Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]



19.xxx

# Messaggio concernente la modifica della legge federale sull'assicurazione per la vecchiaia e per i superstiti (Utilizzazione sistematica del numero AVS da parte delle autorità)

del …

---

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di modifica della legge federale sull'assicurazione pe la vecchiaia e per i superstiti.

Nel contempo vi proponiamo di togliere dal ruolo il seguente intervento parlamentare:

2018 P 17.3968 Piano di sicurezza per gli identificatori personali (N 19.9.18 Commissione degli affari giuridici CN)

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

…

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ueli Maurer
Il cancelliere della Confederazione, Walter Thurnherr

## Compendio

***I processi amministrativi vanno resi più efficienti tramite un'utilizzazione controllata del numero AVS (NAVS). In futuro le autorità federali, cantonali e comunali dovranno avere la possibilità di utilizzare sistematicamente il NAVS in modo generalizzato per adempiere i compiti assegnati loro dalla legge. Si potranno così evitare scambi d'identità nel trattamento degli incarti personali. Il progetto contribuirà ad attuare con successo la Strategia di e-government Svizzera e migliorerà l'efficienza dei costi delle amministrazioni.***

***Situazione iniziale***

*L'assicurazione per la vecchiaia e per i superstiti (AVS) utilizza il numero d'assicurato sin dal 1948, ossia sin dal momento della sua istituzione. A tutt'oggi, questo numero di identificazione personale serve a facilitare il trattamento di informazioni sui contributi e per il calcolo delle corrispondenti prestazioni delle assicurazioni sociali. Nel 2008 è stato introdotto un nuovo NAVS a 13 cifre non significante e nel contempo adottato un nuovo disciplinamento relativo all'ammissibilità della sua utilizzazione sistematica. Da allora l'utilizzazione sistematica del NAVS al di fuori dell'AVS è ammessa soltanto a determinate condizioni. Anzitutto, questa possibilità è riconosciuta ai servizi e alle istituzioni incaricati dell'attuazione di disposizioni di diritto cantonale in stretto rapporto con le assicurazioni sociali. Secondariamente, il NAVS può essere utilizzato sistematicamente se lo prevede una legge speciale federale o cantonale. La disposizione della legge speciale in questione deve specificare lo scopo dell'utilizzazione del NAVS e gli aventi diritto, in modo da permettere il controllo democratico.*

*Nell'ambito del trattamento dei dati relativi a modifiche dello stato civile, l'utilizzazione sistematica del NAVS come identificatore personale permette un aggiornamento automatico, rapido e preciso degli attributi personali, il che garantisce la qualità dei dati contenuti nei registri degli utenti. Inoltre, trattandosi di un numero univoco, la sua utilizzazione sistematica consente di evitare scambi d'identità negli incarti personali e le conseguenti violazioni delle disposizioni sulla protezione dei dati. L'utilizzazione del NAVS migliora altresì l'efficienza dei costi nell'Amministrazione pubblica, semplificando tanto i processi interni quanto i processi trasversali tra autorità. Sull'onda della crescente digitalizzazione dell'attività amministrativa registrata dall'introduzione del NAVS, nel 2008, si è assistito a una forte espansione della sua utilizzazione sistematica.*

*Il vigente disciplinamento previsto dalla legge federale sull'assicurazione per la vecchiaia e per i superstiti (LAVS) ammette in realtà la possibilità di un'utilizzazione sistematica del NAVS da parte delle autorità, ma a determinate condizioni, considerate difficili da adempiere. Inoltre, la prassi legislativa relativa all'autorizzazione all'utilizzazione sistematica del NAVS è contraddittoria. Infine, la possibilità per i Cantoni di autorizzare le proprie autorità a utilizzare il NAVS è limitata all'esecuzione del diritto cantonale. Per queste ragioni, si chiede con crescente insistenza che*

*le autorità federali, cantonali e comunali possano utilizzare il NAVS quale identificatore personale univoco.*

***Contenuto del disegno***

*Con il progetto ci si prefigge di creare i presupposti necessari affinché le autorità federali, cantonali e comunali non necessitino più di una base legale specifica per ogni nuova utilizzazione sistematica del NAVS, ma siano autorizzate in modo generale a utilizzarlo sistematicamente. Il fatto di stabilire condizioni di utilizzazione uguali per tutte le autorità permetterà di aumentare la trasparenza. Le organizzazioni e persone che, pur non avendo carattere di autorità, sono incaricate da una legge di adempiere un compito amministrativo dovranno inoltre essere legittimate a utilizzare sistematicamente il NAVS, purché ciò sia previsto da una disposizione della pertinente legge speciale. L'utilizzazione sistematica di questo numero per scopi prettamente privati dovrà invece rimanere esclusa. Per determinati scopi dovrà inoltre essere mantenuta la possibilità di prescrivere in leggi speciali l'utilizzazione di identificatori personali settoriali invece del NAVS. In tal senso il legislatore conserverà la propria libertà d'azione.*

*Il progetto si limita a sostituire l'attuale necessità di una base legale specifica per ogni utilizzazione sistematica del NAVS con un'autorizzazione generale accordata dal legislatore alle autorità federali, cantonali e comunali e a determinate istituzioni. Attribuisce inoltre la necessaria importanza alla garanzia del rispetto della protezione dei dati e della sicurezza delle informazioni. Chi sarà autorizzato all'utilizzazione sistematica del NAVS dovrà adottare varie misure tecniche e organizzative. In primo luogo, gli accessi alle varie banche dati dovranno essere protetti in modo ottimale onde ridurre al minimo il rischio di un'utilizzazione abusiva. Le prescrizioni di sicurezza per l'accesso alle banche dati che contengono il NAVS concernono l'autenticazione, la trasmissione dei dati, la loro cifratura, i programmi antivirus e i sistemi firewall nonché la registrazione e l'analisi dei processi importanti all'interno dei sistemi informatici. Considerato che le autorità che utilizzano il NAVS saranno tenute a rispettare queste misure di accompagnamento, il progetto comporterà anche un aumento generale della sicurezza delle informazioni nell'Amministrazione pubblica.*

# Messaggio

## 1 Situazione iniziale

### 1.1 Necessità di agire e obiettivi

#### 1.1.1 Evoluzione fino a oggi

Sin dalla sua istituzione, nel 1948, l'assicurazione per la vecchiaia e per i superstiti (AVS) ha sempre utilizzato un numero AVS (NAVS). A tutt'oggi, questo numero di identificazione personale serve per facilitare il trattamento di informazioni sui contributi e per il calcolo delle corrispondenti prestazioni delle assicurazioni sociali. In origine, si trattava di un codice «significante»: dal NAVS era infatti possibile dedurre il gruppo di lettere iniziale del cognome, la data di nascita e il sesso. Ma questa situazione era insoddisfacente dal punto di vista della protezione dei dati e inoltre, con il passare del tempo, sono sorti problemi di disponibilità di NAVS assegnabili, con conseguenti notevoli problemi informatici. La gestione dei NAVS era inoltre soggetta a errori, poiché i numeri venivano modificati in caso di cambiamenti dello stato civile. Nel 2003, nell'ambito della consultazione relativa alla legge sull'armonizzazione dei registri[1], è stata dunque proposta l'introduzione di un identificatore personale unitario per i vari scopi amministrativi e registri (identificatore personale federale, IPF). In seguito alle perplessità manifestate dagli ambienti responsabili della protezione dei dati, il Consiglio federale aveva proposto, nell'ambito di una seconda consultazione indetta nell'estate del 2004, l'introduzione di sei identificatori personali settoriali (SPIN) e la costituzione di un server centrale per l'identificazione e la comunicazione. Ogni settore dell'Amministrazione, tra cui quello delle assicurazioni sociali, avrebbe avuto a disposizione un identificatore personale unitario. Tuttavia, in sede di consultazione è emerso con chiarezza che gli identificatori personali settoriali non avrebbero trovato il consenso della maggioranza dei Cantoni. Si è così giunti a una soluzione che prevedeva l'introduzione di un NAVS non significante a 13 cifre e, al contempo, una regolamentazione concernente l'utilizzazione sistematica di questo numero per scopi amministrativi al di fuori dell'AVS[2].

Sull'onda della crescente digitalizzazione dell'attività amministrativa, dall'introduzione del nuovo NAVS, nel 2008, si osserva una forte espansione della sua utilizzazione sistematica al di fuori dell'AVS, tanto a livello federale quanto a livello cantonale. Presso l'Ufficio centrale di compensazione (UCC) sono attualmente annunciati circa 12 700 utenti. Il NAVS è inoltre utilizzato da circa 60 000 fornitori di prestazioni per la fatturazione nell'assicurazione obbligatoria delle cure medico-sanitarie.

Numerosi attori ritengono che le condizioni poste per l'autorizzazione all'utilizzazione sistematica del NAVS debbano essere allentate. Nel gennaio del 2014, ad esempio, la Conferenza delle direttrici e dei direttori cantonali delle finanze (CDF) ha suggerito di mettere a disposizione il NAVS come identificatore personale generale, per consentire l'avanzamento dei progetti di governo elettronico. La CDF sostiene che

1 RS **431.02**
2 RU **2007** 5259

l'utilizzazione di un identificatore personale univoco consentirebbe una gestione efficiente dell'amministrazione e al tempo stesso migliorerebbe la qualità delle banche dati eliminando i rischi di scambi d'identità sinora presenti. Nell'ambito dell'elaborazione della legge federale del 18 dicembre 2015[3] sullo scambio automatico internazionale di informazioni a fini fiscali (LSAI), su proposta dei Cantoni si è inoltre deciso, per evitare ulteriori oneri amministrativi, di non creare nuovi numeri d'identificazione fiscale, bensì di optare piuttosto per l'utilizzazione del NAVS anche per questo scopo. L'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) e una parte degli incaricati cantonali della protezione dei dati giudicano con occhio critico questa evoluzione, temendo che la protezione dei dati sia messa a repentaglio.

Considerate queste premesse, nel febbraio del 2017 il nostro Consiglio ha incaricato il Dipartimento federale dell'interno di sottoporgli una modifica della legge federale del 20 dicembre 1946[4] sull'assicurazione per la vecchiaia e per i superstiti (LAVS) volta ad agevolare l'utilizzazione sistematica del NAVS da parte delle autorità federali, cantonali e comunali nell'adempimento dei loro compiti legali.

Nel quadro della presente revisione, si tratta di creare le basi legali che consentano un impiego del NAVS adeguato al futuro e garantiscano al tempo stesso la protezione dei dati.

### 1.1.2 Disciplinamento attuale

Attualmente l'utilizzazione sistematica del NAVS al di fuori dell'AVS è disciplinata come segue: se l'esecuzione del diritto federale necessita dell'utilizzazione sistematica del NAVS, può essere introdotta una base legale sufficiente nella pertinente legge federale. La norma di legge in questione deve definire lo scopo dell'utilizzazione e gli aventi diritto (art. 50*d* cpv. 1 e 50*e* cpv. 1 LAVS. Con l'autorizzazione accordata dal legislatore nella pertinente legge speciale, l'utilizzazione sistematica in questione ha un fondamento democratico. Le stesse condizioni si applicano di principio anche all'utilizzazione sistematica per l'esecuzione del diritto cantonale (art. 50*d* cpv. 1 e 50*e* cpv. 3 LAVS), tranne in quattro settori: riduzione dei premi nell'assicurazione malattie, aiuto sociale, legislazione fiscale e istituzioni preposte all'educazione. In questi settori l'autorizzazione all'utilizzazione da parte dei servizi cantonali è già sancita dalla legislazione in materia di AVS (art. 50*e* cpv. 2 LAVS) e pertanto non occorre un'ulteriore base in una legge speciale cantonale. L'utilizzazione sistematica per scopi prettamente privati è invece per principio vietata. Il NAVS è tuttavia utilizzato sistematicamente nel quadro dello scambio automatico di informazioni per questioni fiscali quale numero d'identificazione fiscale nello scambio di dati internazionale. A partire dall'autunno del 2018 viene pertanto trasmesso agli istituti finanziari di oltre 50 Stati e territori.

3 RS **653.1**
4 RS **831.10**

I servizi estranei alle assicurazioni sociali federali che intendono utilizzare il NAVS sistematicamente sono tenuti ad annunciarsi preventivamente all'UCC. Una volta autorizzati a utilizzare sistematicamente il NAVS, possono accedere alla banca dati UPI («Unique Person Identification») gestita dall'UCC, che serve esclusivamente all'identificazione di persone, e non contiene alcun dato fattuale. In questa banca dati sono registrati in modo univoco tutti gli individui ai quali è stato assegnato un NAVS. Oltre al NAVS, la banca dati UPI contiene i caratteri d'identificazione ufficiali di una persona fisica (cognome ufficiale, cognome da celibe/nubile, nomi ufficiali, data di nascita, sesso, nazionalità, Paese e luogo di nascita, cognome e nome del padre e della madre). L'UCC può garantire l'attualità, la completezza e l'univocità dei dati gestiti nella banca dati UPI grazie alle numerose fonti da cui essi sono tratti. Le principali fonti sono gli organi esecutivi del 1° pilastro del sistema sociale svizzero e i registri di persone centrali della Confederazione Infostar (registro informatizzato dello stato civile, per la documentazione dello stato civile delle persone), SIMIC (sistema d'informazione centrale sulla migrazione, nel settore degli stranieri e dell'asilo), E-VERA (sistema d'informazione per la gestione in rete dei dati relativi agli Svizzeri all'estero) e Ordipro (sistema d'informazione per la gestione dei diplomatici stranieri e dei funzionari internazionali). A questi si aggiungono i registri cantonali e comunali degli abitanti, le casse malati e altri utenti del NAVS. Chi ha diritto di accesso è tenuto, nell'interesse della protezione e della qualità dei dati, a prendere le misure tecniche e organizzative sancite a livello d'ordinanza[5].

Nel sistema attuale la decisione relativa all'autorizzazione all'utilizzazione sistematica del NAVS al di fuori dell'AVS è delegata al legislatore competente. Questi attribuisce la pertinente autorizzazione legale in base a una valutazione generale della sicurezza delle informazioni nel settore in questione.

### 1.1.3 Analisi dei rischi in adempimento del postulato 17.3968 Piano di sicurezza per gli identificatori personali, della Commissione degli affari giuridici del Consiglio nazionale

Di seguito sono fornite spiegazioni in adempimento del postulato 17.3968, depositato dalla Commissione degli affari giuridici del Consiglio nazionale il 20 ottobre 2017 e accolto da quest'ultima Camera nel settembre del 2018 nel contesto dei dibattiti parlamentari sulla modernizzazione del registro fondiario[6] e di un'analisi dei rischi svolta nel settembre del 2017[7]. Il postulato incarica il Consiglio federale di illustrare, entro la legislatura corrente, un piano su come affrontare i rischi correlati all'utilizzazione del numero AVS a 13 cifre quale numero d'identificazione personale unico, nonché

5 Ordinanza del DFI del 7 novembre 2007 sugli standard minimi delle misure tecniche e organizzative per l'utilizzazione sistematica del numero d'assicurato AVS al di fuori dell'AVS (RS **831.101.4**).

6 14.034 CC. Atti dello stato civile e registro fondiario.

7 David Basin, *Risk Analysis on different usages of the Swiss AHV number*, Zurigo 2017, disponibile (in inglese) all'indirizzo www.derbeauftragte.ch > Protezione dei dati –> Statistica, registro, ricerca –> Numero AVS.

di illustrare come sia possibile migliorare la protezione dei dati quando Cantoni, Comuni e terzi utilizzano i numeri d'identificazione personali, tenendo conto del giudizio dell'Incaricato federale della protezione dei dati e della trasparenza.

## Osservazione introduttiva

Regolarmente emergono incertezze relative alle caratteristiche e alla funzione degli identificatori personali. Inoltre, circolano numerose supposizioni, non sempre pertinenti, di rischi derivanti dall'utilizzazione sistematica degli identificatori personali in generale, e del NAVS in particolare. Considerate queste premesse, il postulato chiede un chiarimento della situazione.

Gli identificatori moderni quali il NAVS sono «non significanti», vale a dire che non permettono di risalire alle singole persone, nemmeno su Internet («eID»), né di accedere a sistemi informatici. L'unico rischio per la protezione dei dati concretamente ascrivibile all'utilizzazione sistematica di identificatori personali univoci consiste nella possibilità di costituire, in base a questi ultimi, profili della personalità più precisi di quelli costituibili in base ad altre caratteristiche accessibili al pubblico o note a chi li allestisce. Per «profilo della personalità» s'intende una compilazione di dati che permette di valutare caratteristiche essenziali della personalità di una persona fisica. Di seguito si illustra in che misura sussiste questo rischio. Sono inoltre esposti i possibili approcci per ridurlo al minimo in modo ragionevole e attuabile. Spetta per contro al legislatore valutare se, ed eventualmente a quali condizioni quadro, l'utilità dell'utilizzazione sistematica del NAVS prevalga sul rischio residuo.

## Definizione e funzione degli identificatori personali

Un identificatore personale serve ad attribuire correttamente le informazioni specifiche all'interno di una collezione di dati personali. A differenza degli altri attributi quali cognome e nome, che possono figurare più di una volta, un identificatore unico consente di classificare inequivocabilmente serie di dati e persone. Escludendo la possibilità di scambi di incarti, il suo impiego accresce la qualità dei dati dei registri.

Come altri identificatori personali della Confederazione, anche il NAVS serve esclusivamente ad attribuire al giusto individuo una serie di dati personali all'interno di una collezione di dati. Utilizzato soltanto per scopi amministrativi, questo numero d'identificazione personale univoco e invariabile per tutta la vita può essere assegnato a ogni persona fisica poco dopo la nascita sul territorio svizzero o in seguito allo stabilimento del domicilio o della dimora abituale in Svizzera. È vero che non si possono completamente escludere assegnazioni multiple, ma gli attuali meccanismi di controllo sono talmente rigidi che tali errori sono rari e, quando si verificano, vengono rilevati e corretti rapidamente. L'UCC comunica regolarmente i NAVS annullati o disattivati agli utenti, in modo che essi possano aggiornare di conseguenza le proprie banche dati.

Se si considerano i registri disciplinati dal diritto federale nell'ottica degli identificatori personali utilizzati, risulta un quadro eterogeneo. Anche al di fuori delle assicurazioni sociali vi sono registri di persone che si servono del NAVS quale unico identificatore personale, come ad esempio il registro centrale delle dosi delle persone

professionalmente esposte a radiazioni[8]. Altri registri centrali della Confederazione, tra cui ad esempio SIMIC, E-VERA e Ordipro, utilizzano il NAVS in aggiunta a propri identificatori personali specifici. Lo stesso vale anche per il registro federale delle professioni mediche universitarie[9] e il registro delle professioni sanitarie[10]. Conformemente al diritto federale, il NAVS serve inoltre alle autorità cantonali del registro di commercio per identificare persone fisiche. Alle persone registrate nella banca dati centrale viene assegnato anche un numero specifico[11]. Il numero d'identificazione del paziente per la cartella informatizzata di quest'ultimo è un numero specifico, collegato al NAVS, rilasciato e gestito dall'UCC[12].

Il numero d'identificazione delle imprese (IDI) non è un identificatore personale in senso stretto, tanto più che viene attribuito anche a comunità di persone senza personalità giuridica[13]. Lo stesso vale per il Registro delle imprese e degli stabilimenti (RIS), che contiene i dati di tutte le imprese e stabilimenti di diritto pubblico e privato aventi sede in Svizzera[14].

## Nessun dato personale deducibile dal NAVS

Soltanto un identificatore personale «significante» consente di ottenere informazioni su una data persona. Un identificatore personale è significante quando contiene informazioni codificate concernenti lo stato civile, l'età, il sesso o altre caratteristiche personali del titolare. Questo può comportare una divulgazione indesiderata di dati personali. Inoltre, sorgono difficoltà nel momento in cui cambiano alcuni dati personali (p. es. il cognome). Per contro, se un identificatore personale è generato casualmente o quale serie continua di numeri, non contiene informazioni codificate sul titolare ed è non significante[15]. Gli identificatori di uso comune a livello federale sono esclusivamente numeri non significanti[16]. Il NAVS non contiene informazioni sul suo titolare e quindi non consente di risalire alle sue caratteristiche personali. Non era il caso del numero a 11 cifre, sostituito da quello a 13 cifre attualmente utilizzato (cfr. n. 1.1.1). Per rendere visibile la provenienza svizzera del numero, il NAVS inizia con il prefisso «756», ossia il codice del Paese emittente, secondo la norma ISO 3166. Le

8 Art. 72–76 dell'ordinanza del 26 aprile 2017 sulla radioprotezione (ORaP; RS **814.501**).
9 Art. 51 cpv. 4$^{bis}$ della legge del 23 giugno 2006 sulle professioni mediche (LPMed; RS **811.11**).
10 Art. 24 cpv. 3 della legge federale del 30 settembre 2016 sulle professioni sanitarie (LPSan; FF **2016** 6837).
11 Art. 928*c* cpv. 1 e 3 del Codice delle obbligazioni (CO; RS **220**).
12 Cfr. art. 4 e 5 cpv. 1 della legge federale del 19 giugno 2015 sulla cartella informatizzata del paziente (LCIP; RS **816.1**).
13 Unità IDI secondo l'art. 3 cpv. 1 lett. c della legge federale del 18 giugno 2010 sul numero d'identificazione delle imprese (LIDI; RS **431.03**).
14 Art. 3 cpv. 1 dell'ordinanza del 30 giugno 1993 sul Registro delle imprese e degli stabilimenti (ORIS; RS **431.903**).
15 L'art. 25 cpv. 1, secondo periodo dell'ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD; RS **235.11**) recita: «È un elemento identificante non significante un insieme di caratteri attribuito in modo biunivoco a ogni persona registrata in una collezione di dati e che non dà, preso in sé, nessuna informazione sulla persona».
16 Per «identificatore» ai sensi della legge del 23 giugno 2006 sull'armonizzazione dei registri (LArRa; RS **431.02**) s'intende un numero inespressivo e invariabile (art. 3 lett. e LArRa).

posizioni da 4 a 12 contengono un numero intero scelto in modo aleatorio tra quelli ancora disponibili tra 0 e 999 999 999. La posizione 13 contiene la cifra di controllo.

## Il NAVS non è un elemento di autenticazione

Il processo di autenticazione consente di essere sicuri che una persona è effettivamente quella che afferma di essere. Per l'autenticazione tramite password il sistema chiede all'utente di dimostrare la correttezza della sua affermazione mediante l'indicazione di un dato di cui è l'unico a essere a conoscenza (autenticazione basata sulla conoscenza). A tal fine non è possibile menzionare il proprio NAVS.

La verifica dei diritti di accesso alle applicazioni di burotica generali delle amministrazioni pubbliche avviene di regola tramite un'autenticazione a due fattori (p. es. «smartcard» della Confederazione in combinazione con una password personale). Per utilizzare applicazioni specifiche – in particolare quelle che consentono di accedere a dati personali – occorrono dati di accesso supplementari specifici dell'applicazione (codice utente e password). Il NAVS non è né un codice utente né una password con cui si può accedere a sistemi informatici. Il fatto di essere a conoscenza di un identificatore personale come il NAVS non consente dunque di entrare in un sistema informatico cui non si ha legittimo accesso. L'utilizzazione sistematica di identificatori personali in una collezione di dati non accresce quindi la vulnerabilità di quest'ultima. Il NAVS non costituisce nemmeno una prova d'identità (digitale), per esempio per l'utilizzo di Internet. È pertanto escluso che la semplice indicazione di un NAVS sia sufficiente per ottenere prestazioni statali. Il fatto di conoscere il NAVS proprio o altrui non permette di per sé di trarre alcun vantaggio, né finanziario né immateriale.

## Il NAVS non dà un accesso più ampio ad altre banche dati

Le autorità autorizzate a utilizzare il NAVS possono aggiungere ai comuni attributi quali nome o data di nascita delle persone registrate anche il loro NAVS. A quel punto, i dati fattuali di una persona sono attribuiti in primo luogo a questo numero nella banca dati. Per poter aver la garanzia di utilizzare il numero giusto e/o gli attributi corretti, l'autorità ha accesso alla banca dati UPI. Questo non le dà però l'accesso agli altri registri, in particolare al registro centrale degli assicurati e al registro delle prestazioni correnti dell'UCC, né a registri contenenti dati fattuali gestiti da altre autorità. L'autorizzazione a utilizzare il NAVS non consente dunque all'autorità di effettuare un collegamento di dati né la autorizza a farlo (riguardo al collegamento cfr. sotto).

## Collegamenti di dati mediante identificatori personali e profili della personalità

Il collegamento dei dati contenuti in diversi sistemi permette di sintetizzare più caratteristiche di una persona in un cosiddetto profilo della personalità. Quest'ultimo contiene i caratteri d'identificazione di base di una persona, quali cognome, nome e data di nascita, e inoltre, a seconda del contenuto della banca dati consultata, altre informazioni legate alla persona, quali ad esempio dati sulla salute o dati fiscali e simili. Collegamenti illeciti e dunque indesiderati sono tecnicamente possibili solo se si riesce a penetrare in più banche dati. Se in diverse banche dati è utilizzato lo stesso identificatore personale univoco, un collegamento sulla base di quest'ultimo consente di

avere risultati leggermente più esatti. Tuttavia, dal punto di vista tecnico, tali collegamenti sarebbero possibili anche senza identificatori personali, ad esempio mediante quasi-identificatori quali cognome e nome, e l'utilizzazione di identificatori personali non li renderebbe più facili.

I profili della personalità possono essere sfruttati in ambito commerciale. A seconda del loro grado di dettaglio e di individualizzazione, un loro commercio può risultare lucrativo. Gli acquirenti di profili della personalità perseguono di regola l'obiettivo di ampliare la propria clientela o le informazioni relative ai propri clienti. Anche i gestori di banche dati che valutano la solvibilità delle persone sono interessati ai profili della personalità. La cautela è inoltre d'obbligo quando attori statali allestiscono profili della personalità partendo da dati salvati in formato digitale. Se questo avviene nel quadro di processi disposti per legge e legittimati democraticamente, ad esempio a fini statistici o per rispondere a quesiti scientifici dalla chiara formulazione, non vi sono problemi. Per evitare che ne sorgano, le autorità sono autorizzate ad allestire profili della personalità (p. es. a fini statistici) soltanto in presenza di un'esplicita base legale.

Un profilo della personalità può inoltre essere utilizzato abusivamente per commettere un furto di dati o d'identità. Quando si parla comunemente di furto di dati, si pensa generalmente all'acquisizione non autorizzata di informazioni. Se le informazioni in questione si riferiscono a un determinato individuo e vengono poi utilizzate in modo abusivo, si parla di furto d'identità o abuso d'identità. In questo caso ci si avvale dell'identità altrui per ottenere prestazioni cui non si ha diritto, rendendo al contempo più difficile o impossibile l'accertamento della propria identità reale. Dati personali che nel loro insieme costituiscono un'«identità» sono ad esempio il cognome, il nome, la data di nascita, i numeri di carte d'identità, conti bancari o carte di credito, nonché password informatiche, codici di accesso o soprannomi («nickname»). Più sono le informazioni di cui si dispone, più è facile riuscire a fingere di essere qualcun altro. Spesso l'abuso d'identità è volto a danneggiare la reputazione di una persona o a trarre indebitamente un vantaggio finanziario personale. Il successo di questo tipo di operazioni dipende tra l'altro anche dal fatto che la vittima abbia o meno predisposto un'autenticazione mediante documento d'identità ufficiale o eID. Essere a conoscenza di un identificatore personale non è di per sé sufficiente per un furto di dati.

## Probabilità di realizzazione dei rischi e potenziale entità dei danni

Tutti i registri di persone tenuti da autorità comprendono necessariamente attributi d'identificazione delle persone registrate (p. es. cognome, nome e data di nascita). Si tratta di cosiddetti quasi-identificatori. Se una persona (o un programma informatico) riesce a penetrare in diverse banche dati pur non avendovi diritto, i dati personali ivi contenuti potrebbero essere collegati anche solo in base ai quasi-identificatori, quindi anche se in quelle banche dati non sono utilizzati veri e propri identificatori personali come il NAVS. Tuttavia, il grado di attendibilità varia in funzione degli attributi d'identificazione utilizzati nelle banche dati: in presenza soltanto di cognome e nome, l'esattezza dei collegamenti è del 75,89 per cento, mentre se un registro di persone impiega cognome, nome e data di nascita questo valore sale al 99,98 per cento[17]. Se i

17 Cfr. Basin, *op. cit.*, cap. 2.2.3, pag. 11.

dati non sono collegati in base ai menzionati attributi d'identificazione, bensì a un identificatore univoco come il NAVS, il grado di esattezza risulta essere del 100 per cento, il che corrisponde a un incremento dello 0,02 per cento rispetto al collegamento in base a cognome, nome e data di nascita. In questa sede si analizza (soltanto) l'insorgenza del rischio che sorge (esclusivamente) nel caso in cui in futuro un registro di persone comprendesse, oltre ai quasi-identificatori già utilizzati, anche il NAVS, ovvero un identificatore personale univoco.

Si pone dunque la domanda se l'incremento di precisione di 0,02 punti percentuali sia sufficiente per indurre persone non autorizzate a penetrare o a cercare di penetrare in banche dati per costituire senza autorizzazione profili della personalità che altrimenti non avrebbero costituito oppure per migliorare o completare profili della personalità che hanno già allestito. In altre parole, si può presumere che persone non autorizzate considerino questo incremento di precisione come un incentivo decisivo? In questa sede non è possibile valutare con certezza se questi 0,02 punti percentuali in più le inducano effettivamente a penetrare o a cercare di penetrare illegalmente in sistemi d'informazione. Va rilevato che le banche dati svizzere contenenti dati personali sono già molto precise, anche senza l'utilizzo di un identificatore personale come il NAVS, e dunque potrebbero per principio essere interessanti. In ogni caso, il fatto di riuscire o meno a penetrare in tali sistemi senza autorizzazione dipende sostanzialmente dal livello delle misure adottate per garantire la sicurezza delle informazioni. Il fattore determinante è quindi lo sforzo necessario per riuscire a introdursi nel sistema. In altre parole, più un sistema è protetto, minore sarà l'incentivo a penetrarvi per ottenere un incremento di precisione. Se la sicurezza delle informazioni è garantita, si possono escludere furti di dati o d'identità e costituzioni non autorizzate di profili della personalità. Se invece la sicurezza è lacunosa, il rischio aumenta. Tuttavia, il fatto che tra i dati registrati figuri anche un identificatore personale è irrilevante per la vulnerabilità o meno del sistema.

Per valutare un rischio si confronta la sua probabilità di realizzazione con la gravità dei danni che ne risulterebbero. Non è possibile prevedere esattamente se un'utilizzazione sistematica del NAVS più ampia rispetto a oggi comporterebbe la costituzione non autorizzata di profili sulla base di questo numero. La probabilità è tuttavia molto esigua, poiché persone non autorizzate possono farlo con elevata precisione anche senza il NAVS, così come possono rubare dati, se riescono a penetrare in (più) banche dati adeguate. Anche la gravità delle potenziali lesioni della personalità derivanti dalla costituzione non autorizzata di profili è impossibile da valutare in modo generale. Essa dipende infatti dal tipo di dati personali che vengono concretamente collegati tra loro: se si tratta di dati generalmente accessibili (quali indirizzi con dati relativi al sesso), gli effetti sono molto meno seri rispetto, ad esempio, a quelli di un collegamento non autorizzato di dati sulla salute con dati su eventuali precedenti penali. In entrambi i casi, però, se le prescrizioni in materia di sicurezza informatica vengono rigorosamente rispettate, la probabilità di realizzazione del rischio è estremamente bassa.

## Misure

*Misure per prevenire le intrusioni indebite*

La sicurezza informatica non è mai il risultato di una singola misura, bensì un processo che richiede l'osservazione e l'adeguamento costanti di diversi fattori. Per evitare che persone non autorizzate («hacker») penetrino in sistemi informatici per spiarli e collegare dati in essi contenuti, i processi e le procedure di sicurezza vanno costantemente aggiornati. Soprattutto quando i sistemi informatici contengono dati personali, occorre che essi siano controllati incessantemente e minuziosamente. In particolare occorre proteggere le banche dati da consultazioni e manipolazioni non autorizzate. Le banche dati e le applicazioni tecniche gestite dalla Confederazione presentano nel complesso un livello di sicurezza relativamente elevato. Lo stesso vale per numerosi sistemi informatici di Cantoni e Comuni. Tuttavia, al di fuori dell'Amministrazione federale vi sono diversi sistemi che non soddisfano pienamente gli attuali standard di sicurezza. Questa situazione va risolta attuando misure di sicurezza: soltanto osservando prescrizioni organizzative, personali, infrastrutturali e tecniche è infatti possibile garantire un livello di sicurezza sufficiente.

Concretamente, questo significa in primo luogo che vanno regolamentate le responsabilità in materia. Per delimitare gli ambiti di competenza, evitando al contempo lacune, le responsabilità dovranno essere disciplinate chiaramente per tutti i compiti essenziali, in particolare nel processo di sicurezza delle informazioni. I collaboratori che impiegano strumenti informatici vanno formati riguardo alla sicurezza dell'infrastruttura informatica. Direttive e istruzioni sulla sicurezza andranno documentate in forma scritta. Occorrerà inoltre valutare regolarmente i rischi nel settore della sicurezza delle informazioni e predisporre un piano di sicurezza dell'informazione e protezione dei dati (SIPD). Per quanto concerne la sicurezza fisica, va garantita innanzitutto la sicurezza dell'accesso ai mezzi informatici e ai supporti di memoria. È inoltre necessario che questi non contengano più né NAVS né altri dati personali prima di essere riparati, smaltiti o distrutti e che tali dati non possano essere ripristinati.

Inoltre occorrerà ridurre al minimo i rischi tecnici di accesso, il che implica procedure di autenticazione e misure di sicurezza informatica adeguate (programmi antivirus, firewall). Il software dovrà essere conforme allo stato della tecnica ed essere regolarmente aggiornato tramite update di sicurezza e di correzione (*patch*). Nel caso delle reti mobili, i dati andranno cifrati con procedure di cifratura conformi al più recente stato della tecnica. L'analisi regolare e sistematica dei dati di protocollo (log) dei computer permette di individuare irregolarità o disturbi nel funzionamento dei sistemi informatici dovute alla mancanza di programmi o a errori nei medesimi oppure a falle di sicurezza. Gli incidenti di sicurezza vanno trattati in modo rapido ed efficiente, al fine di evitare o limitare lo spionaggio, la manipolazione o la distruzione di dati. Per «incidente di sicurezza» s'intende un evento indesiderato che ha ripercussioni sulla sicurezza delle informazioni e può comportare gravi danni. L'esistenza di una procedura predefinita e collaudata per questi casi può concorrere a ridurre i tempi di reazione. È dunque prioritario definire e applicare regolarmente il trattamento degli incidenti di sicurezza.

*Misure per prevenire il trattamento illecito di dati da parte dello Stato*

Il principio di proporzionalità del trattamento dei dati prescrive che i servizi di ogni autorità possano avere accesso in generale soltanto ai dati di loro diretta competenza. Si deve inoltre badare a che siano raccolti unicamente i dati di cui le autorità hanno

effettivamente bisogno. I processi di scambio dei dati non possono essere estesi a piacimento oltre questi limiti. Nel quadro delle attività legislative relative ai singoli registri è importante tenere conto dei principi di base del diritto in materia di protezione dei dati.

I sistemi d'informazione delle varie autorità sono sempre più interconnessi. Laddove esistono basi legali al riguardo, le autorità che vi hanno diritto si scambiano regolarmente informazioni. In primo luogo i sistemi d'informazione di diverse autorità sono collegati tra loro tramite interfacce e in secondo luogo le autorità ricevono diritti di accesso a banche dati di altre autorità, che possono esercitare mediante procedura di richiamo. Per «procedura di richiamo» s'intende una procedura automatizzata che consente a una persona di acquisire autonomamente le informazioni, senza che l'amministrazione ne sia al corrente o debba esserlo. Va inoltre rilevata la tendenza alla concentrazione del trattamento dei dati, concretizzata nel raggruppamento di diversi sistemi d'informazione in un sistema integrato. Questo ha il vantaggio di rendere superflua l'indicazione separata dei dati di base (p. es. quelli personali) per ogni sistema d'informazione, senza che i singoli servizi possano accedere ai dati degli altri servizi. Va poi tenuto presente che il confronto e la trasmissione dei dati avvengono sempre più per via elettronica. Se le autorità hanno la facoltà di utilizzare sistematicamente un identificatore personale generalmente impiegabile nei loro registri, si realizza uno dei presupposti tecnici affinché uno scambio di dati previsto a livello di legge possa essere effettuato in forma automatizzata e quindi più efficiente.

Per evitare che le autorità possano costituire indebitamente profili della personalità, occorrono misure preventive. Si deve ad esempio badare a che la trasmissione e il confronto di dati vengano automatizzati soltanto ove necessario. Inoltre, dato che spetta al legislatore prendere la decisione necessaria in merito, occorre una base legale esplicita che consenta lo scambio di dati in base al NAVS e quindi in forma automatizzata[18]. Un ulteriore strumento consiste nel sorvegliare sistematicamente le interfacce dei sistemi informatici in seno all'amministrazione, il che richiede lo svolgimento periodico di analisi dei rischi.

*Maggiore sicurezza delle informazioni grazie a identificatori personali settoriali?*

Nella perizia[19] menzionata in precedenza l'autore fa presente che nessun sistema è completamente al riparo da attacchi. La perizia descrive inoltre varie possibilità per prevenire il collegamento di banche dati contenenti dati personali (tramite quasi-identificatori o il NAVS). Per eliminare sostanzialmente i timori relativi alla protezione dei dati, il perito raccomanda di reimpostare l'intero sistema delle banche dati, salvando in banche dati separate i dati d'identificazione personale e quelli fattuali. I primi dovrebbero inoltre essere gestiti in modo da evitare ridondanze. Si parla di ridondanza delle informazioni quando dati dal medesimo contenuto sono registrati più volte. Caratteri d'identificazione quali cognome, nome o NAVS di una persona dovrebbero dunque essere salvati in un'unica banca dati. Il collegamento dei dati personali con quelli fattuali dovrebbe essere possibile esclusivamente sulla base di speciali tabelle di collegamento, che andrebbero mantenute segrete («*linkage tables*»). Per contro, la

18 Cfr. art. 32*a*$^{bis}$ cpv. 2 della legge del 20 giugno 1997 sulle armi (LArm; RS **514.54**).
19 Cfr. Basin, *op. cit.*

semplice introduzione di identificatori settoriali senza le menzionate modifiche all'architettura del sistema sarebbe inutile.

*Migliore protezione dei dati nell'ambito dell'utilizzazione di numeri d'identificazione personali da parte di Cantoni, Comuni e terzi*

Le spiegazioni di cui sopra sugli identificatori personali della Confederazione in generale e sul NAVS in particolare valgono per analogia anche per gli identificatori personali dei Cantoni. Questi ultimi hanno tuttavia la competenza di disciplinare autonomamente l'assegnazione e l'utilizzazione sistematica di questi identificatori. Nell'emanare le prescrizioni di diritto in materia di protezione dei dati, i Cantoni devono rispettare il diritto fondamentale alla protezione della sfera privata garantito dall'articolo 13 capoverso 2 Cost., in base al quale sono tenuti ad adottare tutte le misure necessarie per proteggere i dati personali dei cittadini da un impiego abusivo dei loro dati personali.

### 1.1.4 Excursus: utilizzo del numero d'assicurazione sociale statunitense

Si parla spesso dell'ampio utilizzo del numero d'assicurazione sociale statunitense. Negli Stati Uniti l'utilizzazione del *Social Security Number* (SSN) da parte non solo delle autorità ma anche di privati è molto diffusa. Questo è riconducibile a diversi motivi. In primo luogo va tenuto presente che il sistema ufficiale dei documenti d'identità e dei registri degli USA è di competenza dei singoli Stati federali e dunque regolamentato diversamente in ciascuno di essi. Al contempo, questa struttura riflette perfettamente la concezione delle competenze e dei compiti statali: negli USA sarebbe impensabile introdurre un registro centrale in cui siano salvati tutti i dati relativi all'identità e allo stato civile dell'intera popolazione residente. Un tale sistema, ormai standard in numerosi Stati europei, sarebbe infatti considerato una sorveglianza statale eccessiva e non godrebbe nel complesso del consenso necessario. Considerate queste premesse, la *Social Security Card*, su cui è riportato il SSN, è l'unico mezzo d'identificazione uniforme a livello statunitense, dato che in linea di massima tutta la popolazione residente dispone di un SSN. Questo fa sì che si usi spesso la *Social Security Card* o il SSN quale mezzo d'identificazione e regolarmente anche a fini di autenticazione.

Parallelamente, negli USA anche i privati sono autorizzati a utilizzare sistematicamente il SSN. In particolare i gestori delle tre maggiori banche dati sulla solvibilità e sul merito creditizio lavorano con il SSN. Altrettanto vale per le imprese che emettono carte di credito, le banche, le società di leasing e simili, presso le quali i gestori di queste banche dati si procurano regolarmente informazioni. Mediante il SSN, essi costituiscono quindi profili della personalità relativi alla situazione finanziaria di determinati individui per valutarne la solvibilità. Il rischio di furti d'identità legati al SSN va considerato anche in questa prospettiva. Chi finge di avere un'altra identità per ottenere un credito (preferibilmente l'identità di qualcuno con un elevato rating di solvibilità) deve dunque conoscere anche il SSN della sua vittima.

Tutto ciò va preso in considerazione in questa sede, sottolineando la differenza tra la regolamentazione proposta e la situazione negli USA: anche in futuro in Svizzera l'utilizzazione del NAVS dovrà essere preclusa ai privati. Nel nostro Paese, inoltre, contrariamente a quanto avviene negli USA, esiste un sistema dei documenti d'identità e dei registri uniforme a livello nazionale. Questo garantisce che anche in futuro l'autenticazione sarà effettuata soltanto tramite documenti d'identità ufficiali. Di conseguenza, non vi è da temere il rischio di furto di dati o d'identità in seguito a un'utilizzazione più ampia del NAVS da parte delle autorità federali, cantonali e comunali.

## 1.2 Alternative esaminate e opzione scelta

### 1.2.1 Opzione scelta: utilizzazione sistematica del NAVS da parte di tutte le autorità

L'utilizzazione sistematica del NAVS in una collezione di dati personali permette un'identificazione personale univoca, determinando una migliore qualità del complesso dei dati. Gli eventuali rischi a essa connessi possono essere affrontati con misure accettabili. Conferire un'autorizzazione generalizzata alle autorità federali, cantonali e comunali per l'utilizzazione sistematica del NAVS risulta essere una soluzione equilibrata in termini di utilità, attuabilità e proporzionalità. Di seguito sono esposti i diversi punti da approfondire.

*Eliminazione di onerosi errori amministrativi*

La crescita della popolazione e l'incremento dei compiti delle amministrazioni pubbliche comporta un aumento della quantità di dati e di mutazioni. Vi è inoltre un numero sempre maggiore di nomi complessi (p. es. nomi doppi, con caratteri speciali o che devono essere trascritti in caratteri latini). Il loro trattamento manuale richiede più tempo ed è anche suscettibile di errori. L'impiego di un identificatore personale sotto forma di sequenza di cifre contribuisce notevolmente a risolvere questo problema. Questo vale specialmente per l'impiego del NAVS, tanto più che la serie di dati personali della banca dati UPI, accuratamente gestita dall'UCC, è molto affidabile. Tramite le notifiche di SIMIC e Infostar, gli attributi d'identificazione delle persone registrate nella banca dati UPI vengono costantemente aggiornati. L'elevata qualità dei dati della banca dati UPI garantisce pertanto la corretta identificazione di una persona. L'utilizzazione sistematica del NAVS nel quadro del trattamento dei dati contribuirebbe quindi sostanzialmente a evitare equivoci nell'uso di dati personali.

*Maggiore efficienza grazie allo scambio di dati automatizzato tra le autorità*

L'utilizzazione sistematica di un identificatore personale univoco consente uno scambio di dati senza discontinuità mediale tra le autorità. Per «discontinuità mediale» s'intende un cambiamento del mezzo usato quale supporto d'informazione all'interno di un processo di elaborazione di informazioni. Questo interrompe il processo operativo, poiché i dati devono essere trasmessi in una forma diversa da quelli in cui sono stati ricevuti. Un esempio di discontinuità mediale è il caso in cui informazioni disponibili in forma elettronica vengono stampate su carta e rielaborate prima di essere reinserite a mano in un altro sistema informatico. Laddove il legislatore lo permetterà

espressamente, la comunicazione di dati potrà avvenire in modo automatizzato sulla base del NAVS, il che semplificherà i processi interni e trasversali tra le autorità e accrescerà l'efficienza. Questo a sua volta consentirà un impiego efficace ed economico dei fondi pubblici, come richiesto dall'articolo 43*a* capoverso 5 Cost. e dall'articolo 12 capoverso 4, secondo periodo della legge federale del 7 ottobre 2005[20] sulle finanze della Confederazione (LFC). Si risparmieranno inoltre fondi pubblici grazie al fatto che verrà meno l'onere legislativo per l'adeguamento delle leggi speciali a livello federale, cantonale e comunale.

Anche i collegamenti di dati previsti dal legislatore, e quindi legittimi (p. es. a fini statistici[21]), danno risultati più precisi, se possono essere svolti con un identificatore personale univoco.

*Prevenzione degli scambi d'identità*

Anche per i singoli cittadini, in particolare quelli con nomi molto diffusi, l'utilizzazione sistematica del NAVS comporta un valore aggiunto: ogni persona di cui sono raccolti dati personali ha diritto a che i processi amministrativi si svolgano senza scambi d'identità con altre persone registrate. Tali scambi d'identità possono causare notevoli inconvenienti agli interessati. Essi derivano di regola da una tenuta del registro incompleta, da errori di ortografia nella registrazione o dalla forte diffusione di un nome o di una combinazione di nomi. Dei 2 330 700 allacciamenti telefonici privati figuranti nell'elenco telefonico ufficiale svizzero, ad esempio, circa 950 sono registrati sotto il nome Peter Müller. L'aggiunta di un identificatore personale univoco per la registrazione in una banca dati permette di scongiurare il rischio di scambi d'identità. La migliore qualità del complesso di dati nei registri degli utenti contribuisce all'esattezza dei dati e funge quindi da importante elemento della protezione della personalità nell'ambito del trattamento di dati personali (cfr. n. 1.1.3).

*Mantenimento della possibilità di utilizzare numeri settoriali*

Con la presente revisione rimarrà possibile vietare l'utilizzazione sistematica del NAVS nelle leggi speciali, al fine di poter escludere qualsiasi rischio residuo di costituzione non autorizzata di profili della personalità per i settori con dati particolarmente sensibili.

*Misure di accompagnamento e regolari analisi dei rischi*

Per applicare le misure di accompagnamento, gli utenti del NAVS saranno tenuti ad aggiornare regolarmente i loro sistemi d'informazione. Il disegno di legge comporterà dunque anche un aumento generale della sicurezza delle informazioni nell'Amministrazione pubblica. Se le analisi dei rischi saranno svolte regolarmente e le misure di accompagnamento attuate rigorosamente, l'utilizzazione sistematica del NAVS non pregiudicherà la protezione dei dati né creerà «cittadini trasparenti».

20 RS **611.0**

21 I collegamenti a fini statistici sono realizzati in virtù dell'art. 14*a* della legge del 9 ottobre 1992 sulla statistica federale (RS **431.01**), dell'art. 14 dell'ordinanza del 30 giugno 1993 sulle rilevazioni statistiche (LStat; RS **431.012.1**) e dell'ordinanza del 17 dicembre 2013 sul collegamento di dati (RS **431.012.13**).

### 1.2.2 Alternative esaminate

*Procedura di autorizzazione*

In un sistema che prevedesse un obbligo di autorizzazione per l'utilizzazione sistematica del NAVS, questa sarebbe rilasciata non dal legislatore, bensì mediante decisione da un'autorità preposta, che dovrebbe verificare in ogni caso specifico se l'autorità che richiede l'utilizzazione sistematica del NAVS sia in grado di garantire la protezione dei dati e la sicurezza delle informazioni. L'autorità richiedente dovrebbe dimostrare in particolare di essere in grado di applicare le necessarie misure tecniche e organizzative. L'autorità preposta al rilascio dell'autorizzazione dovrebbe inoltre verificare, tramite controlli a campione periodici presso i titolari dell'autorizzazione, se questi continuino a soddisfare le condizioni richieste e adempiano gli obblighi di diligenza e collaborazione. L'instaurazione di un tale sistema comporterebbe maggiori oneri amministrativi e spese elevate, che non sarebbero adeguatamente compensati da benefici supplementari, tanto più che i sistemi informatici sono per loro natura soggetti a costanti cambiamenti e che un'autorizzazione potrebbe essere rilasciata solo in base a un'istantanea della situazione in quel dato momento. Considerato inoltre l'elevato grado di conformità alla legge delle autorità federali, cantonali e comunali, appare opportuno rinunciare a onerosi meccanismi di controllo e sorveglianza, puntando invece sul principio dell'autocontrollo.

*Numeri settoriali*

È stata vagliata anche l'introduzione di un sistema con identificatori personali settoriali. In un tale sistema, a ogni persona fisica da registrare verrebbero assegnati più identificatori, i quali sarebbero utilizzati esclusivamente per l'attività amministrativa nei rispettivi settori, ad esempio in quello fiscale o in quello delle assicurazioni sociali. Per consentire una comunicazione elettronica efficiente tra due organi amministrativi di diversi settori, occorrerebbe però un server centrale per l'identificazione e la comunicazione. Dato che l'attuale struttura amministrativa non prevede tali settori, questi andrebbero innanzitutto creati. In occasione della procedura di consultazione sull'avamprogetto della legge federale sugli identificatori personali settoriali (legge SPIN), nel 2004, la maggior parte dei Cantoni e delle organizzazioni attive nel governo elettronico e nell'amministrazione elettronica ha ritenuto la settorializzazione troppo complessa e costosa nonché soggetta a errori e, dunque, difficilmente attuabile.

Anche oggi un'introduzione generalizzata di identificatori settoriali o altri identificatori personali alternativi non sarebbe auspicabile per numerose autorità federali, cantonali e comunali, per le quali sarebbe troppo costosa e non concorrerebbe in alcun modo a ridurre i rischi. Per alcune autorità, l'introduzione di un tale sistema sarebbe addirittura un passo indietro, tanto più che esse hanno già adottato disposizioni ed effettuato investimenti confidando nel mantenimento della normativa vigente (con il NAVS quale identificatore personale univoco per le autorità). Considerate queste circostanze, l'introduzione di un sistema globale basato su identificatori personali settoriali non è da approvare. Se in un determinato settore si auspicasse l'impiego di un identificatore personale specifico, questo resterebbe comunque possibile anche con il presente disegno.

## 1.3 Rapporto con il programma di legislatura e con le strategie del Consiglio federale

### 1.3.1 Rapporto con il programma di legislatura

Il progetto non è annunciato né nel messaggio del 27 gennaio 2016[22] sul programma di legislatura 2015–2019, né nel decreto federale del 14 giugno 2016[23] sul programma di legislatura 2015–2019. Contribuisce però all'attuazione della Strategia di e-government Svizzera (cfr. n. 4.2), la quale rientra tra gli affari previsti da detto programma di legislatura.

### 1.3.2 Rapporto con le strategie del Consiglio federale

Con l'adozione della Strategia di e-government Svizzera[24], il Consiglio federale intende migliorare i servizi offerti all'economia e alla popolazione e l'efficienza dell'amministrazione. Lo strumento di attuazione di tale strategia è rappresentato dalle Linee guida 2017–2019[25], le quali contemplano 11 obiettivi operativi. Il settimo obiettivo operativo è così formulato: «Garantire l'attribuzione di dati su una determinata persona nello scambio telematico tra sistemi informatici entro il 2019». Nella formulazione dell'obiettivo si legge inoltre che finora non è stato ancora possibile definire un identificatore univoco delle persone utilizzabile in tutti i settori specialistici e a tutti i livelli statali e che pertanto sussiste una significativa necessità d'intervento al riguardo. In questo senso, il progetto contribuisce all'attuazione della Strategia di e-government Svizzera.

Le menzionate linee guida prevedono inoltre l'introduzione di un'identità elettronica (eID; obiettivo operativo n. 5). L'identificazione sicura delle persone costituisce la base per la certezza del diritto. Il disegno di legge federale sui mezzi d'identificazione elettronica riconosciuti (legge sull'eID)[26] approvato dal nostro Consiglio è inteso a promuovere la sicurezza nelle comunicazioni elettroniche tra cittadini e autorità e tra privati cittadini. Affinché sia possibile svolgere in rete anche transazioni più complesse, i partner contrattuali devono poter confidare nell'identità della controparte. Al fine di soddisfare questa esigenza, in Svizzera saranno creati mezzi d'identificazione elettronica riconosciuti per le persone fisiche. Un numero di registrazione eID indipendente dall'AVS serve a collegare la persona in questione con l'eID rilasciata.

Il piano relativo all'eID prevede una ripartizione dei compiti tra Stato e privati: la Confederazione non rilascerà un'eID propria, ma potrà riconoscere ufficialmente le eID di operatori privati (come la SuisseID della Posta) che adempiono i requisiti di

22 FF **2016** 909
23 FF **2016** 4605
24 La strategia è disponibile all'indirizzo https://www.egovernment.ch/it/umsetzung/e-government-strategie/.
25 Le linee guida sono disponibili all'indirizzo https://www.egovernment.ch/it/umsetzung/schwerpunktplan1.
26 FF **2018** 3375

legge. Con il riconoscimento, gli operatori che offrono servizi identitari (Identity Provider, IdP) vengono autorizzati a utilizzare dati per l'identificazione delle persone gestiti e confermati dallo Stato per la fornitura dei loro servizi. Pertanto, gli IdP saranno autorizzati a utilizzare il NAVS – solo e soltanto – per questo scopo. Per il resto, saranno autorizzati a comunicare il NAVS soltanto ai gestori di servizi che impiegano eID direttamente autorizzati a utilizzare sistematicamente il NAVS. Il fatto che gli IdP non sono un'autorità e non adempiono nemmeno compiti pubblici in senso stretto non deve escludere l'utilizzazione sistematica del NAVS da parte loro. Il presente progetto legislativo non compromette dunque l'auspicata introduzione di un'eID nella forma esposta.

### 1.4 Interventi parlamentari

L'analisi dei rischi richiesta nel postulato 17.3968 Piano di sicurezza per gli identificatori personali, della Commissione degli affari giuridici del Consiglio nazionale, è svolta nel quadro del presente messaggio (n. 1.1.3). Si propone dunque lo stralcio dal ruolo del postulato.

## 2 Procedura preliminare, in particolare procedura di consultazione

### 2.1 Parere della Commissione federale AVS/AI

La Commissione federale AVS/AI è per principio d'accordo con un ampliamento generalizzato dell'utilizzazione sistematica del NAVS da parte delle autorità federali, cantonali e comunali nel quadro dell'adempimento dei loro compiti legali. La Commissione ha tuttavia tenuto a precisare che il nuovo disciplinamento dovrebbe essere impostato nel modo più trasparente possibile.

### 2.2 Procedura di consultazione

Il 7 novembre 2018 il nostro Consiglio ha incaricato il Dipartimento federale dell'interno (DFI) di svolgere una procedura di consultazione sull'avamprogetto di modifica della LAVS. In una lettera della stessa data, il DFI ha quindi invitato i Cantoni, i partiti politici rappresentati nell'Assemblea federale, le associazioni mantello dell'economia e altre associazioni e organizzazioni a esprimersi sull'avamprogetto di legge entro il 22 febbraio 2019. Una sintesi dettagliata dei risultati della procedura di consultazione è proposta nel rapporto sui risultati[27].

In linea di massima, la maggior parte dei partecipanti alla consultazione ha approvato l'introduzione di una norma permissiva generale a favore delle autorità. Su determi-

27 www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione concluse > 2019 > Dipartimento federale dell'interno.

nati punti, però, i pareri sono risultati discordanti. Alcuni partecipanti si sono dichiarati contrari alla regolamentazione delle misure tecniche e organizzative a livello di legge. Per taluni, inoltre, la proposta disposizione sull'analisi dei rischi è superflua, tanto più che già nel quadro dei vigenti piani di protezione dei dati è previsto di tener conto di eventuali rischi legati ai collegamenti. Quasi tutti i partecipanti si sono opposti all'inasprimento della disposizione penale sulle misure tecniche e organizzative, ritenendo che questo comporterebbe problemi di delimitazione irrisolvibili. In seguito alla consultazione, abbiamo deciso di modificare l'avamprogetto, rinunciando a tale inasprimento. Per il resto, il disegno differisce dall'avamprogetto soltanto in alcuni punti di carattere redazionale.

## 3 Diritto comparato

Da un breve esame degli ordinamenti giuridici di altri Stati emerge che gli identificatori personali possono essere disciplinati in modo molto eterogeneo. Se nel sistema austriaco è utilizzato un numero di base criptato per ogni persona, da cui deriva un identificatore personale specifico per settore, la Svezia e altri Paesi scandinavi prevedono un unico identificatore personale applicabile in tutti gli ambiti della vita, sia a livello privato che pubblico. Per quanto concerne gli Stati Uniti, invece, l'ampio utilizzo del numero d'assicurazione sociale deriva dal fatto che esso è l'unico numero d'identificazione uniforme a livello statunitense (cfr. n. 1.1.4).

## 4 Punti essenziali del progetto

### 4.1 La normativa proposta

Le autorità federali, cantonali e comunali dovranno poter utilizzare sistematicamente il NAVS per l'adempimento dei compiti assegnati loro dalla legge senza doversi fondare su una legge speciale. L'autorizzazione all'utilizzazione sistematica dovrà risultare già dalla pertinente disposizione della LAVS, con la quale sarà introdotta una norma permissiva generale per le autorità. In futuro, dunque, per principio non ci sarà più bisogno di alcuna norma permissiva in una legge speciale per ogni singolo scopo di utilizzazione e utente. Tuttavia, il legislatore continuerà ad avere la facoltà di creare identificatori personali settoriali specifici e di vietare l'impiego sistematico del NAVS in un determinato settore.

Le istituzioni non aventi carattere di autorità e alle quali è stato affidato per legge l'adempimento di un compito pubblico necessiteranno invece, come finora, di un'autorizzazione mediante legge speciale per utilizzare il NAVS. Autorizzazioni in tal senso già previste dal diritto vigente in virtù di una legge speciale saranno mantenute, ma con adeguamenti redazionali ad alcune disposizioni. L'autorizzazione all'utilizzazione sistematica da parte delle istituzioni preposte all'educazione rimarrà disciplinata – come già nel diritto vigente – a livello di legislazione AVS, anche se la nuova normativa comprenderà tutte le istituzioni, dato che queste adempiono sia obblighi in materia di assicurazioni sociali che compiti nell'ambito delle statistiche federali.

L'utilizzazione sistematica a livello prettamente privato dovrà invece continuare a essere esclusa. Inoltre, andrà data la dovuta importanza alle misure di sicurezza (per i dettagli al riguardo, cfr. le spiegazioni al n. 4.2).

## 4.2 Misure di accompagnamento

Il diritto vigente contempla già prescrizioni concernenti misure di sicurezza organizzative, personali, infrastrutturali e tecniche, contenute in un'ordinanza dipartimentale[28]. In futuro, i principi fondamentali in materia saranno sanciti a livello di legge. Si tratta di disciplinare le responsabilità, la formazione e la documentazione in materia di sicurezza informatica e di prevedere misure intese a ridurre i rischi di accesso indebito (cfr. l'analisi dei rischi al n. 1.1.3). In futuro si esigerà che chi utilizza sistematicamente il NAVS predisponga un piano SIPD. Inoltre, la Confederazione e i Cantoni saranno tenuti a svolgere analisi dei rischi al fine di individuare ed evitare i rischi di unioni illecite di banche dati, in particolare mediante interfacce, basandosi sugli elenchi delle banche dati in cui il NAVS è utilizzato sistematicamente.

Per quanto riguarda lo scambio di dati, il presente progetto non comporta modifiche alle pertinenti disposizioni, né attribuzioni di nuovi diritti di accesso. Non vi sarà quindi alcun ampliamento degli attuali diritti di consultazione, comunicazione e trattamento. Affinché vi sia uno scambio di dati tra le autorità sulla base del NAVS, occorrerà una base legale esplicita.

Le vigenti regolamentazioni di diritto penale resteranno invariate a livello di contenuto: chi utilizzerà sistematicamente il NAVS senza esservi autorizzato sarà punito con una pena pecuniaria, come avviene già oggi. Il fatto di non adottare misure tecniche e organizzative continuerà a essere considerato quale contravvenzione e sarà punito con la multa.

## 4.3 Nessun obbligo di reimpostare l'architettura delle banche dati

Dalla perizia menzionata in precedenza[29] emerge che le serie di dati di diverse banche dati possono essere collegate con un grado di esattezza del 99,98 per cento anche solo in base ai quasi-identificatori cognome, nome e data di nascita. L'incremento di precisione derivante dall'utilizzazione sistematica del NAVS non sarebbe quindi decisiva per la protezione dei dati. Secondo la perizia i problemi di fondo legati al diritto in materia di protezione dei dati non sarebbero risolti con l'introduzione di numeri settoriali, poiché essi sono insiti nell'architettura delle banche dati, in quanto in una stessa banca dati sono salvati sia dati personali che dati fattuali. Dal punto di vista della protezione delle informazioni, tuttavia, sarebbe ideale impostare un sistema informatico in modo tale che i dati personali siano preservati da ridondanze e salvati in

28 Ordinanza del DFI del 7 novembre 2007 sugli standard minimi delle misure tecniche e organizzative per l'utilizzazione sistematica del numero d'assicurato AVS al di fuori dell'AVS (RS **831.101.4**).

29 Cfr. Basin, *op. cit.*

una banca dati a sé stante, separatamente dai dati fattuali di una persona. Attributi quali cognome, nome, data di nascita e NAVS andrebbero registrati in un'unica banca dati. Il collegamento dei dati personali con quelli fattuali dovrebbe essere reso possibile esclusivamente sulla base di speciali tabelle di collegamento, che andrebbero mantenute segrete («*linkage tables*»).

Una tale reimpostazione dell'architettura del sistema non metterebbe fondamentalmente in discussione lo scambio di dati, ma gli attributi non potrebbero più essere memorizzati a livello decentralizzato e per accedere ai dati si dovrebbe dunque sempre passare per la banca dati centralizzata che contiene questi attributi. In questo modo il traffico di rete e gli accessi alle banche dati aumenterebbero, il che accrescerebbe le probabilità di errori. Sempre secondo la perizia, le banche dati sono "colli di bottiglia" e sistemi critici che vanno tenuti costantemente disponibili. L'impostazione e l'applicazione di un tale sistema sarebbero molto onerose e genererebbero ingenti spese per la Confederazione, i Cantoni e i Comuni. Le esperienze fatte con il *millennium bug* hanno dimostrato che anche solo piccoli cambiamenti nei formati dei dati e nella maniera di salvare ed elaborare i dati possono generare spese molto elevate. Inoltre, l'eliminazione delle ridondanze comporterebbe anche difficoltà nella gestione operativa delle banche dati interessate: senza ridondanze sarebbe infatti più difficile individuare e correggere eventuali errori di registrazione o elaborazione dei dati da parte degli utenti. In caso di perdita dei dati, inoltre, non si potrebbe più ricorrere a copie ridondanti, il che renderebbe necessari ancora più backup del solito. Inoltre, l'assenza di ridondanze renderebbe difficili le prove di coerenza, poiché non sarebbe possibile alcun confronto con altre banche dati (ridondanti).

L'applicazione vincolante su larga scala dell'architettura con una gestione dei dati separata comporterebbe pertanto numerosi svantaggi e spese elevate. Se è vero che in alcuni casi, in campi d'applicazione chiusi (p. es. nel settore sanitario), al momento dell'allestimento di nuove banche dati sarebbe ragionevole predisporre un'architettura con una gestione dei dati minima, è anche vero che ciò sarebbe ragionevole solo se una tale struttura potesse essere introdotta completamente da zero per un campo d'applicazione ampio. Di regola, si tratta però soltanto di creare singole banche dati o di aggiungere nuovi attributi a quelle già esistenti. Per questi motivi (difficoltà operative e scarso valore aggiunto, nonché spese elevate), la legge non imporrà agli utenti del NAVS di reimpostare completamente l'architettura delle loro banche dati. Essi avranno comunque la possibilità di predisporre una gestione dei dati separata, se lo riterranno utile e fattibile.

## 4.4 Mantenimento delle disposizioni concernenti l'obbligo del segreto delle autorità e la comunicazione di dati

Il diritto pubblico svizzero prescrive in generale alle autorità di mantenere segreti i dati personali di cui dispongono. Sono possibili eccezioni al segreto d'ufficio soltanto in presenza di una disposizione legale che autorizzi espressamente le autorità a comunicare dati ad altre autorità oppure a confrontare dati personali con altre autorità. Il

progetto sull'utilizzazione sistematica più ampia del NAVS non modifica questi principi né crea nuove basi legali per la rilevazione o la comunicazione di dati. Laddove la legge consente la comunicazione di dati tramite interfacce, il NAVS potrà essere scambiato quale informazione supplementare soltanto in presenza di una base legale formale che autorizzi un tale scambio. Già nel diritto vigente questo è previsto in determinati settori, come stabilisce ad esempio l'articolo 32*a*bis della legge del 25 giugno 1997[30] sulle armi. Analogamente, la proposta normativa sull'utilizzazione sistematica del NAVS non accrescerà il numero di collegamenti di dati ammessi dalla legge. Come sinora, essi continueranno a essere ammessi soltanto nei casi in cui ciò sia previsto da una base legale formale, come ad esempio nella LStat o nella legge del 22 giugno 2007[31] sul censimento.

## 4.5 Compatibilità tra compiti e finanze

Per finanziare l'ampliamento dell'utilizzazione del NAVS al di fuori dell'AVS potranno essere riscossi emolumenti al fine di coprire le modeste spese che ne deriveranno. Una descrizione dettagliata delle possibili ripercussioni del disegno è presentata ai relativi capitoli (n. 6.1 e 6.2).

## 4.6 Attuazione

Come finora, l'UCC dovrà poter riscuotere emolumenti per l'utilizzazione sistematica del NAVS. I dettagli saranno disciplinati a livello d'ordinanza. Anche in futuro dovranno rimanere possibili eccezioni all'obbligo di pagare emolumenti. Sono inoltre ipotizzabili rimborsi forfettari da parte dei Cantoni in funzione della frequenza di utilizzo.

Le analisi dei rischi che le unità della Confederazione e dei Cantoni di cui all'articolo 153*e* capoverso 1 D-LAVS dovranno svolgere regolarmente potranno essere effettuate nel quadro dei controlli già previsti per la protezione dei dati, aggiungendo ai punti di verifica l'utilizzazione sistematica del NAVS. A livello federale, la tenuta degli elenchi in vista dell'analisi dei rischi secondo l'articolo 153*e* capoverso 2 D-LAVS incomberà ai dipartimenti. A livello cantonale e comunale, spetterà ai singoli Cantoni e Comuni stabilire questa responsabilità.

Le misure di accompagnamento da applicare nell'utilizzazione sistematica del NAVS sono attualmente sancite nell'ordinanza dipartimentale. In futuro i pertinenti principi saranno elevati a rango di legge.

30 RS **514.54**
31 RS **431.112**

# 5 Commento ai singoli articoli

## 5.1 Legge federale sull'assicurazione per la vecchiaia e per i superstiti

*Art. 49a lett. g*

L'assegnazione di un NAVS comporta un'iscrizione nel registro centrale di cui all'articolo 71 capoverso 4 lettera a LAVS. Non se ne può però automaticamente dedurre che la persona in questione sia assicurata nell'AVS. L'espressione «numero d'assicurato» viene pertanto sostituita con «numero AVS».

Si fa inoltre presente che, nel quadro della revisione totale[32] della legge del 19 giugno 1992[33] sulla protezione dei dati (LPD), è stata richiesta la soppressione della nozione di «profilo della personalità». Al termine dei dibattiti parlamentari, si dovrà badare a che i due oggetti siano coordinati tra loro ed eventualmente modificare di conseguenza la frase introduttiva di questo articolo.

*Art. 50d–50g*

Questi articoli vengono abrogati, dato che la regolamentazione dell'utilizzazione sistematica del NAVS al di fuori dell'AVS è ripresa in una nuova parte quarta della LAVS.

*Art. 87 ottavo comma e 88 quarto comma*

Queste disposizioni vengono abrogate, dato che le disposizioni penali figureranno nella parte quarta della LAVS.

*Art. 89*

La responsabilità solidale delle imprese contrasta con il principio del diritto penale secondo cui la multa è assolutamente personale e non può essere ascritta ad altri. Essa costituisce dunque una forma occulta di responsabilità penale dell'impresa. L'articolo 79 della legge federale del 6 ottobre 2000[34] sulla parte generale del diritto delle assicurazioni sociali (LPGA), le cui disposizioni sono applicabili alla prima parte della LAVS (art. 1 cpv. 1 LAVS), rimanda in particolare all'articolo 6 della legge federale del 22 marzo 1974[35] sul diritto penale amministrativo (DPA), che si applica in caso di infrazioni commesse nell'azienda. L'articolo 89 LAVS può pertanto essere abrogato.

32 Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati; FF **2017** 5939.
33 RS **235.1**
34 RS **830.1**
35 RS **313.0**

*Titolo dopo l'art. 153a*

Parte quarta: Utilizzazione sistematica del numero AVS al di fuori dell'AVS

Le attuali disposizioni in materia figurano nella parte prima (Assicurazione), capo quarto (Organizzazione). Dal punto di vista della sistematica, questo non è ideale dato che esse non trattano dell'AVS e della sua organizzazione, bensì dell'utilizzazione del NAVS in settori estranei all'AVS. Nell'interesse della trasparenza legislativa e della reperibilità delle disposizioni giuridiche, l'utilizzazione sistematica del NAVS quale identificatore personale al di fuori dell'AVS deve essere regolamentata in una parte a sé stante della LAVS. Immediatamente prima delle disposizioni finali si introduce pertanto una nuova parte quarta (art. 153*b* segg.), contenente le disposizioni sull'utilizzazione sistematica del NAVS quale identificatore personale al di fuori dell'AVS.

*Art. 153b* Definizione

Questa disposizione stabilisce la definizione legale dell'utilizzazione sistematica, attualmente contenuta nell'articolo 134$^{bis}$ dell'ordinanza del 31 ottobre 1947[36] sull'assicurazione per la vecchiaia e per i superstiti (OAVS). Vista la sua importanza, è giustificato inserirla nella legge. Sul piano materiale non vi saranno modifiche. L'utilizzazione è considerata «sistematica» quando il numero in questione è dati personali sono collegati con il numero in questione e l'utilizzazione concerne un gruppo di persone fisiche chiaramente definito. Il criterio decisivo è se la parte essenziale e caratterizzante del NAVS sarà registrata in una collezione di dati e ivi durevolmente salvata, oppure no. In questo modo si potrà evitare che tramite modifiche sistematiche dei numeri completi in base a sistemi propri (p. es. lasciar via il codice Paese 756 nelle prime tre posizioni del numero a 13 cifre, completare il numero con una lettera o un'altra cifra oppure cifrarlo) si eluda il controllo dell'utilizzo voluto dal legislatore.

*Art. 153c* Aventi diritto

*Cpv. 1*: questo capoverso definisce i possibili aventi diritto.

*Lett. a n. 1 e 2:* questi numeri si riferiscono al livello federale. La formulazione si basa sulla struttura dell'articolo 2 capoversi 1–3 della legge del 21 marzo 1997[37] sull'organizzazione del Governo e dell'Amministrazione (LOGA), che distingue tra unità amministrative centralizzate e decentrate dell'Amministrazione federale.

*N. 3:* a livello cantonale e comunale, è determinante l'appartenenza o meno di un'unità all'amministrazione. Le unità intercantonali o sovracomunali sono esterne all'amministrazione. Nel loro caso, dunque, per consentire l'autorizzazione all'utilizzazione sistematica del NAVS andrebbe menzionata nel contratto intercantonale o intercomunale sul quale esse si fondano una base giuridica in tal senso secondo il numero 4 (cfr. sotto).

36 RS **831.101**
37 RS **172.010**

*N. 4:* questo numero comprende tutte le persone e organizzazioni di diritto pubblico o privato che adempiono compiti amministrativi, senza però appartenere né all'Amministrazione centrale né a quella decentralizzata. Per poter svolgere i compiti amministrativi affidati loro utilizzando sistematicamente il NAVS, queste persone e organizzazioni necessitano di un'autorizzazione a tal fine nella pertinente legge speciale. Quale esempio concreto si possono menzionare i fornitori riconosciuti di prestazioni dell'assicurazione obbligatoria delle cure medico-sanitarie e dell'assicurazione obbligatoria contro gli infortuni. Essi sono incaricati per legge dell'esecuzione delle menzionate assicurazioni sociali, benché non appartengano né all'Amministrazione federale né alle amministrazioni cantonali. Per questo, anche in futuro dovranno avere il diritto all'utilizzazione sistematica del NAVS, già previsto nelle pertinenti leggi speciali. Lo stesso vale per analogia per l'esecuzione della previdenza professionale: anche gli istituti di previdenza dovranno poter utilizzare sistematicamente il NAVS, come previsto attualmente. Le vigenti disposizioni in materia resteranno invariate.

*N. 5:* attualmente le istituzioni preposte all'educazione sono autorizzate all'utilizzazione sistematica del NAVS in virtù dell'articolo 50*e* capoverso 2 lettera d LAVS. Questa possibilità dovrà valere anche in futuro, anche perché tali istituzioni fungono da organi ausiliari dell'AVS. Gli studenti delle scuole universitarie, come pure gli allievi di livello secondario II (formazione professionale duale o formazione professionale a tempo pieno) e quelli di livello terziario che non frequentano scuole universitarie (formazione professionale superiore) sono soggetti all'obbligo di contribuzione AVS. Nella loro funzione di organi ausiliari dell'AVS, le istituzioni preposte all'educazione in questione trasmettono alle casse di compensazione le necessarie notifiche relative agli studenti, ed eventualmente si occupano anche dell'incasso dei contributi (art. 29$^{bis}$ e 29$^{ter}$ OAVS). Affinché i contributi pagati possano essere accreditati correttamente agli interessati, nel trasmettere i dati occorre utilizzare il NAVS. Inoltre, le scuole con piani di studi particolari (scuole speciali) utilizzano il NAVS nel quadro dell'assicurazione invalidità. Infine, in alcuni Cantoni gli allievi sono assicurati contro gli infortuni tramite le scuole.

D'altro canto, le istituzioni preposte all'educazione devono adempiere anche compiti di natura statistica in ambito educativo, quindi al di fuori dell'AVS. Anche per queste rilevazioni viene utilizzato il NAVS. È pertanto ragionevole che anche in futuro sia le istituzioni preposte all'educazione a livello cantonale sia quelle della Confederazione siano autorizzate all'utilizzazione sistematica del NAVS per l'adempimento dei loro compiti statistici.

*Lett. b:* contrariamente all'esecuzione dell'assicurazione sociale malattie e dell'assicurazione obbligatoria contro gli infortuni, quella delle assicurazioni complementari, disciplinate dal diritto privato, non è un compito dell'Amministrazione pubblica. Tuttavia esistono numerosi legami tra le assicurazioni complementari, da un lato, e l'assicurazione obbligatoria contro gli infortuni e l'assicurazione malattie obbligatoria, dall'altro. Le attività esecutive in questi ambiti non possono pertanto essere considerate in modo isolato. Per questo motivo, già nel diritto vigente l'articolo 47*a* della legge del 2 aprile 1908[38] sul contratto d'assicurazione (LCA) autorizza i fornitori di

38 RS **221.229.1**

assicurazioni complementari all'utilizzazione sistematica del NAVS, e dovrà continuare a farlo anche in futuro. Si tratta di una regolamentazione eccezionale, in quanto consente a privati di utilizzare sistematicamente il NAVS per lo svolgimento di un'attività disciplinata dal diritto privato.

Per il resto, il NAVS continuerà a non poter essere utilizzato per scopi prettamente privati, anche qualora le persone interessate acconsentano all'utilizzazione sistematica del loro NAVS da parte di privati. Questo divieto è giustificato dal fatto che l'UCC non può imporre nella stessa misura ai privati i confronti di dati e le correzioni previsti dall'articolo 153*f* lettere b e c al fine di garantire la qualità dei dati. Ma è soprattutto il rischio di collegamenti illeciti in caso di utilizzazione sistematica da parte di privati a essere nettamente superiore a quello in caso di utilizzo da parte di autorità. Lo stesso vale per il rischio di accessi non autorizzati alle collezioni di dati di privati. Nell'ottica della protezione dei dati e della sicurezza delle informazioni, va dunque respinta un'utilizzazione sistematica del NAVS da parte di privati.

*Cpv. 2*: per determinati ambiti il legislatore dovrà continuare a prevedere altri identificatori personali al posto del NAVS. Anche in futuro, pertanto, avrà la possibilità di escludere l'utilizzazione sistematica del NAVS in singoli ambiti, in particolare quelli in cui sono utilizzati dati personali degni di particolare protezione ai sensi dell'articolo 3 lettera c LPD. Si tratta dei dati concernenti opinioni o attività religiose, filosofiche, politiche o sindacali, la salute, la sfera intima o l'appartenenza a una razza, le misure di aiuto sociale, i procedimenti o le sanzioni amministrative e penali.

*Art. 153d* Misure tecniche e organizzative

Le autorità, organizzazioni e persone autorizzate all'utilizzazione sistematica del NAVS dovranno adottare le misure tecniche e organizzative necessarie per garantire la sicurezza delle informazioni e la protezione dei dati e prevenire così una loro utilizzazione abusiva. Questo articolo riunisce gli obblighi in parte previsti nella vigente ordinanza del DFI del 7 novembre 2007[39] sugli standard minimi delle misure tecniche e organizzative per l'utilizzazione sistematica del numero d'assicurato AVS al di fuori dell'AVS. Con la presente revisione, essi vengono inseriti nella legge e aggiornati.

Gli obblighi di diligenza servono a prevenire un'utilizzazione abusiva del NAVS. Le autorità, organizzazioni e persone autorizzate all'utilizzazione sistematica del NAVS dovranno costantemente provvedere a che gli standard di sicurezza applicabili siano rispettati. I sistemi dovranno quindi essere sempre conformi alle prescrizioni vigenti e, se del caso, andranno adeguati di conseguenza.

*Lett. a:* questa lettera stabilisce che i diritti di accesso alle banche dati contenenti il NAVS possono essere concessi solo ai collaboratori che ne necessitano per l'adempimento dei loro compiti. Le autorizzazioni necessarie vanno accordate in misura restrittiva.

*Lett. b:* va designata una persona responsabile per l'utilizzazione sistematica del NAVS. Essa deve prendere atto in modo comprovabile del piano SIPD di cui alla lettera d. Deve inoltre avere la competenza di far applicare le misure necessarie secondo questo piano.

39 RS **831.101.4**

*Lett. c:* il NAVS non può essere utilizzato per scopi diversi da quelli previsti nell'ambito dello svolgimento dei compiti né trasmesso illecitamente a terzi. Le persone con diritto di accesso vanno informate, attraverso misure di formazione e perfezionamento adeguate, del fatto che il NAVS può essere utilizzato unicamente per lo svolgimento dei compiti ed essere comunicato a terzi solo se le prescrizioni legali lo consentono.

*Lett. d:* le autorità, organizzazioni e persone autorizzate all'utilizzazione sistematica del NAVS devono provvedere a che i gestori dei loro mezzi informatici e supporti di memoria predispongano un piano di sicurezza dell'informazione e protezione dei dati (SIPD) che descriva le singole misure di sicurezza e protezione dei dati. Il piano SIPD deve menzionare e analizzare i fattori di rischio rilevanti in base ai criteri di disponibilità, confidenzialità, integrità e tracciabilità e specificare con quali misure concrete vanno adempiuti i requisiti in materia di sicurezza delle informazioni e protezione dei dati. Le misure d'implementazione concernono l'infrastruttura, l'organizzazione, la formazione del personale e l'adeguamento di hardware e software.

Da un lato, occorre garantire fisicamente la sicurezza dell'accesso ai mezzi informatici e ai supporti di memoria. Se sono impiegati mezzi informatici e supporti di memoria portatili si deve garantire, mediante procedure di cifratura conformi allo stato della tecnica, che le persone non autorizzate non possano accedere ai dati.

Dall'altro, l'accesso ai mezzi informatici e ai supporti di memoria deve essere protetto mediante misure di sicurezza informatiche supplementari, conformi allo stato della tecnica e al livello di rischio. Queste misure devono comprendere come minimo l'impiego di programmi usuali nel commercio e aggiornati, in grado di individuare ed eliminare programmi maligni (programmi antivirus) e di un sistema firewall (centrale o locale). Chi è autorizzato ad accedere a mezzi informatici e supporti di memoria deve prima autenticarsi. Se a tal fine è prevista una password, questa deve rimanere segreta: non può essere trasmessa e va immediatamente modificata se si sospetta che persone non autorizzate ne siano venute a conoscenza. Nei mezzi informatici vanno inoltre installati il più rapidamente possibile i più recenti update di correzione (*patch*) del sistema operativo e delle applicazioni. Attività ed eventi importanti nei sistemi informatici vanno registrati e analizzati regolarmente. È inoltre necessario che i mezzi informatici e i supporti di memoria non contengano più né NAVS né altri dati personali prima di essere riparati, smaltiti o distrutti e che questi non possano essere ripristinati.

Infine, quando si trasmettono dati attraverso reti pubbliche, si corre il rischio che i dati giungano a persone cui non sono destinati. Per «pubblica» s'intende ogni rete che non è riservata a una cerchia di utenti definita in modo esaustivo e soggetta a uno speciale controllo d'accesso (p. es. rete interna all'ufficio). Mediante una cifratura conforme allo stato della tecnica è possibile ovviare a questo rischio.

*Lett. e:* nel quadro di un piano d'emergenza, deve essere definita la procedura da seguire in caso di accesso abusivo a banche dati o di utilizzazione abusiva delle medesime. Questa regolamentazione delle misure eventualmente necessarie costituisce una componente del piano SIPD.

*Art. 153e* Analisi dei rischi

*Cpv. 1*: le analisi dei rischi periodiche servono a individuare unioni illecite di banche dati e, se del caso, far sì che le amministrazioni collaborino in modo che le misure tecniche e organizzative siano adottate in base a una stima realistica e rappresentativa dei rischi sistemici globali.

*Lett. a* e *b*: queste lettere precisano quali unità a livello federale e cantonale sono tenute a svolgere l'analisi dei rischi e per quali banche dati.

*Cpv. 2*: la tenuta di elenchi delle banche dati contenenti il NAVS permette un'azione mirata e coordinata nel quadro dell'analisi dei rischi. Per raggiungere questo obiettivo si possono anche sfruttare elenchi di banche dati già esistenti, applicando il criterio dell'utilizzazione sistematica del NAVS.

*Art. 153f* Obblighi di collaborare

Chi utilizza sistematicamente il NAVS ha inoltre diversi obblighi di collaborare nei confronti dell'UCC. Si tratta in primo luogo di garantire l'attendibilità del NAVS.

*Lett. a:* l'UCC necessita di essere informato dagli aventi diritto se essi si avvalgono della loro autorizzazione all'utilizzazione sistematica del NAVS. Per questo motivo, anche dopo la revisione continuerà a sussistere un obbligo di annuncio nei confronti dell'UCC per gli impieghi al di fuori dell'AVS. Quest'obbligo sarà sancito nella legge. In futuro, l'UCC dovrà verificare se le unità che gli annunciano di utilizzare sistematicamente il NAVS siano autorità oppure privati che svolgono compiti amministrativi in virtù di una legge speciale secondo l'articolo 153*c* capoverso 1 lettera a numero 4.

*Lett. b e c:* i previsti obblighi di collaborare sono tesi a far sì che l'UCC possa disporre o svolgere direttamente confronti di dati per verificare i numeri utilizzati e che le eventuali correzioni da esso ordinate vengano effettuate.

*Art. 153g* Comunicazione del numero AVS nell'ambito dell'esecuzione del diritto cantonale o comunale

Il contenuto di questa disposizione corrisponde ampiamente al vigente articolo 50*f* LAVS. La modifica rispetto al diritto vigente consiste nell'inclusione degli utenti sistematici nell'ambito dell'esecuzione del diritto comunale, dal momento che in futuro il NAVS potrà essere utilizzato anche in quest'ambito. Al fine di garantire la protezione dei dati sono stabilite le condizioni alle quali questi utenti potranno comunicare il NAVS a terzi, in casi specifici. In questo contesto vanno osservate le disposizioni legali in materia di comunicazione dei dati vigenti nel relativo settore d'attività.

La comunicazione del NAVS da parte di organi federali rimarrà retta dalle disposizioni della LPD, identiche sul piano materiale.

*Art. 153h* Emolumenti

Già secondo il diritto vigente, in virtù dell'articolo 46*a* LOGA possono essere riscossi emolumenti per l'onere sostenuto dall'UCC in relazione con l'utilizzazione sistematica del NAVS al di fuori dell'AVS. Poiché tale utilizzazione sarà ampliata, per una

maggiore trasparenza la possibilità di riscuotere emolumenti va sancita nella LAVS (cfr. n. 6.1).

*Art. 153i* Disposizioni penali relative alla parte quarta

*Cpv. 1*: questa disposizione coincide materialmente con quella del vigente articolo 87 ottavo comma LAVS. Come finora, l'utilizzazione sistematica del NAVS senza autorizzazione sarà passibile di pena pecuniaria.

*Cpv. 2*: questa disposizione riprende quella del vigente articolo 88 quarto comma. Le contravvenzioni sono punibili sia quando sono commesse intenzionalmente che quando sono dovute a negligenza (art. 333 cpv. 7 del Codice penale[40]).

*Cpv. 3*: poiché la LPGA non è applicabile alla parte quarta della LAVS, è necessario un rimando all'articolo 79 LPGA per permettere l'applicazione delle summenzionate disposizioni penali anche alle infrazioni commesse nell'azienda.

*Titolo prima dell'art. 154*

Parte quinta: Disposizioni finali
In futuro la parte quarta della LAVS disciplinerà l'utilizzazione sistematica del NAVS al di fuori dell'AVS. La vigente parte quarta, contenente le disposizioni finali, diventerà pertanto la parte quinta.

**Disposizioni finali**

Affinché i servizi e le istituzioni che già utilizzano sistematicamente il NAVS possano procedere agli adeguamenti necessari, occorre concedere loro un periodo transitorio. Considerando che già il diritto vigente prescrive l'adozione di misure tecniche e organizzative, il termine di un anno è adeguato.

**Modifica di altri atti normativi**

Le disposizioni concernenti l'utilizzazione sistematica del NAVS al di fuori dell'AVS contenute in altri atti normativi vanno modificate o abrogate, al fine di evitare doppioni. Inoltre, le diverse espressioni utilizzate per indicare il NAVS vengono sostituite con «numero AVS».

## 5.2 Coordinamento con altri atti legislativi

Vi è necessità di coordinamento con il progetto di revisione in corso «Modernizzazione della vigilanza nel 1° pilastro e sua ottimizzazione nel 2° pilastro della previdenza per la vecchiaia, i superstiti e l'invalidità»[41]. A prescindere dal fatto che entri in vigore prima il presente disegno o il disegno della LAVS proposto nel quadro della revisione sulla modernizzazione, saranno determinanti le modifiche di quest'ultimo,

40 RS **311.0**
41 Numero dell'oggetto 19.XXX.

fatta eccezione per l'espressione «numero d'assicurato», che andrà sostituita in tutto l'atto normativo con «numero AVS». Questa sostituzione si applicherà anche alla legge del 17 giugno 2016[42] sul casellario giudiziale, che al momento non è ancora in vigore.

## 6 Ripercussioni

### 6.1 Ripercussioni finanziarie e sull'effettivo del personale per la Confederazione

La possibilità dell'utilizzazione più ampia del NAVS farà innanzitutto aumentare le nuove richieste di accesso ai servizi offerti dall'UCC. Si possono prevedere richieste supplementari da parte degli utenti, il che genererà maggiori spese la cui entità è difficile da stimare, dato che dipenderà notevolmente dal numero di nuove unità che vorranno utilizzare sistematicamente il NAVS e dal loro comportamento di utilizzo. Per un periodo transitorio della durata di due-cinque anni si prevede un aumento degli annunci di utenti e delle richieste di accesso ai servizi dell'UCC. Questo onere supplementare sarà gestito con le risorse di personale disponibili.

Maggiori spese sorgeranno anche per l'infrastruttura della banca dati UPI, dato che la crescita del numero di utenti inciderà sulla capacità dei sistemi informatici. Per quanto concerne l'ammodernamento delle applicazioni per l'amministrazione degli annunci di utilizzazione sistematica del NAVS e di accesso ai servizi dell'UCC, si stimano costi d'investimento compresi tra 500 000 e 1 000 000 franchi. Le spese derivanti da una maggiore vigilanza automatica sull'impiego dei servizi dell'UCC potrebbero ammontare a un importo compreso tra 200 000 e 750 000 franchi. Gli investimenti supplementari si aggireranno quindi complessivamente tra 700 000 e 1 750 000 franchi.

Secondo il diritto vigente, il Consiglio federale ha la possibilità di riscuotere emolumenti per le spese supplementari derivanti dall'utilizzazione sistematica del NAVS al di fuori dell'AVS. L'obbligo di pagare emolumenti è concretizzato negli articoli 134$^{sexies}$ e 134$^{septies}$ OAVS. Essendo previste numerose eccezioni, nella prassi la riscossione di emolumenti è molto rara. Le spese che non sono finanziate tramite emolumenti vengono assunte dall'UCC o dai fondi di compensazione. Questi ultimi vengono finanziati principalmente tramite i contributi degli assicurati e dei datori di lavoro, il contributo federale e l'IVA. Se l'UCC fornisce servizi per utenti del NAVS estranei al primo pilastro, si dovrà evitare di gravare sulle assicurazioni sociali di quest'ultimo. Poiché l'utilizzazione sistematica del NAVS al di fuori dell'AVS sarà ampliata, per una maggiore trasparenza la possibilità di riscuotere emolumenti va sancita nella LAVS. La rielaborazione della vigente regolamentazione derogatoria va fatta a livello d'ordinanza. In questo modo, le spese dell'utilizzazione più ampia potranno essere ripercosse sugli utenti interessati, vale a dire su chi le avrà causate.

Infine, quale fattore di riduzione delle spese vanno menzionati gli aumenti di efficienza presso le nuove autorità federali che utilizzeranno il NAVS. Il miglioramento

42 FF **2016** 4315

della qualità dei dati raccolti dalle autorità semplificherà ed accelererà l'attività amministrativa, rendendo al contempo meno complicato e il più possibile automatizzato il flusso di dati tra le varie autorità. Inoltre, grazie all'autorizzazione generale a favore delle autorità, non sarà più necessario creare una base legale specifica per ogni nuovo scopo di utilizzazione, il che alleggerirà anche il lavoro delle autorità legiferanti. Eventualmente, occorrerà tuttavia aggiornare le misure di accompagnamento, il che può comportare spese supplementari. L'entità dei risparmi e delle uscite supplementari non può essere quantificata.

## 6.2 Ripercussioni finanziarie e sull'effettivo del personale per i Cantoni e i Comuni

L'eventuale riscossione di emolumenti per l'utilizzazione sistematica del NAVS comporterebbe spese supplementari per i Cantoni e i Comuni, che potranno essere stimate solo una volta noti il sistema di riscossione e le regolamentazioni derogatorie, ma che dovrebbero comunque essere marginali. Inoltre, l'obbligo di annuncio causerà un onere iniziale (trascurabile) per gli utenti.

Al contempo, gli aumenti di efficienza nell'attività amministrativa (cfr. n. 6.1) saranno un fattore di riduzione delle spese per i Cantoni e i Comuni. Le singole autorità saranno certamente in grado di valutare il rapporto costi-benefici dell'utilizzazione sistematica del NAVS per la loro attività amministrativa e dunque lo impiegheranno solo se sarà economicamente vantaggioso. Per i Cantoni e i Comuni si possono pertanto presumere ripercussioni positive. Anche l'onere delle autorità legiferanti cantonali e comunali diminuirà, poiché non sarà più necessario creare una base legale specifica per ogni nuovo scopo di utilizzazione. Come nel caso delle autorità federali, però, andranno adeguate le misure di accompagnamento, il che genererà spese supplementari non quantificabili.

## 6.3 Ripercussioni per l'economia

Il progetto non avrà ripercussioni dirette per l'economia. Pur non essendo quantificabili, le ripercussioni indirette saranno invece positive, grazie al miglioramento degli scambi per via elettronica tra cittadini e autorità e tra le varie autorità.

## 6.4 Ripercussioni per la società

Il progetto non avrà ripercussioni dirette per la società.

## 6.5 Ripercussioni per l'ambiente

Il progetto non avrà ripercussioni dirette per l'ambiente.

# 7 Aspetti giuridici

## 7.1 Costituzionalità

### 7.1.1 Competenze

Il progetto poggia sulle norme di competenza della Costituzione federale (Cost.; RS *101*), che autorizzano la Confederazione a legiferare in materia di assicurazione per la vecchiaia e per i superstiti (art. 111 e 112 Cost.). Nella misura in cui le disposizioni applicabili al NAVS riguardano la sua utilizzazione come identificatore personale generale per le autorità, la competenza della Confederazione risulta dall'articolo 173 capoverso 2 Cost., che le attribuisce la competenza di disciplinare l'organizzazione delle autorità federali. Se il legislatore federale consente ai Cantoni e, se il diritto cantonale non prevede altrimenti, ai Comuni di utilizzare sistematicamente il NAVS, al contempo esso ha la facoltà di definire le condizioni di utilizzo di questo strumento e di emanare prescrizioni in merito.

### 7.1.2 Protezione della personalità

Il progetto è anche conforme all'articolo 13 capoverso 2 Cost. Le modifiche della LAVS proposte disciplinano con sufficiente precisione le condizioni alle quali potrà essere ammessa l'utilizzazione sistematica del NAVS, cosicché il requisito della base legale sufficiente è soddisfatto. Anche il principio della conformità allo scopo è rispettato, poiché gli utenti potranno utilizzare sistematicamente il NAVS soltanto per adempiere i compiti attribuiti loro dalla legge. Il disegno di legge definisce inoltre le linee guida per le misure di sicurezza da rispettare e norme concernenti le sanzioni in caso di violazione di tali prescrizioni (cfr. n. 4.2).

## 7.2 Compatibilità con gli impegni internazionali della Svizzera

La tematica del progetto non riguarda alcun impegno di diritto sociale internazionale della Svizzera.

## 7.3 Forma dell'atto

Secondo l'articolo 164 capoverso 1 Cost., tutte le disposizioni importanti che contengono norme di diritto vanno emanate sotto forma di legge federale. Il presente progetto rispetta tale disposizione.

## 7.4 Subordinazione al freno alle spese

Il presente progetto non sottostà al freno alle spese ai sensi dell'articolo 159 capoverso 3 lettera b Cost., poiché non contiene disposizioni in materia di sussidi né crediti d'impegno o dotazioni finanziarie.

## 7.5 Delega di competenze legislative

L'articolo 153*h* delega al Consiglio federale la facoltà di prevedere emolumenti per i servizi che l'UCC fornisce in relazione all'utilizzazione sistematica del NAVS al di fuori dell'AVS.