dibattito pubblico in forma di conferenza cui erano presenti 50 rappresentanti dei Cantoni, dei partiti, degli ambienti scientifici, della società civile e dell'economia, nonché alcuni cittadini interessati.

I partecipanti alla consultazione si sono espressi a favore della soluzione basata sulla *self-sovereign identity (SSI)* e hanno approvato lo sviluppo di un'infrastruttura completa di fiducia in grado di emettere e utilizzare diversi mezzi di autenticazione elettronici. Questa soluzione tiene conto delle richieste espresse dalle mozioni adottate dal Consiglio federale il 14 settembre 2021: i lavori successivi si fondano su questa volontà come anche sui principi della protezione dei dati fin dalla progettazione (*privacy by design*), della minimizzazione dei dati e del loro salvataggio decentralizzato. Inoltre il DFGP ha avviato una collaborazione più stretta con gli uffici e i Cantoni che promuovono progetti pilota in questo ambito.

Fondandosi sui risultati di questa consultazione, il 17 dicembre 2021 il Consiglio federale ha preso una decisione di principio nella quale ha fissato gli elementi fondamentali dell'Id-e, ossia di un futuro mezzo d'identificazione elettronico emesso dallo Stato.

Il titolare di un Id-e deve avere il massimo controllo possibile sui suoi dati (principio della SSI). La protezione dei dati va garantita in particolare dal sistema stesso (principio della privacy by design), ma anche mediante la riduzione del flusso dei dati al minimo necessario (minimizzazione dei dati) e il salvataggio decentralizzato dei dati.

L'Id-e deve basarsi su un'infrastruttura gestita dallo Confederazione che potrà essere messa a disposizione dei servizi pubblici e delle imprese per emettere diversi altri mezzi d'autenticazioni elettronici, per esempio gli estratti del casellario giudiziale, le licenze di condurre, i diplomi universitari o i certificati medici. L'ecosistema di questi mezzi elettronici potrà essere progressivamente ampliato.

Contenuto del progetto

L'avamprogetto di legge prevede l'introduzione di un mezzo d'identificazione elettronico (Id-e) statale per i titolari di un documento d'identità rilasciato dalle autorità svizzere. In questo contesto, lo Stato verifica l'identità del richiedente e gli rilascia un mezzo per identificarsi elettronicamente. Il nuovo progetto persegue un approccio fondato sui principi della protezione dei dati fin dalla progettazione (privacy by design), della minimizzazione dei dati e del loro salvataggio decentralizzato. La richiesta e l'impiego dell'Id-e sono su base volontaria.

L'avamprogetto mira inoltre a creare una completa infrastruttura statale di fiducia che permetterà agli attori dei settori pubblico e privato di rilasciare agli interessati mezzi di autenticazione elettronici utilizzabili in vari settori. A tale riguardo, la Confederazione intende mettere a disposizione un portafoglio elettronico statale che potrà contenere l'Id-e e gli altri mezzi di autenticazione elettronici. I titolari del portafoglio potranno richiedere, ottenere e presentare il loro Id-e o un altro dei loro mezzi di autenticazione elettronici in modo sicuro e trasparente. Un sistema così aperto permetterà di potenziare la diffusione e l'impiego di questi mezzi. L'avamprogetto tiene conto della normativa internazionale e in particolare del 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. Inoltre assegna al Consiglio federale la competenza di concludere accordi internazionali che prevedano il riconoscimento all'estero dell'Id-e svizzero e il riconoscimento in Svizzera degli Id-e stranieri.

1 FF **2019** 6227
*

Rapporto esplicativo

1 Contesto

Alle votazioni del 7 marzo 2021, il 65 per cento circa dei votanti ha respinto la legge federale sui servizi d'identificazione elettronica. Il 10 marzo 2021 sono state depositate da tutti i gruppi parlamentari sei mozioni di identico contenuto che chiedevano un'identità elettronica statale affidabile (21.3124, 21.3125, 21.3126, 21.3127, 21.3128 e 21.3129). Infine l'interpellanza Andrey 21.3310 «La carta d'identità come componente di una futura soluzione Ie» e l'interpellanza Graf-Litscher 21.3718 «Identità elettroniche auto-sovrane» sono state depositate nei tre mesi successivi alla votazione. Le sei mozioni sono state adottate il 14 settembre 2021 dalla prima Camera mentre il dibattito relativo all'interpellanza Andrey 21.3310 è stato rimandato. Il Consiglio federale ha invece deciso di liquidare l'interpellanza Graf-Litscher 21.3718.

In occasione della seduta del 26 maggio 2021, il Consiglio federale ha deciso di proporre al Parlamento di accogliere le mozioni con l'obiettivo di presentare in tempi brevi una nuova soluzione per l'Id-e che tenesse conto delle richieste di questi interventi. Ha quindi incaricato il DFGP di elaborare, entro l'anno e in collaborazione con il DFF e con la CaF, un piano di massima. Il piano, alla cui stesura hanno partecipato i Politecnici federali di Zurigo e Losanna nonché i Cantoni, ha in particolare analizzato le varie possibilità tecniche di attuazione e i rispettivi costi.

Il DFGP ha compilato il «Documento di discussione degli obiettivi dell'Ie» (di seguito «documento di discussione») insieme ai Cantoni e a un gruppo di esperti. Questa analisi proponeva varie definizioni dell'Id-e e della relativa infrastruttura di fiducia, inoltre illustrava tre soluzioni tecniche di realizzazione: l'identità autogestita (self-sovereign identity, SSI), l'infrastruttura a chiave pubblica (PKI) e il fornitore d'identità centrale (IdP) dello Stato illustrandone in dettaglio le rispettive modalità d'integrazione negli scambi economici e sociali e riportando una serie di esempi di impiego di un Id-e statale.

Sulla base del documento di discussione è stata avviata una consultazione pubblica che si è tenuta dal 2 settembre al 14 ottobre 2021 alla quale hanno partecipato le amministrazioni cantonali nonché diversi rappresentanti del mondo scientifico, delle organizzazioni economiche e del mondo imprenditoriale. Complessivamente sono stati inoltrati 60 pareri. Il 14 ottobre 2021, al termine della consultazione, il DFGP ha organizzato un dibattito pubblico in forma di conferenza cui hanno partecipato 50 rappresentati dei Cantoni, dei partiti, del mondo scientifico, della società civile e del mondo economico nonché alcuni cittadini interessati. L'obiettivo della consultazione pubblica era di raccogliere i pareri sulle principali esigenze cui avrebbe dovuto rispondere l'Id-e, sui suoi principali settori d'impiego e sui vantaggi attesi. Inoltre, si trattava di conoscere il parere degli interessati sull'ampliamento dell'ecosistema dell'Id-e. Le informazioni raccolte hanno permesso al Consiglio federale di prendere una decisione di principio sull'orientamento del futuro Id-e.

I partecipanti alla consultazione si sono espressi a favore della soluzione basata sulla SSI ritenendo imprescindibile un'infrastruttura di fiducia del livello di ambizione 3 (cfr. documento di discussione, n. 4.2). Questa soluzione tiene conto delle richieste avanzare dalle mozioni adottate dal Consiglio nazionale il 14 settembre 2021. I lavori successivi hanno quindi considerato questa volontà come anche il principio della protezione dei dati fin dalla progettazione (*privacy by design*), di quello della minimizzazione dei dati e del salvataggio decentralizzato dei dati. Inoltre il DFGP ha rafforzato la collaborazione con gli uffici e i Cantoni che stanno attuando progetti pilota in tale settore.

Sulla base dei risultati della consultazione pubblica, il 17 dicembre 2021 il Consiglio federale ha preso una decisione di principio sull'orientamento del nuovo Id-e. Il futuro mezzo di identificazione elettronico dovrà fondarsi sul principio della protezione dei dati fin dalla progettazione (privacy by design), sul principio della minimizzazione dei dati e sul loro salvataggio decentralizzato nonché su un'infrastruttura di fiducia statale in grado di allestire un ecosistema di mezzi di autenticazione elettronici emessi da soggetti dei settori pubblico e privato. Il Consiglio federale ha prolungato di un mese la consultazione esterna sull'avamprogetto; infine ha chiesto al DFGP di assicurare, in collaborazione con 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 progetti collegati della Confederazione e dei Cantoni.

1.1 Programma di legislatura e strategie nazionali del Consiglio federale

La legge federale sui mezzi d'identificazione elettronica riconosciuti (Legge sull'eID) è stata annunciata nel messaggio del 27 gennaio 2016[2] sul programma di legislatura 2015–2019 e nel decreto federale del 14 giugno 2016[3] 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 di reimpostare i lavori legislativi in materia di identificazione elettronica. Il presente avamprogetto non è stato annunciato né nel messaggio del 29 gennaio 2020[4] sul programma di legislatura 2019-2023, né nel decreto federale del 21 settembre 2020[5] sul programma di legislatura 2019-2023.

1.2 Stralcio degli interventi parlamentari

L'avamprogetto proposto attua gli interventi parlamentari seguenti:

- le mozioni 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129 presentate da tutti i gruppi parlamentari e aventi tutte il seguente titolo «Identità elettronica statale affidabile». Le mozioni chiedevano al Consiglio federale di creare uno strumento d'identificazione elettronica statale, comparabile alla carta d'identità o al passaporto nel mondo reale,

2 FF **2016** 909, 966 e 1026
3 FF **2016** 4605, 4607
4 FF **2020** 1565
5 FF **2020** 7365

che rispettasse il principio della «privacy by design», il principio della minimizzazione dei dati e la registrazione decentralizzata dei dati (come la registrazione dei dati dei documenti d'identità presso gli utenti). Le mozioni sono state accettate il 14 settembre 2021 dal Consiglio nazionale, secondo quanto proposto dal Consiglio federale. Non sono ancora state discusse nel Consiglio degli Stati.

Nel quadro della sua elaborazione, sono stati presi in considerazione anche gli interventi parlamenti 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 dibattito è stato rimandato perché le risposte non erano soddisfacenti.

– 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 Confronto con il diritto straniero, in particolare europeo

L'Unione europea (UE) ha avviato una serie di riforme in materia di identificazione elettronica. Il Consiglio federale ritiene necessario tener conto di questi sviluppi nella pertinente riflessione condotta a livello nazionale. Il 3 giugno 2021, la Commissione europea ha adottato una proposta[6] che modifica il regolamento (UE) n. 910/2014 (regolamento eIDAS)[7] e introduce un quadro giuridico per un'identità digitale europea. In base al nuovo regolamento, nei dodici mesi successivi all'entrata in vigore delle nuove disposizioni, gli Stati membri offrono ai cittadini e alle imprese portafogli elettronici che collegano la loro identità elettronica nazionale agli attestati di altri attributi personali (come la licenza di condurre, un diploma, un conto bancario). Questi portafogli potranno essere forniti dalle autorità pubbliche o da enti privati riconosciuti dagli Stati membri. A fine giugno 2022 si terrà un dibattito presso la commissione responsabile (ITRE) del Palamento europeo. Il voto in commissione è fissato per ottobre 2022 mentre quello al plenum per novembre 2022.

Per realizzare l'iniziativa entro tempi opportuni, la proposta è accompagnata da una raccomandazione. La Commissione ha infatti esortato gli Stati membri ad istituire un pacchetto di strumenti comune entro ottobre 2022 e ad avviare immediatamente i lavori preparatori necessari. Il pacchetto di strumenti comprenderà un'architettura tecnica nonché una serie di norme comuni e di linee guida sulle buone pratiche.

Il quadro definito dalla Commissione europea si fonda sui principi dell'identità autogestita (*SSI*), ma non dà indicazioni su come attuare tali principi sotto il profilo tecnico. Da settembre 2021, gli Stati membri stanno negoziando direttamente tra loro le norme tecniche.

La Svizzera non è giuridicamente tenuta a recepire il regolamento dell'Unione europea 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. L'avamprogetto 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. 27). A tale riguardo l'Id-e statale svizzero mira a ottenere il riconoscimento almeno del livello di garanzia significativo. In questo modo sarà possibile arrivare a un riconoscimento reciproco in particolare con l'UE. L'avamprogetto è stato redatto in modo da essere compatibile con la pertinente legislazione europea.

3 Il progetto a grandi linee

3.1 Normativa proposta

L'avamprogetto prevede l'introduzione di un'identità elettronica statale, gratuita e volontaria, per i titolari di un documento d'identità rilasciato dalle autorità svizzere. In tale contesto lo Stato continua a svolgere il suo compito principale di verifica dell'identità di una persona e di rilascio del relativo mezzo di identificazione elettronico. Come chiesto dagli autori delle mozioni presentate al Consiglio nazionale, l'avamprogetto persegue un approccio fondato sui principi della protezione dei dati fin dalla progettazione, della minimizzazione dei dati e del loro salvataggio decentralizzato.

La normativa proposta prevede inoltre l'introduzione di un'infrastruttura statale di fiducia che permetta agli attori dei settori pubblico e privato[8] di emettere e utilizzare mezzi di autenticazione elettronici. In tale contesto, la Confederazione gestirà i sistemi di base necessari (registro di base, sistema di conferma degli identificativi) e offrirà un portafoglio elettronico statale dove conservare l'Id-e e gli altri mezzi di autenticazione elettronici. I titolari del portafoglio potranno presentare il loro Id-e e gli altri mezzi di autenticazione in modo sicuro e trasparente. Una simile apertura del sistema permetterà di promuovere la diffusione e l'impiego di tali mezzi nonché di aumentare la fiducia di cui godono i processi digitali presso la popolazione.

6 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 final, 3 giugno 2021.

7 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.

8 Secondo l'art. 18 cpv. 2, il Coniglio federale potrà prevedere che la Confederazione confermi anche gli identificativi e le chiavi crittografiche degli emittenti e dei verificatori privati.

Un'infrastruttura elettronica di fiducia gestita dalla Confederazione è uno sviluppo nuovo e importante. Il progetto è il risultato di un'innovativa procedura partecipativa comprendente una consultazione informale, dibattiti pubblici e un forum dedicato online; inoltre integra l'esperienza acquisita nel quadro di progetti pilota con altri uffici e gli scambi intercorsi con altri Paesi.

L'aspetto dell'impiego dell'Id-e nei vari settori sarà esaminato in occasione della consultazione esterna; l'avamprogetto lo disciplina solo a titolo indicativo (cfr. modifica di altri atti normativi: LEF e LDEP).

3.2 Armonizzazione tra compiti e finanze

Gli aspetti relativi all'armonizzazione tra compiti e finanze saranno analizzati al termine della consultazione. È stata fatta una stima iniziale dei costi (cfr. 5.1 Risorse relative alle finanze e all'effettivo del personale).

3.3 Attuazione

Le disposizioni esecutive necessarie per attuare la presente legge saranno disciplinate a livello di ordinanza (cfr. art. 27 e i relativi commenti).

4 Commento ai singoli articoli

Ingresso

L'avamprogetto si fonda sugli articoli 38 capoverso 1, 81 e 121 capoverso 1 della Costituzione.

Trattandosi dell'identità elettronica statale, l'avamprogetto si fonda sugli articoli 38 capoverso 1 e 121 capoverso 1 della Costituzione svizzera (Cost; RS 101). 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, è evidente che riconoscono alla Confederazione la facoltà di disciplinare i documenti d'identità richiesti anche se questi non sono utilizzati esclusivamente per dimostrare la cittadinanza dei cittadini svizzeri e lo status di soggiorno dei cittadini stranieri. Fondandosi su questi due articoli, la legge del 22 giugno 2001[9] sui documenti d'identità (LDI) e la legge del 16 dicembre 2005[10] 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 ai cittadini stranieri. Dal momento che l'Id-e statale serve a dimostrare la propria identità nel mondo virtuale, è giustificato fondare l'avamprogetto sulle stesse basi costituzionali su cui si basa la certificazione ufficiale dell'identità, della cittadinanza e dello status 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 sua parte. Viceversa sostenere la realizzazione e la gestione di opere di terzi non può basarsi sull'articolo 81, ma al limite su una competenza federale. Le «opere pubbliche», oggetto dell'articolo costituzionale, sono tradizionalmente di natura fisica (p. es. una galleria). Tuttavia, secondo la perizia dell'Ufficio federale di giustizia (UFG) sulla cooperazione a livello di TIC tra la Confederazione e i Cantoni[11], «[z]usammengefasst wäre es nach einem in der Lehre teilwiese befürworteten Ansatz möglich, grössere Informatikvorhaben und andere Elemente zur Schaffung einer einheitlichen elektronischen Verwaltungslandschaft unter dem Werkbegriff von Art. 81 BV zu subsumieren»[12] (*ndt.: in sintesi sarebbe possibile, secondo un approccio sostenuto in parte anche dalla dottrina, far rientrare nel concetto di «opera» di cui all'art. 81 Cost. anche progetti informatici più ampi e altri elementi necessari alla costituzione di un panorama amministrativo elettronico uniforme)*. In effetti, seguendo l'interpretazione evolutiva e teleologica di Lendi[13] e di Biaggini[14], 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 avamprogetto 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[15].

L'avamprogetto disciplina determinati aspetti di diritto civile relativi ai rapporti tra gli emittenti e i titolari di un Id-e 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.

9 RS **143.1**
10 RS **142.20**
11 DFGP, Ufficio federale di giustizia, Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten del 22 dic. 2011, JAAC 2012.1 (pagg. 1 – 17, edizione del 1° mag. 2021(*disponibile solo in tedesco)*.
12 Ibid, pag. 8.
13 Ibid; Lendi, Martin, in St. Galler Kommentar, 2a ed. 2008, art. 81 marg. 6
14 Ibid; Biaggini, Giovanni in BV-Kommentar, Zurigo 2007, art. 81 marg. 2, criticato da Markus Kern nel Basler Kommentar, marg. 6 e 9.
15 Ibid; Biaggini, G., ibid, art. 81 marg. 3

Sezione 1 Oggetto e scopo

Art. 1

Cpv. 1

L'avamprogetto definisce il quadro giuridico dei mezzi di autenticazione elettronici in Svizzera e quindi anche dell'Id-e statale. Disciplina inoltre i requisiti dell'infrastruttura di fiducia utilizzata per l'emissione, la revoca, la verifica, la conservazione e la presentazione dei mezzi di autenticazione elettronici. Infine regola i ruoli e le competenze nella gestione e nell'utilizzo dell'infrastruttura di fiducia.

Cpv. 2

Lett. a

L'avamprogetto introduce un mezzo d'identificazione elettronico (Id-e) statale sicuro che potrà essere utilizzato tra privati cittadini e nei rapporti con le autorità pubbliche. L'Id-e permetterà al titolare di identificarsi più facilmente per effettuare transazioni nel mondo digitale, tale mezzo consente infatti di sostituire gli attuali processi di identificazione (online) molto più complessi. Essendo scaricabile sullo smartphone, l'Id-e può essere utilizzato anche nel mondo reale.

Lett. b

A garanzia della protezione dei dati, la lettera b riprende lo scopo di cui all'articolo 1 della legge del 25 settembre 2020[16] sulla protezione dei dati (nLPD) e ricorda che il trattamento dei dati personali, nell'ambito del rilascio e dell'utilizzo dell'Id-e, deve rispettare i requisiti in materia di protezione dei dati. Questo obiettivo è in particolare raggiunto attuando i requisiti posti dalle sei identiche mozioni intitolate «Identità elettronica statale affidabile» (cfr. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) depositate da tutti i gruppi parlamentari dopo che il vecchio progetto di legge è stato respinto nella votazione del 7 marzo 2021. Secondo gli autori delle mozioni, lo strumento di identificazione elettronica statale deve rispettare i principi della *privacy by design*, della minimizzazione dei dati e del loro salvataggio decentralizzato (come la registrazione dei dati dei documenti d'identità presso gli utenti). La lettera b ribadisce questi requisiti come obiettivi specifici da raggiungere nel contesto della protezione dei dati personali.

La nLPD si applica al trattamento dei dati personali previsto dal presente avamprogetto. Per evitare ripetizioni e agevolare la leggibilità, le disposizioni dell'avamprogetto non rinviano ai pertinenti articoli della LPD (cfr. n. 6.8 Protezione dei dati).

Lett. c

La lettera c garantisce che la configurazione dell'Id-e e dell'infrastruttura di fiducia corrisponda all'attuale stato della tecnica.[17] Utilizzando questa nozione, il legislatore mira a un elevato livello di sicurezza e di protezione dei dati da raggiungere mediante procedure avanzate. A tal fine è necessario promuovere la verifica regolare dell'aggiornamento e del livello innovativo dei provvedimenti di sicurezza implementati nonché controllarne l'efficacia rispetto agli obiettivi di protezione richiesti. Ciò significa che tali provvedimenti vanno confrontati con i prodotti di sicurezza esistenti sul mercato.[18]

Lett. d

Per facilitare l'ottenimento e l'impiego dell'Id-e, l'avamprogetto fissa in materia di emissione, verifica e revoca dell'Id-e nuovi standard o armonizza quelli esistenti. 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, lo sviluppo tecnico non va limitato; l'avamprogetto disciplina dunque la scelta della soluzione tecnica soltanto quando strettamente necessario per raggiungere gli obiettivi legislativi. Prevede in particolare una gestione decentralizzata dei dati escludendo quindi qualsiasi soluzione tecnica in base alla quale un fornitore di servizi di identificazione si interpone tra il titolare e il verificatore di un mezzo di autenticazione elettronico. In questo modo non si lasciano tracce presso tale fornitore e si concede al titolare un maggiore controllo 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 l'avamprogetto possa essere attuato nel contesto tecnologico che si presenterà dopo la sua entrata in vigore ossia in un contesto che attualmente non è ancora noto. Vari aspetti da disciplinare a livello di ordinanza saranno, sotto il profilo tecnologico, molto ambigui e ancora più 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 vanno prese solamente le decisioni tecnologiche assolutamente necessarie. Nella misura del possibile dovrebbe essere lasciata agli attori coinvolti la scelta della tecnologia da utilizzare sul loro lato dell'interfaccia per formattare, memorizzare ed elaborare i dati.

Sezione 2 Id-e

16 FF **2020** 6695

17 La nozione di «attuale stato della tecnica» è concettualmente diversa dagli altri stati analoghi della tecnica di cui alle espressioni «le regole riconosciute della tecnica» e «lo stato della scienza e della ricerca». In altri termini, la nozione di «stato attuale della tecnica» è più innovativa della definizione di «regole riconosciute della tecnica» e meno attuale dell'espressione «stato della scienza e della ricerca». Questa distinzione è essenziale per determinare il livello di sicurezza richiesto. Anche l'articolo 7 capoverso 2 nLPD esige l'introduzione di provvedimenti che corrispondano allo «stato della tecnica», ma non stabilisce i criteri in base ai quali determinare cosa si debba intendere per «stato della tecnica». Tuttavia non si deve dedurre che ciò che non è concretamente definito nella legge non è verificabile e quindi neppure applicabile.

18 Una misura ritenuta in un dato momento corrispondere allo «stato della tecnica», in un momento successivo può essere considerata una delle «regole riconosciute della tecnica» a causa del gap innovativo in quanto tale misura è superata rispetto ad altre misure disponibili.

Art. 2 Forma e contenuto

Cpv. 1

La Confederazione allestisce un'infrastruttura di fiducia (cfr. Sezione 5) che permetterà a soggetti pubblici e privati (cfr. i limiti di cui all'art. 18 cpv. 3) di emettere diversi mezzi di autenticazione elettronici che potranno essere utilizzati per dimostrare la propria identità, un fatto o un avvenimento (mezzi di autenticazione elettronici). L'Id-e è un mezzo d'identificazione elettronico emesso da fedpol mediante l'infrastruttura statale di fiducia.

Cpv. 2

Un Id-e contiene i seguenti dati d'identificazione personale: cognome ufficiale, nomi, data e luogo di nascita, sesso, cittadinanza e l'immagine del viso registrata nel sistema d'informazione per documenti d'identità ISA o nel sistema d'informazione centrale sulla migrazione SIMIC. Si tratta di dati riportati dai registri ufficiali dello Stato cui fedpol ha accesso secondo l'articolo 11 capoverso 3. Se un verificatore chiede un giustificativo, il titolare può comunicargli tutti questi dati o alcuni di essi.

Cpv. 3

Oltre ai dati d'identificazione personale, un Id-e contiene determinate informazioni supplementari ossia: il numero AVS, il numero dell'Id-e, la data di emissione e quella di scadenza dell'Id-e, una serie di informazioni sul documento d'identità utilizzato nella procedura di emissione dell'Id-e, in particolare sul tipo, il numero e la durata di validità di detto documento e infine alcune informazioni sulla procedura di emissione, queste ultime saranno definite in dettaglio a livello di ordinanza.

Art. 3 Requisiti personali

Osservazione preliminare

La formulazione potestativa dell'articolo sottolinea il fatto che non vi è alcun obbligo di avere o utilizzare un Id-e. Tuttavia, se i requisiti personali sono soddisfatti, fedpol è tenuto a emettere un Id-e alla persona che ne fa richiesta e che sarà il titolare una volta emesso.

Lett. a

Un cittadino svizzero titolare di un documento d'identità valido ai sensi della LDI può richiedere l'Id-e. Diversamente dalle persone fisiche, le persone giuridiche, che operano sempre mediante il loro organo, non possono essere titolari di un Id-e e sono identificate mediante il numero d'identificazione delle imprese (IDI)[19].

Lett. b

Un cittadino straniero titolare di un permesso valido ai sensi della legge del 16 dicembre 2005[20] sui stranieri e la loro integrazione (LStr) e dell'ordinanza del 24 ottobre 2007[21] sull'ammissione, il soggiorno e l'attività lucrativa (OASA) può ottenere un Id-e. Di seguito l'elenco dei permessi:

- permesso L: permesso di soggiorno di breve durata (art. 32 LStrI e art. 71 cpv. 1 OASA)
- permesso B: permessi di dimora (art. 33 LStrI e art. 71 cpv. 1 OASA)
- permesso C: permesso di domicilio (art. 34 LStrI e art. 71 cpv. 1 OASA)
- permesso Ci: permesso di dimora con attività lucrativa (art. 30 cpv. 1 lett. g e 98 cpv. 2 LStrI e art. 45 e 71*a* cpv. 1 lett. e OASA)
- permesso N: permesso per richiedenti l'asilo (art. 42 LAsi e 71*a* cpv. 1 lett. b OASA)
- permesso F: permesso per persone ammesse provvisoriamente (art. 41 cpv. 2 LStrI e art. 71*a* cpv. 1 lett. c OASA)
- permesso S: permesso per persone bisognose di protezione (art. 74 LAsi e art. 71*a* cpv. 1 lett. d OASA)
- permesso G: permesso per frontalieri (art. 35 LStrI e 71*a* cpv. 1 lett. a OASA)

Non vi è alcuna differenza fondamentale tra l'Id-e rilasciato a un cittadino svizzero e quello rilasciato a un cittadino straniero: in linea di massima questi due Id-e sono impiegati allo stesso modo. Va ricordato che possedere un Id-e non garantisce l'accesso a tutti i servizi che vi sono abbinati; ad esempio non vi è la certezza che tale mezzo permetta al titolare di beneficiare di tutti i servizi online. Infatti, alcuni prestatori potranno decidere di limitare, per ragioni di sicurezza legate all'affidabilità della verifica dell'identità dei cittadini stranieri, l'accesso ai loro servizi soltanto ai titolari di una determinata categoria di permessi di soggiorno. Il presente avamprogetto non introduce alcuna limitazione di accesso ai servizi online e al riguardo lascia ai prestatori di servizi interessati un certo margine di manovra.

Per determinate categorie di permessi (p. es. i permessi N, F, S e Ci), non è chiaro sin dall'inizio se l'identità abbia potuto essere verificata in modo affidabile. Nel corso della procedura d'asilo molti richiedenti l'asilo non sono infatti in grado di presentare un documento d'identità e quindi non possono essere identificati in modo affidabile. Il DFGP (SEM) riceve molte domande di modifica o di rettifica dei dati d'identificazione personale di persone ammesse provvisoriamente e spesso tali domande sono prive dei necessari documenti d'identità adattati. Per questa ragione, è giustificato introdurre

19 Cfr. Ufficio federale di statistica > Registri > Registri delle imprese > Numero d'identificazione delle imprese IDI
20 RS **142.20**
21 RS **142.201**

la possibilità di riconoscere l'Id-e rilasciato a un cittadino straniero: ogni Id-e include dati sul documento d'identità impiegato per la sua emissione. Se è giustificato ed espressamente previsto dalla legge, si può limitare l'accesso a determinati servizi ai cittadini stranieri, titolari di un permesso, la cui identità non ha potuto essere verificata in modo affidabile.

Infine, per motivi di efficacia e rapidità, la procedura per ottenere l'Id-e si fonda sulla presentazione di un documento d'identità svizzero valido. È stata inoltre presa in considerazione un'ulteriore verifica dell'identità del richiedente, ma questa possibilità è stata abbandonata per ragioni di costo, praticità e rapidità. Questo approccio, infatti, sarebbe stato più oneroso che l'ottenimento di un documento d'identità.

Art. 4 Emissione

Osservazione preliminare

Per ottenere un Id-e si fa domanda a fedpol che avvia la procedura di emissione dopo aver verificato i requisiti personali di cui all'articolo 3.

Cpv. 1

Non vi è l'obbligo di avere un Id-e; chi desidera averlo, deve farne domanda a fedpol. La domanda deve essere presentata dal futuro titolare dell'Id-e (richiedente) o dal suo rappresentante legale (cfr. cpv. 2, per i minori di 14 anni e le persone sotto curatela generale). Il ricorrente o il rappresentante legale potrà depositare una domanda per l'emissione di un Id-e collegandosi al sistema d'informazione di fedpol o mediante il suo portafoglio elettronico.

Cpv. 2

Secondo questa disposizione, i minori al di sotto dei 14 anni e le persone sotto curatela generale devono avere l'autorizzazione del loro rappresentante legale per ottenere l'Id-e. Il limite di età previsto per i minori si fonda sull'articolo 8 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[22], secondo cui « (...) il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni» (par. 1). Inoltre, «Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni». La Svizzera non è giuridicamente tenuta a rispettare quanto prescritto dall'articolo 8 del regolamento citato, del resto questa disposizione non è stata neppure ripresa nel quadro della riforma della legge sulla protezione dei dati. Tuttavia, la lex specialis sull'identificazione elettronica può limitare l'accesso dei minori e delle persone sotto curatela generale. Tali soggetti infatti vanno protetti in modo particolare in quanto sono meno coscienti dei rischi, delle conseguenze, delle garanzie e dei diritti legati al trattamento dei dati personali. Il limite di età per ottenere un Id-e è inferiore rispetto a quello per ottenere un documento d'identità svizzero (ossia 18 anni; art. 5 cpv. 1 LDI). Dal momento che gli adolescenti utilizzano principalmente Internet per svolgere i propri compiti quotidiani, l'avamprogetto intende permettere loro di ottenere un Id-e a partire dal momento in cui sono in grado di capire le conseguenze del trattamento dei loro dati personali. Il motivo principale di questa disposizione è proteggere i soggetti coinvolti ma anche evitare di limitare indebitamente le loro attività nel mondo virtuale.

Cpv. 3

Dopo essersi assicurato che il richiedente soddisfa i requisiti di cui all'articolo 3, fedpol verifica la sua identità confrontando le informazioni fornite dall'interessato con quelle riportate nei registri federali ai sensi dell'articolo 11 capoverso 3. Se la verifica si conclude con successo, fedpol trasmette al richiedente un Id-e con i dati di cui all'articolo 2 capoversi 2 e 3.

Cpv. 4

Il capoverso attua i requisiti di cui all'articolo 34 capoverso 2 lettera a nLPD secondo cui, è necessaria una base legale in una legge in senso formale per permettere agli organi federali di trattare dati personali degni di particolare protezione. Secondo l'articolo 5 lettera c numero 4 nLPD, «i dati biometrici che identificano in modo univoco una persona» costituiscono dati personali degni di particolare attenzione. I dati biometrici in oggetto «sono 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.»[23]. In questo modo, il capoverso attua una base legale in senso formale che permette al Consiglio federale di prevedere, mediante un'ordinanza, l'utilizzo dell'immagine di cui all'articolo 2 capoverso 2 lettera g e dei dati biometrici rilevati durante l'emissione dell'Id-e. Questo modo di procedere è necessario per verificare se l'immagine registrata dal richiedente per la procedura di emissione dell'Id-e corrisponde a quella nei registri federali ISA e SIMIC.

Cpv. 5

Il Consiglio federale preciserà i dettagli della procedura di emissione in un'ordinanza nella quale fisserà in particolare lo svolgimento della procedura nonché gli standard e i protocolli tecnici applicabili alla comunicazione dei dati.

Art. 5 Revoca

22 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, GU L-119 del 4.5.2016, pag. 1-88.

23 Messaggio del 15 set. 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, 6012.

L'avamprogetto di legge prevede la possibilità di revocare un Id-e nei casi elencati alle lettere a-e. Tecnicamente non è infatti possibile bloccare o sospendere un Id-e direttamente nel portafoglio elettronico del titolare vista la natura decentralizzata del sistema di emissione di un Id-e. Il titolare o il rappresentante legale di un minore al di sotto dei 14 anni o di una persona sotto curatela generale può chiedere la revoca rispettivamente del proprio Id-e o dell'Id-e della persona che rappresenta. fedpol revoca l'Id-e anche se vi è il fondato sospetto di un impiego abusivo di tale mezzo e prima di procedere alla revoca verifica le informazioni che gli sono state trasmesse. Inoltre revoca l'Id-e anche quando apprende del decesso del titolare, del ritiro del documento d'identità utilizzato per emettere l'Id-e o della modifica dei dati d'identificazione personale di cui all'articolo 2 capoverso 2. L'Id-e è revocato anche quando il titolare ne ottiene uno nuovo. Un Id-e revocato non può più essere riattivato: la persona interessata deve richiederne uno nuovo a fedpol procedendo secondo l'articolo 4 capoverso 1.

Art. 6 Durata di validità

Per ragioni di sicurezza, l'Id-e vale per un periodo limitato. Il Consiglio federale disciplina in un'ordinanza i requisiti relativi alla durata. Tale ordinanza dovrà anche stabilire se la durata di validità dell'Id-e debba corrispondere a quella del documento utilizzato per l'emissione dell'Id-e. La durata di validità sarà indicata nell'Id-e (art. 2 cpv. 3 lett. d). Se il documento utilizzato per emettere l'Id-e viene ritirato dalle autorità, fedpol revoca l'Id-e nel momento in cui viene a conoscenza del ritiro di tale documento (art. 5 lett. d n. 1).

Una volta scaduto, l'Id-e non può più essere utilizzato per accedere ai servizi online, ma può ancora servire per provare i dati già verificati che contiene come il nome, il cognome o l'età del titolare.

Art. 7 Dovere di diligenza

Cpv. 1

Gli obblighi di diligenza imposti dall'avamprogetto al titolare di un Id-e corrispondo a quelli da rispettare abitualmente quando si utilizza una carta di credito o una carta bancaria. Ad esempio è imprescindibile e ragionevole non rivelare un eventuale codice PIN e non conservarlo insieme al supporto dell'Id-e, attivare la protezione contro l'accesso (p. es. PIN o riconoscimento dell'impronta digitale) e installare una protezione contro i virus sul dispositivo mobile usato come supporto dell'Id-e.

Pur prendendo tutte le possibili precauzioni, l'usurpazione dell'identità non si può totalmente evitare. Andrebbero pertanto introdotte sanzioni penali adeguate per punire un tale abuso. La nLPD introduce nel Codice penale l'articolo 179^{decies}, ossia una disposizione che punisce l'usurpazione d'identità con una pena detentiva sino a un anno o con una pena pecuniaria. Per evitare doppioni, l'avamprogetto non contiene disposizioni che sanzionano lo stesso reato.

Cpv. 2

Il titolare è tenuto a comunicare senza indugio a fedpol ogni sospetto di impiego abusivo del suo Id-e. Si può trattare di eventi verificatisi dopo la perdita del supporto su cui è conservato l'Id-e o di informazioni di terzi su un impiego inusuale dell'Id-e.

Art. 8 Servizi di contatto cantonali

La trasformazione digitale è in atto non solo a livello federale ma anche a quello cantonale e comunale. L'Id-e permette di accedere a diversi processi digitali per eseguire più facilmente transazioni online. Dal momento che determinati compiti o attività possono essere compiuti da casa propria, la presenza fisica dell'interessato non è più necessaria. Nonostante la crescente digitalizzazione della società, alcuni strati della popolazione non sono pronti ad affrontare questo cambiamento e, in caso di bisogno, preferiscono recarsi di persona dall'autorità. L'articolo prevede pertanto l'istituzione di servizi cantonali, incaricati di fornire assistenza agli interessati, la cui denominazione e organizzazione spetterà ai Cantoni. Questi servizi di contatto forniranno un'assistenza generale per vari processi di *e-government* e affiancheranno il supporto tecnico fornito da fedpol in merito all'emissione, all'impiego o alla revoca dell'Id-e.

È molto probabile che la maggior parte delle richieste di assistenza in materia di digitalizzazione si registrerà a livello cantonale. Questa disposizione mira pertanto a istituire punti di contatto vicino a coloro che potrebbero averne bisogno. Alcuni Cantoni hanno per altro già creato servizi simili; nel Canton Giura, ad esempio, un sistema di punti di contatto offre assistenza sul posto per i servizi di *e-government* cantonali. A livello internazionale, anche la Danimarca ha optato per un simile approccio.

A livello federale, la Confederazione fornirà assistenza ai servizi cantonali per gli aspetti legati all'infrastruttura di fiducia (supporto di secondo livello).

Art. 9 Obbligo di accettare l'Id-e

Se ricorrono all'identificazione elettronica, le autorità e i servizi che adempiono compiti pubblici devono accettare l'Id-e statale ai sensi del presente avamprogetto. La norma si rivolge anche alle autorità cantonali e comunali ed è opportuna poiché l'Id-e è concepito come un mezzo d'identificazione elettronico statale atto a dimostrare la propria identità nel mondo virtuale e quindi paragonabile alla carta d'identità o al passaporto nel mondo fisico ossia a documenti accettati da qualsiasi autorità per identificare una persona.

L'Id-e statale potrà essere utilizzato in combinazione con gli attuali mezzi di accesso ai servizi di *e-governement*. La disposizione riflette l'importanza dell'Id-e ai sensi della presente legge e la sua accoglienza da parte della popolazione, come

evidenziato dalla strategia «Svizzera digitale»[24] e dalla strategia di *e-government* Svizzera 2020-2023[25]. L'obbiettivo è da un lato sostenere gli investimenti della Confederazione per implementare l'Id-e e dall'altro contribuire a diffondere tale strumento nell'ambito dell'*e-government*; a trarne profitto non saranno soltanto la Confederazione, i Cantoni e i Comuni, che potranno risparmiare a medio termine, ma anche la popolazione svizzera.

Gli aspetti legati all'impiego dell'Id-e e le relative conseguenze giuridiche non sono materia del presente avamprogetto. Questi aspetti vanno regolati in modo specifico per ciascun settore. L'avamprogetto affronta in particolare il caso della cartella informatizzata del paziente e quello delle esecuzioni e del fallimento. In sede di consultazione saranno esaminati altri scenari ed eventualmente l'avamprogetto sarà completato.

Art. 10 Presentazione dell'Id-e

Secondo l'articolo, il titolare di un Id-e non è obbligato a presentarlo quando interagisce nel mondo reale. Pur riconoscendo i vantaggi offerti dall'Id-e, non si tratta di escludere la possibilità di presentare un documento d'identità fisico. Di conseguenza se è possibile identificare una persona mediante un documento d'identità nell'ambito di una procedura che richiede la presenza di tale persone, l'esibizione dell'Id-e (o parti di esso) può essere richiesta solo a titolo supplementare.

Art. 11 Sistema d'informazione per l'emissione e la revoca dell'Id-e

Cpv. 1

fedpol gestirà un sistema d'informazione che tratterà i dati d'identificazione personale di cui all'articolo 2. Detto sistema permetterà di raccogliere le domande dei richiedenti e di garantire l'esecuzione dei compiti di fedpol nell'ambito dell'emissione e della revoca di un Id-e.

Cpv. 2

Il sistema d'informazione contiene i dati di cui all'articolo 2 capoverso 3 e le informazioni sulla revoca di un Id-e. Inoltre vi sono conservati anche i dati, detti secondari, generati durante il processo di verifica dell'identità e la procedura di emissione dell'Id-e e necessari per scopi d'analisi statistica, di assistenza e di prevenzione degli abusi. I dati d'identificazione personale sono consultati direttamente nei registri federali e non sono memorizzati nel sistema (cfr. cpv. 3).

Cpv. 3

Al fine di emettere l'Id-e, il sistema d'informazione potrà consultare i seguenti registri di persone gestiti a livello federale:

- il sistema d'informazione per documenti d'identità (ISA);
- il sistema d'informazione centrale sulla migrazione (SIMIC);
- il registro informatizzato dello stato civile (Infostar) previsto all'articolo 39 del Codice civile (CC)[26] e all'articolo 6a dell'ordinanza del 28 aprile 2004[27] sullo stato civile (OSC);
- il registro centrale dell'Ufficio centrale di compensazione dell'AVS (UCC-UPI) previsto all'articolo 71 della legge del 20 dicembre 1946[28] su l'assicurazione per la vecchiaia e i superstiti (LAVS).

fedpol potrà così adempiere i compiti necessari per emettere un Id-e in modo automatizzato. Su questa base fedpol può verificare l'identità del richiedente e comunicargli i dati elencati all'articolo 2 capoverso 3 attraverso un canale sicuro. I dati consultati non sono né duplicati né salvati nel sistema d'informazione di fedpol.

Cpv. 4

Il Consiglio federale disciplina mediante ordinanza i termini di conservazione delle varie categorie di dati. I dati di cui ai capoversi 2 e 3 possono essere conservati al massimo per cinque anni dopo la scadenza dell'Id-e. La conservazione dei dati intende permettere di esaminare eventuali casi di abuso.

Sezione 3 Altri mezzi di autenticazione elettronici

Art. 12 Emissione

Cpv. 1

Le autorità e i privati (cfr. i limiti di cui all'art. 18 cpv. 3) possono utilizzare l'infrastruttura di fiducia della Confederazione di cui alla sezione 5 per emettere mezzi di autenticazione elettronici diversi dall'Id-e statale il cui rilascio compete esclusivamente a fedpol. Si tratta di una disposizione potestativa che non obbliga né le autorità né i privati a servirsi di tale infrastruttura. Inoltre, il capoverso non pone limitazioni ai tipi di mezzi di autenticazione elettronici che possono essere emessi e mira ad aprire l'infrastruttura di fiducia a diversi attori e a permettere loro di emettere mezzi di autenticazione elettronici di vario genere.

Cpv. 2

24 Cfr. www.uvek.admin.ch > Comunicazione > Svizzera digitale»
25 Cfr. www.amministrazione-digitale-svizzera.ch/application/files/5616/3636/7740/E-Government-Strategie-Schweiz-2020-2023_I_def.pdf.
26 RS **210**
27 RS **211.112.2**
28 RS **831.10**

I mezzi di autenticazione elettronici comprendono diversi dati. Oltre al contenuto di base stabilito dall'emittente, devono contenere anche l'identificativo dell'emittente e la data di emissione.

Art. 13 Revoca

L'articolo riflette la prassi attuale secondo cui gli emittenti possono revocare i mezzi di autenticazione elettronici da loro emessi. Né le autorità né le persone fisiche possono revocare mezzi di autenticazione elettronici emessi da altri. Inoltre l'articolo elenca una serie di requisiti applicabili alla revoca dell'Id-e. L'obiettivo è attuare determinati standard minimi comuni per proteggere il titolare dei mezzi di autenticazione elettronici nel caso in cui il contratto concluso con l'emittente, il diritto cantonale o il diritto delle obbligazioni non preveda standard simili. La disposizione permette così al titolare o al rappresentante di un minore con meno di 14 o di una persona sotto curatela generale di chiedere la revoca rispettivamente del proprio mezzo d'identificazione o di quello di cui è titolare la persona che rappresenta. Inoltre l'emittente è tenuto a revocare il mezzo di autenticazione elettronico se vi è un fondato sospetto di un impiego abusivo di tale mezzo. Prima di procedere alla revoca, l'emittente verifica le informazioni che ha ricevuto. Un mezzo di autenticazione elettronico revocato non può più essere riattivato: l'interessato deve presentare una nuova domanda presso l'emittente.

Sezione 4 Utilizzo di mezzi di autenticazione elettronici

Art. 14 Forma e conservazione dei mezzi di autenticazione elettronici

Il titolare riceve il mezzo di autenticazione elettronico come pacchetto di dati memorizzato su un supporto tecnico di proprietà del titolare ed è totalmente sotto il controllo di quest'ultimo (i terzi non possono accedervi). L'avamprogetto non prevede alcun requisito in merito ai supporti tecnici su cui conservare il mezzo di autenticazione elettronico; la scelta di tale supporto spetta al titolare.

Art. 15 Trasferibilità dei mezzi di autenticazione elettronici

Cpv. 1

Un mezzo di autenticazione elettronico personalizzato (rilasciato a una persona fisica) non può essere trasferito a terzi[29]. Il divieto sancito dal capoverso riflette la crescente pratica degli emittenti di evitare gli abusi rilasciando mezzi di autenticazione elettronici personalizzati. Questa misura di protezione degli utenti è particolarmente importante nel contesto di un'infrastruttura di fiducia messa a disposizione dalla Confederazione.

Cpv. 2

Se si cambia supporto tecnico (smartphone, computer, ecc.), in genere è possibile ripristinare le applicazioni installate sul vecchio supporto. La Confederazione potrà offrire la stessa possibilità ai titolari di mezzi di autenticazione elettronici istituendo il sistema per le copie di sicurezza di cui all'articolo 21. In questo modo il titolare di simili mezzi potrà facilmente scaricare su un nuovo supporto quelli che aveva sul vecchio apparecchio. Il trasferimento dei mezzi di autenticazione elettronici nel sistema per le copie di sicurezza di cui all'articolo 21 permetterà di offrire questa possibilità di ripristino rapido ai titolari. Il capoverso delega al Consiglio federale la competenza di emanare le prescrizioni tecniche richieste per il trasferimento dei mezzi di autenticazione elettronici nel sistema per le copie di sicurezza.

Art. 16 Presentazione dei mezzi di autenticazione elettronici

Cpv. 1

Il titolare di un mezzo di autenticazione elettronico non è obbligato a presentarlo integralmente, egli è libero di decidere quali parti di tale mezzo o quali informazioni deducibili da esso trasmettere al verificatore affinché quest'ultimo proceda alla verifica richiesta nel caso concreto. L'avamprogetto non prevede alcun requisito concernente la categoria di dati che vanno comunicati al momento del controllo dei mezzi di autenticazione elettronici; questa decisione è di competenza dei verificatori. Ne consegue che il margine di manovra del titolare è quindi limitato dai requisiti posti dai verificatori nel quadro del processo di verifica. Se il titolare decide di non trasmettere gli elementi richiesti, non potrà far valere il suo mezzo di autenticazione elettronico. La legge sulla protezione dei dati pone tuttavia una serie di limiti a ciò che i verificatori possono chiedere al titolare di un mezzo di autenticazione elettronico, in particolare sono tenuti a rispettare il principio della finalità, della proporzionalità e della minimizzazione dei dati. Ciò significa che i verificatori possono trattare esclusivamente i dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Trattandosi di principi generali relativi alla protezione dei dati personali che si applicano indipendentemente dalla presente legge, non è necessario menzionarli in modo esplicito nell'avamprogetto.

Cpv. 2

I sistemi elencati alla sezione 5 non permettono all'emittente di accedere alle informazioni concernenti la presentazione e la verifica di un mezzo di autenticazione elettronico. Sono infatti impostati in modo tale da non permette tecnicamente un tale accesso.

Cpv. 3

Nella misura del possibile, il gestore dei sistemi di cui alla sezione 5 non è a conoscenza del contenuto dei mezzi di autenticazione elettronici. Questi sistemi sono impostati in modo tale che sia impossibile dedurre qualsiasi informazione sull'impiego di tali mezzi nonché sulle autorità e sulle persone private coinvolte.

29 Per la presentazione dei mezzi di prova elettronici, cfr. l'art. 16.

Sezione 5 Infrastruttura di fiducia

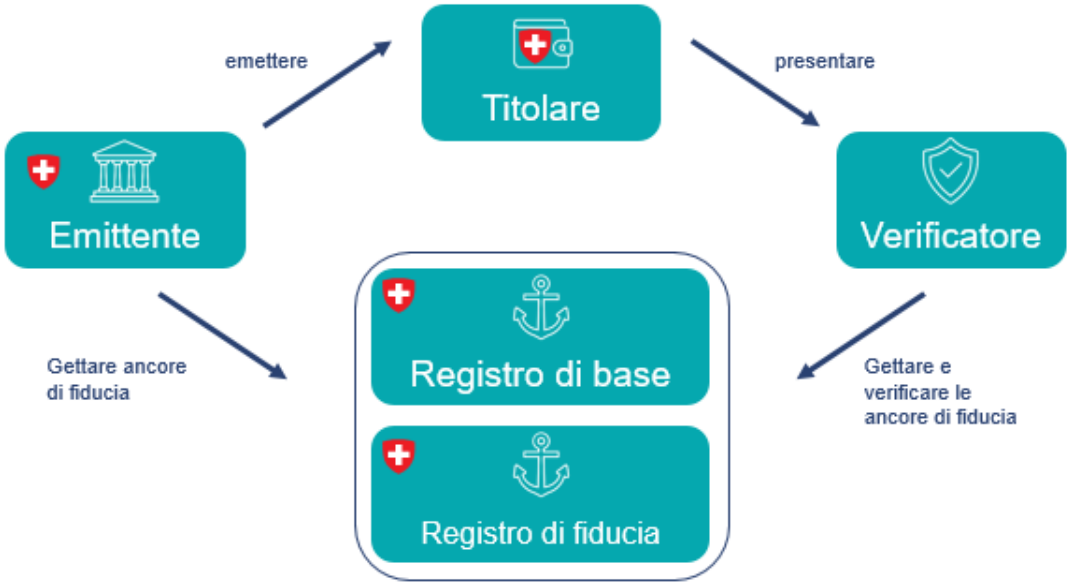
Osservazioni preliminari

Alla Confederazione compete la gestione e lo sviluppo di un'infrastruttura informatica in grado di emettere, impiegare, gestire, convalidare e revocare mezzi di autenticazione elettronici. Alla base di tale infrastruttura vi è una serie di regolamenti, procedure, piani ed elementi infrastrutturali, accettati e utilizzati da una vasta platea, che assicurano la fiducia nei processi digitali e la loro conformità. In tale contesto, la Confederazione realizza e gestisce l'infrastruttura informatica nell'interesse del Paese ai sensi dell'articolo 81 Cost. La presente sezione si discosta dunque da un'interpretazione rigorosa dell'articolo 81 Cost. secondo cui le opere pubbliche sono materiali o fisiche come un edificio o una galleria. Visto il progresso tecnico ed economico, la nozione di «opera pubblica» va interpretata in modo più vicino ai recenti sviluppi[30], ossia comprendente anche opere immateriali o non tangibili, come un sistema informatico o un sistema di comunicazione di dimensioni paragonabili all'infrastruttura di fiducia proposta.

L'obiettivo di tale infrastruttura è permettere l'emissione e l'impiego dell'Id-e e di altri mezzi di autenticazione elettronici. Una simile apertura del sistema è necessaria alla luce degli sviluppi tecnici ed economici su scala internazionale ed europea.

Non è ancora stato stabilito quali servizi dell'Amministrazione federale saranno responsabili della creazione e della gestione dei vari elementi dell'infrastruttura di fiducia. Per questa ragione, nella sezione 5 si parla ancora genericamente di «Confederazione». Questo aspetto andrà chiarito in base alle esperienze con i progetti pilota e definito al momento di elaborare il messaggio.

L'infrastruttura di fiducia si compone degli attori e degli elementi seguenti:



Art. 17 Registro di base

Cpv. 1

La Confederazione mette a disposizione delle autorità e dei privati interessati un registro di base che rappresenta una componente essenziale dell'infrastruttura di fiducia e costituisce il primo elemento dell'ancora di fiducia del sistema. Tale registro permette a un verificatore di controllare l'autenticità e l'integrità dei mezzi di autenticazione elettronici, rilasciati dall'emittente, che gli sottopone il titolare.

Il registro può basarsi sulla tecnologia distribuita (*distributed ledger technology, DLT*), ad esempio mediante blockchain. Tuttavia, la scelta della soluzione tecnica non è disciplinata dall'avamprogetto, che rimane, per quanto possibile, neutrale in merito agli aspetti tecnici (cfr. commento all'art. 1 lett. c).

Cpv. 2

Le informazioni inserite nel registro di base comprendono: gli identificativi degli emittenti, le chiavi crittografiche di questi ultimi per poter verificare sia i loro identificativi sia l'autenticità e l'integrità dei mezzi di autenticazione elettronici, e le indicazioni sui mezzi di autenticazione elettronici revocati. Il registro di base contiene questi dati sotto forma di sequenza di segni alfanumerici da cui non è possibile trarre conclusioni sull'identità degli emittenti e dei verificatori. Inoltre il registro di base non contiene gli indirizzi, i numeri di telefono, gli indirizzi e-mail o altre coordinate degli emittenti e dei verificatori e neppure i dati personali dei titolari.

30 Cfr. n. 3.1.

Cpv. 3

Gli emittenti iscrivono nel registro di base i propri dati permettendo così a un verificatore di controllare l'autenticità e l'integrità dei mezzi di autenticazione elettronica emessi dall'emittente in oggetto. Al momento dell'iscrizione, i dati sono protetti da un algoritmo crittografico pertanto non possono essere falsificati.

L'emittente e il verificatore che intendono annunciarsi in un sistema di conferma degli identificativi, iscrivono i propri dati nel registro di base. In questo caso si rinuncia a verificare l'identità dell'emittente o del verificatore prima che possa iscriversi nel registro di base. Una tale verifica comporterebbe un'onerosa procedura di autorizzazione che porterebbe a una serie inevitabile di lungaggini inutili e costose. Omettendo la verifica c'è il rischio che emittenti e verificatori possano rilasciare mezzi di autenticazione elettronici sulla base di un'identità fittizia, ma tale rischio potrebbe essere da un lato ridotto pubblicando informazioni su casi di fondato sospetto di un impiego abusivo dell'infrastruttura di fiducia di cui all'articolo 22 e dall'altro completamente escluso mediante il sistema di conferma degli identificativi di cui all'articolo 18. L'esclusione di emittenti o verificatori registrati non è tecnicamente possibile nel registro di base, ma lo è nel sistema di conferma degli identificativi di cui all'articolo 18.

Cpv. 4

Il registro di base non contiene dati concernenti i mezzi di autenticazione elettronici come i dati personali o materiali dei titolari e neppure tracce dell'emissione. Le autorità e i cittadini privati che utilizzano il registro di base non hanno accesso ai dati personali trattati nell'ambito dell'emissione dei mezzi di autenticazione elettronici.

Art. 18 Sistema di conferma degli identificativi

Cpv. 1

La Confederazione istituisce un meccanismo statale che permette di verificare se un identificativo ed eventuali chiavi crittografiche corrispondono a un emittente iscritto nel registro di base o a un verificatore interessato. Tale meccanismo costituisce il secondo elemento dell'ancora di fiducia del sistema e permette ai titolari e ai verificatori di conoscere con chi hanno effettivamente a che fare. La Confederazione potrebbe, ad esempio, utilizzare un archivio di fiducia o certificati emessi da un'autorità competente.

Un meccanismo di conferma dell'identificativo ha lo scopo di stabilire un collegamento tra il mondo virtuale e quello reale: permette di associare un identificativo tecnico iscritto nel registro di base a un'organizzazione, un ente o un cittadino privato esistente nel mondo reale. Questo meccanismo è molto importante per gli utenti e i verificatori. Non avendo necessariamente un rapporto diretto con un emittente, il verificatore può ricorrere a questo meccanismo per accettare mezzi di autenticazione elettronici solamente di emittenti affidabili. Ad esempio, l'Id-e sarà emesso da fedpol e l'identificativo tecnico dell'emittente apparirà nell'Id-e. Un verificatore ricorrerà al meccanismo di conferma dell'identificativo per assicurarsi che tale identificativo e le chiavi crittografiche dell'emittente dell'Id-e corrispondano effettivamente a fedpol.

La Confederazione si assicura che il meccanismo di conferma dell'identificativo sia accessibile a tutte le autorità e cittadini privati interessati. Questo accesso garantisce loro che l'interlocutore nel mondo virtuale è proprio l'organizzazione, l'ente o la persona che dice di essere. Permette di verificare se la controparte in una transazione è autentica.

Il sistema di conferma degli identificativi degli emittenti e dei verificatori sarà realizzato in diverse tappe. Fin dall'inizio è stata delegata alla Confederazione la competenza di confermare l'identità delle autorità federali, cantonali e comunali che agiscono in qualità di emittenti e verificatori. La Confederazione incarica un ente dell'Amministrazione federale di gestire e manutenere il sistema di conferma dell'identità. Questo ente tiene un elenco delle autorità attive come emittenti e verificatori e lo pubblica sul proprio sito aggiornandolo regolarmente.

Cpv. 2

Il Consiglio federale potrà eventualmente prevedere che la Confederazione confermi l'identificativo e le chiavi crittografiche degli emittenti e dei verificatori del settore privato. Se l'ecosistema dell'Id-e dovesse svilupparsi in proporzioni sufficienti e la domanda del settore privato diventasse abbastanza forte, questa opzione potrebbe rivelarsi necessaria. In questo modo aumenterebbe anche il livello di fiducia di cui gode l'infrastruttura nell'ambito dell'identificazione elettronica. Il Consiglio federale potrà quindi definire in un'ordinanza i requisiti applicabili alla conferma dell'identificativo di tali organizzazioni, enti e cittadini privati. Vanno inoltre pianificate le misure tecniche e organizzative da prendere in tale contesto.

Non è escluso che gli attori del settore privato decidano di introdurre, per conto proprio e separatamente, un meccanismo privato (non statale) di conferma degli identificativi; il capoverso non limita le loro attività in questo ambito.

Cpv. 3

Ogni autorità o cittadino privato interessato può consultare gli attributi degli identificativi confermati dal sistema nel quadro del controllo dei mezzi di autenticazione elettronici.

Art. 19 Applicazione per conservare e presentare i mezzi di autenticazione elettronici

La Confederazione mette a disposizione delle persone che ne fanno richiesta un portafoglio elettronico statale, ossia un'applicazione per conservare e presentare i mezzi di autenticazione elettronici. Si tratta di un'app che consente di richiedere e ottenere in modo sicuro mezzi di autenticazione elettronici, ed eventualmente anche l'Id-e, nonché archiviarli, selezionarli, combinarli e condividerli in modo trasparente e tracciabile per l'utente. Nella misura del possibile, l'implementazione del portafoglio elettronico statale rispetta gli standard attualmente fissati dall'UE.

Il titolare del mezzo di autenticazione elettronico conserva quest'ultimo in un portafoglio elettronico su un supporto di sua scelta come per esempio lo smartphone. Il verificatore può chiedere al titolare di trasmettergli determinati dati utilizzando

un canale di comunicazione sicuro. Il titolare a sua volta può decidere quali dati trasmettere effettivamente al verificatore dal suo portafoglio elettronico.

La legge non disciplina l'impiego dei portafogli elettronici emessi dagli attori privati. Oltre al portafoglio elettronico statale, gli utenti possono servirsi di altre applicazioni per conservare e presentare i loro mezzi di autenticazione elettronici. La Confederazione può sottoporre i prestatori che offrono portafogli elettronici a una procedura di valutazione e di certificazione ai sensi dell'articolo 13 nLPD. Pertanto non è più necessario disciplinare la possibilità di certificazione nell'avamprogetto.

Art. 20 Applicazione per verificare i mezzi di autenticazione elettronici

La presente disposizione potestativa permette al Consiglio federale di incaricare la Confederazione di creare un'applicazione che permetta di verificare la validità dei mezzi di autenticazione elettronici. Si tratta di una misura di sicurezza supplementare che potrà essere adottata in caso di necessità e servire in particolare a potenziare l'affidabilità di cui gode l'infrastruttura di fiducia presso la popolazione.

Art. 21 Sistema per le copie di sicurezza

Cpv. 1

In seguito alla perdita o all'acquisto di un smartphone, è ormai consuetudine per gli utenti ripristinare le applicazioni scaricate sul vecchio dispositivo grazie al backup. In questo modo è possibile recuperare rapidamente le funzionalità del vecchio sistema dopo aver cambiato apparecchio. La Confederazione potrà decidere di offrire la stessa possibilità ai titolari di mezzi di autenticazione elettronici. Il capoverso delega al Consiglio federale la competenza di prevedere l'istituzione, da parte della Confederazione, di un sistema informatico in cui i titolari potranno salvare una copia dei loro mezzi di autenticazione elettronici. In caso di cambiamento del supporto tecnico (smartphone, computer, ecc.), sarà possibile recuperare velocemente i mezzi di autenticazione elettronici memorizzati. Questo backup può essere fornito su cloud o localmente sul supporto tecnico del titolare.

L'impiego del sistema per le copie di sicurezza sarà su base volontaria. Ogni titolare sarà libero di impiegare l'opzione di backup per i suoi mezzi di autenticazione elettronici.

Cpv. 2

Solamente i titolari avranno accesso alle copie di sicurezza protette. Il sistema non permette a terzi di accedervi.

Cpv. 3

Le copie di sicurezza potranno essere distrutte su richiesta del loto titolare o del rappresentante legale di un minore al di sotto di 14 anni o di una persona sotto curatela generale titolari di un mezzo di autenticazione elettronico.

Art. 22 Impiego abusivo dell'infrastruttura di fiducia

Mettendo a disposizione un'infrastruttura di fiducia, la Confederazione di impegna anche ad attuare le misure di sicurezza richieste per ridurre al minimo il rischio di un impiego abusivo. Poiché non è tecnicamente possibile escludere un emittente nel registro di base, l'avamprogetto prevede questa misura allo scopo di contrastare eventuali abusi. L'articolo incarica la Confederazione di gestire una piattaforma su cui riportare le cattive pratiche nonché rendere attente le autorità e la popolazione in generale sui potenziali rischi. Ciò non deve tuttavia fornire il presupposto secondo cui i cittadini, che forse non sono a conoscenza delle informazioni pubblicate sulla piattaforma, violino automaticamente il loro obbligo di diligenza ai sensi dell'articolo 7 capoverso 1. Inoltre, la piattaforma deve riportare solamente i casi per i quali vi è un sospetto sufficientemente fondato, di impiego abusivo dell'infrastruttura di fiducia. Questa misura ha un carattere complementare rispetto al sistema di conferma degli identificativi e mira a proteggere gli utenti e ad assicurare un funzionamento trasparente dell'infrastruttura di fiducia. L'avamprogetto non definisce il termine «abuso» per non limitare o escludere indebitamente eventuali casi. Inoltre è importante non creare confusione rispetto ai casi di abuso già disciplinati dalla legge, come ad esempio l'usurpazione d'identità (art. 179^{decies} CP, introdotto dalla nLPD). L'abuso di cui al presente articolo comprende i casi di impiego dell'infrastruttura di fiducia non conformi agli scopi e ai requisiti previsti dall'avamprogetto.

Art. 23 Codice sorgente dell'infrastruttura di fiducia

La Confederazione pubblica su Internet il codice sorgente delle componenti dell'infrastruttura di fiducia di cui alla sezione 5, di modo che chi fosse interessato lo possa reperire. Lo sviluppo del codice e altri diritti collegati non sono disciplinati dal presente articolo ma dall'articolo 9 della legge federale del ... [31] concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità (LMeCA).

Art. 24 Gestione dell'infrastruttura di fiducia

Le componenti dell'infrastruttura di fiducia sono gestite da un prestatore di servizi interno all'Amministrazione federale. L'articolo adempie i requisiti delle sei identiche mozioni intitolate «Identità elettronica statale» (cfr. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 et 21.3129) che chiedevano di affidare la gestione complessiva della soluzione ad autorità

31 FF **2022** 805

statali specializzate. In questo modo vi è inoltre la garanzia che la Confederazione gestisca l'intera infrastruttura di fiducia all'interno dell'Amministrazione federale.

L'Ufficio federale dell'informatica e delle telecomunicazioni (UFIT) assumerà probabilmente il ruolo principale nella gestione dell'infrastruttura di fiducia.

Art. 25 Progresso tecnico

Cpv. 1

Il progresso tecnico è in rapida evoluzione e la tecnologia continuerà a evolversi anche dopo l'entrata in vigore dell'avamprogetto. Per garantire che quest'ultimo sia attuato, il presente capoverso delega al Consiglio federale la competenza di emanare, mediante ordinanza, disposizioni complementari che permettano di adeguare l'infrastruttura di fiducia al progresso tecnico e di garantire che essa continui a soddisfare gli obiettivi definiti dalla presente legge.

Cpv. 2

Per diversi motivi, le disposizioni complementari possono richiedere l'introduzione di una base legale formale. Per esempio, secondo l'articolo 34 capoverso 2 lettera a nLPD, non basta prevedere il trattamento di dati personali degni di particolare protezione in un'ordinanza, ma è necessaria una base legale in una legge in senso formale. In questo caso, le disposizioni decadono: se, due anni dopo la loro entrata in vigore, il Consiglio federale non ha sottoposto all'Assemblea federale un progetto di base legale; se l'Assemblea federale respinge tale progetto oppure quando entra in vigore la base legale prevista.

Sezione 6 Emolumenti

Art. 26

Cpv. 1

Gli emittenti e i verificatori verseranno un emolumento per l'iscrizione dei dati (l'identificativo, il materiale crittografico e le revoche dei mezzi di autenticazione elettronici) nel registro di base e nel sistema di conferma degli identificativi.

Poiché l'importo dell'emolumento non è previsto nella legge, sarà successivamente definito nell'ordinanza. A tale riguardo, il legislatore si baserà sugli importi già fissati nelle pratica[32].

Cpv. 2

Se il Consiglio federale decide di introdurre il sistema per le copie di sicurezza di cui all'articolo 20, potrà prevedere per via di ordinanza un emolumento per il suo utilizzo.

Cpv. 3

Il Consiglio federale disciplinerà per via di ordinanza la riscossione degli emolumenti conformemente all'articolo 46*a* della legge del 21 marzo 1997[33] sull'organizzazione del Governo e dell'Amministrazione (LOGA).

Cpv. 4

Le restanti prestazioni fornite dalla Confederazione in base alla presente legge sono esenti da emolumenti; il che significa che non viene prelevato alcun emolumento né per l'emissione dell'Id-e, né per il suo utilizzo e la sua verifica. Inoltre sono gratuiti l'utilizzo del portafoglio elettronico emesso dalla Confederazione, la lettura del registro di base e l'utilizzo del meccanismo di conferma dell'identificativo.

Con la rinuncia parziale alla riscossione di emolumenti si intende favorire l'impiego e la diffusione dell'Id-e. La Confederazione è molto interessata al fatto che l'Id-e sia sempre più utilizzato; in questo modo infatti lo scambio tra autorità e privati viene semplificato.

Sezione 7 Accordi internazionali

Art. 27

Dati i suoi stretti rapporti commerciali e sociali con la maggior parte dei Paesi membri dell'UE, la Svizzera ha tutto l'interesse ad essere integrata prima o poi nel sistema europeo per l'interoperabilità dei mezzi d'identificazione elettronici ed eventualmente in altri sistemi stranieri. Per poterlo fare è necessario un accordo internazionale. L'articolo delega al Consiglio federale la competenza sia di concludere accordi internazionali, destinati a facilitare l'impiego e il riconoscimento a livello internazionale dell'Id-e, sia di adottare le disposizioni esecutive necessarie. Un simile accordo permetterebbe di garantire il mutuo riconoscimento del sistema d'identificazione svizzero e di quelli notificati secondo il regolamento eIDAS o adottati da alcuni Stati membri dell'UE o da Stati terzi.

Sezione 8 Disposizioni finali

32 Si rimanda, a titolo di esempio, alle indicazioni fornite dalla fondazione Sovrin: Write To The Sovrin Public Ledger
33 RS **172.010**

Art. 28 Disposizioni di esecuzione

Le disposizioni di esecuzione della presente legge disciplinano l'attuazione degli aspetti tecnici e organizzativi legati alla comunicazione dei mezzi di autenticazione elettronici nonché il funzionamento delle componenti dell'infrastruttura di fiducia. Si tratta in particolare di disciplinare il formato di tali mezzi, gli standard e i protocolli applicabili ai processi di comunicazione dei dati al momento dell'emissione e della presentazione di tali mezzi, le componenti e il funzionamento del registro di base, del sistema di conferma degli identificativi, dell'applicazione per la conservazione e la presentazione di tali mezzi e del sistema per le copie di sicurezza nonché i mezzi di autenticazione da presentare per l'iscrizione nel sistema di conferma degli identificativi. Infine, il Consiglio federale ha anche la competenza di disciplinare mediante ordinanza i provvedimenti tecnici e organizzativi volti a garantire la sicurezza e la protezione dei dati nella gestione e nell'utilizzo dell'infrastruttura di fiducia. Queste disposizioni di esecuzione mirano in particolare a fissare nuovi standard e ad armonizzare quelli esistenti a livello internazionale ed europeo al fine di facilitare l'attuazione di questa legge. Per ragioni di chiarezza e trasparenza, sono state riunite in un unico articolo.

Art. 29 Modifica di altri atti normativi

L'avamprogetto propone di modificare altri atti normativi. Tali adattamenti mirano principalmente a permettere a fedpol di accedere ai sistemi d'informazione ISA, Infostar, e SIMIC, ma anche a disciplinare, a titolo indicativo, l'utilizzo dell'Id-e in determinati settori, come la cartella informatizzata del paziente e il settore delle esecuzioni e dei fallimenti. In occasione della consultazione, si dovrà verificare se è necessario modificare altre leggi federali (o se si potrà procedere a queste modifiche mediante ordinanza).

Art. 29 Referendum ed entrata in vigore

Come tutte le leggi federali, l'avamprogetto di legge sottostà a referendum e il Consiglio federale è incaricato di fissarne l'entrata in vigore.

Modifica di altri atti normativi

Osservazione preliminare

In base ai dati attualmente disponibili, si prevede che le condizioni d'identificazione e di autenticazione per le applicazioni di *e-government* vadano applicate, se necessario, a livello di ordinanza o di direttiva. L'attuazione delle disposizioni della LIdE implica pertanto un adeguamento di diverse ordinanze e direttive.

1. Legge federale del 20 giugno 2003[34] sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA)

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

L'articolo 9 capoverso 1 elenca le autorità cui la SEM può permettere di accedere con procedura di richiamo ai dati del settore degli stranieri che ha trattato o ha fatto trattare nel sistema d'informazione disciplinato nella LSISA. La lettera c precisa le finalità dell'accesso accordato alle autorità federali competenti in materia di polizia. L'avamprogetto integra questo elenco con una finalità nuova, ossia l'adempimento dei compiti assegnati a dette autorità dalla nuova legge sull'Id-e.

L'articolo 9 capoverso 2 elenca le autorità cui la SEM può permettere di accedere con procedura di richiamo ai dati del settore dell'asilo che ha trattato o fatto trattare nel sistema d'informazione secondo la LSISA. La lettera c definisce per quali finalità un tale accesso può essere accordato alle autorità federali competenti in materia di polizia. L'avamprogetto integra questo elenco con una finalità nuova, ossia l'adempimento dei compiti assegnati a tali autorità dalla nuova legge sull'Id-e.

2. Legge del 22 giugno 2001[35] sui documenti d'identità (LDI)

Art. 11 cpv. 2

L'articolo 11 capoverso 2 elenca le finalità del trattamento dei dati nell'ambito della gestione dell'ISA da parte di fedpol. Il presente avamprogetto cambia la struttura del capoverso e aggiunge una nuova finalità al trattamento, ossia l'adempimento dei compiti previsti dalla nuova legge sull'Id-e.

3. Codice civile (CC)[36]

Art. 43a cpv. 4 n. 9

L'articolo 43*a* CC disciplina l'accesso mediante procedura di richiamo ai registri elettronici impiegati nella gestione dello stato civile. All'elenco dei servizi e delle autorità che hanno accesso a Infostar viene aggiunto fedpol.

34 RS **142.51**
35 RS **43.1**
36 RS **210**

4. Legge federale dell'11 aprile 1889[37] sulla esecuzione e sul fallimento (LEF)

Come illustrato nei commenti agli articoli 9 e 28, questioni come l'obbligo di riconoscere un Id-e o le conseguenze giuridiche dell'impiego di tale mezzo non possono essere disciplinate in modo generale nella legge sull'Id-e la quale riporta solo determinati ambiti giuridici a titolo esemplificativo. In sede di consultazione si dovrà analizzare se anche altri ambiti giuridici richiedono disposizioni analoghe.

Art. 8a cpv. 2bis

Per richiedere un estratto del registro delle esecuzioni vi sono varie possibilità: presentarsi allo sportello dell'ufficio d'esecuzione oppure inviare una domanda scritta per posta o per via elettronica su uno dei portali messi a disposizione dalla Confederazione, dai Cantoni o dall'economia privata. Se la domanda riguarda una terza persona, è necessario, secondo l'articolo 8*a* capoverso 1 LEF, rendere verosimile un interesse. Per ottenere un cosiddetto estratto personale, il richiedente deve identificarsi spedendo ad esempio una fotocopia della carta d'identità o del passaporto. Richiedendo l'estratto su un portale online è possibile semplificare la procedura di ordinazione per tutti i soggetti coinvolti se il richiedente può identificarsi presentando un Id-e. Inoltre la qualità dell'identificazione è decisamente migliore rispetto a una fotocopia più o meno leggibile (e facilmente falsificabile) di una carta d'identità o di un passaporto.

Art. 33a cpv. 2bis

Ai sensi dell'articolo 33*a* capoverso 1 LEF, un atto scritto può essere trasmesso per via elettronica agli uffici di esecuzione e agli uffici dei fallimenti, nonché alle autorità di vigilanza. L'atto deve essere munito di una firma elettronica qualificata (art. 33*a* cpv. 2 LEF) grazie alla quale l'atto può essere chiaramente attribuito a una persona fisica. Poiché questa attribuzione univoca può essere garantita anche presentando un Id-e, sui portali online della Confederazione o di un Cantone si potrebbe rinunciare all'apposizione di una firma elettronica qualificata. In questo modo si semplifica la procedura per tutti i soggetti interessati.

5. Legge federale del 19 giugno 2015[38] sulla cartella informatizzata del paziente (LCIP)

Art. 7

La presente modifica sostituisce l'espressione «identità elettronica», di cui all'articolo 7 LCIP, con «strumento d'identificazione». L'espressione «strumento d'identificazione» corrisponde meglio al senso del presente articolo. Inoltre occorre evitare qualsiasi tipo di confusione con il presente avamprogetto che disciplina i termini legali del mezzo d'identificazione elettronica statale. Quest'ultimo certifica sotto forma elettronica l'identità di una persona e non è uno strumento di autenticazione per poter accedere a un servizio o a un'applicazione. Per ragioni di chiarezza, conviene 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 accedere alla cartella informatizzata del paziente sono emessi da privati che devono essere certificati da un organismo riconosciuto. A lungo termine anche questi strumenti d'identificazione verranno rilasciati dalla Confederazione; l'obiettivo è tener conto anche nell'ambito della LCIP della volontà politica, espressa dal popolo nel respingere la legge sull'eID alla votazione del 7 marzo 2021, di non demandare tale compito ai privati.

Se la Confederazione si assume tale compito, dovrà soddisfare i requisiti posti dalla legislazione sulla cartella informatizzata del paziente, ma non sarà più necessaria una certificazione del competente servizio federale, pertanto se ne dovrebbe fare a meno. Poiché gli strumenti privati di identificazione per accedere alla cartella informatizzata del paziente continueranno ad essere impiegati nel periodo di transizione, l'articolo 11 lettera c ora stabilisce che gli emittenti privati di strumenti di identificazione devono continuare a essere certificati.

6. Legge del 18 marzo 2016[39] sulla firma elettronica (FiEle)

Art. 9 cpv. 4bis

Chi chiede il rilascio di una firma elettronica deve presentarsi di persona. Quest'obbligo viene a cadere se l'identità è dimostrata con un mezzo di identificazione elettronico ai sensi della presente legge. Il Consiglio federale può prevedere mediante un'ordinanza che la presenza del richiedente non sia necessaria se quest'ultimo prova, con la debita affidabilità, la sua identità in altro modo.

7. Legge federale del …[40] concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità (LMeCA)

37 RS **210**
38 RS **816.1**
39 RS **943.03**
40 FF **2022** 805

Il presente avamprogetto fissa il quadro giuridico applicabile al mezzo d'identificazione elettronico statale. Tale mezzo permette al titolare di identificarsi ma non di autenticarsi per accedere a un servizio online o a un'applicazione. Per questa ragione la presente legge modifica la LMeCA affinché quest'ultima includa un sistema di autenticazione da intendere come «mezzo TIC» ai sensi dell'articolo 11 capoversi 1-3 LMeCA. Questo sistema di autenticazione si fonda sull'Id e può permettere di accedere a un servizio o a un'applicazione.

Questo sistema per l'autenticazione delle persone fisiche è disponibile, come mezzo TIC, anche per i Cantoni e i Comuni nonché per le organizzazioni e le persone di diritto pubblico o privato, se tenute ad applicare il diritto federale.

È stato previsto che la LMeCA entri in vigore prima dell'avamprogetto di legge sull'Id-e; non ci sarà bisogno di coordinare i due progetti di legge. Se, in sede di deliberazione parlamentare, dovesse emergere che la situazione è cambiata, si dovrà prevedere nel presente avamprogetto una disposizione di coordinamento.

5 Ripercussioni per la Confederazione

5.1 Ripercussioni finanziarie e sull'effettivo del personale

L'avamprogetto sull'Id-e comporterà nella fase iniziale costi per i lavori legislativi nonché in altri ambiti, in particolare la comunicazione e il supporto ad altri progetti collegati. Se la richiesta di finanziamento del DFGP viene accettata, questi costi potranno essere coperti dai fondi destinati alla realizzazione dell'ambizione 3 «Diffondere l'identità digitale in modo trasversale alle autorità» dell'agenda dell'Amministrazione digitale Svizzera (ADS). Per il 2022, le risorse finanziarie richieste (CHF 750 000) sono state approvate dagli organi dell'ADS. Inoltre nella pianificazione preparatoria dell'ADS, sono stati stanziati 1 000 000 franchi per il 2023 a tale scopo.

Una stima iniziale dei costi progettuali e operativi è stata realizzata sulla base dell'esperienza acquisita nel quadro dell'emissione del certificato COVID. Inoltre, i test pilota previsti permetteranno di definire più precisamente questi costi quando verrà elaborato il messaggio.

Secondo questa stima, i costi di progetto vanno dai 25 ai 30 milioni di franchi e comprendono lo sviluppo e la messa in servizio dell'infrastruttura di fiducia e più precisamente lo sviluppo del sistema informatico e l'adeguamento dell'infrastruttura del Servizio delle identità. Dall'avvio fino alla messa in servizio (go live) dell'infrastruttura di fiducia, il progetto durerà dai 24 ai 36 mesi.

I costi operativi sono stimati tra i 10 e i 15 milioni di franchi. Inoltre sarà necessario valutare la portata del supporto che andrà fornito sia per l'infrastruttura di fiducia sia per l'emissione dell'Id-e. Tale stima dovrà basarsi sui feedback dei test pilota e sulla valutazione delle potenziali sinergie sia tra gli uffici per i sistemi esistenti e futuri, sia con i Cantoni.

Per finanziare gli investimenti, saranno necessari i contributi dell'ADS, poiché l'identificazione elettronica in modo trasversale alle autorità rientra negli obiettivi della sua agenda. La gestione e lo sviluppo vanno finanziati il più possibile attraverso emolumenti.

5.2 Ripercussioni per i Cantoni e i Comuni

Se ricorrono all'identificazione elettronica, i Cantoni e i Comuni sono tenuti ad accettare l'Id-e statale in quanto è un mezzo di identificazione elettronica, rilasciato dalla Stato, atto a dimostrare l'identità del titolare nel mondo virtuale e quindi è paragonabile alla carta d'identità e al passaporto nel mondo reale, ossia a documenti d'identità accettati da tutte le autorità.

I Cantoni e i Comuni utilizzano diversi sistemi di *e-government*. I processi di identificazione e di autenticazione per accedere a tali sistemi potrebbero essere notevolmente semplificati grazie all'introduzione dell'Id-e e al ricorso all'infrastruttura di fiducia. L'identificazione semplice e sicura favorisce l'utilizzo dei servizi di *e-government* offerti dalle città e dai Comuni.

Inoltre, l'infrastruttura di fiducia permetterà ai Cantoni, ai Comuni e alle città di assolvere determinati compiti in modo più efficace, ad esempio potranno emettere licenze di pesca, contrassegni di parcheggio o certificati di domicilio elettronici. Gli emittenti non dovranno più occuparsi dell'applicazione software dell'utente (portafoglio elettronico) né delle misure di sicurezza, ma unicamente dei loro processi e sistemi di gestione. In quest'ottica, l'infrastruttura di fiducia farà progredire sotto il profilo della digitalizzazione diverse attività pubbliche a tutti i livelli.

È difficile quantificare i costi per adattare i sistemi offerti dai Cantoni, dalle città e dai Comuni per permettere l'identificazione mediante l'Id-e. Tali costi dovrebbero essere coperti dai risparmi che questi attori realizzeranno a medio termine grazie l'introduzione dei processi digitali. Inoltre, l'impiego dell'infrastruttura di fiducia della Confederazione permetterà ai Cantoni di risparmiare se questi ultimi potranno, ad esempio, utilizzare l'infrastruttura della Confederazione per rilasciare in futuro una licenza di condurre elettronica e dunque non dovranno investire in un'infrastruttura propria. La legge prevede che i Cantoni e le altre collettività territoriali, come gli utenti privati, versino un emolumento per iscriversi nel registro di base e per ottenere la conferma degli identificativi nell'apposito sistema. Tali emolumenti contribuiranno a finanziare la gestione dell'infrastruttura di fiducia dell'Id-e e i costi connessi sono comunque molto più bassi rispetto a quelli per allestire un'infrastruttura propria.

La trasformazione digitale è in atto a livello federale, cantonale e comunale. Nonostante la tendenza alla digitalizzazione della società, alcuni strati della popolazione non sono preparati ad affrontare questo cambiamento e, se necessitano di assistenza, preferiscono recarsi personalmente presso un servizio. Per questo motivo, i Cantoni sono tenuti ad allestire

servizi, la cui denominazione e organizzazione è di loro competenza cantonale, incaricati di fornire assistenza agli interessati. Poiché detti servizi forniranno un supporto di carattere generale e non legato esclusivamente all'Id-e, il loro impatto sarà relativamente basso.

5.3 Ripercussioni per l'economia

Il Consiglio federale intende contribuire in modo opportuno alla digitalizzazione della società svizzera. In tale ottica, ha adottato una serie di misure volte principalmente ad adattare il quadro legale o a creare le infrastrutture necessarie.

L'introduzione di un mezzo di identificazione elettronico e l'infrastruttura di fiducia sono elementi chiave per realizzare un ampio ecosistema di mezzi di autenticazione elettronici che garantisca affidabilità e sicurezza nelle transazioni digitali. Effettuare elettronicamente le transazioni complesse con lo Stato o tra partner privati ne aumenta l'efficienza.

5.4 Ripercussioni per la società

La digitalizzazione della società avanza rapidamente: un numero crescente di transazioni può ormai svolgersi online e l'obbligo di presentarsi di persona è sempre meno richiesto. In futuro si potranno probabilmente eseguire compiti sempre più diversi per via elettronica e preferibilmente mediante lo smartphone. Sebbene i mezzi di comunicazione per farlo non manchino, non è ancora possibile creare, gestire e presentare mezzi di autenticazione elettronici che siano sufficientemente funzionali e accettati dalla maggior parte dei prestatori di servizi. L'infrastruttura di fiducia della Confederazione intende colmare questa lacuna creando un ecosistema che permetta di emettere, utilizzare e presentare mezzi di autenticazione elettronici in modo sicuro. Si tratta di un insieme di standard, processi, strategie ed elementi infrastrutturali che garantiscono la fiducia nei processi digitali e la loro conformità, ossia di un insieme di componenti accettate e utilizzate da un vasto pubblico. Le transazioni elettroniche nei settori pubblico e privato potranno essere eseguite in modo più efficiente e sicuro nel rispetto dei requisiti fissati nella nLPD. Una simile infrastruttura permette di aumentare sia l'interconnessione tra diversi attori sia il livello di fiducia di cui beneficiano transazioni di questo tipo.

Per quanto riguarda l'Id-e, uno dei suoi principali vantaggi è permettere al titolare di presentare i propri dati a un interlocutore su Internet. Da un lato, il titolare ha un maggiore controllo sui propri dati e dall'altro maggiore responsabilità, in termini di dovere di diligenza, nell'ambito delle transazioni elettroniche. La portata di questa responsabilità come anche le sue conseguenze saranno definite più precisamente a livello di ordinanza. Inoltre, possedere un Id-e richiede un certo livello di conoscenze del suo sistema di funzionamento. Il dibattito pubblico sull'avamprogetto di legge permetterà di avviare presso la popolazione svizzera una prima alfabetizzazione digitale sull'argomento.

6 Aspetti giuridici

6.1 Costituzionalità

La competenza di disciplinare l'Id-e, gli altri mezzi di autenticazione elettronici e l'infrastruttura di fiducia si basa sugli articoli 38 capoverso 1, 81, 95 capoverso 1 e 121 capoverso 1 della Cost.

Trattandosi del mezzo di identificazione elettronico statale, l'avamprogetto 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, la Confederazione deve avere la facoltà di disciplinare i documenti d'identità richiesti anche se questi non sono utilizzati esclusivamente per dimostrare la cittadinanza dei cittadini svizzeri o lo status di soggiorno dei cittadini stranieri. Poiché l'Id-e statale sostituirà questi documenti in determinati settori d'attività, è legittimo fondare il presente progetto di legge su queste basi costituzionali per quanto riguarda l'attestazione ufficiale dell'identità, della cittadinanza e dello status di soggiorno degli stranieri.

La competenza di creare un'infrastruttura di fiducia è disciplinata all'articolo 81 Cost. che permette alla Confederazione di realizzare e gestire, nell'interesse del Paese o di una sua gran parte, opere pubbliche o di sostenerne la realizzazione. Le «opere pubbliche», oggetto di questa disposizione, sono tradizionalmente di natura fisica (p. es. una costruzione o una galleria). Tuttavia, seguendo l'interpretazione evolutiva e teleologica di Lendi[41] e di Biaggini[42], le «opere pubbliche» possono essere anche immateriali o non tangibili, come un sistema informatico o un sistema di comunicazione di dimensioni paragonabili all'infrastruttura di fiducia proposta. Pertanto sarebbe possibile fondare sull'articolo 81 un avamprogetto che mira a introdurre un'infrastruttura di fiducia in grado di emettere e convalidare diversi mezzi di autenticazione elettronici. Al riguardo, va ricordato che l'articolo 81 Cost, non conferisce alla Confederazione la competenza di emanare e imporre standard tecnici e operativi vincolanti per la cooperazione tra la Confederazione e i Cantoni[43] in materia di TIC.

41 DFGP, Ufficio federale di giustizia, Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen, Gutachten del 22 dic. 2011, JAAC 2012.1 (pagg. 1 - 17), edizione del 1° mag. 2012, pag. 8; Lendi, Martin, nel St. Galler Kommentar, 2a ed. 2008, art. 81 nota marg. 6

42 Ibid; Biaggini, Giovanni in BV-Kommentar, Zurigo 2007, art. 81 nota marg. 2, criticato da Markus Kern nel Basler Kommentar, Nota marg. 6 e 9.

43 Ibid; Biaggini, G., ibid, art. 81 nota marg. 3

6.2 Compatibilità con gli impegni internazionali della Svizzera

L'avamprogetto è compatibile con gli impegni internazionali vigenti. Nel corso della sua elaborazione, il Consiglio federale si è adoperato affinché fosse mantenuta la possibilità di assicurare l'interoperabilità internazionale. Se auspicato in un secondo momento, l'Id-e svizzero potrà ottenere il riconoscimento internazionale. A tale scopo sarà necessario concludere trattati internazionali.

6.3 Forma dell'atto

In ragione 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.

Su richiesta dell'ambiente politico, l'avamprogetto è stato redatto in tempi molto stretti. È inoltre molto astratto a causa della sua neutralità sotto il profilo tecnologico e tocca un ambito del tutto nuovo con le disposizioni sull'introduzione di un'infrastruttura pubblica immateriale della Confederazione (cfr. art. 81 Cost.). Sarà necessario adattarlo in funzione dei risultati della consultazione, in particolare sulla base dei feedback dei test pilota e dell'impiego settoriale previsto dalle autorità pubbliche.

6.4 Subordinazione al freno alle spese

Secondo l'articolo 159 capoverso 3 lettera b Cost., il progetto richiede l'approvazione della maggioranza dei membri di ciascuna Camera, visto che comporta nuove spese ricorrenti di oltre 2 milioni di franchi.

6.5 Rispetto del principio di sussidiarietà e del principio dell'equità fiscale

L'introduzione dell'Id-e e dell'infrastruttura di fiducia è incontestata. La prevista ripartizione dei compiti e il loro adempimento non violano né il principio di sussidiarietà né quello dell'equità fiscale. Le ripercussioni finanziarie del progetto per la Confederazione superano i 10 milioni di franchi, mentre quelle per i Cantoni non sono ancora calcolabili.

6.6 Deleghe di competenze legislative

L'avamprogetto non contiene deleghe di competenze legislative. Gli articoli 6, 11 capoverso 5, 25, 26 e 27, conferiscono al Consiglio federale semplicemente la competenza di emanare disposizioni che permettono di applicare la legge.

6.7 Protezione dei dati

Le disposizioni sulla protezione dei dati (nLPD e relative ordinanze) si applicano a tutte le parti coinvolte. I singoli soggetti, 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, l'avamprogetto non rimanda alle pertinenti disposizioni della nLPD.

La protezione dei dati è uno degli scopi dell'avamprogetto ed è esplicitamente citata nel campo di applicazione. L'articolo 1 capoverso 2 riprende inoltre lo scopo fissato all'articolo 6 nLPD precisando, ai numeri 1-4, come tale scopo sarà attuato nel contesto dell'Id-e. Si tratta in particolare di integrare i requisiti posti dalle sei identiche mozioni intitolate «Identità elettronica statale affidabile» (cfr. 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 b riformula questi requisiti come scopi specifici da raggiungere nell'ambito della protezione dei dati personali.

Inoltre, l'articolo 1 capoverso 2 lettera c dell'avamprogetto di legge mira a garantire che l'impostazione dell'Id-e e dell'infrastruttura di fiducia corrisponda allo stato attuale della tecnica. La nozione di «attuale stato della tecnica» è concettualmente diversa dagli altri stati analoghi della tecnica di cui alle espressioni «le regole riconosciute della tecnica» e «lo stato della scienza e della ricerca». In altri termini, la nozione di «stato attuale della tecnica» è più innovativa della definizione di «regole riconosciute della tecnica» e meno attuale dell'espressione «stato della scienza e della ricerca». Questa distinzione è essenziale per determinare il livello di sicurezza richiesto. Anche l'articolo 7 capoverso 2 nLPD esige l'introduzione di provvedimenti che corrispondano allo «stato della tecnica», ma non stabilisce i criteri in base ai quali determinare cosa si debba intendere per «stato della tecnica». Tuttavia non si deve dedurre che ciò che non è concretamente definito nella legge non è verificabile e quindi neppure applicabile. Utilizzando questa nozione, il legislatore mira a un elevato livello di sicurezza e di protezione dei dati da raggiungere mediante procedure avanzate. A tal fine è necessario promuovere la verifica regolare dell'aggiornamento e del livello innovativo dei provvedimenti di sicurezza implementati nonché controllarne l'efficacia rispetto agli obiettivi di protezione richiesti. Ciò significa che tali provvedimenti vanno anche confrontati con i prodotti di sicurezza esistenti sul mercato: una misura ritenuta in un dato momento corrispondere allo «stato della tecnica», in un momento successivo può essere considerata una delle «regole riconosciute della tecnica» a causa del gap innovativo in quanto tale misura è superata rispetto ad altre misure disponibili.

Per ragioni di trasparenza, l'articolo 2 elenca i dati registrati nell'Id-e ossia i dati di identificazione personale (cpv. 2) e alcuni dati supplementari (cpv. 3). I dati di identificazione personale sono: il cognome ufficiale, i nomi, la data di nascita, il sesso, il luogo di nascita, la cittadinanza e l'immagine del visto registrata in ISA e in SIMIC. Si tratta di dati reperibili nei registri ufficiali dello Stato ai quali fedpol ha accesso conformemente all'articolo 11 capoverso 3. Oltre ai dati di identifica-

zione personale, un Id-e contiene anche il numero AVS e alcuni dati supplementari creati da fedpol al momento dell'emissione dell'Id-e, ossia il numero dell'Id-e, la sua data di emissione e quella di scadenza nonché alcune informazioni sulla procedura di emissione. L'Id-e contiene anche le informazioni relative al documento d'identità utilizzato per emettere il mezzo di identificazione elettronico, ossia il numero, il tipo e la durata di validità del documento. I dettagli saranno precisati a livello di ordinanza.

In virtù dell'articolo 34 capoverso 1 nLPD, un organo federale ha diritto di trattare e di comunicare dati personali soltanto se lo prevede una base legale. Ai sensi dell'articolo 6 capoverso 3 nLPD, lo scopo del sistema proposto deve essere definito in modo preciso e intelligibile per gli interessati. L'avamprogetto prevede quindi norme precise che permettono a fedpol di gestire un sistema d'informazione per l'identificazione dei richiedenti. L'articolo 11 definisce la natura, il contenuto e lo scopo di questo sistema e al capoverso 2 tale articolo elenca le categorie di dati che il sistema contiene, ossia i dati di cui all'articolo 2 capoverso 3 nonché le indicazioni relative alla revoca di un Id-e. Inoltre vi sono conservati anche i dati, detti secondari, generati durante il processo di verifica dell'identità e la procedura di emissione dell'Id-e e necessari per scopi d'analisi statistica, di assistenza e di prevenzione degli abusi. I dati di identificazione personale sono consultati direttamente nei registri federali e non sono salvati nel sistema d'informazione di fedpol (cfr. cpv. 3). L'articolo 11 capoverso 3 elenca i registri federali cui fedpol avrà accesso per confrontare i dati personali. Lo scopo del sistema previsto dall'avamprogetto è permettere a fedpol di svolgere i suoi compiti in relazione all'emissione e alla revoca dei mezzi di identificazione elettronici. Inoltre, ai sensi del capoverso 5, i dati possono essere conservati nel sistema al massimo per cinque anni dopo la scadenza o la revoca dell'Id-e. Al Consiglio federale è delegata la competenza di disciplinare a livello di ordinanza i termini di conservazione delle varie categorie di dati.

L'infrastruttura di fiducia prevista dall'avamprogetto si fonda sui principi della minimizzazione dei dati, della protezione dei dati fin dalla progettazione e per impostazione predefinita e del salvataggio decentralizzato dei dati. Gli elementi principali di questa infrastruttura sono disciplinati alla sezione 5 che comprende le disposizioni sul registro di base, sul sistema di conferma degli identificativi e sull'applicazione per conservare e presentare i mezzi di autenticazione elettronici. Il registro di base e il sistema di conferma degli identificativi non contengono traccia di tali mezzi; solamente il registro di base contiene informazioni legate alla loro revoca. I dati dei titolari dell'Id-e e dei mezzi di autenticazione elettronici sono scambiati solamente tra l'emittente, il titolare e il verificatore, senza intermediari. Una base legale ai sensi dell'articolo 31 capoverso 1 nLPD non è pertanto richiesta. L'idea alla base dell'infrastruttura di fiducia è creare un sistema nel quale i flussi di dati sono diretti e trasparenti per tutti gli utenti, in cui gli emittenti non sappiano come sono usati i mezzi di autenticazione elettronici emessi senza per questo perdere il diritto di revocarli e in cui i titolari beneficiano delle misure di sicurezza corrispondenti allo stato attuale della tecnologia.

Infine, l'articolo 28 lettera e delega al Consiglio federale anche la competenza di disciplinare a livello di ordinanza i provvedimenti tecnici e organizzativi per garantire la protezione e la sicurezza dei dati nell'ambito della gestione e dell'utilizzo dell'infrastruttura di fiducia.