Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

17.028

Messaggio concernente la legge sulla sicurezza delle informazioni

del 22 febbraio 2017

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di una legge sulla sicurezza delle informazioni.

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

22 febbraio 2017

In nome del Consiglio federale svizzero:

La presidente della Confederazione, Doris Leuthard
Il cancelliere della Confederazione, Walter Thurnherr

Compendio

Ispirandosi a standard internazionalmente riconosciuti, il presente progetto crea un quadro legale formale uniforme per la sicurezza delle informazioni in seno alla Confederazione. Il progetto si concentra in particolare sulle informazioni e sui sistemi più critici nonché sulla standardizzazione delle misure, mirando così a migliorare in maniera economica e duratura la sicurezza delle informazioni in seno alla Confederazione.

Situazione iniziale

Per quanto concerne la protezione delle informazioni in seno alla Confederazione, diversi attacchi sferrati ai sistemi d'informazione della Confederazione hanno evidenziato la presenza di lacune che possono essere ricondotte anche all'anacronismo delle basi legali. Attualmente si riscontra una dispersione delle basi legali formali per la sicurezza delle informazioni, che sono distribuite tra molteplici atti normativi e contengono prescrizioni impostate in modo settoriale, scarsamente coordinate nonché molto lacunose e contraddittorie. Per questo la Confederazione gestisce attualmente, dal punto di vista sia legale che organizzativo, strutture parallele per sottosettori della sicurezza delle informazioni. L'evoluzione verso una società dell'informazione ha reso più complesse e dinamiche le relative minacce, che devono essere affrontate con un approccio professionale, interconnesso e integrale. La prassi ha dimostrato che l'orientamento settoriale in seno alla Confederazione è ormai inadeguato e inefficiente. Le misure concernenti la sicurezza delle informazioni devono essere armonizzate con le esigenze della società dell'informazione, applicate per quanto possibile tenendo conto dei rischi e coordinate tra tutte le autorità. È pertanto indispensabile che dette misure vengano riunite in una normativa unica e moderna. Tale soluzione è anche in linea con gli standard internazionali, che disciplinano la sicurezza delle informazioni con un approccio integrale.

Il Consiglio federale ha incaricato il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) di elaborare basi legali formali per la sicurezza delle informazioni della Confederazione, chiedendo l'introduzione di standard minimi di sicurezza validi per tutte le autorità federali. Nel corso dei lavori il Consiglio federale ha inoltre deciso numerose misure da tenere in considerazione nel progetto legislativo. I risultati della procedura di consultazione, prevalentemente positivi, hanno confermato che nel settore della sicurezza delle informazioni sussiste una necessità d'intervento e che il progetto rappresenta una soluzione adeguata in tal senso.

Contenuto del progetto

Con il presente progetto il Consiglio federale persegue due obiettivi ambiziosi: da un lato, concentrare in un unico atto normativo le principali basi legali volte a garantire la sicurezza delle informazioni e dei mezzi informatici della Confederazione (atto normativo unico) colmando le lacune nel diritto vigente e tenendo in

considerazione numerose richieste avanzate dalle autorità parlamentari di vigilanza; dall'altro, estendere il campo d'applicazione della normativa a tutte le autorità e tutte le organizzazioni della Confederazione affinché quest'ultima possa raggiungere un livello di sicurezza il più possibile uniforme. Nel contempo, tuttavia, si tratta di una normativa di entità modesta per due motivi: in primo luogo, il progetto si fonda su standard internazionali già riconosciuti e consolidati nella prassi; in secondo luogo, non fissa misure dettagliate per garantire la sicurezza delle informazioni, bensì crea soltanto un quadro legale formale sulla cui base le singole autorità federali emaneranno, a livello di ordinanze e di istruzioni, le disposizioni concrete in materia di sicurezza delle informazioni.

La legge disciplina in particolare la gestione dei rischi, la classificazione delle informazioni, la sicurezza in occasione dell'impiego di mezzi informatici, le misure in materia di personale e la protezione fisica di informazioni e mezzi informatici. Per raggiungere un livello di sicurezza il più possibile uniforme e ridurre i costi della sicurezza delle informazioni occorre standardizzare i requisiti e le misure. Il principio di trasparenza nell'Amministrazione dovrà continuare a essere applicato senza restrizioni ed è per questo che nel disegno viene sancita esplicitamente la preminenza della legge sulla trasparenza (LTras).

Il disciplinamento dei controlli di sicurezza relativi alle persone viene trasferito dalla legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI; RS 120*) alla presente legge e, contemporaneamente, adeguato alle odierne esigenze in materia di sicurezza delle informazioni. Il Consiglio federale intende ridurre l'impiego del controllo di sicurezza relativo alle persone al livello minimo indispensabile per individuare rischi considerevoli. L'obiettivo è ridurre notevolmente, in futuro, il numero di controlli effettuati.*

Per garantire la sicurezza delle informazioni nell'ambito dell'aggiudicazione a terzi di mandati sensibili sotto il profilo della sicurezza, compresi gli acquisti critici della Confederazione in materia di tecnologie dell'informazione e della comunicazione (TIC), il Consiglio federale vuole estendere agli acquisti civili il campo d'applicazione della procedura di sicurezza relativa alle aziende in ambito militare, applicando questo nuovo strumento in modo mirato e non burocratico. Il Consiglio federale intende inoltre creare una base per il rilascio di dichiarazioni di sicurezza a favore delle imprese svizzere che concorrono per mandati esteri e che, a tal fine, necessitano di una dichiarazione di sicurezza nazionale.

Al fine di fornire appoggio ai gestori di infrastrutture critiche per quanto concerne la sicurezza tecnica delle informazioni, gli organi competenti della Confederazione devono trattare elementi d'indirizzo nel settore delle telecomunicazioni ed è possibile che tali elementi siano considerati dati personali degni di particolare protezione. Il disegno crea la base necessaria per il trattamento e lo scambio di questi elementi.

La legge si rivolge primariamente alle autorità federali. Il Consiglio federale intende tuttavia migliorare anche la collaborazione con i Cantoni. Questi ultimi devono garantire un livello di sicurezza delle informazioni equivalente quando trattano informazioni classificate della Confederazione o accedono ai suoi mezzi informatici. Allo scopo di rafforzare la collaborazione, i Cantoni saranno rappresentati nel

nuovo organo di coordinamento previsto e concorreranno alla standardizzazione delle misure.

I costi dell'attuazione dipendono in gran parte dal livello di sicurezza che le autorità federali intendono raggiungere e dal pertinente diritto esecutivo. Il fabbisogno di personale supplementare per il miglioramento della sicurezza delle informazioni sarà in gran parte compensato da una riduzione delle spese per il personale nell'ambito dei controlli di sicurezza relativi alle persone. Secondo le stime attuali, a medio termine potrebbero essere necessari da quattro a undici posti supplementari.

Indice

Compendio **2564**

1 Punti essenziali del progetto **2569**

1.1 Situazione iniziale 2569
1.1.1 Evoluzione verso una società dell'informazione 2569
1.1.2 Rischi della società dell'informazione 2571
1.1.3 Necessità di una nuova legge federale 2575
1.1.4 Mandati del Consiglio federale 2578

1.2 La nuova normativa proposta 2583
1.2.1 Sicurezza delle informazioni 2584
1.2.2 Campo d'applicazione e collaborazione con i Cantoni 2586
1.2.3 Rapporto con la legge sulla trasparenza e con la legislazione sulla protezione dei dati 2588
1.2.4 Misure generali 2589
1.2.5 Controlli di sicurezza relativi alle persone 2593
1.2.6 Procedura di sicurezza relativa alle aziende 2598
1.2.7 Infrastrutture critiche 2601
1.2.8 Esecuzione 2603
1.2.9 Organizzazione 2604

1.3 Motivazione e valutazione della soluzione proposta 2609
1.3.1 Alternative esaminate 2609
1.3.2 Procedura di consultazione 2613
1.3.3 Valutazione complessiva 2614

1.4 Diritto comparato 2615

1.5 Attuazione 2621

2 Commento ai singoli articoli **2622**

2.1 Legge sulla sicurezza delle informazioni 2622

2.2 Coordinamento con altri atti normativi 2685

2.3 Modifica di altri atti normativi 2687

3 Ripercussioni **2694**

3.1 Ripercussioni per la Confederazione 2694
3.1.1 Ripercussioni finanziarie 2695
3.1.2 Ripercussioni in materia di personale 2696

3.2 Ripercussioni per i Cantoni e i Comuni, per le città, gli agglomerati e le regioni di montagna 2699

3.3 Ripercussioni per l'economia 2700

3.4 Ripercussioni per la società 2700

3.5 Ripercussioni per l'ambiente 2700

3.6 Altre ripercussioni 2700

4 Programma di legislatura e strategie nazionali del Consiglio federale **2701**
4.1 Rapporto con il programma di legislatura 2701
4.2 Rapporto con le strategie nazionali del Consiglio federale 2701
4.2.1 Strategia per una società dell'informazione in Svizzera 2701
4.2.2 Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2701
4.2.3 Strategia nazionale per la protezione delle infrastrutture critiche 2701

5 Aspetti giuridici **2702**
5.1 Costituzionalità e legalità 2702
5.2 Compatibilità con gli impegni internazionali della Svizzera 2703
5.3 Forma dell'atto 2703
5.4 Subordinazione al freno alle spese 2703
5.5 Conformità alla legge sui sussidi 2704
5.6 Delega di competenze normative 2704
5.7 Protezione dei dati 2705

Abbreviazioni **2707**

Legge federale sulla sicurezza delle informazioni in seno alla Confederazione Legge sulla sicurezza delle informazioni, LSIn *(Disegno)* **2711**

Messaggio

1 Punti essenziali del progetto

1.1 Situazione iniziale

1.1.1 Evoluzione verso una società dell'informazione

Da alcuni decenni, il mondo sta vivendo un profondo mutamento sociale, indotto dallo sviluppo, tuttora in fase di accelerazione, dell'informatica. Le nuove possibilità per acquisire e scambiare informazioni in qualsiasi momento e da qualsiasi luogo interessano tutti gli aspetti della società: cultura, economia, formazione e ricerca, sanità, trasporti ed energia, difesa eccetera. Questi sviluppi sono contemporaneamente un'ineluttabile manifestazione collaterale e una condizione imprescindibile dell'incalzante globalizzazione. Tutte le società odierne sono più interconnesse e più mobili nonché, nella maggior parte dei casi, più trasparenti che mai. In tempi storicamente brevissimi, il nostro stile di vita è radicalmente cambiato.

Nell'ambito dell'evoluzione verso una società dell'informazione, il ricorso all'informatica offre alla Svizzera molteplici opportunità. Le nuove possibilità tecniche e le interconnessioni che si creano comportano tuttavia anche rischi che non devono essere ignorati. Le informazioni possono acquisire grande valore. La perdita, il furto, la divulgazione e l'utilizzazione abusiva di informazioni o la perturbazione dei mezzi che servono a trattarle (mezzi informatici) possono pregiudicare gravemente interessi pubblici essenziali o i diritti di terzi, comportare pesanti conseguenze finanziarie e addirittura compromettere l'adempimento di compiti legali critici della Confederazione.

Strategia per una Svizzera digitale

Il Consiglio federale è consapevole della fondamentale importanza dell'informatica per la Svizzera in quanto piazza economica e ambiente di vita. Già nel 1998[1] ha adottato una Strategia per una società dell'informazione in Svizzera, che è stata successivamente aggiornata nel 2006[2] e nel 2012[3]. Il 20 aprile 2016 il nostro Consiglio ha adottato la sua strategia per una Svizzera digitale[4] che sostituisce la strategia del 2012. La nuova strategia mira a sfruttare appieno le opportunità offerte dalla digitalizzazione affinché la Svizzera possa affermarsi quale luogo di vita attrattivo nonché polo economico e scientifico innovativo e orientato al futuro. Al fine di conseguire tale scopo la strategia definisce linee guida per la realizzazione di interventi statali e indica in che modo le autorità, l'economia, la scienza, la ricerca e la società civile devono cooperare affinché i processi di trasformazione derivanti dalla digitalizzazione volgano a vantaggio della Svizzera.

1 FF **1998** III 1869
2 FF **2006** 1755
3 FF **2012** 3353
4 FF **2016** 3515

In relazione con la trasformazione sociale in atto, il Consiglio federale ha commissionato numerosi progetti (ad es. e-government, e-justice, e-health, Gestione elettronica degli affari [GEVER] ecc.). Inoltre, ha assegnato al Dipartimento federale di giustizia e polizia (DFGP) diversi mandati per l'elaborazione delle basi legali necessarie. Questi progetti evidenziano un'interconnessione sempre più complessa e dinamica sia dello scambio di informazioni e dei sistemi dei cittadini e delle autorità sia dei sistemi delle autorità tra loro.

Strategia di e-government Svizzera

Il 24 gennaio 2007[5] il Consiglio federale ha adottato la Strategia di e-government Svizzera. Questa strategia nazionale, sviluppata in stretta collaborazione con i Cantoni e i Comuni sotto la direzione dell'Organo direzione informatica della Confederazione (ODIC), costituisce il documento sulla cui base la Confederazione, i Cantoni e i Comuni orientano i propri sforzi verso obiettivi comuni. Stabilisce inoltre i principi, le procedure e gli strumenti di attuazione e persegue tre obiettivi strategici:

- la popolazione può disbrigare elettronicamente le principali operazioni con le autorità, ossia quelle frequenti o che comportano un grande dispendio;
- l'economia disbriga elettronicamente le relazioni con le autorità;
- le autorità modernizzano i loro processi e comunicano elettronicamente tra di loro.

La versione ulteriormente sviluppata della «Strategia di e-government Svizzera» è stata adottata alla fine del 2015[6].

Principio di trasparenza nell'Amministrazione federale

Nel messaggio LTras il Consiglio federale aveva riconosciuto che il principio della tutela del segreto allora vigente in seno all'Amministrazione non rispondeva più alle esigenze di controllo democratico effettivo dell'attività amministrativa da parte dei cittadini. Di conseguenza, alla fine del 2004 è stata adottata la legge sulla trasparenza, la quale garantisce a chiunque il diritto di consultare documenti ufficiali e di chiedere alle unità amministrative informazioni sul contenuto di simili documenti senza dover dimostrare interessi particolari. Il principio della trasparenza è caratterizzato da una dimensione che trascende il contesto puramente giuridico. Esso implica che lo Stato elabori le proprie informazioni su incarico e in nome del Popolo svizzero, il quale può esercitare il proprio diritto di controllo in qualsiasi momento. Sono possibili eccezioni al principio di trasparenza, ma la legge le enumera esaustivamente. Tuttavia, se l'accesso a un documento viene eccezionalmente limitato, differito o negato per proteggere interessi pubblici o privati preponderanti, il documento in questione deve in seguito essere protetto conformemente alle effettive necessità di protezione.

5 La strategia è consultabile al seguente indirizzo Internet: www.egovernment.ch/it > strategia comune > attuazione > E-government Svizzera 2008–2015.

6 La strategia è consultabile al seguente indirizzo Internet: www.egovernment.ch/it > strategia comune > attuazione > Strategia di e-government Svizzera.

Strategia Open Government Data Svizzera

La nozione di *OGD* (Open Government Data, dati liberamente accessibili dell'amministrazione pubblica) mira a garantire l'accessibilità e il riutilizzo dei dati prodotti nell'ambito dell'attività amministrativa. La pubblicazione e il libero utilizzo secondario di dati delle autorità possono rivelarsi utili dal punto di vista economico e politico nonché all'interno dell'Amministrazione stessa. Poiché da una ponderazione delle opportunità e dei rischi legati agli OGD è emerso un interessante potenziale di trasparenza e di efficienza nella gestione dell'amministrazione nonché di creazione di valore aggiunto a livello economico, il 16 aprile 2014[7] il Consiglio federale ha adottato una strategia Open Government Data Svizzera per gli anni dal 2014 al 2018 (Strategia sul libero accesso ai dati pubblici in Svizzera 2014–2018), nella quale illustra la sua visione nonché i suoi obiettivi strategici e definisce principi e misure concrete per l'attuazione. La pubblicazione di dati nel senso di OGD viene presa in considerazione soltanto per i dati in possesso delle autorità federali e il cui riutilizzo non sia vietato per motivi di protezione dei dati e delle informazioni o dei diritti d'autore. Le autorità devono inoltre garantire che i dati resi accessibili siano integri (corretti) e tracciabili nonché stabilire e attuare le relative misure di carattere giuridico, organizzativo e tecnico.

1.1.2 Rischi della società dell'informazione

Intendiamo ridurre il rischio che la trasformazione sociale avvenga ai danni della popolazione e dell'economia o che comporti la violazione dei diritti della personalità. In particolare, esistono rischi che non riguardano primariamente le ripercussioni della trasformazione sociale (p. es. i cosiddetti *divari digitali*), bensì le stesse informazioni e le infrastrutture di informazione e di comunicazione interconnesse. Purtroppo il reale valore delle informazioni viene spesso riconosciuto soltanto dopo un incidente e nel momento in cui si manifestano ripercussioni negative. La perdita, il furto, la divulgazione non autorizzata o l'utilizzazione abusiva di informazioni possono avere conseguenze estremamente spiacevoli, tanto per i servizi pubblici quanto per le imprese e i privati cittadini. Anche le infrastrutture di informazione e di comunicazione, nonché i singoli mezzi informatici impiegati dalle autorità e dalle imprese come supporto per i loro processi aziendali, sono vulnerabili. Il mancato funzionamento di un sistema informatico può per esempio, a seconda della sensibilità degli affari trattati, comportare pesanti conseguenze finanziarie. Se riguarda il gestore di un'infrastruttura critica che fornisce servizi indispensabili per il funzionamento della società, dell'economia o della Confederazione, un simile mancato funzionamento può avere, nel caso peggiore, conseguenze catastrofiche, compresa la perdita di vite umane.

Pericoli per informazioni e mezzi informatici

I media riportano pressoché quotidianamente notizie di spionaggio, attacchi, mancato funzionamento di servizi informatici e altri eventi nell'ambito della sicurezza delle informazioni. Tali pericoli vengono descritti anche nella Strategia nazionale

7 FF **2014** 3027

per la protezione della Svizzera contro i cyber-rischi (SNPC). Per ottenere un quadro realistico della situazione in questo settore occorre considerare i tre aspetti esposti qui di seguito.

I pericoli devono essere presi sul serio. Se è vero che gli specialisti tendono spesso a drammatizzare la gravità dei pericoli e delle loro potenziali ripercussioni, è altrettanto vero che non bisogna sottovalutare i rischi. La criminalità organizzata può utilizzare risorse finanziarie e competenze tecniche considerevoli per rubare i dati dei clienti in linea (in particolare carte bancarie e di credito) o ricattare privati cittadini, ma si tratta di mezzi insignificanti rispetto alle risorse finanziarie e di personale impiegate da determinati attori statali per svolgere attività di spionaggio politico, diplomatico, scientifico ed economico. Alcuni Stati praticano in modo mirato lo spionaggio economico e industriale come misura prioritaria per l'industrializzazione e lo sviluppo della propria economia o per la modernizzazione delle loro forze armate.

Inoltre, i pericoli da prendere sul serio non sono legati soltanto alla protezione della confidenzialità delle informazioni. Anche la disponibilità di infrastrutture e di servizi pubblici e privati è infatti minacciata a causa della dipendenza di tali infrastrutture e servizi dall'informatica. Sebbene, a questo proposito, tra gli ipotetici pericoli vengano citate soprattutto le azioni di sabotaggio, come l'attacco mediante il software maligno (malware) *Stuxnet* scoperto nel giugno del 2010 contro gli impianti iraniani di arricchimento dell'uranio, i problemi di funzionamento causati da guasti tecnici, manipolazioni inappropriate o fenomeni atmosferici, come un'interruzione di corrente o un incendio, sono molto più frequenti e possono avere conseguenze altrettanto gravi.

Non vanno infine dimenticate la sorveglianza di massa del traffico Internet, in particolare tramite la compromissione di servizi informatici di ampia diffusione, e la corruzione sistematica di standard di cifratura. Oggi sappiamo che in realtà le ipotesi di fondo relative all'integrità di Internet e dei servizi di base non corrispondono a verità: non si può partire dal presupposto che le informazioni siano trattate in modo sicuro.

Si sta verificando una corsa agli armamenti digitali. La maggior parte dei Paesi sviluppati è consapevole della propria dipendenza dall'informatica e, pertanto, dell'esposizione alle relative minacce. Per questo attuano apposite misure di protezione. Non tutti gli Stati perseguono però strategie puramente *difensive*. Al contrario, molti di essi stanno sviluppando capacità *offensive* a livello militare e di intelligence. Anche in Svizzera c'è chi chiede un ampliamento di tali capacità offensive. Tuttavia, contrariamente a quanto avviene nella corsa agli armamenti classica, alla corsa agli armamenti digitali non partecipano soltanto attori statali o finanziati dagli Stati. Poiché lo sviluppo di nuovi programmi di protezione o malware non è particolarmente complicato e costoso o richiede infrastrutture di grandi dimensioni, sono molti gli informatici, i matematici e gli altri esperti in campo tecnologico che vi lavorano instancabilmente. Viste le risorse impiegate e l'eterogeneità degli attori, la corsa agli armamenti digitali sembra essere solo all'inizio. Arginare questa dinamica rappresenterà un'enorme sfida per la quale attualmente non esiste alcuna risposta. L'unica certezza è che nessun Paese è in grado di affrontarla da solo.

Concentrarsi esclusivamente sull'ambito «cyber» è pericoloso. In seguito alla digitalizzazione e all'interconnessione tra i sistemi di trattamento, in particolare tramite Internet, sono emersi nuovi tipi di minacce. Il fatto che la protezione da queste nuove minacce sia attualmente al centro dell'attenzione e delle attività è pertanto comprensibile. Ciò non deve tuttavia comportare una riduzione della protezione delle informazioni e dei mezzi informatici alla sola tutela contro i cyber-attacchi. Esistono infatti pericoli di fondamentale importanza che hanno poco o soltanto indirettamente a che vedere con Internet o con i malware. Lo spionaggio viene per esempio ancora condotto con *vecchi* metodi. Anche se l'uso di mezzi di spionaggio elettronici è relativamente conveniente dal punto di vista economico e meno rischioso rispetto all'impiego di spie vere e proprie, la componente umana continua a essere indispensabile per l'acquisizione di informazioni di alta qualità. Determinate informazioni vengono ancora oggi scambiate oralmente o trattate su carta. I rischi legati a tale procedura non devono essere ignorati se si vuole garantire la sicurezza delle informazioni.

Strategia nazionale per la protezione della Svizzera contro i cyber-rischi

In collaborazione con le autorità, l'economia privata e i gestori di infrastrutture critiche, intendiamo ridurre al minimo i cyber-rischi a cui tutti questi attori sono quotidianamente esposti. La SNPC identifica i cyber-rischi soprattutto in quanto inerenti ai processi e alle responsabilità vigenti. Di conseguenza, essi vanno integrati nei processi attuali di gestione dei rischi.

Gli obiettivi che perseguiamo sono i seguenti:

- individuazione precoce delle minacce e dei pericoli nel cyberspazio;
- incremento della resistenza delle IC agli attacchi;
- riduzione efficace dei cyber-rischi.

A tal fine intendiamo approfondire la collaborazione tra le autorità e l'economia nel campo del cyberspazio e consolidare le fondamenta già poste. È stata potenziata la collaborazione tra l'ODIC e il Servizio delle attività informative della Confederazione (SIC) in seno alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), che ha già svolto questo compito sino ad ora sulla base di partenariati pubblico-privato. Abbiamo inoltre dato incarico ai dipartimenti di procedere, sia nel loro settore di competenza sia nell'ambito di un dialogo con le autorità cantonali e l'economia, all'attuazione di una serie di misure che spaziano dall'analisi dei rischi relativi alle infrastrutture informatiche critiche fino a una migliore tutela degli interessi svizzeri sul piano internazionale. Per coordinare l'attuazione della SNPC è stato istituito un organo di coordinamento in seno al Dipartimento federale delle finanze (DFF). Puntiamo quindi sulle strutture esistenti e rinunciamo a istituire un organo centrale di gestione e coordinamento nazionale sul modello di quelli che vengono attualmente creati in altri Paesi.

La SNPC sarà aggiornata nel corso del 2017.

Rischi per le autorità federali

Anche le autorità federali sono esposte ai pericoli descritti nella SNPC. Esse gestiscono infatti anche infrastrutture di informazione e di comunicazione la cui perturbazione, interruzione o distruzione può compromettere l'adempimento di compiti legali critici, con gravi ripercussioni sulla società, sull'economia o sullo Stato stesso.

Per l'adempimento dei propri compiti, la Confederazione tratta inoltre quotidianamente grandi quantità di informazioni, tra cui anche informazioni che risultano particolarmente importanti per la sicurezza interna o esterna, le relazioni internazionali o gli interessi di politica economica della Svizzera e che, per questo motivo, devono essere protette mediante classificazione. Le informazioni classificate non sono però le uniche informazioni caratterizzate da maggiori necessità di protezione. In passato, lo spionaggio mirava principalmente all'acquisizione di informazioni militari e di politica estera, mentre oggi si orienta sempre più alle informazioni di carattere economico. Nel contesto di forte competitività legato alla globalizzazione, chi riesce ad appropriarsi delle conoscenze (risultati della ricerca e dello sviluppo, know-how ecc.) dei suoi concorrenti beneficia di un vantaggio decisivo. Di conseguenza, da qualche anno le attività di spionaggio economico e industriale si sono intensificate, in particolar modo nel settore dell'alta tecnologia. Proprio sotto questo aspetto, l'Amministrazione federale costituisce un centro nevralgico estremamente sensibile, in quanto regolamenta l'economia privata, verifica determinati prodotti e decide in merito alla loro omologazione, controlla determinate imprese, acquista per suo conto prodotti e servizi di grande valore, eccetera. Nello svolgimento di queste attività, cura un dialogo permanente con i propri partner del settore pubblico e privato in Svizzera e all'estero e tratta una moltitudine di informazioni che contengono segreti d'affari e di fabbricazione di terzi, rischiando in tal modo di finire nel mirino di chi vuole appropriarsi di questo tipo di informazioni. I terzi che, in virtù di un obbligo legale o di un contratto, affidano le loro informazioni alle autorità federali si aspettano però giustamente che, nelle mani di tali autorità, queste informazioni siano anche effettivamente protette.

La Confederazione tratta inoltre grandi quantità di dati personali, i quali, secondo le prescrizioni della legislazione sulla protezione dei dati, devono essere trattati esclusivamente in modo lecito, proporzionato e conforme allo scopo indicato, nonché protetti mediante provvedimenti organizzativi e tecnici. In caso di abuso in materia di dati personali, possono verificarsi gravi violazioni dei diritti della personalità degli interessati. Certi dati personali sono ricercati tanto quanto le informazioni tecnologiche dell'industria. L'acquisizione e la divulgazione di dati riferiti a persone sono infatti oggetto di un fiorente mercato.

Questi rischi per la Confederazione non sono ipotesi astratte e improbabili. All'inizio del 2016, presso l'impresa parastatale d'armamento RUAG è stato per esempio individuato un malware finalizzato ad attività di spionaggio e rimasto occultato nella rete RUAG per molto tempo. Negli anni precedenti, anche il DFAE aveva subito un attacco simile. Non vanno inoltre dimenticati i pericoli derivanti da collaboratori della Confederazione. A tale proposito, nel maggio del 2012 è stato scoperto un grave furto di dati presso il SIC. Grazie alle autorizzazioni d'accesso di cui disponeva, un collaboratore del SIC aveva memorizzato grandi quantità di informazioni sensibili su supporti di dati amovibili per divulgarli al di fuori del Servi-

zio. Prima di essere arrestato, il collaboratore in questione aveva già preso le prime disposizioni in vista della vendita dei dati sottratti.

Spesso si verificano anche fatti meno gravi quali il furto o lo smarrimento di computer portatili, di smartphone o di supporti di informazioni classificati, la divulgazione non autorizzata, perlopiù a scopo politico, di informazioni confidenziali, e problemi di funzionamento causati da interruzioni dei server, reti sovraccariche o configurazioni errate dei software. Poiché la maggior parte di questi incidenti non è oggetto di rilevamenti sistematici o, per lo meno, non viene trasmessa agli organi specializzati affinché possano effettuare una valutazione, è difficile stimare i danni complessivi subiti dalla Confederazione. Il verificarsi di incidenti gravi o ripetuti può pregiudicare seriamente la fiducia nelle autorità federali. Ciò può inoltre addirittura privare la Confederazione di importanti informazioni fintanto che non comprovi di poter garantire in modo affidabile la loro protezione.

1.1.3 Necessità di una nuova legge federale

La domanda che si pone è perché sia necessaria una legge in senso formale per la sicurezza delle informazioni delle autorità federali. Qui di seguito sono esposti in breve i tre principali motivi di tale necessità. Il fabbisogno normativo dettagliato e le soluzioni proposte sono spiegati al numero 1.2.

Scambio elettronico delle informazioni e interconnessione tra i sistemi informatici

Per adempiere i loro compiti costituzionali e legali, le autorità federali scambiano informazioni tra loro e con terzi. Questo scambio di informazioni avviene sempre più spesso e con sempre maggiore intensità in forma elettronica. Si sta inoltre assistendo a una sempre maggiore interconnessione tra i sistemi informatici delle autorità federali. Saranno quindi sempre più numerose le interfacce comuni tra i sistemi delle diverse autorità federali e aumenterà di conseguenza il rischio che eventuali attacchi e minacce contro una determinata autorità si estendano anche agli ambiti di competenza di altre autorità interessate. Se vengono trattate informazioni anche al di fuori dell'organizzazione, non basta più proteggere soltanto il proprio ambito di competenza, in quanto le misure di protezione devono produrre effetti anche al di fuori del proprio perimetro abituale. Le misure di protezione devono essere connesse all'informazione stessa, per questo è indispensabile che le singole autorità siano obbligate a coordinare tra loro le proprie misure di sicurezza a livello organizzativo, tecnico, fisico e di personale per la protezione delle informazioni e dei mezzi informatici e che i terzi che trattano informazioni della Confederazione rispettino le direttive di sicurezza di quest'ultima.

Oggi, tuttavia, le basi legali formali vigenti per la sicurezza delle informazioni sono distribuite – nella maggior parte dei casi senza un'esplicita menzione – tra molteplici atti normativi (p. es. legge sull'organizzazione del Governo e dell'Amministrazione, LOGA; legge sul Parlamento, LParl; legge militare, LM; Codice penale svizzero, CP; legge federale sulle misure per la salvaguardia della sicurezza interna, LMSI; legge sul personale federale, LPers; legge federale sugli acquisti pubblici, LAPub;

legge sull'archiviazione, LAr; legge federale sulla protezione dei dati, LPD; legge sulla trasparenza, LTras) che si applicano soltanto a determinate autorità. A titolo di esempio:

- sebbene la classificazione di informazioni sia determinante per lo svolgimento dei controlli di sicurezza relativi alle persone (CSP) (v. art. 19 cpv. 1 LMSI), i relativi criteri di classificazione sono fissati in un atto normativo (Ordinanza sulla protezione delle informazioni, OPrI) che si applica all'Amministrazione federale e all'esercito ma non alle altre autorità federali, le quali, in linea di principio, attualmente sono libere di definire i propri livelli di classificazione. Pertanto, né i criteri né le misure di protezione tra le autorità federali sono coordinati tra loro;
- le basi legali formali che disciplinano la sicurezza in occasione dell'impiego di mezzi informatici sono concepite quasi esclusivamente in base al principio della «protezione perimetrale» (LOGA per l'Amministrazione federale, LParl per il Parlamento ecc.);
- in linea di principio, i CSP possono essere eseguiti esclusivamente su impiegati federali, militari e terzi che collaborano a progetti classificati della Confederazione. Solo in pochi casi possono essere controllati anche gli impiegati cantonali. Non è inoltre chiaro se anche gli impiegati delle altre autorità federali siano compresi nel campo d'applicazione della LMSI;
- visto il suo campo d'applicazione, al momento la procedura di tutela del segreto può essere eseguita esclusivamente per gli acquisti classificati dal punto di vista militare. Non può però essere eseguita in caso di acquisti critici effettuati da autorità civili.

È necessario che il campo d'applicazione degli attuali strumenti volti a garantire la sicurezza delle informazioni includa tutte le persone e tutte le organizzazioni a cui la Confederazione affida il trattamento delle sue informazioni o concede l'accesso alle sue reti e ai suoi sistemi informatici. Soltanto in questo modo è infatti possibile garantire la sicurezza necessaria e la fiducia reciproca.

Inefficienza delle normative attuali

Oltre alle lacune nel campo d'applicazione, le attuali basi legali per la sicurezza delle informazioni presentano anche ulteriori essenziali carenze e punti deboli sul piano materiale. La maggior parte degli strumenti è impostata in modo settoriale e le relative disposizioni materiali sono scarsamente coordinate tra loro e spesso non sono orientate alle esigenze pratiche di una società dell'informazione. A titolo di esempio:

- la protezione dei dati, la protezione di informazioni classificate, la sicurezza informatica, i CSP, la procedura di tutela del segreto, la gestione dei rischi e la sicurezza fisica sono tutti aspetti disciplinati in atti normativi separati. Di conseguenza, la Confederazione gestisce strutture organizzative parallele distinte per ognuno di questi sottosettori della sicurezza delle informazioni. Ciò comporta un onere considerevole a livello di coordinamento interdisciplinare, rende praticamente impossibile una valutazione globale dell'efficacia e dell'economicità e rende notevolmente difficile il coordinamento degli

affari politici aventi dei nessi con la sicurezza delle informazioni nonché la collaborazione con i Cantoni e i partner internazionali;

- per quanto concerne il trattamento sicuro delle informazioni, nella maggior parte dei casi la legislazione si concentra soprattutto sulla protezione della confidenzialità. Nonostante le ripercussioni di una perdita di disponibilità di informazioni o sistemi d'informazione possano essere molto più gravi di quelle di una perdita di confidenzialità, attualmente non è possibile eseguire CSP o procedure di tutela del segreto per le persone o le aziende che gestiscono mezzi informatici critici presso la Confederazione o per conto di quest'ultima;
- alcuni atti normativi stabiliscono che le informazioni (e i dati) devono essere protette conformemente allo stato della tecnica (v. p. es. art. 8 cpv. 2 lett. d LPD e art. 3 lett. k OPrI), ma non precisano chi debba definire quale sia tale stato della tecnica.

L'evoluzione verso una società dell'informazione ha reso più complesse e dinamiche le relative minacce, che devono essere affrontate con un approccio professionale, interconnesso e integrale. La prassi ha dimostrato che l'orientamento settoriale in seno alla Confederazione è ormai inadeguato e inefficiente. Per questo le principali misure concernenti la sicurezza delle informazioni devono essere riunite in una normativa unica e moderna e gestite in maniera globale. Tale soluzione è anche in linea con gli standard internazionali, che disciplinano la sicurezza delle informazioni con un approccio integrale.

Limitazioni dei diritti costituzionali e trattamento di dati personali degni di particolare protezione

Secondo l'articolo 36 capoverso 1 secondo periodo e l'articolo 164 capoverso 1 lettera b della Costituzione federale (Cost.), le disposizioni fondamentali sulle limitazioni dei diritti costituzionali devono essere contenute in una legge in senso formale. Il grado di dettaglio delle relative disposizioni dipende dalla gravità dell'ingerenza. Inoltre, secondo l'articolo 17 capoverso 2 LPD, gli organi federali hanno il diritto di trattare dati personali degni di particolare protezione e profili della personalità soltanto se lo prevede esplicitamente una legge. Basi legali formali sono necessarie per:

- l'impiego di sistemi d'informazione per il controllo centralizzato delle identità, poiché tramite tali sistemi vengono trattati dati personali degni di particolare protezione;
- i CSP, poiché l'esecuzione di un CSP è legata a una sensibile ingerenza nei diritti fondamentali di privati cittadini;
- la procedura di sicurezza relativa alle aziende (PSA), poiché l'esecuzione di una PSA è legata a una sensibile ingerenza nei diritti fondamentali di privati cittadini e di persone giuridiche;
- il sostegno da parte della Confederazione ai gestori di infrastrutture critiche, poiché in tale ambito possono essere trattati dati personali degni di particolare protezione;

– la classificazione di informazioni, l'attribuzione di mezzi informatici a determinati livelli di sicurezza e la definizione di zone di sicurezza, poiché tali attività costituiscono i presupposti per lo svolgimento di CSP e PSA e sono pertanto determinanti per la limitazione dei diritti costituzionali.

1.1.4 Mandati del Consiglio federale

Alla luce di questi sviluppi e dei nuovi rischi, il Consiglio federale ha conferito numerosi mandati volti a migliorare la sicurezza delle informazioni della Confederazione. Qui di seguito sono riportati soltanto i mandati che sono stati determinanti ai fini dell'elaborazione del progetto legislativo o che comunque hanno influito in modo considerevole, dopodiché vengono indicate le raccomandazioni degli organi parlamentari di vigilanza, anch'esse prese in considerazione nel progetto.

Approvazione dell'ordinanza sulla protezione delle informazioni e mandato d'esame

A metà 2007 il Consiglio federale ha approvato la nuova OPrI, che ha sostituito le due ordinanze precedentemente applicabili all'ambito civile e a quello militare, rinunciando alla ormai praticamente impossibile distinzione tra informazioni di carattere civile e informazioni di carattere militare. Le prescrizioni della nuova ordinanza riguardanti la classificazione e il trattamento hanno inoltre introdotto per la prima volta un livello di protezione uniforme per tutta l'Amministrazione federale. L'OPrI è stata concepita come atto normativo transitorio e, di conseguenza, la durata della sua validità è limitata. Contemporaneamente all'approvazione di questa ordinanza, il Consiglio federale ha incaricato il DDPS di presentare entro la fine del 2009 un rapporto sull'esecuzione e sull'efficacia dell'OPrI nonché sui costi occasionati dalla sua attuazione e di sottoporgli una proposta per la creazione di basi legali formali.

Decisione del Consiglio federale concernente l'adozione di misure per incrementare la sicurezza delle informazioni nell'Amministrazione federale

In seguito all'attacco sferrato ai sistemi del DFAE, il 16 dicembre 2009 e il 4 giugno 2010 il Consiglio federale ha deciso di adottare opportune misure per incrementare la sicurezza delle informazioni nell'Amministrazione federale, definendo tutta una serie di misure organizzative e tecniche destinate, a breve e medio termine, a migliorare la protezione delle informazioni nell'ambito del loro trattamento con mezzi informatici dell'Amministrazione federale. Ha inoltre chiesto al Controllo federale delle finanze (CDF) di verificare lo stato dell'attuazione di tali misure. Il primo rapporto di revisione del CDF è stato presentato al Consiglio federale il 2 dicembre 2011[8]. Nonostante la portata limitata del controllo, questo rapporto fornisce una buona panoramica delle necessità d'intervento nel campo dell'impiego dell'informatica.

8 www.cdf.admin.ch/index.php?lang=it > Pubblicazioni > Verifiche trasversali > Verifica trasversale della sicurezza IT nell'Amministrazione federale (testo in tedesco con riassunto in italiano).

Mandato del Consiglio federale concernente la creazione di basi legali formali per la protezione e la sicurezza delle informazioni

Il rapporto sull'efficacia dell'OPrI, richiesto dal Consiglio federale contemporaneamente all'approvazione dell'ordinanza in questione, ha evidenziato che, nella maggior parte dei casi, il periodo transitorio in essa previsto per la realizzazione degli adeguamenti necessari a garantire la protezione tecnica delle informazioni, ossia fine 2009, non era stato rispettato. Sussistevano dunque considerevoli lacune riguardo alla protezione elettronica di informazioni classificate. Dopo aver preso atto del rapporto del DDPS e traendo insegnamento dall'attacco informatico sferrato dagli hacker contro il DFAE, il 12 maggio 2010 il Consiglio federale ha conferito al DDPS il mandato di elaborare basi legali formali per la protezione delle informazioni. Il nuovo disciplinamento doveva in particolare:

- estendere il campo d'applicazione delle prescrizioni di sicurezza a tutte le persone a cui la Confederazione affida il trattamento di informazioni protette;
- creare basi legali formali unitarie per l'esecuzione della procedura di tutela del segreto in ambito militare e civile;
- attribuire al Consiglio federale la competenza di concludere autonomamente trattati internazionali in materia di protezione delle informazioni.

Il Consiglio federale ha inoltre incaricato il DDPS di verificare se e in quale misura sussistessero, a livello di protezione delle informazioni, altri problemi materiali da disciplinare in una base legale formale e se le competenze e le responsabilità nell'ambito della sicurezza delle informazioni fossero conformi ai requisiti attuali.

Completamento del mandato del Consiglio federale del 12 maggio 2010

Il 14 gennaio 2011 il capo del DDPS ha istituito un gruppo interdipartimentale di esperti diretto dal prof. dr. iur. Markus Müller, professore ordinario di diritto costituzionale e amministrativo all'Università di Berna, con l'incarico di elaborare un concetto normativo e, in base a quest'ultimo, un avamprogetto di legge. Il 29 giugno 2011 il gruppo di esperti ha presentato il concetto normativo elaborato al capo del DDPS, il quale ha successivamente informato il Consiglio federale. Sulla base di tale concetto, con decisione del 30 novembre 2011 il Consiglio federale ha esteso il campo oggetto della futura normativa dalla pura protezione di informazioni classificate a una sicurezza delle informazioni completa. Ha inoltre constatato che, in seguito al progressivo aumento degli scambi elettronici di informazioni con le altre autorità e alla crescente interconnessione tra i sistemi informatici, una sicurezza delle informazioni efficace può essere ottenuta soltanto applicando standard minimi di sicurezza uniformi e validi per tutte le autorità federali. Per questo ha deciso di estendere il campo d'applicazione della futura legge a tutte le autorità e a tutte le organizzazioni della Confederazione, pur lasciando alle autorità federali interessate la competenza di emanare le disposizioni esecutive dettagliate e specifiche per i rispettivi settori. Ha infine incaricato il DDPS di coordinare i lavori legislativi con i mandati inerenti all'elaborazione della SNPC e alla Strategia per una società dell'informazione in Svizzera.

In seguito all'estensione del campo d'applicazione e del settore oggetto della normativa e vista l'esigenza di un coordinamento con i progetti summenzionati, è stato ampliato il gruppo di esperti, formato ora da rappresentanti di: Cancelleria federale, Dipartimento federale degli affari esteri, Dipartimento federale di giustizia e polizia (Segreteria generale, Ufficio federale di giustizia, Ufficio federale di polizia), Dipartimento federale della difesa, della protezione della popolazione e dello sport (Segreteria generale, Stato maggiore dell'esercito), Dipartimento federale delle finanze (Segreteria generale, Organo direzione informatica della Confederazione, Ufficio federale dell'informatica e della telecomunicazione), Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (Ufficio federale delle comunicazioni), Incaricato federale della protezione dei dati e della trasparenza, Servizi del Parlamento, tribunali della Confederazione e Cantoni (Conferenza svizzera sull'informatica). Occasionalmente sono stati interpellati anche la centrale MELANI e il SIC.

Mandato aggiuntivo e trasformazione del gruppo di esperti in un gruppo di lavoro interdipartimentale

In seguito alla scoperta di un increscioso episodio avvenuto in seno al SIC, il 24 ottobre 2012 il Consiglio federale ha incaricato il gruppo di esperti di elaborare un rapporto su rischi e lacune nella sicurezza delle informazioni in seno all'Amministrazione federale e di presentare proposte per l'adozione di misure immediate. In seguito al conferimento di questo mandato aggiuntivo, il gruppo di esperti è stato ulteriormente ampliato con rappresentanti del Dipartimento federale dell'interno (DFI) e del Dipartimento federale dell'economia, della formazione e della ricerca (DEFR), formando così un gruppo di lavoro interdipartimentale (GLID). Il 29 gennaio 2013 il GLID LSIn ha presentato al DDPS il proprio rapporto, corredato di raccomandazioni. Sulla base di tale rapporto, il 15 marzo 2013 il Consiglio federale ha deciso di introdurre una formazione per i quadri dirigenti dell'Amministrazione federale. L'attuazione delle misure in materia di formazione spetta all'Ufficio federale del personale (UFPER)

Mandato del Consiglio federale per l'armonizzazione e lo snellimento dei CSP

Il 1° febbraio 2012 il Consiglio federale ha incaricato il DDPS di esaminare un'armonizzazione e una riduzione delle funzioni da sottoporre al controllo e dei rispettivi livelli di controllo come pure ulteriori misure di ottimizzazione con incidenza sulle risorse. Dopo aver preso atto del rapporto del GLID istituito a tal fine (GLID CSP), il 29 novembre 2013 il Consiglio federale ha tra l'altro incaricato il GLID LSIn di tenere conto delle raccomandazioni del rapporto nei propri lavori e, laddove opportuno, di farle confluire nel disegno di legge (v. n. 1.2.5).

Approvazione dell'ordinanza sull'esecuzione di procedure di sicurezza relative alle aziende nel quadro dei programmi europei di navigazione satellitare Galileo e EGNOS

Con decisione del 13 dicembre 2013[9] il Consiglio federale ha approvato l'Accordo di cooperazione tra la Svizzera e l'Unione europea e i suoi Stati membri sui pro-

9 RS **0.741.826.8**

grammi europei di navigazione satellitare Galileo e EGNOS (Accordo di cooperazione tra la Confederazione Svizzera, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra, sui programmi europei di navigazione satellitare). L'accordo ha garantito alle imprese svizzere un accesso non discriminato ai bandi di concorso inerenti a tali programmi. Con questo accordo, inoltre, la Svizzera si è impegnata a proteggere entrambi i programmi, in particolare dall'utilizzazione abusiva, da disturbi delle frequenze e da atti ostili. In tale ambito, è tenuta a garantire un livello di sicurezza paragonabile a quello dell'UE. Le aziende o gli istituti di ricerca svizzeri che intendono partecipare ad appalti o a mandati di ricerca rilevanti per la sicurezza necessitano, a tal fine, di una dichiarazione di sicurezza aziendale (DSA) nazionale. Poiché attualmente le relative PSA sono eseguibili esclusivamente in ambito militare, in virtù dell'ormai obsoleta ordinanza del Dipartimento militare federale del 29 agosto 1990[10] sulla tutela del segreto, il 6 giugno 2014 il Consiglio federale ha adottato, a titolo di soluzione transitoria fino all'entrata in vigore della LSIn, un'ordinanza[11] che si fonda direttamente sulla Cost. e consente al servizio specializzato competente del DDPS di rilasciare DSA per appalti e mandati nel quadro dei programmi Galileo ed EGNOS.

Mandato per la creazione di una base legale per il programma IAM Confederazione

Per l'adempimento dei loro compiti, le autorità e le organizzazioni della Confederazione utilizzano numerosi sistemi d'informazione. Per ognuno di essi occorre garantire che le persone e le applicazioni giuste ottengano l'accesso corretto nel momento opportuno, il che presuppone un sistema di gestione delle identità e degli accessi (Identity and Access Management, IAM). In seguito alla sempre maggiore utilizzazione di informazioni anche al di fuori delle singole organizzazioni, le esigenze in materia di protezione e funzionalità possono ormai essere soddisfatte in maniera efficiente soltanto mediante sistemi coordinati tra tutti gli attori coinvolti. Con il programma IAM Confederazione si prevede di eseguire l'autenticazione degli utenti, nonché la verifica di determinate caratteristiche e autorizzazioni, non più separatamente per ogni singola applicazione specifica ma complessivamente per diverse applicazioni. Per motivi legati alla protezione dei dati, determinati aspetti del trattamento centralizzato dei dati personali richiedono una base legale formale. Pertanto, poiché una gestione efficiente delle identità e degli accessi risulta decisiva per la sicurezza delle informazioni, il 14 gennaio 2015 il nostro Consiglio ha incaricato il DDPS di integrare nel disegno della LSIn, in collaborazione con il DFF, una base legale concernente i sistemi di gestione delle identità.

Raccomandazioni degli organi parlamentari di vigilanza

Le Commissioni della gestione (CdG) e la Delegazione delle Commissioni della gestione (DelCG) si occupano regolarmente di temi inerenti alla sicurezza delle informazioni e, negli ultimi anni, hanno formulato raccomandazioni volte ad apportare diversi miglioramenti in quest'ambito. Nell'elaborazione del presente disegno abbiamo tenuto conto di tali raccomandazioni.

10 RS **510.413**
11 RS **510.661**

- *Gestione della crisi diplomatica tra la Svizzera e la Libia da parte delle autorità federali, Rapporto della CdG-S del 3 dicembre 2010*[12]*, raccomandazione 12:* nell'ambito della sua verifica relativa alla crisi tra la Svizzera e la Libia, la CdG-S ha riscontrato una serie di problemi a livello di protezione delle informazioni. Nel suo rapporto, ha constatato che *«simili incidenti sono la prova delle gravi lacune esistenti a livello dell'Amministrazione federale per quanto riguarda la protezione delle informazioni e dei mezzi tecnici messi a disposizione dei collaboratori, lacune alle quali è necessario porre rapidamente rimedio»*. La CdG ha pertanto invitato il Consiglio federale *«a prendere le misure necessarie, nel proprio settore di competenza, per poter garantire in futuro la segretezza anche ai più alti livelli dell'Amministrazione federale. Ciò facendo, il Consiglio federale veglierà con la dovuta attenzione anche agli aspetti tecnici degli apparecchi messi a disposizione dei collaboratori»*.
- *Verifica riguardante l'ispezione sulle circostanze della nomina di Roland Nef a capo dell'esercito, Rapporto della CdG-N del 12 aprile 2013*[13]
  - *Raccomandazione 1:* la CdG-N ha chiesto al Consiglio federale di esaminare in modo approfondito nel quadro dell'elaborazione della nuova legge sulla sicurezza delle informazioni l'opportunità di definire nella legge formale che cosa è un rischio per la sicurezza nell'ottica del CSP e qual è l'obiettivo finale di questo genere di controlli.
  - *Raccomandazione 5:* la CdG-N ha chiesto al Consiglio federale di provvedere affinché la situazione delle persone senza cittadinanza svizzera sia rapidamente chiarita e che i due servizi specializzati CSP seguano su questo punto una prassi uniforme fondata su basi legali chiare.
- *Sicurezza informatica in seno al Servizio delle attività informative della Confederazione, Rapporto della DelCG del 30 agosto 2013 (riassunto):* Il 15 ottobre 2012 la DelCG ha deciso di eseguire un'ispezione formale sulla sicurezza informatica in seno al SIC. All'inizio di luglio del 2013 ha quindi elaborato un rapporto esaustivo all'attenzione del Consiglio federale e ha pubblicato un rapporto breve contenente undici raccomandazioni. Ai fini del presente disegno sono importanti in particolare tre raccomandazioni:
  - *raccomandazione 5:* la DelCG ha raccomandato al Consiglio federale di provvedere affinché, mediante una revisione dell'ordinanza sui controlli di sicurezza relativi alle persone (OCSP), vengano definite per i collaboratori esterni le stesse condizioni di CSP degli impiegati della Confederazione che adempiono compiti identici. Il servizio federale che è il destinatario finale della prestazione fornita da aziende e collaboratori esterni si assume la responsabilità che osservino le pertinenti disposizioni. In occasione della verifica riguardante l'ispezione, con lettera del 30 giugno 2014 la DelCG ha chiesto al Consiglio federale di provvedere affinché la LSIn disciplinasse i CSP dei collaboratori esterni in

12 FF **2011** 3859
13 FF **2013** 5397

modo altrettanto preciso e completo di quelli degli impiegati della Confederazione (v. rapporto annuale 2014 delle CdG/DelCG del 30 gennaio 2015[14], n. 4.3.4);

- *raccomandazione 6:* la DelCG ha raccomandato al Consiglio federale di illustrare esaustivamente nel presente messaggio quali ruoli rivestono i CSP e la gestione del personale nella sicurezza delle informazioni e di differenziarli chiaramente l'uno dall'altro. Parallelamente, in un rapporto separato occorre indicare l'entità delle risorse di personale che la Confederazione intende impiegare per l'esecuzione dei CSP e quale contributo essa intende in tal modo apportare alla protezione delle informazioni;
- *raccomandazione 9:* la DelCG ha raccomandato al Consiglio federale di elaborare delle proposte al fine di migliorare la procedura di controllo dello stato della sicurezza informatica in seno alla Confederazione. Le misure devono permettere al Consiglio federale, nel quadro di una procedura istituzionalizzata, di identificare tempestivamente i rischi inerenti alla sicurezza informatica, di adottare le misure necessarie per ridurli e di monitorare la loro applicazione.

– *Collaboratori esterni dell'Amministrazione federale, Rapporto della CdG-S del 7 ottobre 2014*[15]*:* in questo rapporto la CdG-S ha esaminato le constatazioni e i risultati emersi da una valutazione eseguita dal Controllo parlamentare dell'amministrazione (CPA) in merito all'ampiezza, alla legalità, alla trasparenza e all'opportunità del ricorso a collaboratori esterni nell'Amministrazione federale, formulando sei raccomandazioni all'attenzione del Consiglio federale. Nella sua raccomandazione 6, la CdG-S ha invitato il Consiglio federale ad attribuire particolare attenzione al CSP nel caso di collaboratori esterni con compiti in ambito informatico perché essi hanno accesso a informazioni o materiale classificati «confidenziale» o «segreto». Ha inoltre invitato il Consiglio federale a modificare le basi legali del CSP in modo tale che il risultato di questo controllo sia noto prima dell'entrata in funzione del collaboratore interessato.

1.2 La nuova normativa proposta

Con la nuova normativa proposta intendiamo creare un quadro giuridico unitario per tutte le autorità federali nell'ambito della gestione e dell'attuazione della sicurezza delle informazioni. Tutti i principi e tutte le misure inerenti alla sicurezza delle informazioni saranno riunite in un unico atto normativo al fine di garantirne l'attuazione secondo un approccio integrale e raggiungere un livello di sicurezza il più possibile uniforme per tutte le autorità. Nel contempo saranno colmate le lacune presenti nel diritto vigente affinché le autorità federali possano disporre di basi legali moderne e orientate alle esigenze della società dell'informazione. Inoltre, le necessarie competenze centralizzate della Confederazione per l'attuazione della SNPC

14 FF **2015** 4283
15 FF **2015** 2905

saranno disciplinate mediante una base legale formale e l'organizzazione specialistica della sicurezza delle informazioni diventerà più professionale ed efficiente.

Qui di seguito sono illustrati il fabbisogno normativo dettagliato e le soluzioni proposte per i punti essenziali della nuova legge.

1.2.1 Sicurezza delle informazioni

Oggi la maggior parte delle informazioni viene trattata in forma elettronica. Per questo motivo, la protezione delle informazioni dipende sempre più dalle procedure e dai mezzi elettronici utilizzati per trattarle. Attualmente la protezione elettronica di informazioni di ogni genere presenta importanti lacune in materia di sicurezza. In questo contesto va tuttavia precisato che, in brevissimo tempo, i compiti dei servizi competenti per la definizione o per l'attuazione delle direttive in materia di sicurezza informatica sono diventati molto più complessi. Ciò è da ricondurre in particolare alle continue innovazioni tecnologiche, ai nuovi pericoli e punti deboli ad esse connessi e alla scarsità delle risorse finanziarie e di personale. Di fronte all'emergere delle suddette sfide in ambito tecnico, già nel 2008 la centrale MELANI aveva annunciato nel suo rapporto semestrale la necessità di un nuovo orientamento:

> «Anche con l'ausilio di misure tecniche di sicurezza e una buona dose di buon senso gli attuali attacchi mirati IT non possono sempre essere parati efficacemente. È pertanto necessaria una nuova focalizzazione che riporti la protezione dell'informazione al centro delle preoccupazioni e non si limiti alla sola protezione dei computer e delle reti. […], il che comporta una gestione rafforzata delle informazioni e dei dati, una classificazione delle informazioni e simili[16]».

Queste affermazioni rivestono un'importanza centrale ai fini della comprensione della nuova normativa proposta. La sicurezza informatica a livello tecnico, da sola, non è più sufficiente. Per garantire una protezione efficace delle informazioni sono molto più importanti le misure di carattere organizzativo. In seno alla Confederazione sussistono carenze organizzative in particolare per quanto riguarda le basi legali e la gestione della sicurezza delle informazioni.

Sussistono carenze innanzitutto a livello di quadro giuridico. Le odierne basi legali per la protezione delle informazioni sono impostate in modo molto settoriale e risultano scarsamente coordinate nonché, spesso, lacunose. Di conseguenza la Confederazione gestisce attualmente sistemi paralleli, a livello sia giuridico che organizzativo, per la protezione dei dati, la protezione di informazioni classificate, la sicurezza informatica, la sicurezza fisica e la gestione dei rischi. Inoltre, l'esecuzione di CSP e PSA è oggi prevista esclusivamente per le persone e le aziende che trattano informazioni classificate della Confederazione, ma non per le persone che amministrano o gestiscono i suoi mezzi informatici critici. Va altresì osservato che spesso le basi legali non sono in linea con le esigenze pratiche legate al trattamento elettronico delle informazioni.

16 www.melani.admin.ch/melani/it/home.html > Documentazione > Rapporti di situazione

Nell'economia privata, il fatto che la sicurezza sia di competenza dei capi e che una gestione efficiente della sicurezza delle informazioni risulti utile dal punto di vista economico viene compreso al più tardi quando si verificano danni e occorre adottare misure atte a contenerli. Nelle pubbliche amministrazioni, invece, spesso la sicurezza è considerata soltanto un fattore di costo e un ostacolo, soprattutto perché, in caso di incidente, il settore pubblico non *può* subire alcun danno concorrenziale. Di conseguenza, la perdita di produttività, causata per esempio dall'interruzione di servizi informatici, non viene in genere né analizzata né ponderata con i costi dell'attuazione di eventuali misure volte a ridurre i rischi.

Si osserva una situazione simile anche a livello di Confederazione. Spesso, per esempio, la sicurezza informatica viene considerata una questione puramente tecnica e non è percepita come un compito direttivo. Per questo, di regola, la linea gerarchica mostra poca comprensione per il proprio ruolo nel processo in materia di sicurezza e le usuali attività direttive (p. es. definizione di obiettivi, controllo dell'attuazione o verifica dell'efficacia delle misure) vengono applicate soltanto raramente all'ambito della sicurezza. Non è inoltre possibile una presentazione trasparente dei costi della sicurezza, il che impedisce di valutare l'economicità delle misure (analisi costi-benefici). Solo raramente, infine, i responsabili di incidenti o di violazioni delle prescrizioni vengono chiamati a renderne conto.

Le informazioni possono essere degne di protezione per diverse ragioni. I pacchetti di misure organizzative e tecniche di volta in volta indispensabili per soddisfare le necessità di protezione specifiche sono tuttavia essenzialmente gli stessi. Disciplinando, organizzando e dirigendo l'attuazione di queste misure in modo uniforme è possibile sfruttare le sinergie migliorando al tempo stesso anche la protezione. A tal fine, le basi legali devono essere obbligatoriamente armonizzate con le esigenze della società dell'informazione e da parte della linea gerarchica è necessaria una percezione più chiara dei propri compiti.

Siamo consapevoli delle crescenti interdipendenze tra la protezione tecnica e la protezione organizzativa delle informazioni, come pure delle carenze organizzative summenzionate. Abbiamo quindi impostato di conseguenza i lavori legislativi relativi alla LSIn, mirando a una *sicurezza delle informazioni* globale che tenga conto anche degli aspetti organizzativi e tecnici. La nuova normativa deve fondarsi su *standard internazionali riconosciuti.* Questa *sicurezza integrale delle informazioni* corrisponde a ciò che, nell'economia privata e in molte pubbliche amministrazioni a livello mondiale, rappresenta già da alcuni anni la *regola dell'arte*. È codificata da alcuni standard internazionali, tra cui in particolare le norme ISO/IEC 27001 e 27002[17]. Tali standard hanno poco a che vedere con la tecnica e l'accento viene posto quasi esclusivamente sui compiti della direzione (*management*) per la protezione dei propri valori in tema di informazioni nonché sulle corrispondenti misure organizzative. Gli standard contengono tuttavia anche le migliori prassi (*best practices*), concrete e di provata efficacia, per l'attuazione di misure tecniche, edili e in materia di personale. Vengono adeguati periodicamente per tenere conto delle nuove

17 Il testo delle norme è consultabile al seguente indirizzo Internet: www.iso.org/iso/fr > Store > Normes ISO.

conoscenze, soprattutto empiriche, acquisite nell'ambito di ricerche o in seguito a incidenti, e definiscono pertanto lo stato della scienza.

La LSIn crea una base legale formale uniforme per la gestione della sicurezza delle informazioni in seno alla Confederazione. Il suo contenuto e la sua struttura si basano in larga misura sulle suddette norme e ne perseguono l'attuazione in funzione delle esigenze specifiche. In tale ambito, la sicurezza delle informazioni viene considerata *secondo un approccio integrale*, vale a dire che, per quanto possibile, tutti gli aspetti che la riguardano sono gestiti, concretizzati, verificati e migliorati congiuntamente. Per questo il progetto concentra in un unico atto normativo le misure organizzative più importanti volte a garantire la protezione di tutte le informazioni e la sicurezza in occasione dell'impiego di mezzi informatici.

1.2.2 Campo d'applicazione e collaborazione con i Cantoni

Campo d'applicazione materiale

Il campo d'applicazione materiale si evince, in linea di principio, dalla nozione stessa di sicurezza delle informazioni. La protezione si concentra su tutte le informazioni di competenza delle autorità federali. Si tratta principalmente di informazioni prodotte dalle autorità federali stesse, ma sono comprese anche le informazioni che ricevono da terzi, assumendosi pertanto anche la responsabilità del loro trattamento sicuro e conforme al diritto, come pure le informazioni di cui le autorità federali affidano il trattamento a terzi. La legge si applica alle informazioni di qualsiasi genere, per esempio non solo a testi, ma anche a rappresentazioni grafiche, e in qualsiasi forma, ossia non soltanto alle informazioni elettroniche, ma anche alle informazioni contenute in documenti cartacei.

Il disegno comprende tutti i mezzi informatici impiegati dalle autorità federali o il cui esercizio viene commissionato da queste ultime. In realtà, i mezzi tecnici utilizzati per il trattamento delle informazioni non devono essere tutelati per se stessi, bensì, piuttosto, per proteggere le informazioni trattate e i processi aziendali da essi supportati. Tuttavia, poiché nella prassi i mezzi informatici sono annoverati tra gli *oggetti da proteggere*, vengono anch'essi inclusi espressamente nella LSIn.

Campo d'applicazione istituzionale

Per ampi tratti, il presente disegno costituisce un atto normativo di carattere organizzativo. La legge deve tuttavia essere applicata da tutte le autorità federali come pure dalle organizzazioni loro subordinate nei rispettivi ambiti di competenza. Soltanto in questo modo, infatti, si può aspirare a una sicurezza delle informazioni efficace. Anche le unità dell'Amministrazione federale decentralizzata e le organizzazioni di diritto pubblico e privato che svolgono compiti amministrativi devono applicare integralmente o parzialmente la legge se esercitano attività della Confederazione sensibili sotto il profilo della sicurezza o se, per l'adempimento dei propri compiti, devono impiegare mezzi informatici della Confederazione o accedere a questi ultimi. Tale soluzione, conforme ai rischi, corrisponde alla nostra intenzione di estendere il campo d'applicazione delle norme sulla protezione delle informazioni a tutte le persone a cui la Confederazione affida il trattamento di informazioni protette.

I motivi per i quali tutte le autorità federali, anche quelle legislative e giudiziarie, devono essere incluse nel campo d'applicazione della legge sono molteplici. Innanzitutto, per adempiere i loro compiti previsti dalla Costituzione e dalla legge, le autorità federali si scambiano regolarmente informazioni. Uno dei nostri obiettivi è quello di puntare maggiormente e con più decisione sullo scambio elettronico delle informazioni e sui servizi elettronici (e-government), comprese le informazioni classificate o altre informazioni con una necessità di protezione elevata. Sebbene la classificazione sia già oggi determinante per lo svolgimento dei CSP, le autorità federali non applicano attualmente un sistema di classificazione uniforme. Di conseguenza, le misure di sicurezza adottate dalle singole autorità sono molto diverse e scarsamente coordinate tra loro. Tutte le autorità federali devono pertanto applicare gli stessi principi di classificazione e adottare misure di protezione equivalenti. Soltanto in questo modo può essere garantita la necessaria fiducia reciproca nell'ambito della gestione di tali informazioni.

Si sta inoltre assistendo a una sempre maggiore interconnessione tra i sistemi informatici delle autorità federali. Saranno quindi sempre più numerose le interfacce comuni tra i sistemi delle diverse autorità federali e aumenterà di conseguenza il rischio che eventuali attacchi e minacce contro una determinata autorità si estendano anche agli ambiti di competenza di altre autorità interessate. Per questo è indispensabile che le autorità federali coinvolte applichino criteri e metodi equivalenti per la valutazione del rischio e che, nell'impiego dei mezzi informatici, le rispettive misure di sicurezza organizzative, tecniche, fisiche e in materia di personale, siano coordinate tra loro.

Infine, secondo l'articolo 3 capoverso 1 della legge sulla responsabilità (LResp), la Confederazione risponde del danno cagionato illecitamente a terzi dal personale delle autorità e delle organizzazioni assoggettate nell'esercizio delle sue funzioni. Il campo d'applicazione della LSIn corrisponde pertanto a quello della LResp, ma comprende anche il Parlamento e l'esercito.

Collaborazione con i Cantoni

Per adempiere i rispettivi compiti, Confederazione e Cantoni dipendono da una stretta collaborazione. Si scambiano reciprocamente moltissime informazioni e tale scambio avviene in misura sempre maggiore in forma elettronica. Le infrastrutture e i sistemi informatici della Confederazione e dei Cantoni vengono inoltre sempre più collegati fra loro. Aumenta così il rischio che le minacce nell'ambito di competenza di un'autorità si propaghino agli ambiti degli altri partecipanti.

I Cantoni sono direttamente competenti per la sicurezza delle proprie informazioni. Il nostro Collegio non intende né può, per motivi di carattere costituzionale, fissare prescrizioni generali per i Cantoni. La Confederazione ha tuttavia un diretto interesse a garantire che i Cantoni e i servizi loro subordinati assicurino un livello di sicurezza equivalente quando trattano informazioni protette della Confederazione o accedono ai suoi mezzi informatici. Analogamente a quanto previsto dalla soluzione contemplata nella legislazione sulla protezione dei dati (v. art. 37 cpv. 1 LPD), le prescrizioni della Confederazione vanno però applicate soltanto nel caso in cui le prescrizioni e le misure dei Cantoni non siano sufficienti a soddisfare i requisiti stabiliti dalla Confederazione in materia di sicurezza (sussidiarietà). I Cantoni saran-

no altresì tenuti a verificare periodicamente l'efficacia delle misure di protezione adottate e a comunicare gli esiti di tali verifiche al servizio competente della Confederazione (v. anche art. 37 cpv. 2 LPD).

Intendiamo inoltre coinvolgere strettamente i Cantoni nell'attuazione al fine di raggiungere anche con questi ultimi un livello di sicurezza il più possibile uniforme. Per questo nell'organo di coordinamento inter-autorità siederanno due rappresentanti dei Cantoni, che coordineranno l'esecuzione della LSIn con i servizi federali competenti e collaboreranno alla standardizzazione.

1.2.3 Rapporto con la legge sulla trasparenza e con la legislazione sulla protezione dei dati

Rapporto con la legge sulla trasparenza

Uno degli obiettivi del progetto legislativo è tutelare, conformemente alla necessità di protezione, le informazioni che per motivi legali e contrattuali devono rimanere confidenziali. Il disegno fissa anche, per esempio, i criteri per la classificazione delle informazioni ai fini della protezione della Svizzera stessa e della Confederazione. Ciò è in contrasto con la LTras, che garantisce a chiunque il diritto di consultare documenti ufficiali e di chiedere alle unità amministrative informazioni sul contenuto di simili documenti senza dover dimostrare interessi particolari. La LSIn risolve tale contrasto stabilendo la preminenza della LTras e chiarendo così che il campo d'applicazione della LTras non viene limitato in alcun modo dal disciplinamento della sicurezza delle informazioni. Di conseguenza, le disposizioni della LSIn concernenti la classificazione non possono rientrare nemmeno nella riserva di cui all'articolo 4 LTras relativa alle disposizioni speciali che dichiarano segrete determinate informazioni. Per tutte le autorità assoggettate alla LTras, le disposizioni della LTras sull'accesso ai documenti ufficiali si applicano pertanto anche alle informazioni che sono state classificate in virtù della LSIn. La valutazione di documenti nel quadro della procedura in virtù della LTras avviene indipendentemente dalle disposizioni della LSIn. Per le domande di accesso a documenti ufficiali, il servizio competente verifica dunque, indipendentemente da un'eventuale nota di classificazione, se l'accesso va accordato, limitato, differito o negato. Nella valutazione di documenti in virtù della LTras, la classificazione può essere tuttavia considerata come indizio del carattere non pubblico del corrispondente documento. La decisione sulla classificazione presuppone infatti una valutazione della necessità di proteggere l'informazione nei confronti di un pregiudizio per gli interessi pubblici da tutelare secondo la LSIn che deve corrispondere materialmente a una valutazione in merito alla limitazione, al differimento o alla negazione di cui all'articolo 7 capoverso 1 LTras.

Gli interessi da tutelare con la LSIn non coincidono completamente con il catalogo delle eccezioni secondo l'articolo 7 LTras. La LSIn, infatti, non si concentra soltanto sulla protezione della confidenzialità, bensì protegge anche la disponibilità, l'integrità e la tracciabilità delle informazioni. Sotto il profilo del contenuto, tuttavia, le disposizioni riguardanti la classificazione sono impostate in maniera tale da non contraddire il suddetto catalogo delle eccezioni. Del rimanente, occorre segnalare

che il campo d'applicazione personale della LSIn è più ampio rispetto a quello della LTras, in quanto la LSIn è applicabile a tutte le autorità federali.

Rapporto con la legislazione sulla protezione dei dati

La legislazione sulla protezione dei dati disciplina, sia per i privati che per gli organi federali, la protezione della personalità e dei diritti fondamentali delle persone i cui dati sono oggetto di trattamento (art. 1 LPD). La LPD stabilisce tra l'altro che i dati personali possono essere trattati soltanto in modo lecito, proporzionato, conforme allo scopo indicato e il più possibile trasparente per le persone interessate (art. 4 LPD). Rimane inteso che i dati personali nel settore di compiti delle autorità federali devono continuare a essere trattati secondo le norme della legislazione sulla protezione dei dati, che costituisce pertanto una legislazione speciale rispetto alla LSIn. La legislazione sulla protezione dei dati fissa tuttavia anche requisiti per la protezione pratica della confidenzialità, della disponibilità e dell'integrità dei dati stessi. L'articolo 7 LPD stabilisce per esempio che i dati personali devono essere protetti contro ogni trattamento non autorizzato mediante provvedimenti tecnici e organizzativi appropriati. Il Consiglio federale ha fissato requisiti per la protezione dei dati personali in particolare negli articoli 8–11 dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD). Detti articoli prevedono tra l'altro che le misure tecniche e organizzative tengano conto dello sviluppo tecnico. L'ordinanza non definisce tuttavia tale sviluppo tecnico, né stabilisce le competenze per la sua definizione.

Le prescrizioni della LSIn saranno applicate al trattamento di dati personali a titolo di diritto suppletorio. Ai sensi della LSIn, infatti, i dati personali sono informazioni di cui le autorità federali devono proteggere la confidenzialità, la disponibilità, l'integrità e la tracciabilità. Di regola, i dati personali non sono oggetto di una classificazione formale, che è riservata a interessi pubblici della Confederazione rigorosamente definiti. Tuttavia, nelle disposizioni esecutive sarà attribuito alle informazioni e ai dati un determinato *livello di protezione* in funzione della necessità di proteggerne la confidenzialità, la disponibilità, l'integrità e la tracciabilità. La standardizzazione delle misure secondo lo stato della scienza e della tecnica, associata al rispettivo livello di protezione, servirà anche a soddisfare i requisiti per la sicurezza dei dati sanciti nella legislazione sulla protezione di questi ultimi, garantendo così una maggiore protezione dei dati in seno alla Confederazione.

1.2.4 Misure generali

Principi della sicurezza delle informazioni

La sicurezza delle informazioni è di competenza dei capi. La relativa responsabilità incombe alla direzione dell'autorità in questione. In tale ambito, il disegno stabilisce determinati obblighi che possono essere adempiuti esclusivamente dalle singole autorità coinvolte. Le massime autorità dovranno organizzare, attuare e verificare la sicurezza delle informazioni secondo lo stato della scienza e della tecnica, definendo a tal fine anche il livello di sicurezza da raggiungere e disciplinando la competenza per la gestione dei rischi. Il disegno rafforza inoltre il ruolo operativo dei massimi

organi direttivi in diversi settori, tra cui la sicurezza in occasione dell'impiego di mezzi informatici o i CSP.

Oggi le informazioni e i sistemi d'informazione non possono più essere protetti allo stesso modo da tutti i pericoli e tutte le minacce, bensì occorre dare la priorità ai valori più importanti e più critici. Tale contesto esige che le autorità federali si concentrino maggiormente su una valutazione sistematica della necessità di protezione delle informazioni e su un'analisi continua dei relativi rischi. Ciò presuppone a sua volta una gestione dei rischi efficace nel campo della sicurezza delle informazioni e una verifica periodica dell'attuazione, dell'efficacia e dell'economicità delle misure di riduzione dei rischi. Queste due condizioni sono oggi quasi completamente inadempiute. Oggi gli audit sono uno dei principali punti deboli nell'ambito della sicurezza delle informazioni della Confederazione, in quanto vengono effettuati soltanto in singoli casi o dopo un incidente. Solo con audit adeguati, tuttavia, le autorità e le organizzazioni possono conoscere lo stato della sicurezza delle proprie informazioni, quali sono i rischi e quali sono le eventuali misure correttive necessarie. Inoltre, data la pressoché totale assenza di audit, nella maggior parte dei casi mancano attualmente il know-how e il personale necessari per il loro svolgimento. Occorre pertanto partire dal presupposto che, per adempiere tale compito, le autorità assoggettate non potranno fare a meno di impiegare risorse supplementari (v. anche il n. 1.1.4: Sicurezza informatica in seno al Servizio delle attività informative della Confederazione, Rapporto della DelCG, raccomandazione 9).

Classificazione delle informazioni

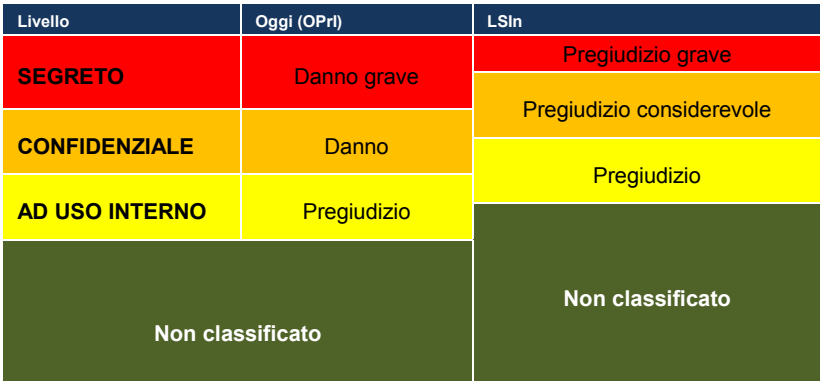
La classificazione è una misura che viene da sempre impiegata nelle organizzazioni per proteggere informazioni interne la cui conoscenza da parte di persone non autorizzate può pregiudicare gli obiettivi perseguiti o addirittura danneggiare le organizzazioni stesse. Nonostante la classificazione sia determinante per l'esecuzione dei CSP, ogni autorità assoggettata è, in linea di principio, libera di definire il proprio sistema di classificazione (sempre che intenda adottarne uno), i propri motivi di classificazione, nonché le proprie prescrizioni in materia di trattamento. Alcuni incidenti verificatisi negli ultimi anni hanno mostrato che questo trattamento variabile delle informazioni classificate può incrementare la mancanza di fiducia. Uno degli obiettivi della normativa è pertanto l'introduzione di un sistema di classificazione che sia valevole per tutte le autorità e venga applicato secondo principi per quanto possibile uniformi. Il sistema a tre livelli proposto consente di garantire una protezione delle informazioni adeguata ai rischi. In tal modo si mira a raggiungere un livello di sicurezza uniforme, auspicato anche in campo internazionale. Facendo salvo il diritto procedurale applicabile si garantisce inoltre che la classificazione non rappresenti un ostacolo all'adempimento dei compiti da parte dell'Assemblea federale, dei tribunali e dei ministeri pubblici.

Nell'elaborazione del sistema di classificazione si è tenuto conto delle maggiori aspettative dei cittadini per quanto concerne la trasparenza dell'operato delle autorità federali. La classificazione sarà pertanto concepita come un'eccezione, da motivare, al principio di trasparenza, e per le autorità e organizzazioni interessate la LTras continuerà a essere applicabile, senza alcuna limitazione, anche alle informazioni

classificate. È inoltre necessario innalzare gli attuali valori soglia per la classificazione, al fine di classificare di meno ma in modo più mirato (v. figura 1).

Figura 1

Innalzamento della soglia per la classificazione secondo la LSIn



Sicurezza in occasione dell'impiego di mezzi informatici

A causa della crescente interconnessione dei sistemi e della crescente dipendenza delle autorità federali da questi mezzi nell'adempimento dei loro compiti legali, da qualche anno a questa parte l'importanza della sicurezza in occasione dell'impiego di mezzi informatici è notevolmente aumentata. Numerosi incidenti avvenuti all'estero e in Svizzera dimostrano la vulnerabilità dei mezzi informatici e le potenziali conseguenze di simili episodi. Oggi è impossibile fare a meno di prevedere a livello di legge formale determinati parametri della sicurezza informatica, in particolare perché l'interconnessione tra tutte le autorità e lo scambio di informazioni per via elettronica sono destinati a intensificarsi ulteriormente ed esigono pertanto, in misura sempre maggiore, soluzioni e processi comuni a tutte le autorità. Inoltre, le disposizioni concernenti l'attribuzione dei mezzi informatici ai vari livelli di sicurezza sono ora determinanti anche ai fini dell'esecuzione dei CSP e delle PSA. Tuttavia, considerata la rapidità dello sviluppo tecnologico, la maggior parte delle misure concrete dovrà continuare a essere definita a livello di ordinanze o di istruzioni.

Spesso la sicurezza in occasione dell'impiego di mezzi informatici è considerata una questione tecnica. In realtà, l'aspetto tecnico è solo marginale, in quanto la stragrande maggioranza delle misure di sicurezza nel campo dell'informatica è di natura organizzativa. In quest'ambito la competenza spetta prevalentemente alle autorità e alle organizzazioni che decidono di impiegare i mezzi informatici (beneficiari di prestazioni) e non alle organizzazioni che gestiscono i relativi mezzi su mandato di tali autorità e organizzazioni (fornitori di prestazioni). La maggiore necessità d'intervento si riscontra pertanto in ambito organizzativo.

La LSIn si fonda su processi e procedure esistenti che vengono adeguati in funzione del fabbisogno riconosciuto. In tale ambito persegue tre obiettivi principali:

- *raggiungere un livello di sicurezza il più possibile uniforme per tutte le autorità:* il disegno stesso non stabilisce quasi nessuna misura di sicurezza dettagliata, ma esige che le autorità assoggettate definiscano i processi, le competenze e le misure necessari. Sebbene l'esecuzione spetti alle singole autorità assoggettate, la legge presuppone che esse disciplinino tali processi, competenze e misure congiuntamente e in modo per quanto uniforme;
- *disciplinare in modo chiaro le competenze e le responsabilità tra i beneficiari e i fornitori di prestazioni:* la responsabilità principale della sicurezza in occasione dell'impiego di mezzi informatici incombe ai beneficiari di prestazioni, che sono competenti per la valutazione del fabbisogno in materia di sicurezza delle informazioni e per la definizione delle necessarie misure. I fornitori di prestazioni sono invece competenti per garantire la sicurezza dei mezzi informatici durante il loro esercizio e devono osservare e attuare le misure e i requisiti contemplati dalla presente legge come pure i requisiti supplementari concordati con i beneficiari di prestazioni;
- *concentrarsi sui mezzi informatici maggiormente critici:* il disegno esige che i mezzi informatici da impiegare siano attribuiti a un determinato livello di sicurezza in base alle informazioni che devono essere trattate con tali mezzi e ai compiti adempiuti dall'autorità o dell'organizzazione in questione. Da un lato, l'attribuzione di un mezzo informatico a un determinato livello di sicurezza serve a consentire alle autorità di valutare la criticità delle loro informazioni e dei loro mezzi informatici affinché definiscano in seguito le misure di sicurezza focalizzandole sui loro valori più critici. Dall'altro, per ogni livello di sicurezza sono previste esigenze e misure di sicurezza minime standard che devono essere attuate prima della messa in esercizio del mezzo informatico.

Misure in materia di personale e misure di protezione fisica

Nell'ambito della gestione delle informazioni e dei mezzi informatici, i collaboratori e i terzi incaricati sono responsabili del rispetto delle relative prescrizioni. Per poter assumere tale responsabilità è indispensabile disporre di una formazione adeguata e conforme al rispettivo livello. Si tratta di un ambito in cui si registra una particolare necessità d'intervento. È stato per esempio constatato che moltissime persone che sono state sottoposte a un CSP non hanno mai ricevuto una formazione sulla gestione di informazioni classificate. Ai fini della tutela della sicurezza delle informazioni è inoltre di fondamentale importanza che per il trattamento delle informazioni e l'accesso a queste ultime, come pure per l'accesso a determinati locali e settori, vengano concesse esclusivamente le autorizzazioni di cui le persone in questione necessitano effettivamente per adempiere i propri compiti. Attualmente tale principio non viene applicato, attuato e verificato ovunque. Per questo la LSIn fissa entrambi i principi come requisiti minimi per il personale. Inoltre, poiché l'adempimento dei compiti avviene sempre più spesso in forma digitale, sono necessari anche nuovi metodi per verificare l'identità delle persone (autenticazione) che chiedono di

accedere a informazioni o a sistemi d'informazione della Confederazione. La LSIn autorizza le autorità ad applicare a tal fine metodi di verifica biometrici.

I controlli alle entrate e altre misure di protezione fisica sono misure efficaci per garantire la sicurezza delle informazioni. In tale ambito, la LSIn stabilisce il requisito minimo necessario per disciplinare tale protezione. Crea inoltre una base per l'allestimento delle cosiddette zone di sicurezza, ossia locali e settori in cui sono trattate frequentemente informazioni classificate «confidenziale» o «segreto» o vengono gestiti mezzi informatici del livello di sicurezza «protezione elevata» o «protezione molto elevata» e che sono pertanto protetti in modo particolare. Nella prassi, queste zone di sicurezza vengono allestite principalmente per proteggere i locali che ospitano server, i locali di condotta o i locali di sicurezza. Le zone di sicurezza sono diffuse a livello internazionale, mentre risultano pressoché sconosciute in seno alla Confederazione. Una base legale formale è necessaria in quanto le zone di sicurezza vengono associate a misure che possono rappresentare una grave ingerenza nei diritti della personalità (p. es. videosorveglianza, esecuzione di CSP o PSA).

Sistemi di gestione delle identità

Una delle misure operative più idonee a garantire la sicurezza delle informazioni consiste nella gestione e nel controllo efficaci delle identità e degli accessi. In seguito alla sempre maggiore utilizzazione di informazioni provenienti da fonti diverse e al di là dei limiti delle singole organizzazioni, le esigenze in materia di protezione e funzionalità possono ormai essere soddisfatte in maniera efficiente soltanto mediante sistemi coordinati tra tutti gli attori coinvolti. Per l'Amministrazione federale, un sistema di questo tipo sarà introdotto nel quadro del programma IAM Confederazione. Di per sé, il Consiglio federale e le altre autorità federali hanno senz'altro la competenza di introdurre tali sistemi di gestione delle identità (denominati anche sistemi IAM), ma, per motivi inerenti alla protezione dei dati, determinati aspetti del trattamento dei dati personali richiedono una base legale formale. La legge stabilisce lo scopo, l'architettura e il funzionamento dei sistemi di gestione delle identità al fine di disciplinare, su tale base, le competenze e le restrizioni per il trattamento di dati personali. Nelle disposizioni esecutive saranno disciplinati, tra l'altro, i diritti e gli obblighi dei diversi attori coinvolti, i requisiti in materia di protezione e la sicurezza dei dati, un elenco dettagliato dei dati da trattare nonché la trasmissione dei dati.

1.2.5 Controlli di sicurezza relativi alle persone

Le basi legali formali per l'esecuzione di CSP si trovano attualmente in due leggi. Per quanto concerne la Confederazione, al momento i CSP sono disciplinati dalla LMSI. Per il personale impiegato dagli esercenti di centrali nucleari, l'articolo 24 della legge federale sull'energia nucleare (LENu) prevede controlli dell'affidabilità. Sebbene l'articolo 113 capoverso 1 lettera d LM preveda parimenti un CSP, non si tratta in quel caso di un CSP ai sensi della LMSI, bensì di una valutazione del potenziale di violenza in vista della cessione dell'arma militare personale. Con la legge federale sulle attività informative (LAIn), la LMSI sarà quasi integralmente abro-

gata. Saranno mantenuti soltanto i CSP e i compiti il cui adempimento rientra nelle competenze dell'Ufficio federale di polizia (fedpol). Poiché l'attuale disciplinamento dei CSP nella LMSI è finalizzato *quasi esclusivamente* alla protezione di informazioni (v. art. 19 cpv. 1 LMSI), è opportuno trasferire questo disciplinamento nella LSIn. Intendiamo approfittare di tale trasferimento per apportare adeguamenti sostanziali al quadro legale formale dei CSP e, in questo contesto, vogliamo precisare qual è lo scopo perseguito con i CSP nonché snellirli di conseguenza.

Scopo dei CSP

Negli ultimi tempi il CSP è stato oggetto di continue critiche. Sono state regolarmente sottoposte al controllo persone che non svolgevano compiti particolarmente sensibili per la Confederazione (p. es. personale di pulizia). In alcuni di questi casi l'emanazione di una decisione sui rischi è stata dichiarata non conforme al principio della proporzionalità (v. sentenza del Tribunale amministrativo federale A6797/2013; v. inoltre l'interpellanza 14.3085 del 12 marzo 2014 e il postulato 14.4076 del 4 dicembre 2014: Gestione dei rischi inerenti al personale dell'Amministrazione federale). È stato inoltre criticato il fatto che per determinate funzioni, in particolare nel settore informatico, non siano stati eseguiti controlli e che collaboratori esterni e interni con funzioni simili non siano stati controllati allo stesso modo (v. n. 1.1.4: Rapporto della CdG-S sui collaboratori esterni dell'Amministrazione federale; v. inoltre la mozione 14.3031 del 4 marzo 2014: FINMA. Inchiesta di sicurezza concernente i dirigenti prima della loro nomina). Infine vi sono regolarmente critiche sulla durata dei controlli, a volte molto lunghi. Alla luce di questa situazione la DelCG raccomanda al Consiglio federale, nel suo rapporto sulla sicurezza informatica in seno al SIC (v. n. 1.1.4), di spiegare in modo dettagliato nel presente messaggio quali ruoli rivestono il PSP e la gestione del personale nell'ambito della sicurezza delle informazioni e di differenziarli chiaramente l'uno dall'altro. Parallelamente il Consiglio federale dovrebbe indicare l'entità delle risorse di personale che intende impiegare per i CSP e descrivere il contributo che ciò dovrà apportare alla sicurezza delle informazioni.

Il CSP è una misura preventiva per la protezione nei confronti di «persone che agiscono dall'interno». Il suo obiettivo è quello di identificare l'eventuale rischio che, in seguito all'esercizio di un'attività sensibile sotto il profilo della sicurezza da parte di una determinata persona, vengano pregiudicati intenzionalmente o per negligenza interessi pubblici essenziali. Al termine del controllo, spetta esclusivamente all'autorità o all'organizzazione competente per l'attribuzione del mandato o per l'assunzione della persona interessata decidere se intende assumersi un eventuale rischio più elevato, se intende ridurlo ponendo determinate condizioni o evitarlo non assumendo o licenziando la persona interessata. La valutazione dell'affidabilità di una persona deve pertanto continuare a essere svolta in primo luogo dalle persone responsabili della selezione nel quadro di un colloquio diretto con la candidata o il candidato e sulla base di determinati documenti di candidatura. Per l'occupazione di posti, l'assegnazione di funzioni militari o le attività nell'ambito di mandati militari sono perlopiù sufficienti i dati raccolti durante la procedura di selezione diretta. Inoltre, nella maggior parte dei casi, un abuso di fiducia non provoca danni considerevoli agli interessi pubblici secondo la presente legge. Se tuttavia si prevede un simile danno, un CSP può rivelare i fattori di rischio derivanti dal passato della

persona controllata o dall'ambiente in cui vive. Una valutazione del rischio per la sicurezza da parte del servizio specializzato competente (servizio specializzato CSP) che comporta una dichiarazione di sicurezza, non svincola i superiori gerarchici dalla loro responsabilità direttiva e dal loro obbligo di identificare e gestire i rischi nell'ambito del personale. I CSP hanno pertanto caratteristiche simili agli assessment che spesso il datore di lavoro commissiona prima dell'assunzione di una persona destinata a ricoprire una funzione dirigenziale o una posizione chiave.

In quanto misura statale in materia di sicurezza delle informazioni, il CSP deve essere impiegato in funzione dei rischi e in modo economico. Il CSP deve inoltre soddisfare requisiti elevati per quanto concerne il principio di proporzionalità, dal momento che è necessariamente legato a una sensibile ingerenza nei diritti personali della persona da sottoporre al controllo. Nell'ambito dell'elaborazione del primo elenco di persone da controllare conformemente all'ordinanza del 15 aprile 1992[18] relativa ai controlli di sicurezza nell'Amministrazione federale, abrogata dal 1° febbraio 1999, il Consiglio federale aveva deciso, sulla base di considerazioni politiche, di sottoporre al controllo un numero il più possibile ristretto di funzioni, prevedendo un elenco di 1200 funzioni in totale. Dall'entrata in vigore della LMSI, nel 1998, il numero di persone controllate ogni anno è però aumentato in modo costante. Dal 2012 vengono per esempio effettuati dai 70 000 agli 80 000 controlli ogni anno, di cui oltre 60 000 su persone soggette all'obbligo di leva e militari, includendo anche le valutazioni del potenziale di violenza secondo l'articolo 113 LM. È stato quindi necessario aumentare regolarmente le risorse dei servizi specializzati CSP. Ciononostante, il numero di casi pendenti è costantemente cresciuto.

Sulla base di questa evoluzione constatiamo che oggi il CSP non viene più impiegato in funzione dei rischi e in modo conforme al principio di proporzionalità. Il CSP non è da intendersi come una misura di protezione di base da applicare in modo capillare a tutti i collaboratori interni ed esterni. L'onere relativo ai CSP e l'ingerenza nei diritti personali sono infatti giustificabili solo se l'esercizio della funzione o del compito per i quali è previsto un CSP può realmente pregiudicare in modo considerevole interessi fondamentali della Confederazione. Vogliamo quindi ridurre l'impiego dei CSP al minimo indispensabile per identificare e gestire rischi rilevanti per la sicurezza delle informazioni. La nuova normativa proposta consentirà di ridurre nettamente il numero di funzioni per il cui esercizio è necessario un CSP.

Il disegno di legge prevede diverse misure che, nel loro insieme, contribuiranno a ridurre il numero di funzioni sottoposte al controllo, per esempio:

– viene innalzato il valore soglia per le classificazioni «confidenziale» e «segreto». In questo modo in futuro ci saranno anche meno funzioni per il cui adempimento è necessario trattare informazioni di questi due livelli di classificazione;
– le attività per le quali è necessario un controllo sono definite in modo più chiaro rispetto alla LMSI. Con la nozione di *attività sensibile sotto il profilo della sicurezza*, i motivi del controllo vengono ridotti alle strette esigenze della sicurezza delle informazioni. Alcuni dei motivi attuali del controllo

18 RU **1992** 1022

vengono stralciati definitivamente. Tra questi figura in particolare il motivo, previsto finora, dell'accesso regolare a dati personali degni di particolare protezione la cui divulgazione potrebbe gravemente pregiudicare i diritti individuali delle persone interessate (v. art. 19 cpv. 1 lett. e LMSI). Nella prassi è infatti pressoché impossibile determinare le informazioni che rientrano in questa definizione;

– la LSIn provvede a una gestione a più livelli dei CSP. Il Servizio specializzato della Confederazione per la sicurezza delle informazioni sarà responsabile dell'elaborazione e della verifica periodica degli elenchi delle funzioni. L'obiettivo è garantire che i criteri della legge siano applicati in modo restrittivo e che il loro rispetto venga adeguatamente verificato. In seno alle autorità federali e ai dipartimenti gli incaricati della sicurezza delle informazioni assumeranno anch'essi un ruolo di gestione. Inoltre, in seno alla Conferenza degli incaricati della sicurezza delle informazioni saranno discussi, e nel limite del possibile risolti in modo unitario, i problemi di esecuzione concernenti i CSP.

– Per evitare che si crei un vuoto in materia di sicurezza è necessario mettere a disposizione dei datori di lavoro altri strumenti, maggiormente conformi al principio della proporzionalità, per soddisfare le loro più che legittime esigenze in materia di sicurezza. Se necessario ai fini della tutela dei propri interessi, i datori di lavoro devono poter esigere dai candidati o dagli impiegati un estratto del casellario giudiziale e del registro delle esecuzioni. Si propone pertanto una revisione in tal senso della LPers.

Eliminazione di lacune giuridiche

Nel quadro della rielaborazione delle disposizioni relative ai CSP sono state apportate innumerevoli modifiche al sistema attuale con l'obiettivo di eliminarne le carenze. Le modifiche più significative sono le seguenti:

– *densità normativa più elevata:* secondo il principio di legalità sancito dalla Costituzione, per gravi ingerenze nei diritti della personalità è indispensabile una base legale formale dettagliata. Sotto questo profilo, il disciplinamento proposto è molto più dettagliato di quello contemplato attualmente dalla LMSI e soddisfa pertanto anche le aspettative del Parlamento in merito a una definizione legale formale del rischio per la sicurezza (v. n. 1.1.4);

– *controlli secondo la legislazione speciale:* sebbene il disciplinamento dei CSP nella LMSI sia finalizzato quasi esclusivamente alla protezione di informazioni nell'ambito della sicurezza interna ed esterna, nell'OCSP i motivi atti a giustificare lo svolgimento di un CSP sono stati ampliati al di là dei criteri sanciti dalla LMSI. Solo pochi direttori di uffici dell'Amministrazione federale svolgono per esempio compiti nell'ambito della sicurezza interna o esterna o hanno regolarmente accesso a informazioni della Confederazione classificate «segreto». Tuttavia, prima di essere nominati dal Consiglio federale, devono essere sottoposti a un CSP ampliato con audizione, ovvero il livello di controllo più elevato secondo l'OCSP. Sono sottoposte a un controllo di sicurezza ampliato le persone che, in occasione di un impiego all'estero, rappresentano la Svizzera nell'ambito di una missione ufficiale. È

ampiamente condivisibile che i titolari di queste funzioni debbano adempiere requisiti di affidabilità elevati. Ci si può però chiedere in quale misura queste funzioni abbiano effettivamente un nesso con la protezione della sicurezza interna ai sensi della LMSI.

Vogliamo fare chiarezza sulla questione. Nella LSIn solo le attività strettamente legate alla sicurezza delle informazioni della Confederazione devono poter giustificare l'esecuzione di un CSP. Di conseguenza anche il danno che si vuole evitare, o di cui si vuole ridurre la probabilità di insorgenza, mediante un CSP secondo la LSin va inteso come un danno per la sicurezza delle informazioni. La probabilità elevata di una perdita di reputazione per la Confederazione non potrà quindi di norma giustificare alcun rischio per la sicurezza secondo la LSIn. Qualora sia necessario svolgere un controllo per altre attività, occorrerà disciplinare i motivi del controllo nella legislazione speciale. Per poter garantire una distinzione chiara tra i CSP basati sulla LSIn e quelli disciplinati da altri atti normativi si utilizzerà per questi ultimi una terminologia diversa (*verifica dell'affidabilità*). Nell'allegato viene pertanto proposta una modifica sia della LPers che della LM affinché le persone destinate a rappresentare regolarmente la Svizzera all'estero o a esercitare competenze decisionali o compiti di vigilanza in affari finanziari essenziali possano essere sottoposte a una verifica dell'affidabilità. Questi nuovi controlli saranno ordinati in modo molto restrittivo dal Consiglio federale;

– *stralcio del criterio della regolarità per l'assoggettamento al CSP:* l'attuale criterio della regolarità (v. art. 19 cpv. 1 LMSI) si fonda tra l'altro su una valutazione del SIC, secondo cui la minaccia nell'ambito della protezione dello Stato risulta particolarmente elevata negli ambiti in cui i collaboratori hanno accesso regolarmente e per periodi prolungati a informazioni classificate. Le persone che hanno accesso soltanto occasionalmente e per periodi limitati a tali informazioni sono esposte a un rischio minore, essendo meno interessanti per i servizi che intendono acquisire informazioni. Il criterio della regolarità comporta tuttavia due problemi. In primo luogo, le attività di acquisizione di informazioni da parte dei servizi informazioni sono solo una delle tante minacce alla sicurezza delle informazioni. Anche solo accedendo un'unica volta a un'informazione classificata «segreto», una persona può arrecare un grave pregiudizio alla Confederazione. Questo può avvenire, per esempio, quando la persona divulga pubblicamente informazioni concernenti la strategia negoziale della Svizzera in questioni di particolare importanza. Il pregiudizio in sé deriva pertanto soprattutto dal contenuto delle informazioni. Inoltre, il termine *regolare* non è univoco e ha spesso dato luogo a interpretazioni non uniformi. Ai fini dell'assoggettamento degli impiegati della Confederazione ai CSP è più importante sapere se, per l'adempimento dei propri compiti, la persona che occupa una determinata funzione *deve* trattare informazioni classificate «confidenziale» o «segreto», *deve* provvedere all'amministrazione, all'esercizio, alla manutenzione o alla verifica di mezzi informatici del livello di sicurezza «protezione elevata» o «protezione molto elevata» oppure *deve* avere accesso a zone di sicurezza. Se una simile attività è *necessaria* per l'adempimento dei compiti inerenti alla funzione, allora – e solamente allora – la funzione deve essere inserita nell'elenco delle fun-

zioni da sottoporre al controllo. Le autorità e organizzazioni assoggettate devono far sì che il numero di persone incaricate di esercitare attività sensibili sotto il profilo della sicurezza sia ridotto al minimo;

– *riduzione da tre a due livelli di controllo:* il diritto vigente (art. 9–12 OCSP) prevede tre livelli di controllo: un CSP di base, un CSP ampliato e un CSP ampliato con audizione. Mentre nei primi due livelli contemplati dall'OCSP lo scopo del controllo risulta chiaro, si pone la questione di stabilire quali siano le informazioni o le attività che, secondo il diritto svizzero, dovrebbero necessitare di una protezione maggiore rispetto a quella prevista per le informazioni classificate «segreto». Per accedere a queste ultime è già ora necessario un CSP ampliato (art. 11 OCSP). In seno alla Confederazione non esiste tuttavia un livello di classificazione «segretissimo» (top secret) per il quale potrebbe eventualmente essere richiesto un controllo secondo l'articolo 12 OCSP. Pertanto nella presente legge i livelli di controllo vengono ridotti da tre a due. La raccolta dei dati nell'ambito dei due livelli di controllo rimanenti viene riorganizzata e se necessario completata per incrementare l'efficacia dei CSP.

È stato oggetto di discussioni anche l'attuale sistema che prevede un elenco delle funzioni emanato mediante un apposito atto normativo e che comporta i seguenti svantaggi: la stesura degli elenchi è particolarmente onerosa, questi non sono praticamente armonizzati tra i dipartimenti e con la Cancelleria federale e devono essere continuamente adeguati in seguito a riorganizzazioni e a cambiamenti delle denominazioni delle varie funzioni. Gli elenchi risultano inoltre problematici per motivi di sicurezza, poiché forniscono una panoramica di tutte le funzioni delle autorità che prevedono attività sensibili sotto il profilo della sicurezza e, una volta pubblicati, diventano accessibili a tutti in qualsiasi parte del mondo, compresi i servizi informazioni di altri Paesi. Gli elenchi presentano tuttavia un vantaggio decisivo rispetto alle possibili varianti, in quanto garantiscono la certezza del diritto e restringono la cerchia delle persone da sottoporre al controllo, il che dovrebbe impedire un'eccessiva proliferazione di controlli. Prima dell'emanazione delle disposizioni esecutive valuteremo eventualmente se sia opportuno pubblicare gli elenchi senza alcuna restrizione.

1.2.6 Procedura di sicurezza relativa alle aziende

La PSA (sinora denominata *procedura di tutela del segreto*) mira alla tutela della sicurezza delle informazioni nell'ambito dell'assegnazione di mandati da parte delle autorità federali a terzi (di seguito denominati *aziende*) che non sottostanno direttamente alla loro vigilanza. La procedura serve, da un lato, a verificare l'affidabilità delle aziende alle quali si intende affidare un mandato e, dall'altro, consente di controllare e imporre le misure necessarie per garantire la sicurezza delle informazioni durante l'esecuzione del mandato. La PSA non serve invece a garantire la sicurezza dei prodotti, che spetta ovviamente soltanto al servizio che assegna il mandato (mandante).

Con la PSA si mira tra l'altro a impedire che informazioni sensibili sotto il profilo della sicurezza o vettori di attacco pratici contro mezzi informatici critici della Confederazione siano resi accessibili ad aziende che, per i loro rapporti di proprietà, le loro strutture organizzative o le loro relazioni d'affari, sono per esempio controllate o influenzate in modo determinante da servizi informazioni esteri o da organizzazioni di stampo criminale (*Foreign Ownership, Control or Influence [FOCI]*). La verifica dell'affidabilità delle aziende che forniscono servizi – in particolare la potenziale esclusione delle aziende sotto FOCI dalla procedura di aggiudicazione – ha acquisito una maggiore importanza a livello politico dopo le rivelazioni di Edward Snowden. Determinati servizi informazioni possono infatti ordinare all'industria informatica del proprio Paese, per legge o con metodi repressivi, di non rispettare l'obbligo di mantenere il segreto sancito dalla legislazione o concordato nei relativi contratti. Le aziende asservite ai servizi informazioni di tali Paesi non possono garantire in maniera credibile di considerare preminenti gli obblighi di tutela del segreto concordati conformemente al diritto nazionale. Inoltre, le aziende così controllate e influenzate possono non solo compromettere la confidenzialità delle informazioni, ma anche mettere in pericolo la disponibilità e l'integrità dei mezzi informatici. In questo contesto, attualmente gli Stati escludono sempre di più gli offerenti stranieri dagli appalti per la fornitura di servizi informatici statali critici. A tale proposito è quindi importante precisare che, ai fini della valutazione del rischio per la sicurezza, sono sempre determinanti la sensibilità del mandato dal punto di vista della sicurezza e la situazione concreta dell'azienda da sottoporre al controllo. La LSIn non giustifica l'esclusione generale *a priori* di offerenti stranieri, che costituisce anche una distorsione della concorrenza.

La PSA è appropriata e comunemente applicata a livello internazionale (v. p. es. l'art. 11 della «decisione del Consiglio, del 23 settembre 2013[19], sulle norme di sicurezza per proteggere le informazioni classificate UE [2013/488/UE]» e la sezione VII delle «Regeln und Vorschriften der Europäischen Weltraumorganisation vom 15. Dezember 2011»[20]). Nell'ottica del diritto internazionale in materia di acquisti pubblici, la PSA non rappresenta un problema poiché le eccezioni all'Accordo del 15 aprile 1994[21] sugli appalti pubblici ammettono simili misure nell'ambito del diritto in materia di acquisti pubblici (v. art. XXIII). In Svizzera la PSA viene eseguita sin dalla fine degli anni 1970 per i mandati della Confederazione il cui contenuto è classificato dal punto di vista militare. A causa del ristretto campo d'applicazione materiale dell'ordinanza sulla tutela del segreto, attualmente la procedura è applicata soltanto per i mandati classificati dal punto di vista militare. Il Consiglio federale ha riconosciuto già molto tempo fa la mancanza di una procedura di sicurezza relativa alle aziende unitaria, ossia eseguibile anche per mandati del settore civile. Tale mancanza non solo ha comportato la necessità di adottare di volta in volta misure di sicurezza speciali per i mandati classificati della Confederazione a livello non militare, ma ha anche ripetutamente impedito a imprese svizzere di concorrere per progetti classificati in ambito non militare all'estero, tra cui per

19 http://eur-lex.europa.eu/legal-content/it/TXT/PDF/?uri=CELEX:32013D0488
20 Il regolamento è consultabile al seguente indirizzo Internet: www.esa.int/About_Us/Security_at_ESA > Regeln und Vorschriften der Europäischen Weltraumorganisation.
21 RS **0.632.231.422**

esempio la fabbricazione di documenti d'identità o di mezzi di pagamento per Stati terzi oppure la partecipazione a progetti scientifici. Ciò ha inciso anche sulla competitività dell'economia svizzera. Il nostro Collegio vuole ora colmare questa lacuna.

A grandi linee, la PSA si svolge nel modo seguente: il mandante chiede l'avvio della procedura al servizio specializzato per la sicurezza aziendale (servizio specializzato SA). Una volta avviata la procedura, d'intesa con il servizio richiedente, il servizio specializzato SA stabilisce innanzitutto i requisiti in materia di sicurezza, dopodiché verifica l'idoneità delle aziende in questione dal punto di vista della sicurezza. Occorre in particolare verificare se le aziende interessate sono controllate o influenzate da altri Stati e, eventualmente, se tale controllo o influenza è conciliabile con la sicurezza delle informazioni della Confederazione. Il mandante assegna quindi il mandato a un'azienda giudicata idonea. Successivamente l'azienda, sotto la supervisione del servizio specializzato SA, definisce in un apposito piano in materia di sicurezza le modalità con cui applicherà i requisiti di sicurezza previsti. Dopo l'attuazione delle misure di sicurezza necessarie, all'azienda viene rilasciata la dichiarazione di sicurezza aziendale. Infine, una volta conclusi i CSP e in presenza delle necessarie dichiarazioni di sicurezza, il mandante può mettere a disposizione dell'azienda i mezzi (informazioni, dati ecc.) indispensabili per l'adempimento del mandato sensibile sotto il profilo della sicurezza. La dichiarazione di sicurezza aziendale comporta particolari conseguenze tanto per l'azienda quanto per il servizio specializzato SA. Quest'ultimo acquisisce in particolare il diritto di ispezionare l'azienda senza preavviso e di adottare ulteriori misure.

La normativa presenta in parte un nesso relativamente stretto con il CSP, ma se ne distingue per alcuni punti essenziali. In linea di principio, si procede anche in questo caso a una verifica dell'affidabilità e, a seconda del risultato, viene poi rilasciata una dichiarazione di sicurezza aziendale, la quale attesta l'affidabilità dell'azienda e le consente di esercitare attività della Confederazione (o di un'autorità estera) sensibili sotto il profilo della sicurezza. A differenza del CSP, la PSA non si conclude con il rilascio della dichiarazione di sicurezza. Il rispetto delle misure può infatti essere verificato in qualsiasi momento. Al contrario del CSP, nel caso della PSA il mandante è vincolato dalla valutazione del servizio specializzato SA, che per questo motivo emana anche una decisione impugnabile. Un'eccezione è ammessa qualora, per l'esecuzione di un determinato mandato entrano in linea di conto unicamente aziende che comportano certi rischi. Questo caso riguarda in particolare le prestazioni di servizi in ambito informatico, nel quale alcune aziende detengono quasi il monopolio del mercato. Se per mancanza di alternative si assegna il mandato a una di queste aziende, non è consentito rilasciarle un certificato di sicurezza svizzero. La PSA viene quindi abbandonata e la responsabilità dell'applicazione e della verifica delle misure di sicurezza viene trasferita al mandante. Per la legge quest'ultimo ha diritti di imposizione analoghi al servizio specializzato SA.

Vogliamo impiegare la PSA in modo mirato e meno burocratico possibile. Il disegno di legge prevede quindi che si possa rinunciare all'esecuzione della procedura se il rischio può essere adeguatamente ridotto con altre misure. Concretizzeremo tale norma a livello di ordinanza.

1.2.7 Infrastrutture critiche

Nella SNPC abbiamo ribadito il principio del disciplinamento decentralizzato delle infrastrutture critiche (v. n. 1.1.2). Se, in settori specifici, sussiste una necessità d'intervento a livello di legge formale, occorre adeguare la pertinente legislazione speciale. La verifica del fabbisogno normativo incombe pertanto in linea di principio ai dipartimenti che, nel quadro dell'adempimento dei rispettivi compiti, sono investiti di poteri normativi nei confronti dei gestori di infrastrutture critiche (p. es. il DATEC per il settore dell'approvvigionamento energetico). Vi sono tuttavia determinati compiti che devono essere svolti a livello intersettoriale e che, per motivi di efficienza e di costo, non possono essere assunti dagli enti regolamentatori decentralizzati. Si tratta in primo luogo dell'appoggio ai gestori di infrastrutture critiche mediante lo scambio reciproco di informazioni sulle minacce nel campo della sicurezza delle informazioni, particolarmente utile per individuare tempestivamente i rischi e sventare eventuali pericoli. In quest'ambito la prassi ha dimostrato che la collaborazione con un unico servizio centrale della Confederazione è espressamente auspicata dai gestori di infrastrutture critiche. Questo ruolo di interlocutore centrale è oggi assunto dalla centrale MELANI.

Secondo le decisioni del Consiglio federale del 29 ottobre 2003 e del 24 gennaio 2007, la centrale MELANI è gestita congiuntamente da ODIC e SIC sulla base delle rispettive basi legali. La direzione strategica di MELANI e il centro tecnico di competenza sono aggregati all'ODIC; il polo informativo, rappresentato dall'*Operation and Information Center*, è gestito dal SIC. Il partenariato pubblico-privato istituito nel quadro della centrale MELANI si è rivelato particolarmente efficace, anche grazie alla possibilità di quest'ultima di accedere alle informazioni del SIC. Oltre alle informazioni messe a disposizione, è apprezzato soprattutto il mantenimento, da parte dei rispettivi fornitori, del controllo sulle informazioni («a chi può essere inoltrata l'informazione») scambiate in caso di incidente. I gestori di infrastrutture critiche valutano inoltre positivamente il carattere volontario della collaborazione nonché l'approccio secondo cui l'appoggio a favore del processo relativo alla sicurezza delle informazioni e alla gestione dei rischi viene garantito mediante informazioni ed eventualmente raccomandazioni e non prescrivendo misure.

Per adempiere i suoi compiti, la centrale MELANI tratta regolarmente elementi d'indirizzo nel settore delle telecomunicazioni secondo l'articolo 3 lettera f della legge sulle telecomunicazioni (in particolare nomi di dominio, indirizzi IP ed e-mail) connessi a minacce o pericoli concreti e li scambia con i gestori di infrastrutture critiche. Le infrastrutture utilizzate come strumenti per atti criminali consistono infatti spesso in computer di proprietari ignari infettati con software maligni, nomi di domini registrati sotto falso nome, siti web (di per sé legittimi) abusivamente modificati e server affittati ricorrendo a una falsa identità. Grazie alle informazioni fornite dalla centrale MELANI i gestori di infrastrutture critiche possono proteggere i propri sistemi, per esempio bloccando le richieste di comunicazione provenienti da computer infettati. Poiché si riferiscono a persone determinate o determinabili (o ad apparecchi o collegamenti di telecomunicazione che a loro volta possono essere attribuiti a una persona determinata o determinabile), gli elementi d'indirizzo possono essere considerati dati personali. Se vi è una denuncia penale o se vengono raccolte informazioni nel quadro di indagini di polizia, questi elementi d'indirizzo risultano

collegati a procedimenti penali e possono pertanto essere considerati dati personali degni di particolare protezione secondo l'articolo 3 lettera c numero 4 LPD. Tuttavia, poiché che con la sola denuncia penale il rischio – almeno a breve termine – non è scongiurato, è essenziale informare le infrastrutture critiche su tali vettori di attacco, in modo che queste possano proteggere i loro sistemi ed eventualmente riconoscere attacchi già in atto o avvenuti. Per poter trattare tali informazioni e dati e scambiarli con i gestori di infrastrutture critiche, la centrale MELANI ha tuttavia bisogno di una base legale formale (v. art. 17 cpv. 2 LPD), che oggi manca.

Con decisione del 30 novembre 2011, il Consiglio federale ha incaricato il DDPS di integrare nella presente legge la base legale necessaria per il trattamento dei dati nel quadro dell'appoggio fornito dalla Confederazione ai gestori di infrastrutture critiche. La LSIn disciplina i compiti principali della centrale MELANI per l'appoggio ai gestori di infrastrutture critiche e crea altresì le basi legali formali indispensabili per il trattamento e lo scambio di dati personali nella misura in cui ciò è necessario per garantire la sicurezza tecnica delle informazioni presso le infrastrutture critiche. Poiché questo scambio di informazioni deve per forza avvenire anche con i partner esteri e internazionali della Svizzera, la LSIn stabilisce i principi della cooperazione internazionale nonché i limiti necessari in tale ambito. Questo disciplinamento rende per esempio possibile lo scambio di elementi d'indirizzo con il *Bundesamt für Sicherheit in der Informationstechnik* tedesco, l'*Agence nationale de la sécurité des systèmes d'information* francese o i *National Cyber Security Centers* di Paesi Bassi e Finlandia. Le unità organizzative competenti per la protezione di infrastrutture (d'informazione) critiche sono strutturate in modo diverso a seconda del Paese: possono essere indipendenti oppure aggregate alla polizia, a un servizio informazioni, all'ambito militare o all'ente regolatore delle telecomunicazioni.

La cooperazione con tutti i partner in Svizzera e all'estero si fonda sulla volontarietà e sulla trasparenza. I servizi competenti non possono applicare misure coercitive e, a ogni richiesta di informazioni e di dati, devono provare correttamente la loro identità e comunicare al potenziale fornitore dei dati in questione a quale scopo questi ultimi vengono richiesti e utilizzati. I dati sono tuttavia comunicati spontaneamente alle organizzazioni partner qualora siano idonei a individuare o a eliminare eventuali incidenti nella loro sfera di competenza.

Sebbene il SIC sia designato dal Consiglio federale quale organo (cor)responsabile dell'esecuzione di compiti previsti dalla presente legge, per il trattamento di dati nell'ambito degli altri suoi compiti la LSIn non gli conferisce diritti supplementari rispetto a quelli già contemplati dalla LAIn. Il campo d'applicazione della LSIn è essenzialmente incentrato sulla sicurezza tecnica delle informazioni e mira soprattutto a far sì che le infrastrutture dell'informazione, e quindi anche Internet e i sistemi connessi, funzionino in modo conforme alle disposizioni. In futuro i servizi competenti dovranno poter svolgere tali compiti indipendentemente dalla loro aggregazione amministrativa e da eventuali basi legali delle rispettive organizzazioni da cui dipendono. L'utilizzo di conoscenze e capacità in seno all'ODIC e al SIC ha fornito un contributo decisivo ai risultati positivi ottenuti finora dalla centrale MELANI, motivo per cui questa cooperazione sarà portata avanti. La legislazione d'esecuzione disciplinerà in modo trasparente lo scambio di informazioni tra i vari attori nel settore della sicurezza delle informazioni. Il Consiglio federale garantirà inoltre che

il trattamento dei dati venga periodicamente controllato da un servizio esterno. Potrà pertanto disporre che il trattamento dei dati nell'ambito del campo d'applicazione della LSIn, nella misura in cui esso avviene in seno al SIC, sia controllato anche da un ulteriore organo oltre che dagli organi di vigilanza e di controllo di quest'ultimo.

1.2.8 Esecuzione

Per quanto riguarda il disciplinamento dell'esecuzione, la sfida consiste nel garantire l'applicazione della legge secondo criteri il più possibile uniformi. Se non è possibile ottenere un'esecuzione uniforme, la sicurezza delle informazioni nello scambio di informazioni tra autorità sarà inevitabilmente lacunosa. È tuttavia necessario rispettare l'autonomia delle autorità interessate sul piano dell'organizzazione e dell'esecuzione. La competenza riconosciuta dalla Costituzione alle singole autorità non può essere messa in discussione da disposizioni esecutive in parte di portata generale emanate da un'autorità particolare (p. es. il Consiglio federale). La LSIn prende in considerazione tali esigenze, di per sé contraddittorie, con i tre meccanismi seguenti:

- *clausola di esenzione («opting out»):* ogni autorità esegue autonomamente l'atto normativo nel proprio ambito ed emana il corrispondente diritto esecutivo. Le disposizioni esecutive del Consiglio federale sono tuttavia applicabili per analogia anche alle altre autorità federali fintanto che queste ultime non emanano disciplinamenti propri;
- Non si tratta di questioni organizzative di principio, bensì di processi, mezzi e servizi secondari (rilevamento delle necessità di protezione delle informazioni, metodi per la valutazione del rischio, cifratura ecc.). L'obiettivo è raggiungere un livello di sicurezza uniforme, riducendo però nel contempo anche i costi di progetto e di attuazione. Il Consiglio federale avrà la possibilità di delegare la definizione di tali requisiti e misure a organi specializzati competenti sotto il profilo tecnico;
- *istituzione di un organo di coordinamento:* la creazione di una conferenza degli incaricati della sicurezza delle informazioni nella quale siano rappresentate tutte le autorità federali, i Cantoni e l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) è una misura di fondamentale importanza. Gli incaricati della sicurezza delle informazioni responsabili della direzione tecnica dell'attuazione della LSIn otterranno una panoramica completa dei problemi connessi alla sicurezza delle informazioni nel proprio ambito di competenza, in particolare per quanto concerne la realizzabilità, l'efficacia e l'economicità delle prescrizioni e delle misure stabilite. La conferenza servirà a garantire l'esecuzione della legge da parte di tutte le autorità, in modo uniforme e adeguato ai rischi, come pure il coordinamento con i Cantoni e con l'IFPDT. A tal fine, la conferenza collaborerà in modo determinante anche alla standardizzazione dei requisiti e delle misure.

La soluzione proposta garantisce l'indipendenza delle autorità federali nell'ambito dell'esecuzione, che avviene in modo decentralizzato. L'auspicato livello di sicurezza uniforme viene raggiunto mediante l'unitarietà della dottrina, l'elaborazione di standard nonché il supporto professionale da parte di organi specializzati.

Il disegno disciplina principalmente il quadro generale valido per tutte le autorità. L'esecuzione in seno all'Amministrazione federale spetta esclusivamente al Consiglio federale. La sua autonomia sul piano dell'esecuzione è pressoché illimitata. La legge gli lascia un ampio margine di manovra per quanto riguarda l'organizzazione. In tale contesto, il Consiglio federale deciderà se mantenere l'attuale forma di esecuzione, perlopiù decentralizzata, o se centralizzare determinate competenze e responsabilità. L'esecuzione da parte delle unità dell'Amministrazione federale decentralizzata assoggettate alla legge nonché delle organizzazioni di diritto pubblico e privato che adempiono compiti amministrativi sarà determinata in base all'entità dell'assoggettamento e dell'autonomia di tali unità e organizzazioni.

1.2.9 Organizzazione

In occasione dell'elaborazione del disegno è stato verificato se e in quale misura le competenze e responsabilità esistenti in materia di sicurezza delle informazioni corrispondessero alle odierne esigenze. Sebbene il mandato d'esame riguardasse, in linea di principio, soltanto l'Amministrazione federale, i risultati ottenuti forniscono importanti riscontri in merito all'organizzazione della sicurezza delle informazioni per tutte le autorità.

Organizzazione attuale della sicurezza delle informazioni nell'Amministrazione federale

Nell'Amministrazione federale le competenze e le responsabilità in materia di protezione delle informazioni sono disciplinate da atti normativi ed enti regolamentatori diversi a seconda del tipo di informazione (p. es. informazioni classificate o dati personali) oppure in base al tipo di trattamento o di misura di protezione (elettronici o fisici). Di conseguenza, la Confederazione gestisce anche diverse organizzazioni parallele che si occupano di compiti principali o parziali in materia di sicurezza delle informazioni (protezione delle informazioni, protezione dei dati, sicurezza informatica ecc.).

Organizzazione della protezione delle informazioni

La protezione delle informazioni è disciplinata principalmente nell'OPrI. Sono previste disposizioni complementari nei cosiddetti accordi sulla protezione delle informazioni. L'OPrI si applica solo all'Amministrazione federale e all'esercito. L'attuazione della protezione delle informazioni è decentralizzata e viene coordinata a livello centrale da organi ai quali non è riconosciuta la facoltà di impartire istruzioni. La Conferenza dei segretari generali (CSG) è competente per le prescrizioni di dettaglio (catalogo di classificazione e prescrizioni in materia di trattamento). Le prescrizioni in materia di trattamento contengono anche prescrizioni di comportamento per la gestione elettronica di informazioni classificate e definiscono requisiti tecnici per quanto riguarda la sicurezza in occasione dell'impiego di mezzi informatici. I dipartimenti e la Cancelleria federale devono designare un proprio incaricato della protezione delle informazioni. Sebbene l'OPrI non lo esiga, tutti i dipartimenti hanno designato ulteriori consulenti per la protezione delle informazioni a livello di unità amministrativa. Un comitato di coordinamento provvede a un'esecuzione

uniforme in seno alla Confederazione e prepara i documenti all'attenzione della CSG. È appoggiato da un organo di coordinamento.

Organizzazione della protezione dei dati

Le basi legali applicabili al trattamento di dati personali sono contenute nelle rispettive leggi speciali. L'organizzazione della protezione dei dati in seno alla Confederazione è invece, in linea di principio, definita nella LPD e nell'OLPD. A differenza dell'OPrI, questi atti normativi si applicano anche ai privati. L'esecuzione della protezione dei dati è decentralizzata, ma è sottoposta alla sorveglianza centralizzata dell'IFPDT e coordinata dal Gruppo interdipartimentale per la protezione dei dati, organo informale privo della facoltà di impartire istruzioni. I dipartimenti e la Cancelleria federale devono designare un proprio consulente per la protezione dei dati. Sebbene non fosse obbligatorio, tutti i dipartimenti hanno designato ulteriori consulenti per la protezione dei dati a livello di unità amministrativa.

Organizzazione della sicurezza informatica

L'organizzazione della sicurezza informatica è definita principalmente nell'ordinanza sull'informatica nell'Amministrazione federale (OIAF), ma le competenze e responsabilità specifiche sono influenzate anche da numerosi altri atti normativi (OPrI, accordi sulla protezione delle informazioni, OLPD, ordinanza GEVER ecc.). Il Consiglio federale emana istruzioni riguardanti la sicurezza informatica. L'esecuzione della sicurezza informatica è decentralizzata. I dipartimenti e la Cancelleria federale sono responsabili dell'attuazione nei rispettivi ambiti. L'esecuzione è però coordinata a livello centrale da un organo con la facoltà di impartire istruzioni (ODIC). L'ODIC decide in merito a disciplinamenti speciali in relazione all'attribuzione di diritti e mandati rilevanti sotto il profilo della sicurezza, in particolare riguardo a firewall, diritti d'accesso e privilegi. Decide misure di sicurezza specifiche qualora l'Amministrazione federale fosse esposta a rischi. Accerta, quale organo peritale incaricato da un dipartimento o dalla Cancelleria federale, i fatti connessi a incidenti in materia di sicurezza presunti o avvenuti. Nomina l'incaricato della sicurezza informatica della Confederazione.

L'ODIC è affiancato da due organi consultivi. Il Comitato per la sicurezza informatica appoggia l'ODIC quale organo consultivo per tutte le questioni di sicurezza informatica e ha un ruolo di coordinamento interdipartimentale. Il Consiglio informatico della Confederazione è l'organo consultivo dell'ODIC per gli affari informatici (compresi quelli relativi alla sicurezza) per i quali è richiesta la concertazione con i dipartimenti e la Cancelleria federale, in particolare per l'emanazione di direttive e l'approvazione di deroghe. Per l'esecuzione, i dipartimenti, la Cancelleria federale e le unità amministrative devono designare ognuno un incaricato della sicurezza informatica che svolga compiti di coordinamento.

Oltre a queste strutture organizzative di base, in seno alla Confederazione vi è un gran numero di altri organi o servizi che si occupano di sicurezza informatica, in particolare la SIO presso lo Stato maggiore dell'esercito, il *Computer Emergency Response Team* (CERT) militare e il settore Sicurezza dell'informazione e Crittologia della Base d'aiuto alla condotta dell'esercito (BAC), il settore Scienza e tecnologia presso armasuisse (armasuisse è il servizio della Confederazione competente per gli acquisti di beni e servizi nell'ambito della crittologia), la centrale MELANI, lo

Stato maggiore speciale per la sicurezza dell'informazione e il *Computer Security Incident Response Team* (CSIRT) dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT). Il CDF svolge le revisioni in campo informatico in seno all'Amministrazione federale.

Lacune e punti deboli in ambito organizzativo

L'attuale organizzazione presenta molteplici lacune e punti deboli, per esempio:

- oggi la Confederazione gestisce sia dal punto di vista legale che organizzativo strutture parallele per sottosettori della sicurezza delle informazioni. In tale contesto, spesso la delimitazione delle competenze non è chiara. L'attenzione dedicata alle interfacce è insufficiente. A risentirne non è solo l'effettiva sicurezza delle informazioni: anche il coordinamento di affari politici che hanno relazioni con la sicurezza delle informazioni e la collaborazione con i Cantoni e con i partner internazionali risultano molto più difficoltosi;
- troppi attori non dispongono di sufficienti conoscenze specialistiche, perché possono occuparsi della sicurezza delle informazioni solo come compito accessorio;
- spesso gli attuali incaricati dispongono di risorse insufficienti per adempiere i propri compiti. La massa critica non viene mai raggiunta. In alcune organizzazioni le risorse sarebbero sufficienti nel loro complesso, ma vengono sfruttate male perché suddivise tra moltissime persone;
- la maggior parte dei costi della sicurezza non viene presentata in modo trasparente, il che impedisce di valutare l'economicità delle misure;
- i poteri degli specialisti sono insufficienti: nella maggior parte dei casi svolgono solo compiti di coordinamento e non possono quindi né eseguire audit né intervenire nel caso di carenze accertate. Inoltre gli specialisti, in particolare nel settore informatico, sottostanno spesso a un settore specialistico del quale dovrebbero valutare i rischi in modo indipendente, il che comporta conflitti di interesse;
- la gestione della sicurezza è carente. La sicurezza delle informazioni è considerata una mera questione tecnica. Le usuali attività direttive (p. es. definizione di obiettivi, controllo dell'attuazione o verifica dell'efficacia) vengono quindi applicate soltanto raramente all'ambito della sicurezza. La linea gerarchica a tutti i livelli deve beneficiare di una consulenza, un'assistenza e una formazione più competente;
- la consapevolezza in materia di sicurezza non è sufficiente. Spesso le misure di formazione non vanno a beneficio delle persone che svolgono compiti sensibili sotto il profilo della sicurezza. Un considerevole numero di persone viene sottoposto a un CSP, ma non viene formato in modo adeguato sugli aspetti relativi alla sicurezza delle informazioni.

L'attuale organizzazione si è sviluppata sotto la spinta di necessità giuridiche e materiali settoriali. Per lungo tempo ha dato risultati sufficienti. Con l'evoluzione in atto verso una società dell'informazione, tuttavia, le minacce che incombono sulle

informazioni e sui mezzi informatici sono diventate sempre più complesse e dinamiche. Queste minacce devono essere affrontate con un approccio integrale e professionale, che richiede un corrispondente assetto giuridico e organizzativo e maggiori conoscenze e competenze specialistiche. Manifestamente l'organizzazione della Confederazione non soddisfa queste esigenze.

I vari organi specializzati devono essere per quanto possibile raggruppati per sfruttare le sinergie e ottenere effetti di scala. Il raggruppamento consente anche di trovare una soluzione sistemica ai problemi di competenza e di accumulare maggiori conoscenze specialistiche interdisciplinari. Le competenze dei vari incaricati possono essere sviluppate grazie alla crescente professionalizzazione. La professionalità migliorerebbe se i compiti legati alla gestione della sicurezza delle informazioni fossero concentrati su un numero di titolari il più possibile ridotto.

Nuovo disciplinamento dell'organizzazione a livello di Confederazione

Il disegno fornisce la base per chiarire e semplificare le competenze e le responsabilità. Pone l'accento sullo sviluppo del know-how dei servizi competenti per l'esecuzione, il quale avviene in particolare con il sostegno di specialisti e un'intensificazione dello scambio di informazioni. Il disegno prevede di conseguenza un'unica figura di incaricato, un unico organo di coordinamento e un servizio specializzato della Confederazione che dovranno svolgere tutti i compiti trasversali in materia di sicurezza delle informazioni. Con il nuovo disciplinamento si mira a fondere le strutture di esecuzione appartenenti ai settori della protezione delle informazioni e della sicurezza delle informazioni, finora separati.

Incaricati della sicurezza delle informazioni

La nuova figura dell'incaricato della sicurezza delle informazioni assume un ruolo centrale per l'esecuzione. La sua funzione è soprattutto una funzione di gestione. Il compito principale degli incaricati della sicurezza delle informazioni non sarà quello di occuparsi delle questioni altamente tecniche legate alla sicurezza delle informazioni, bensì di dirigere, su mandato della rispettiva autorità (o dei dipartimenti e della Cancelleria federale) la sicurezza delle informazioni e di verificare l'attuazione delle misure decise. Dovranno inoltre concentrarsi sulla gestione dei rischi e sul coordinamento con altri ambiti. Per poter adempiere i propri compiti in maniera efficace, oltre a beneficiare di un chiaro sostegno da parte delle rispettive direzioni gli incaricati della sicurezza delle informazioni devono necessariamente operare in stretta collaborazione con i servizi competenti per la gestione generale dei rischi, la protezione dei dati e la sicurezza. Gli incaricati della sicurezza delle informazioni rappresenteranno pertanto l'elemento di collegamento tra le direzioni e i servizi competenti per l'attuazione delle misure.

In seno ai dipartimenti e alla Cancelleria federale, questa nuova funzione sostituirà i ruoli degli incaricati della protezione delle informazioni e degli incaricati della sicurezza informatica, finora separati. Il Consiglio federale dovrà decidere, a livello di ordinanza, in merito all'adeguatezza e alla necessità di un raggruppamento delle funzioni anche a livello delle unità organizzative subordinate.

Conferenza degli incaricati della sicurezza delle informazioni

In virtù dell'indipendenza delle autorità sancita dalla Costituzione federale, un livello di sicurezza uniforme può essere raggiunto soltanto se, in materia di sicurezza delle informazioni, vige una dottrina specifica il più possibile unitaria nonostante le esigenze in parte divergenti. Grazie alla loro posizione, gli incaricati della sicurezza delle informazioni dispongono di ampie conoscenze della situazione e dei problemi relativi alla sicurezza delle informazioni nel proprio ambito di competenza, in particolare per quanto concerne la realizzabilità e l'efficacia delle prescrizioni e delle misure. È pertanto opportuno istituzionalizzare a livello di legge, in qualità di organo di coordinamento, una conferenza che riunisca tutti questi incaricati.

La Conferenza si occuperà principalmente del coordinamento dell'esecuzione tra tutte le autorità e della valutazione degli standard proposti. In tale ambito, svolgerà un ruolo importante per lo sviluppo di una dottrina uniforme. Nella Conferenza sono rappresentati anche i Cantoni e l'IFPDT. Per le questioni strategiche la Conferenza potrà rivolgersi a specialisti del mondo scientifico e dell'economia. Per l'Amministrazione federale, sostituirà l'attuale Comitato di coordinamento per la protezione delle informazioni in seno alla Confederazione (contemplato dall'OPrI) e il Comitato per la sicurezza informatica (previsto dall'OIAF), mentre le questioni tecniche continueranno a essere trattate da organi specializzati subordinati.

Servizio specializzato della Confederazione per la sicurezza delle informazioni

La sicurezza delle informazioni deve essere organizzata, diretta e verificata secondo un approccio integrale. Vari compiti, tra quelli menzionati dalla presente legge, sono già oggi svolti da diversi organi specializzati. Di conseguenza, tali compiti vengono concepiti e affrontati da un punto di vista settoriale e risultano poco coordinati tra loro. Migliorare il coordinamento non è sufficiente, di per sé, a realizzare l'approccio integrale. È quindi necessario creare un servizio specializzato centrale quale centro di competenza per i compiti comuni a tutte le autorità. Si tratta di un servizio specializzato, sprovvisto della facoltà di impartire istruzioni, che in linea di principio opera sempre su richiesta o su mandato di un'autorità assoggettata e che va inteso come organo con compiti di assistenza e consulenza.

Nella legge vengono stabiliti in modo esaustivo i compiti concreti del servizio specializzato che concernono tutte le autorità. Oltre a fornire consulenza e assistenza, su richiesta il servizio specializzato può anche valutare i rischi in occasione dell'impiego di nuove tecnologie o dirigere e coordinare la sicurezza delle informazioni nell'ambito di progetti importanti che coinvolgono più autorità. Un altro compito fondamentale del servizio specializzato è inoltre quello di esaminare (su richiesta delle autorità assoggettate), per determinati processi, mezzi e prestazioni, gli aspetti rilevanti sotto il profilo della sicurezza. Se i risultati dell'esame confermano che tali aspetti soddisfano i requisiti stabiliti dalla Confederazione, essi possono essere standardizzati e, di conseguenza, impiegati anche da altre autorità o organizzazioni della Confederazione (riduzione dell'onere). Il servizio specializzato può inoltre effettuare, su richiesta, controlli e audit in materia di sicurezza. Sarà infine l'interlocutore per i contatti specializzati con servizi esteri e internazionali nel campo della sicurezza delle informazioni, ruolo necessario per l'attuazione di trattati internazionali (v. n. 5.2).

Il Consiglio federale disciplinerà a livello di ordinanza l'organizzazione del servizio specializzato. Dovrà stabilire quali compiti il servizio specializzato deve adempiere autonomamente e quali in collaborazione con altri servizi federali. Attualmente, nell'ambito della sicurezza delle informazioni, molti servizi dell'Amministrazione federale svolgono compiti trasversali che figurano nell'elenco dei compiti del futuro servizio specializzato della Confederazione. Il servizio specializzato dovrà per esempio svolgere per l'Amministrazione federale determinati compiti che oggi vengono svolti dal settore Sicurezza dell'ODIC e dalla SIO. Di conseguenza, i compiti delle unità organizzative esistenti verranno ridefiniti a livello di ordinanza e sarà necessario verificare alcune interfacce.

Nuovo disciplinamento per l'Amministrazione federale

Secondo quanto sopra menzionato, il servizio specializzato della Confederazione per la sicurezza delle informazioni non dispone, a livello giuridico, di poteri esecutivi nei confronti delle autorità. Per l'Amministrazione federale il Consiglio federale può invece conferire ulteriori competenze al servizio specializzato e impostare in modo differenziato il rapporto che tale servizio intrattiene con i superiori gerarchici e con gli incaricati della sicurezza delle informazioni. Sebbene la responsabilità della decisione e dell'attuazione delle direttive debba essere lasciata alla linea gerarchica, una netta maggioranza dei partecipanti ai lavori legislativi si è espressa a favore dell'attribuzione di una maggiore competenza esecutiva al servizio specializzato, in particolare per quanto concerne gli audit. L'organizzazione della sicurezza delle informazioni presso le unità assoggettate dell'Amministrazione federale decentralizzata e presso le organizzazioni di cui all'articolo 2 capoverso 4 LOGA sarà esaminata dal Consiglio federale in sede di emanazione del diritto esecutivo. La LSIn prevede tuttavia che il Consiglio federale conceda una sufficiente autonomia a tali organizzazioni.

1.3 Motivazione e valutazione della soluzione proposta

Le motivazioni che stanno alla base del disciplinamento proposto sono state descritte nel dettaglio al numero 1.2. Di seguito verrà posto l'accento sulle alternative esaminate e su vantaggi e svantaggi della soluzione scelta.

1.3.1 Alternative esaminate

Atto normativo unico

Le basi legali della Confederazione per la protezione delle informazioni si sono sviluppate in modo molto settoriale, risultano poco coordinate tra loro e spesso lacunose. Inoltre non sono in linea con le esigenze della società dell'informazione. L'impronta settoriale complica la gestione degli affari politici e operativi che hanno una relazione con la protezione delle informazioni. Dal momento che le responsabilità sono suddivise in base all'ambito specialistico, la spesa necessaria per il coordinamento è aumentata notevolmente. Tutte le misure che la Confederazione deve

adottare per la protezione delle informazioni dovranno quindi convergere in un unico atto normativo. Questo approccio integrale è conforme agli standard internazionali.

È stata presa in esame la possibilità di elaborare una legge specifica per i CSP e per la PSA. Una soluzione di questo tipo avrebbe il vantaggio che le misure generali della sicurezza delle informazioni (secondo capitolo) acquisirebbero più importanza grazie al numero di disposizioni. È stata però scartata perché sia i CSP che le PSA costituiscono già oggi misure della sicurezza delle informazioni, e l'esecuzione di entrambi dipende dalle disposizioni concernenti la classificazione, il livello di sicurezza dei mezzi informatici e le zone di sicurezza. La soluzione richiederebbe altresì la definizione di nuove competenze e responsabilità, il che aumenterebbe l'onere di coordinamento sia giuridico che organizzativo.

È stata anche esaminata la possibilità di completare o modificare leggi già esistenti (LOGA, LParl, LM, LPers ecc.). Questa soluzione sarebbe vantaggiosa perché permetterebbe di evitare la creazione di una nuova legge. Comporterebbe però anche svantaggi determinanti. Tutte le leggi da adeguare presentano un campo di applicazione strettamente settoriale, il che impedirebbe nella pratica un'esecuzione orientata a un approccio integrale. Le lacune individuate potrebbero quindi essere colmate – sempre che sia possibile – solo con un onere di coordinamento sproporzionato. Una tale soluzione impedirebbe di fatto anche la necessaria applicazione di criteri e misure uniformi a tutte le autorità. Il Consiglio federale ha quindi scartato fin dal principio questa alternativa.

La sicurezza delle informazioni (compresi i CSP e la PSA) presenta un nesso molto stretto con la protezione degli oggetti. Attualmente la materia è disciplinata in vario modo da diverse disposizioni legali di struttura piuttosto disparata. L'esame effettuato ha evidenziato che, pur essendo auspicabile armonizzare in una certa misura queste disposizioni o creare una base legale uniforme, un simile intervento, data la sua portata sul piano materiale e organizzativo, andrebbe al di là del quadro della LSIn. Il progetto contiene tuttavia due disposizioni sulle misure di protezione fisica delle informazioni.

Si è inoltre rinunciato a definire fattispecie materiali di rilevanza penale. Le disposizioni del Codice penale e del Codice penale militare relative alla tutela del segreto d'ufficio e alla protezione di informazioni della Confederazione classificate o degne di protezione non dovrebbero essere rivedute a titolo accessorio nel quadro di un atto normativo speciale di natura organizzativa, bensì nell'ambito di un progetto legislativo indipendente.

Campo d'applicazione

Campo d'applicazione materiale

Il disegno di legge ingloba tutte le informazioni e tutti i dati e mira a proteggerli per quanto riguarda la loro confidenzialità, disponibilità, integrità e tracciabilità. L'ampio campo d'applicazione materiale è conforme allo stato della scienza e della prassi e limitarlo alle informazioni sensibili non sarebbe opportuno. Per valutare se un'informazione è sensibile sono infatti indispensabili criteri e meccanismi di valutazione che, inevitabilmente, devono essere applicati a tutte le informazioni. Inoltre,

una simile limitazione renderebbe impossibili sia l'aumento dell'efficienza cui si mira con la prevista standardizzazione sia le sinergie auspicate.

Campo d'applicazione istituzionale

I motivi per cui tutte le autorità federali devono essere contemplate dalla legge sono ampiamente illustrati al numero 1.2.2. Se si limitasse la legge all'Amministrazione federale e all'esercito, il Consiglio federale sarebbe l'unico responsabile dell'esecuzione e la LSIn verrebbe notevolmente ridotta, ma permarrebbero le lacune nel quadro generale valido per tutte le autorità. Inoltre, le altre autorità federali non potrebbero beneficiare di importanti risorse specialistiche dell'Amministrazione federale (p. es. CSP o PSA). L'obiettivo di garantire un livello di sicurezza uniforme potrebbe essere raggiunto solo con un enorme onere amministrativo (numerosi accordi). Per questi motivi riteniamo che un ampio campo d'applicazione con un'esecuzione decentralizzata sia la soluzione più efficiente ed economica.

Classificazione

Visto che, da un lato, il modello a tre livelli agevola la collaborazione con partner esteri e internazionali, i quali applicano principalmente un sistema a quattro livelli, e, dall'altro, permette anche una protezione delle proprie informazioni più adeguata ai rischi, abbiamo respinto un modello di classificazione alternativo a due livelli. È pure stata respinta la classificazione di dati personali nonché di segreti d'affari e di fabbricazione, in quanto i criteri di classificazione sono stabiliti nella legislazione settoriale (LPD) oppure devono essere convenuti con i proprietari delle informazioni.

Inoltre si è esaminato se il trattamento delle informazioni della Confederazione classificate «segreto» debba in linea di principio essere riservato ai cittadini svizzeri. Simili restrizioni sono usuali nel contesto internazionale. Siccome le autorità federali devono ricorrere a specialisti stranieri anche nell'ambito della sicurezza, abbiamo deciso di rinunciarvi.

Sistemi di gestione delle identità

È stata presa in esame una rinuncia all'utilizzazione del numero d'assicurato AVS. Siamo tuttavia convinti che la soluzione proposta sia più economica e semplice e garantisca una protezione dei dati almeno equivalente.

CSP

Riteniamo che il disciplinamento proposto tenga meglio conto delle esigenze attuali in materia di sicurezza delle informazioni e che nel contempo si presti a ridurre nettamente il numero di CSP da eseguire. Ciò permetterebbe anche di ridurre il relativo onere finanziario e amministrativo. Si è inoltre esaminato se l'esecuzione di CSP in Svizzera debba ancora essere ammessa solo per il trattamento di informazioni classificate «segreto», per l'amministrazione e l'esercizio di mezzi informatici del livello di sicurezza «protezione molto elevata» e per l'accesso alle corrispondenti zone di sicurezza, nel qual caso sarebbe comunque fatta salva l'esecuzione di CSP per l'accesso a informazioni classificate «confidenziale» provenienti dall'estero. Un simile approccio si applicherebbe anche alla verifica dell'affidabilità secondo la

LPers e la LM. Questa soluzione ridurrebbe ulteriormente l'onere. Ciononostante è stata respinta in quanto sul piano internazionale rappresenterebbe un'eccezione e sarebbe contraria all'armonizzazione auspicata nell'ambito della collaborazione internazionale.

PSA

Riteniamo che il nuovo disciplinamento permetterà di impiegare in modo mirato e poco burocratico la PSA. Il relativo onere sarà limitato al minimo. Analogamente al disciplinamento in materia di CSP, si è esaminato se la PSA debba essere eseguita solo per il trattamento di informazioni classificate «segreto», per l'amministrazione e l'esercizio di mezzi informatici del livello di sicurezza «protezione molto elevata» e per l'accesso alle corrispondenti zone di sicurezza, il che troverebbe una più ampia applicazione nel contesto internazionale. Tuttavia, per gli stessi motivi addotti nel caso dei CSP, questa variante è stata respinta.

È inoltre stata analizzata una regolamentazione secondo cui la valutazione da parte del servizio specializzato SA non sarebbe vincolante per il mandante. Questo sistema corrisponderebbe al disciplinamento del CSP. Il vantaggio consisterebbe nel fatto che l'intera responsabilità per l'assegnazione del mandato verrebbe lasciata al mandante, il quale dovrebbe anche assumere rischi più elevati. Per diversi motivi, questa alternativa non è tuttavia stata presa in considerazione. In primo luogo, la DSA rappresenta una sorta di «sigillo di sicurezza» dello Stato che deve essere rilasciato dall'autorità di sicurezza nazionale e la tutela dell'integrità di questo sigillo può essere garantita solo se la decisione concernente l'idoneità è presa da specialisti. In secondo luogo, contrariamente al CSP, la PSA non termina dopo il controllo dell'azienda, ma si estende anche al controllo dell'attuazione delle misure. Se il mandante non fosse vincolato alla valutazione, queste competenze in materia di controllo non avrebbero senso. In terzo luogo, nella prassi è piuttosto raro che un'azienda sia considerata problematica sotto il profilo della sicurezza. Se dovesse verificarsi un simile caso eccezionale, occorre provvedere affinché l'azienda in questione non esegua alcun mandato sensibile per la Confederazione.

Infrastrutture critiche

I motivi per una rinuncia, nel campo della sicurezza delle informazioni, a direttive e obblighi di comunicazione centralizzati per le infrastrutture critiche sono spiegati nella SNPC.

Esecuzione

Il campo d'applicazione istituzionale non deve limitare l'indipendenza costituzionale delle autorità interessate. Pertanto, le autorità federali devono eseguire autonomamente la legge, anche se il disegno definisce diversi strumenti per garantire disposizioni e misure unitarie. L'esecuzione autonoma presenta uno svantaggio, ossia i requisiti organizzativi minimi che devono essere soddisfatti da tutte le autorità federali devono essere imperativamente stabiliti nella legge. Di conseguenza il disegno di legge contiene anche diverse disposizioni che, sotto il profilo della gerarchia normativa, corrispondono piuttosto al livello di un'ordinanza.

È pure stata esaminata una delega di competenze normative all'Assemblea federale (ordinanza parlamentare) o al Consiglio federale per tutte le autorità. Una simile delega permetterebbe di fissare numerose disposizioni a livello di ordinanza. Il disegno di legge risulterebbe di conseguenza più snello. Nel quadro delle diverse consultazioni, le autorità federali interessate si sono tuttavia opposte a qualsiasi assoggettamento al diritto esecutivo di un'altra autorità. Per lo stesso motivo si è rinunciato a un organo direttivo inter-autorità con la facoltà di impartire istruzioni. La soluzione dell'esecuzione decentralizzata tutela l'indipendenza costituzionale delle differenti autorità federali e permette un'esecuzione flessibile e adeguata ai rischi secondo le necessità di sicurezza effettive delle rispettive autorità. Dal nostro punto di vista, i vantaggi della soluzione proposta sono chiaramente maggiori rispetto agli svantaggi.

Organizzazione

L'organizzazione proposta incrementa la professionalità nell'ambito della sicurezza delle informazioni, definisce chiaramente le competenze e tiene conto dell'esecuzione decentralizzata. In generale si fonda su strutture e organi esistenti, che vengono in parte raggruppati e dotati di compiti adeguati alle esigenze di una società dell'informazione. Una rinuncia a questi organi, in particolare al servizio specializzato della Confederazione per la sicurezza delle informazioni, renderebbe molto più difficile un'esecuzione unitaria efficace. Inoltre, le autorità e le organizzazioni dovrebbero sviluppare autonomamente le capacità (p. es. crittologia e audit tecnici) che, per motivi economici, dovrebbero piuttosto essere messe a disposizione a livello centralizzato.

1.3.2 Procedura di consultazione

Pareri risultanti dalla procedura di consultazione

Il 26 marzo 2014 il Consiglio federale ha licenziato l'avamprogetto concernente la legge federale sulla sicurezza delle informazioni e ha avviato la procedura di consultazione, che si è conclusa il 4 luglio 2014. Sono stati invitati a partecipare alla consultazione 62 destinatari. Complessivamente sono pervenute al DDPS 55 risposte (26 Cantoni, 4 partiti politici, 24 organizzazioni e altre cerchie interessate).

Una vasta maggioranza dei partecipanti alla consultazione ha in linea di massima accolto positivamente la creazione di una legge sulla sicurezza delle informazioni. In parte sono state formulate riserve su singoli punti dell'avamprogetto. Solo un partito (UDC) ha respinto l'avamprogetto di legge nella sua totalità. Un Cantone e un'associazione mantello nazionale dell'economia hanno invece affermato di poter approvare il disegno solo dopo una sostanziale rielaborazione di alcuni aspetti normativi e della documentazione accompagnatoria.

In particolare è stato chiesto di migliorare i seguenti aspetti:

- collaborazione tra Confederazione e Cantoni;
- normativa in materia di infrastrutture critiche;
- ripercussioni finanziarie per la Confederazione e i Cantoni.

Adeguamento dell'avamprogetto posto in consultazione

Il 5 novembre 2014 il Consiglio federale ha preso conoscenza del rapporto sui risultati della procedura di consultazione[22] e ha incaricato il DDPS di elaborare un messaggio.

Le modifiche più importanti apportate all'avamprogetto posto in consultazione sono le seguenti:

- il disciplinamento della collaborazione tra Confederazione e Cantoni è stato ora concepito secondo il modello della legislazione sulla protezione dei dati. Inoltre, i Cantoni concorreranno strettamente all'elaborazione delle disposizioni esecutive e degli standard. Saranno rappresentati nella Conferenza degli incaricati della sicurezza delle informazioni e potranno usufruire della consulenza e del sostegno del servizio specializzato della Confederazione per la sicurezza delle informazioni. Il Consiglio federale potrà infine autorizzare i Cantoni a utilizzare per le proprie necessità le prestazioni dei servizi specializzati previsti dalla presente legge;
- le disposizioni sulle infrastrutture critiche sono state rielaborate, in particolare per quanto concerne il disciplinamento del trattamento dei dati;
- la LSIn è stata completata con una sezione sull'impiego di sistemi d'informazione centralizzati per la gestione delle identità (IAM Confederazione);
- la protezione penale nei confronti della violazione del segreto d'ufficio secondo l'articolo 320 CP e della violazione del segreto di servizio secondo l'articolo 77 CPM è stata estesa agli ausiliari esterni. In considerazione del fatto che oggi il ricorso a prestazioni di servizi informatici esterni da parte della Confederazione e dei Cantoni è inevitabile, il Consiglio federale ritiene che tale estensione debba essere attuata al più presto;
- alcune disposizioni sono state adeguate in modo tale da preservare la libertà d'azione delle autorità assoggettate, e in particolare del Consiglio federale, per quanto riguarda i costi dell'attuazione e l'organizzazione.

Inoltre sono state effettuate numerose semplificazioni. Diverse osservazioni sono state prese in considerazione mediante complementi o precisazioni dei commenti.

1.3.3 Valutazione complessiva

Negli ultimi tempi la sicurezza delle informazioni è diventata sempre più importante, anche dal punto di vista politico. Numerosi incidenti e gli sviluppi internazionali hanno mostrato quanto, con la maggiore dipendenza dall'informatica, la nostra società sia diventata vulnerabile. Dal punto di vista politico non vi sono dubbi che la Confederazione debba tutelarsi meglio dalle nuove minacce. Si tratta infatti, in ultima analisi, di garantire l'adempimento di compiti fondamentali come la salva-

22 www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione ed indagini conoscitive concluse > 2014 > DDPS > Legge federale sulla sicurezza delle informazioni

guardia della sicurezza interna ed esterna, degli interessi in materia di politica economica, finanziaria e monetaria della Svizzera nonché la tutela della capacità di decisione e d'azione delle autorità federali. Con questo progetto riteniamo di proporre un quadro legale formale equilibrato e nel contempo adeguato per una sicurezza delle informazioni moderna in seno Confederazione. I risultati della consultazione confermano ampiamente questa opinione. Le richieste più importanti dei partecipanti alla consultazione, in particolare quelle dei Cantoni, sono state prese in considerazione.

1.4 Diritto comparato

Osservazioni generali

Alla luce degli sviluppi nell'informatica, la maggior parte degli Stati limitrofi della Svizzera e le organizzazioni internazionali con cui quest'ultima intrattiene intense relazioni sta procedendo a una verifica delle proprie prescrizioni in materia di sicurezza. Non è possibile presentare una panoramica di questi lavori in corso. Inoltre, spesso le normative nel campo della sicurezza sono difficilmente accessibili. In un compendio tematico vengono confrontati regolamenti e prescrizioni di alcuni Paesi nel contesto europeo della Svizzera concentrandosi su determinati aspetti della sicurezza delle informazioni. Per la comparazione sono stati scelti i seguenti Paesi: Germania, Francia, Italia e Austria, in quanto Stati confinanti con la Svizzera, nonché Gran Bretagna, Paesi Bassi e Svezia. Sono stati analizzati in particolare i seguenti aspetti: il tipo di disciplinamento della sicurezza delle informazioni e il rispettivo campo d'applicazione istituzionale, il sistema di classificazione, il CSP, la PSA e l'organizzazione delle autorità.

Tipo di disciplinamento della sicurezza delle informazioni

La Germania stabilisce i principi della sicurezza delle informazioni a livello di legge con prescrizioni amministrative e direttive esecutive. In Francia numerosi atti normativi a livello di Costituzione, leggi e ordinanze disciplinano la sicurezza delle informazioni. In Italia il settore della sicurezza delle informazioni è definito in una legge, due decreti del Presidente del Consiglio dei Ministri e in istruzioni dell'Autorità nazionale per la sicurezza, mentre nei Paesi Bassi è disciplinato in diversi atti normativi di vari livelli. In Svezia le normative in materia di sicurezza delle informazioni sono contenute in diverse leggi. Per l'ambito della sicurezza industriale non esistono atti normativi specifici. L'Austria non dispone di alcun disciplinamento unitario che copra integralmente la sicurezza delle informazioni. La legge austrica relativa alla sicurezza delle informazioni disciplina tuttavia la classificazione nonché l'esecuzione di CSP. Nei singoli Stati federati (Bundesländer) si applicano solo le disposizioni della normativa in materia di pubblico impiego (Beamtendienstrecht), per esempio quelle relative al segreto d'ufficio (Amtsverschwiegenheit). Nemmeno in Gran Bretagna esistono leggi specifiche concernenti la sicurezza delle informazioni. Tuttavia esiste una base costituita da diversi atti normativi. Le linee direttive della politica di sicurezza nazionale sono stabilite nel cosiddetto *Security Policy Framework*, che definisce le condizioni cui Amministrazione, Governo, autorità e mandanti devono assolutamente attenersi.

L'UE disciplina in maniera pressoché completa la protezione delle proprie informazioni classificate. Sia la decisione del Consiglio del 23 settembre 2013[23] sulle norme di sicurezza per proteggere le informazioni classificate UE (2013/488/UE) sia la decisione della Commissione del 13 marzo 2015[24] sulle norme di sicurezza per proteggere le informazioni classificate UE (2015/444/UE, Euratom) disciplinano le classificazioni, la sicurezza del personale – inclusi i CSP – e la sicurezza materiale nonché la sicurezza informatica e la sicurezza industriale. Per quanto riguarda la sicurezza tecnica delle informazioni va inoltre citato il regolamento UE n. 526/2013 del 21 maggio 2013[25] relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004.

Campo d'applicazione istituzionale

In Germania rientrano nel campo d'applicazione le autorità federali e gli enti direttamente sottoposti ad autorità federali. Inoltre esistono direttive per le aziende che trattano informazioni classificate (Verschlusssachen, VS). La Francia applica per tutti i ministeri un disciplinamento concernente la protezione delle informazioni che può comunque essere oggetto di ulteriori precisazioni da parte dei singoli ministri. In Italia le prescrizioni si applicano all'intero settore pubblico, all'industria e alle singole persone che trattano informazioni classificate. I parlamentari, i ministri e i giudici che, in forza della loro funzione, necessitano dell'accesso a informazioni classificate non vengono controllati. In Austria le normative si applicano esclusivamente agli uffici federali. L'industria è obbligata da convenzioni di diritto privato ad applicare le disposizioni federali. In Gran Bretagna il *Security Policy Framework* è applicabile a tutti i servizi di autorità, agenzie e mandanti che si occupano di mandati classificati. Alcune parti si applicano anche alla polizia. Nei Paesi Bassi il *Security Investigation Act* si applica a tutte le unità amministrative e all'industria. Le prescrizioni in materia di trattamento delle informazioni classificate e di sicurezza delle informazioni si applicano solo all'Amministrazione. Le norme relative alla sicurezza industriale nel settore della difesa si applicano alle corrispondenti imprese. In Svezia determinati atti normativi sono applicabili a tutte le autorità, altri si applicano al Governo, ma non al Parlamento.

Nell'UE le disposizioni sono ampiamente armonizzate, ma ogni organo indipendente emana le proprie prescrizioni in modo autonomo (Parlamento, Consiglio e Commissione).

Sistema di classificazione

Francia e Gran Bretagna ricorrono a un sistema di classificazione a tre livelli. Germania, Italia, Austria e Paesi Bassi prevedono invece un sistema di classificazione a quattro livelli. La Svezia applica quattro livelli di classificazione nel settore militare e solo due per le altre autorità.

23 http://eur-lex.europa.eu/legal-content/it/TXT/PDF/?uri=CELEX:32013D0488
24 http://eur-lex.europa.eu/legal-content/it/TXT/PDF/?uri=OJ:JOL_2015_072_R_0011
25 http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32013R0526

Per l'UE si applicano i quattro livelli di classificazione seguenti:

- *TRÈS SECRET UE/EU TOP SECRET:* la divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri;
- *SECRET UE/EU SECRET:* la divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;
- *CONFIDENTIEL UE/EU CONFIDENTIAL:* la divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri;
- *RESTREINT UE/EU RESTRICTED:* la divulgazione non autorizzata potrebbe essere pregiudizievole per gli interessi dell'Unione europea o di uno o più Stati membri.

CSP

In Germania i presupposti necessari per eseguire un CSP sono l'accesso immediato ed effettivo a informazioni classificate o la possibilità di conoscere tali informazioni. Il controllo è eseguito dall'Ufficio federale della protezione della Costituzione (Bundesamt für Verfassungsschutz), la cui valutazione è vincolante. In Francia, per un CSP la funzione della persona interessata nell'Amministrazione o nell'economia privata deve essere riportata in un elenco delle funzioni. La relativa autorizzazione è rilasciata, a seconda del livello di classificazione, da una determinata autorità. La valutazione dei rischi non è vincolante. In Italia, nella richiesta relativa al CSP devono essere indicati i motivi per cui la persona necessita dell'accesso a informazioni classificate nonché il livello di classificazione. La persona da sottoporre al controllo deve confermare di essere informata in merito alla necessità del CSP e dare il proprio consenso. La procedura è eseguita dall'autorità competente in collaborazione con la polizia, la Guardia di finanza, le Forze armate e l'Amministrazione. La valutazione è vincolante.

In Austria le persone possono essere controllate su richiesta di imprese qualora vengano impiegate in funzioni sensibili o in settori critici per la sicurezza e acconsentano al CSP. Nel settore militare è determinante l'intenzione di accedere a informazioni classificate. I controlli spettano a un'autorità diversa per ciascun settore, civile o militare. In Gran Bretagna si esegue un CSP al fine di confermare l'identità di una persona e di verificarne la fidatezza prima di concederle l'accesso a informazioni e materiali classificati o a infrastrutture critiche nazionali. In Svezia è determinante anche l'accesso a informazioni classificate. Nei Paesi Bassi le funzioni che richiedono un CSP sono inserite in un elenco delle funzioni, che vengono definite da ogni ministero. Il criterio è il danno che può essere causato nell'esercizio di tali funzioni. I CSP sono eseguiti dal servizio informazioni generale e da quello militare, le cui valutazioni dei rischi sono vincolanti.

Nell'UE è richiesto un CSP per l'accesso a informazioni classificate CONFIDENTIEL UE/EU CONFIDENTIAL o di livello più elevato. La valutazione è effettuata dall'autorità di sicurezza nazionale dello Stato membro conformemente alle prescri-

zioni legali interne. La decisione dell'autorità di sicurezza nazionale è vincolante per l'autorità dell'UE.

PSA

Ai fini dello svolgimento di una PSA, in Germania è necessaria l'aggiudicazione concreta di un mandato classificato CONFIDENZIALE o di livello più elevato oppure la partecipazione a un bando corrispondente. Il Ministero tedesco dell'economia e dell'energia esegue la valutazione dei rischi, che è vincolante per il mandante. In Francia, per l'esecuzione di una PSA si richiede un contratto per il cui adempimento è necessario l'allestimento di informazioni classificate o di materiale classificato oppure l'accesso a simili informazioni o materiali. La valutazione dei rischi non è vincolante. In Italia spetta al mandante provvedere all'avvio della PSA riguardo all'azienda interessata dopo l'aggiudicazione di un mandato classificato «segreto». La valutazione dei rischi è vincolante. In Austria è determinante l'intenzione di accedere a informazioni classificate. La valutazione dei rischi non è vincolante. In Gran Bretagna la condizione per l'avvio di una PSA è che, in relazione a un mandato del Governo, l'azienda in questione tratti informazioni classificate «segreto» o di livello più elevato oppure materiale con una classificazione corrispondente. Nei Paesi Bassi, per una PSA si presuppone che l'azienda sia prevista quale possibile mandataria per un mandato classificato del settore della difesa. L'esecuzione della procedura incombe a un servizio del Ministero della difesa. Se l'azienda è prevista quale possibile mandataria per un mandato internazionale classificato, la procedura è eseguita dal Ministero dell'interno e dei territori d'oltremare, la cui valutazione è vincolante. In Svezia, il *Protective Security Act* esige che le autorità che intendono procedere ad acquisti in relazione con la sicurezza nazionale concludano con l'azienda prevista quale mandataria un accordo in materia di sicurezza. L'azienda deve previamente sottoporsi a un audit secondo i criteri prestabiliti nell'*Industrial Security Manual*. Non appena noti i risultati, l'agenzia competente per gli acquisti di armamenti effettua controlli presso l'azienda.

Nell'UE la PSA è richiesta per gli acquisti pubblici che prevedono un accesso a informazioni classificate a partire dal livello EU CONFIDENTIAL. La procedura si basa sulle prescrizioni legali dello Stato membro. La decisione dell'autorità di sicurezza nazionale è vincolante per l'autorità dell'UE.

Organizzazione delle autorità

In Germania l'autorità nazionale di sicurezza è il Ministero dell'interno. Il Ministero federale dell'economia e dell'energia ha la competenza esclusiva per la tutela del segreto nell'economia. In Francia, il Segretario generale della Difesa e della sicurezza nazionale è l'unica autorità nazionale di sicurezza. L'*Agence nationale de la sécurité des systèmes d'information* è competente per la sicurezza delle tecnologie dell'informazione. In Italia il Presidente del Consiglio dei ministri rappresenta l'autorità nazionale di sicurezza. Egli può in parte delegare le sue competenze in materia al Segretario di Stato e beneficia dell'assistenza di un comitato per la sicurezza nazionale (Comitato interministeriale per la sicurezza della Repubblica), il cui segretario è direttore generale del *Dipartimento delle informazioni per la sicurezza*. In Austria esiste una Commissione per la sicurezza delle informazioni per il settore

civile e il servizio di intelligence militare (Abwehramt) per il settore militare. Anche se in Gran Bretagna il *Cabinet Office* funge da autorità nazionale di sicurezza, le singole unità amministrative e agenzie continuano a essere responsabili della sicurezza delle loro informazioni nonché di quelle dei loro mandatari.

Nei Paesi Bassi esistono due autorità nazionali di sicurezza: l'autorità nazionale civile di sicurezza presso il servizio generale di intelligence e sicurezza del Ministero dell'interno e dei territori d'oltremare e l'autorità nazionale militare di sicurezza in seno al Ministero della difesa olandese. Nemmeno in Svezia esiste un'autorità di sicurezza globale. Il compito è ripartito tra le forze armate e il Ministero degli esteri (per le informazioni di ESA, UE e NATO). Per poter adempiere tutti i compiti di un'autorità nazionale di sicurezza, il Ministero degli esteri coordina tuttavia le differenti competenze.

Anche nell'UE esistono diverse autorità di sicurezza. In seno al Consiglio, l'Ufficio di sicurezza del segretariato generale è responsabile delle normative tecniche per la protezione delle informazioni classificate, mentre presso la Commissione europea questo ruolo è svolto dalla direzione «Sicurezza». Nel settore della sicurezza delle reti e dell'informazione l'organo competente è invece l'ENISA.

Infrastrutture critiche

La sicurezza delle informazioni presso le infrastrutture critiche è già stata oggetto di confronti approfonditi nel quadro della SNPC, per cui in questa sede non si entra più nel merito in modo dettagliato. Ciononostante, dall'adozione della SNPC sia l'UE che la Germania hanno sviluppato nuove normative che sono riassunte qui di seguito.

Unione europea

L'8 agosto 2016 è entrata in vigore la direttiva (UE) 2016/1148[26] del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Per l'UE un'infrastruttura informatica sicura è essenziale per il funzionamento affidabile del mercato interno. Tale obiettivo sarà raggiunto obbligando gli Stati membri a incrementare la propria preparazione e a migliorare la collaborazione tra di loro. Inoltre, i gestori di infrastrutture critiche e determinati fornitori di servizi digitali (mercati in linea, motori di ricerca in linea e servizi di cloud computing) saranno obbligati a intraprendere misure minime per gestire i rischi in materia di sicurezza e a notificare alle autorità nazionali competenti eventuali incidenti gravi. Gli obblighi di sicurezza per i fornitori di servizi digitali sono tuttavia meno rigidi rispetto a quelli dei gestori di infrastrutture critiche. In linea di principio, le piccole e medie imprese nonché le amministrazioni pubbliche sono esonerate da tali obbligo.

La direttiva stabilisce una serie di misure organizzative per le autorità. Ad esempio, ogni Stato membro è tenuto a:

– definire una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;

26 GU L 194 del 19.7.2016, pag. 1.

- istituire una o più autorità nazionali incaricate di controllare l'applicazione delle direttive da parte dei gestori di infrastrutture critiche e dei fornitori di servizi digitali;
- designare un punto di contatto che svolge una funzione di collegamento per garantire la cooperazione transfrontaliera degli Stati membri;
- designare uno o più Gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) che gestiscono un servizio nazionale di preallerta e un punto di contatto nell'ambito della sicurezza tecnica delle informazioni a favore dei gestori di infrastrutture critiche e dei fornitori di servizi digitali assoggettati (cfr. anche art. 75 LSIn).

La direttiva definisce inoltre i requisiti concernenti la cooperazione a livello nazionale e internazionale nonché le risorse delle competenti autorità specializzate.

Gli Stati membri sono tenuti a integrare la direttiva nella rispettiva legislazione nazionale entro maggio 2018. Di conseguenza negli anni a venire numerosi Stati membri dell'UE adegueranno la propria legislazione nazionale per quanto riguarda la sicurezza delle informazioni.

Germania

La legge tedesca del 17 luglio 2015 per l'incremento della sicurezza dei sistemi IT (IT-Sicherheitsgesetz) persegue obiettivi simili a quelli della direttiva dell'UE summenzionata; l'entrata in vigore è tuttavia antecedente. La normativa prevista si concentra sulle infrastrutture critiche, i cui gestori devono rispettare un livello minimo di sicurezza delle informazioni e notificare gli incidenti all'Ufficio federale tedesco per la sicurezza in ambito IT (Bundesamt für Sicherheit in der Informationstechnik [BSI]). Le informazioni confluite nel BSI vengono valutate e messe a disposizione degli operatori affinché possano migliorare la protezione delle proprie infrastrutture. Parallelamente è stata rafforzata la funzione di consulenza del BSI in questo ambito. Gli offerenti di servizi di telecomunicazione sono tenuti a garantire la sicurezza *secondo lo stato della tecnica*. Inoltre, devono comunicare immediatamente determinati incidenti e informare gli utenti interessati in merito ai guasti noti.

Contrariamente alla direttiva dell'UE che esclude dal suo campo d'applicazione le autorità pubbliche, il campo d'applicazione della legge per l'incremento della sicurezza dei sistemi IT (IT-Sicherheitsgesetz) comprende anche le autorità federali tedesche, fatta eccezione per il Bundestag.

Risultato dell'analisi di diritto comparato

In molti Paesi europei le basi legali per la sicurezza delle informazioni vengono adeguate alla nuova realtà della società dell'informazione. Dato che in parte gli ordinamenti giuridici e le strutture statali dei diversi Paesi si differenziano sostanzialmente, la gerarchia normativa e il campo d'applicazione dei corrispondenti disciplinamenti possono difficilmente essere confrontati. Si può invece affermare che, in linea di principio, le disposizioni della LSIn corrispondono o sono perlomeno in sintonia con le normative degli Stati presi in esame. Sotto il profilo organizzativo, grazie al servizio specializzato della Confederazione per la sicurezza delle informazioni la Confederazione disporrà di un unico punto di contatto sul piano internazio-

nale. La collaborazione internazionale nel campo della sicurezza delle informazioni sarà quindi più semplice ed efficiente.

Nel settore delle infrastrutture critiche, con la SNPC e la LSIn il nostro Collegio assume invece una posizione diversa da quella dell'UE o della Germania e molto meno vincolante per i gestori di tali infrastrutture. Puntiamo sull'autoresponsabilità delle infrastrutture critiche nonché su un sostegno da parte della Confederazione mirato e in funzione delle esigenze. Non è pertanto nostra intenzione definire standard minimi per le infrastrutture critiche né obbligare queste ultime a effettuare notifiche in caso di incidenti gravi.

1.5 Attuazione

Per quanto riguarda il disciplinamento dell'esecuzione da parte delle autorità assoggettate vedi il numero 1.2.9. Le autorità assoggettate sono tenute a eseguire la legge in maniera autonoma. Esse emanano le necessarie disposizioni esecutive, fermo restando che le disposizioni esecutive del Consiglio federale si applicano alle altre autorità federali nella misura in cui queste ultime non emanano disposizioni esecutive proprie (sussidiarietà). Questo principio esecutivo è stato convenuto con le autorità interessate.

Nel quadro della consultazione è stata messa in discussione l'attuabilità dell'avamprogetto in relazione ai Cantoni. Si è criticato in particolare il fatto che i criteri per l'applicazione del progetto ai Cantoni non sono chiari, per cui è pressoché impossibile definire le ripercussioni per questi ultimi. Nell'ambito della valutazione dei risultati della consultazione si è pertanto deciso di concepire la collaborazione con i Cantoni secondo il modello affermato della legislazione sulla protezione dei dati (cfr. art. 37 LPD). Anche le altre richieste dei Cantoni (partecipazione all'elaborazione delle disposizioni esecutive, accesso alle risorse della Confederazione per lo svolgimento di CSP, consulenza da parte del servizio specializzato della Confederazione per la sicurezza delle informazioni ecc.) sono state ampiamente prese in considerazione (v. n. 1.2.2).

Nella prassi il servizio specializzato della Confederazione per la sicurezza delle informazioni preparerà i progetti delle disposizioni esecutive e degli standard e li sottoporrà alla Conferenza degli incaricati della sicurezza delle informazioni ai fini della valutazione dell'efficacia, dell'economicità, e dell'attuabilità. Le norme consolidate verranno in seguito approvate dal Consiglio federale. Le autorità federali e i Cantoni saranno invitati a esprimere il proprio parere in merito a tutti i disciplinamenti importanti generanti dei costi. In tal modo, da un lato, si consegue un livello di sicurezza il più uniforme possibile e, dall'altro, si tiene debitamente conto delle esigenze di tutte le autorità federali e dei Cantoni.

Per determinati oggetti della normativa, il diritto esecutivo può essere emanato in modo rapido e semplice. Ciò concerne in particolare il CSP (cap. 3), la PSA (cap. 4) e la sicurezza delle informazioni presso le IC (cap. 5), ma anche i sistemi d'informazione per il controllo centralizzato delle identità (cap. 2, sez. 6). Per l'esecuzione delle misure generali in materia di sicurezza delle informazioni (cap. 2) sono invece necessari ulteriori chiarimenti. In tale contesto si tratta di processi fondamentali e

requisiti che devono essere adeguati e armonizzati per tutte le autorità secondo lo stato della scienza e della tecnica.

La LSIn prevede tempo sufficiente per un'attuazione ragionevole. Il nostro Consiglio la porrà in vigore solo quando le disposizioni esecutive e le basi necessarie saranno pronte. Se del caso sarà possibile un'entrata in vigore a tappe. Faremo esaminare periodicamente l'efficacia della legge e riferiremo all'autorità di vigilanza competente. I corrispondenti controlli a livello cantonale spetteranno ai Cantoni stessi.

2 Commento ai singoli articoli

2.1 Legge sulla sicurezza delle informazioni

Titolo

L'atto normativo non costituisce alcuna legge generale sulla sicurezza delle informazioni. Si rivolge in primo luogo alle autorità federali e a organizzazioni di diritto pubblico e privato, da determinare, incaricate di eseguire compiti federali. Anche se terzi possono rientrare nel campo d'applicazione della legge qualora utilizzino informazioni o di mezzi informatici della Confederazione, tuttavia ciò accade solamente con l'applicazione delle disposizioni rilevanti da parte di un'autorità o di un'organizzazione della Confederazione.

La nozione di *sicurezza delle informazioni* si rifà, in linea di massima, alle norme attualmente in uso. La sicurezza delle informazioni comprende quindi la totalità di tutti i requisiti e tutte le misure con i quali si proteggono la confidenzialità, l'integrità, la disponibilità e la tracciabilità di informazioni, nonché la disponibilità e l'integrità di mezzi informatici (v. art. 6). Non può essere ridotta alla sicurezza informatica: comprende infatti tutti i processi di elaborazione, dunque anche documenti cartacei e affermazioni orali, e non soltanto il trattamento elettronico. La nozione include anche la sicurezza dei dati secondo l'articolo 7 LPD o l'attuazione di altre leggi che stabiliscono requisiti per la protezione di informazioni.

L'integrazione del disciplinamento del CSP e della PSA nel progetto legislativo significa che entrambi gli strumenti sono da intendersi quali misure *particolari* della sicurezza delle informazioni. I motivi per lo svolgimento di simili controlli derivano dalle misure generali per la sicurezza delle informazioni.

Ingresso

Vedi numero 5.1.

Capitolo 1: Disposizioni generali

Art. 1 Scopo

Il capoverso 1 segnala che sia le informazioni in quanto tali sia i mezzi informatici rientrano nel campo d'applicazione della legge. Il termine di *informazione* non viene definito nella LSIn, poiché il termine nella LSIn coincide con l'uso colloquiale. In linea di principio, la legge non distingue tra *informazioni* e *dati*: entrambe le nozioni vengono sussunte sotto il termine di *informazioni*. Il termine *dati* viene utilizzato solamente se sono interessati dati personali ai sensi della LPD. Il termine *mezzi informatici* viene definito all'articolo 5.

Capoverso 2: la sicurezza non è fine a se stessa. La protezione delle informazioni serve a determinati interessi pubblici o interessi propri della Confederazione in quanto istituzione. Qui vengono dunque protetti in primo luogo gli interessi della Confederazione o della Svizzera e non quelli di terzi. Questi interessi vengono elencati esaustivamente (lett. a–e). L'elenco si rifà sostanzialmente all'elenco dell'articolo 7 capoverso 1 LTras, che menziona gli ambiti nei quali il diritto di accesso a un documento ufficiale può essere limitato, differito o negato. L'elenco dell'articolo 1 capoverso 2 LSIn non è tuttavia del tutto identico a quello della LTras, poiché gli obiettivi e il campo d'applicazione di quest'ultima e della LSin non coincidono (v. anche n. 1.2.3).

La presente legge protegge gli interessi seguenti:

- la protezione della capacità di decisione e d'azione delle autorità federali (lett. a) mediante misure per la sicurezza delle informazioni è un interesse cruciale di questa legge. Per l'adempimento dei loro compiti costituzionali e legali le autorità federali dipendono sempre di più dalla disponibilità, dall'integrità e, in determinati casi, dalla confidenzialità delle loro informazioni, nonché dal funzionamento affidabile dell'infrastruttura informatica (v. art. 7 cpv. 1 lett. a e b LTras e n. 2.2.2.1.1 e 2.2.2.1.2 del messaggio LTras);
- ai sensi della lettera b vengono protette in primo luogo informazioni dai settori della polizia, delle dogane, del servizio informazioni e degli affari militari e dell'approvvigionamento del Paese, nonché i mezzi che le autorità federali impiegano per garantire la sicurezza interna ed esterna. Siffatte informazioni spesso presentano un'elevata esigenza di confidenzialità, poiché il loro utilizzo abusivo rischia di pregiudicare la sopravvivenza dello Stato, della popolazione o di determinate persone o gruppi di persone. Per lo stesso motivo, i mezzi informatici delle autorità impiegati per supportare compiti di sicurezza critici devono rimanere sempre disponibili e funzionanti anche in tempi di crisi (v. art. 7 cpv. 1 lett. c LTras e n. 2.2.2.1.3 del messaggio LTras);
- insieme alle questioni relative alla sicurezza, le relazioni estere (lett. c) sono fra i settori sensibili dell'attività dello Stato. Qui l'accento è posto sulla tutela della confidenzialità delle informazioni. In particolare l'acquisizione di informazioni su situazioni e fatti all'estero, nonché sulle intenzioni di autorità estere e internazionali, assumono grande rilevanza per dirigere la politica

estera e curare le relazioni internazionali. Per condurre a buon fine dei negoziati è fondamentale che le relative strategie e intenzioni non vengano rese note alla controparte o al pubblico. Lo stesso dicasi per gli interventi diplomatici nei rapporti tra gli Stati. Occorre infine menzionare che, a motivo di impegni assunti nell'ambito di trattati internazionali o di una prassi riconosciuta tra gli Stati, la Svizzera può essere tenuta a non rendere accessibili al pubblico taluni documenti esteri (v. art. 7 cpv. 1 lett. d LTras e n. 2.2.2.1.4 del messaggio LTras);

– lettera d: la comunicazione non autorizzata o la falsificazione di determinate informazioni, nonché il disturbo dei sistemi d'informazione delle autorità federali, possono danneggiare considerevolmente gli interessi in materia di politica economica, finanziaria o monetaria della Svizzera. Nell'implacabile concorrenza internazionale attuale, questi interessi economici assumono ancora maggiore importanza (v. art. 7 cpv. 1 lett. f LTras e n. 2.2.2.1.6 del messaggio LTras);

– alla lettera e viene considerato il settore della *compliance*, vale a dire il rispetto degli impegni assunti in virtù di leggi e trattati dalle autorità federali per proteggere informazioni che non rientrano nelle lettere a–d. Per adempiere i loro compiti legali, le autorità federali trattano moltissime informazioni che devono proteggere in virtù delle più disparate disposizioni legali (LPD, LOGA, LParl, LBN, LAPub, LFC ecc.) o che ricevono da terzi soltanto a condizione di garantire una protezione adeguata. I segreti professionali, d'affari o di fabbricazione o la tutela della confidenzialità e integrità di dati personali non rappresentano interessi diretti della Confederazione, ma essa è tenuta a proteggere tali informazioni in virtù della legge o di un accordo. Qualora dovesse emergere che le autorità federali non rispettano i loro impegni per proteggere queste informazioni, la loro affidabilità potrebbe soffrirne considerevolmente. La lettera e rappresenta quindi un collettore per tutte le informazioni che le autorità federali trattano e proteggono, ma non necessariamente devono classificare. Tale lettera protegge inoltre l'interesse delle autorità federali a mantenere la loro elevata affidabilità (v. art. 7 cpv. 1 lett. e, g e h LTras e n. 2.2.2.1.5, 2.2.2.1.7 e 2.2.2.1.8 del messaggio LTras).

Art. 2 Autorità e organizzazioni assoggettate

Quali autorità assoggettate ai sensi del capoverso 1 vengono menzionati l'Assemblea federale, il Consiglio federale, i tribunali della Confederazione (Tribunale federale, Tribunale penale federale, Tribunale amministrativo federale, Tribunale federale dei brevetti, tribunali militari, tribunali militari di appello e Tribunale militare di cassazione), il Ministero pubblico della Confederazione e la sua autorità di vigilanza, nonché – nell'interesse della politica monetaria ed economica della Confederazione – la Banca nazionale svizzera. Nella loro attività in qualità di autorità, tutte queste istituzioni non sono assoggettate alla facoltà diretta di emanare istruzioni di alcuna altra autorità. In conseguenza del flusso di informazioni tra autorità, esse vanno però obbligate ad applicare il presente atto normativo nel proprio ambito di competenza organizzativo. Purché la legge contenga deleghe legislative, si rivolge a queste autorità designandole sempre *autorità assoggettate*. Riguardo ai motivi per

cui tutte le autorità federali debbano rientrare nel campo d'applicazione della legge, vedi il numero 1.2.2.

Rimane inteso che, in singole normative, la LSIn deve tenere conto dello statuto costituzionale e delle particolarità delle varie autorità o istituzioni. Essa contiene perciò, ad esempio, deroghe all'obbligo del CSP per le persone elette dal Popolo, nonché deroghe per determinate competenze esecutive, in particolare nell'ambito dei tribunali della Confederazione. In quelle disposizioni dell'atto normativo che contengono solamente obblighi per determinate autorità od organizzazioni, questi vengono specificati di conseguenza (p. es. art. 7 o 10 cpv. 2). A livello di legge, non vanno però stabilite l'intera organizzazione esecutiva delle varie autorità e le competenze dei loro organi o servizi. Ciò deve avvenire mediante le relative disposizioni d'esecuzione delle singole autorità.

Il capoverso 2 considera che le autorità menzionate nel capoverso 1 devono occuparsi soltanto in misura limitata di veri e propri compiti esecutivi e che le organizzazioni a esse subordinate, nell'ambito dei propri compiti legali, vanno assoggettate direttamente alle nuove normative nell'ambito delle proprie competenze. La ripartizione tra autorità e organizzazioni subordinate è intesa in particolare a garantire che il differente diritto organizzativo delle autorità considerate non venga toccato dalla nuova normativa. Da un lato, le autorità assoggettate non devono avere l'obbligo di assumere in proprio compiti esecutivi subordinati e, dall'altro, le autorità considerate non devono però ottenere competenze normative o decisionali in deroga al diritto organizzativo. L'espressione *organizzazioni assoggettate* viene introdotta come designazione abbreviata nell'interesse della semplificazione, sotto il profilo della tecnica legislativa, degli articoli successivi. Si tratta in particolare dei Servizi del Parlamento, delle amministrazioni dei singoli tribunali della Confederazione, dei Dipartimenti, della Cancelleria federale (CaF), dell'esercito e dell'Amministrazione federale, ivi comprese le unità amministrative decentrate ai sensi dell'articolo 2 capoverso 3 LOGA.

Sono sostanzialmente assoggettate alla legge anche le organizzazioni di diritto pubblico e privato che adempiono compiti amministrativi della Confederazione ai sensi dell'articolo 2 capoverso 4 LOGA (v. in proposito art. 8 cpv. 4 e 5 LOGA). Si tratta, in particolare, di organizzazioni che per legge sono autorizzate a emanare decisioni nei confronti di privati. Per tali organizzazioni la Confederazione risponde infatti soltanto a titolo sussidiario (v. art. 19 LResp). L'assoggettamento delle unità amministrative decentrate e delle organizzazioni che adempiono compiti amministrativi al di fuori dell'Amministrazione federale non è assoluto. Dato che in virtù delle rispettive disposizioni organizzative i rapporti tra queste organizzazioni e la Confederazione sono in parte caratterizzati da una grande eterogeneità, l'assoggettamento effettivo si giustifica soltanto nei casi in cui queste organizzazioni hanno un carattere rilevante per la sicurezza della Confederazione, come previsto al capoverso 3 per le organizzazioni che esercitano attività sensibili sotto il profilo della sicurezza oppure utilizzano mezzi informatici della Confederazione o strettamente connessi a quelli della Confederazione. Il Consiglio federale esaminerà la rilevanza delle varie organizzazioni sotto il profilo della sicurezza nell'ambito della normativa d'esecuzione e definirà a livello di ordinanza quali di esse devono applicare integralmente o in parte la LSIn. Questo aspetto può essere disciplinato negli atti norma-

tivi d'esecuzione della LSIn o nelle disposizioni d'esecuzione delle pertinenti leggi speciali. Se necessario, il Consiglio federale può fare applicare da queste organizzazioni soltanto parti della legge (p. es. disposizioni sulla classificazione, sull'impiego di mezzi informatici o sui CSP). In tale contesto stabilirà inoltre, conformemente al capoverso 4, se e in che misura le organizzazioni in questione devono occuparsi autonomamente dell'esecuzione della legge. Le organizzazioni escluse dal campo d'applicazione della LSIn sono considerate terzi.

Il capoverso 5 stabilisce anzitutto in maniera generale che il sostegno fornito dalle organizzazioni che gestiscono infrastrutture critiche (organizzazioni IC) è retto dalle disposizioni del capitolo 5. Le organizzazioni IC esterne alla Confederazione possono concludere volontariamente un partenariato con la Confederazione e in tale ambito beneficiare del suo sostegno, ed è per questa ragione che i pertinenti articoli vengono in linea di principio dichiarati applicabili – benché non obbligatori – a dette organizzazioni. È evidente che le infrastrutture critiche gestite direttamente dalla Confederazione devono invece applicare la LSIn senza restrizioni. La LSIn fornisce alla Confederazione strumenti particolari nell'ambito della sicurezza delle informazioni dei quali taluni regolatori e organizzazioni IC vorrebbero servirsi, in particolare il CSP, ma in parte anche le disposizioni relative alla classificazione o alla sicurezza dei mezzi informatici. Determinate organizzazioni IC già oggi si servono di questi strumenti della Confederazione. Ciò è ad esempio il caso nell'ambito delle centrali nucleari, nel quale la Confederazione prescrive determinate misure per la sicurezza delle informazioni (v. art. 5 e 24 LENu). Si mantiene perciò il principio che in caso di necessità la legislazione speciale può prevedere un assoggettamento alla LSIn (o a parti di essa) per talune organizzazioni IC.

Art. 3 Applicabilità ai Cantoni

Sulla collaborazione con i Cantoni, vedi il numero 1.2.2; sui CSP per gli impiegati cantonali, vedi gli articoli 30 e 32; sull'esecuzione da parte dei Cantoni, vedi l'articolo 87.

Art. 4 Rapporto con altre leggi federali

Sul rapporto con la LTras e con la legislazione sulla protezione dei dati, vedi il numero 1.2.3. Il capoverso 1 stabilisce che la LTras prevale sulla LSIn; il suo campo d'applicazione non viene dunque limitato in alcun modo da quest'ultima. Il capoverso 2 disciplina il rapporto del nuovo atto normativo con le numerose leggi federali che stabiliscono requisiti per la protezione della confidenzialità, della disponibilità, dell'integrità o della tracciabilità di informazioni o per la disponibilità e l'integrità di mezzi informatici. L'applicabilità a titolo completivo significa che la LSIn crea una cornice unitaria per la valutazione della necessità di protezione di queste informazioni e per l'applicazione dei requisiti di sicurezza posti a queste informazioni dalla legislazione speciale.

Art. 5 Definizioni

Alcune definizioni o espressioni, fondamentali per il progetto legislativo, non possono essere definite con maggiore precisione a livello di legge, poiché altrimenti

limiterebbero eccessivamente il margine di manovra necessario di autorità, organizzazioni e servizi. È il caso, in particolare, di espressioni quali *pregiudizio*, *pregiudizio considerevole* e *pregiudizio grave* per gli interessi di cui all'articolo 1 capoverso 2.

Lettera a: il termine *mezzi informatici* viene utilizzato quale termine generale per tutti i mezzi delle tecnologie dell'informazione e della comunicazione. A livello di ordinanza e di istruzioni saranno, dove necessario, utilizzati e definiti termini più dettagliati (sistema d'informazione, rete, applicazione, trasmissione vocale, telefonia ecc.). Un mezzo informatico può comprendere più sistemi o mezzi costituenti un'unità funzionale.

Lettera b: l'*attività sensibile sotto il profilo della sicurezza* rappresenta una nozione centrale. L'esercizio di una simile attività, infatti, non è importante solamente per l'applicazione della legge a organizzazioni di cui all'articolo 2 capoversi 3 e 4 LOGA, ma anche come presupposto per l'esecuzione di CSP e di PSA. Viene definita nello stretto contesto della sicurezza delle informazioni secondo la presente legge.

– Indicando il livello di classificazione «confidenziale» come punto di partenza per definire l'attività sensibile sotto il profilo della sicurezza, il numero 1 stabilisce implicitamente che la sensibilità sotto il profilo della sicurezza di un'attività viene presunta soltanto se gli interessi di cui all'articolo 1 capoverso 2 possono venire pregiudicati almeno *considerevolmente*. Sensibile sotto il profilo della sicurezza è inoltre non il semplice *accesso* a queste informazioni, bensì il loro *trattamento* effettivo e autorizzato. In altre parole, ad esempio, il personale addetto alle pulizie non esercita, di regola, alcuna attività sensibile sotto il profilo della sicurezza ai sensi della presente legge, sebbene sia grande la probabilità che durante la sua attività possa talvolta accedere di fatto a informazioni classificate perché i collaboratori non sempre rispettano le prescrizioni di sicurezza. Non è espressamente menzionata ma è comunque compresa anche l'utilizzazione di *materiale classificato* a partire dal livello «confidenziale». Il materiale non deve essere confuso con il *supporto di informazioni*, che serve a portare materialmente l'informazione immateriale per i fini più diversi. Per materiale classificato si intendono invece apparecchi e oggetti le cui caratteristiche possono rivelare informazioni classificate: il materiale *è* o contiene *inscindibilmente* l'informazione (immateriale) protetta. Si tratta principalmente di oggetti d'armamento o di sistemi di comunicazione integrati in ambito militare. Sovente uno Stato terzo che ha autorizzato la fornitura alla Svizzera prescrive la classificazione.

– Al numero 2 vengono considerate le attività connesse a particolari diritti di accesso a mezzi informatici dei due livelli di sicurezza più elevati o nell'esercizio delle quali delle persone sono in grado, ad esempio, di pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2 attraverso il furto di dati o il sabotaggio. Il semplice utilizzo di questi mezzi informatici non viene dunque considerato come sensibile sotto il profilo della sicurezza (si decide se gli utenti esercitano un'attività sensibile sotto il profilo della sicurezza in base ai contenuti delle informazioni trattate). Vengono inclusi soprattutto amministratori o responsabili delle applicazioni dei siste-

mi con necessità di protezione elevata o molto elevata. Ai sensi di questo numero, il termine *esercizio* si riferisce all'attività dei fornitori di servizi secondo l'articolo 19 LSIn. Tale termine va chiaramente distinto dall'espressione *gestire sistemi d'informazione* utilizzata nella legislazione in materia di protezione dei dati per disciplinare in realtà *l'impiego* di sistemi d'informazione da parte dei beneficiari di prestazioni (v. p. es. l'art. 24 cpv. 1 LSIn).

– Al numero 3 viene infine designato come sensibile sotto il profilo della sicurezza l'accesso alle zone di sicurezza (art. 23), poiché in queste zone, a causa delle informazioni e dei mezzi informatici che vi si trovano, il potenziale di danno in caso di spionaggio o di sabotaggio è molto alto. Viene incluso anche l'accesso alle zone di protezione 2 o 3 secondo la legislazione sulla protezione di impianti militari, considerate zone di sicurezza (v. art. 19 cpv. 1 lett. c LMSI).

Rispetto all'attuale norma riguardante il presupposto per lo svolgimento di CSP (v. art. 19 cpv. 1 LMSI), la nozione di *attività sensibile sotto il profilo della sicurezza* ha, da un lato, un'accezione più ampia, poiché considera le maggiori esigenze in materia di sicurezza nel settore dell'informatica. Dall'altro, è però anche concepita in modo più limitato, perché non comprende più l'accesso regolare a dati personali degni di particolare protezione, la cui divulgazione potrebbe gravemente pregiudicare i diritti individuali delle persone interessate (v. n. 1.2.5).

Lettera c: questa definizione è identica a quella dell'articolo 6 capoverso 1 lettera a numero 4 LAIn. Entrambe le definizioni si ispirano alla terminologia in materia di protezione della popolazione.

Capitolo 2: Misure generali

Sezione 1: Principi

Art. 6 Sicurezza delle informazioni

L'articolo 6 considera il contenuto materiale della sicurezza delle informazioni e i più importanti principi in base ai quali deve essere attuata. Esso completa quindi l'articolo sullo scopo (art. 1), in quanto illustra dettagliatamente gli obiettivi di protezione.

Capoverso 1: la necessità di protezione delle informazioni viene definita nell'ottica del potenziale pregiudizio per gli interessi di cui all'articolo 1 capoverso 2 e definita in relazione ai dettagliati criteri del capoverso 2. Per sua stessa natura, la specifica necessità di protezione assai sovente viene implicitamente prevista da altre leggi (v. anche art. 1 cpv. 2 lett. e nonché art. 4 cpv. 2).

Sotto il profilo materiale, la dottrina e la prassi menzionano per lo più quattro criteri di protezione inerenti alla sicurezza delle informazioni, da ponderare di volta in volta secondo le circostanze: tutela della confidenzialità, dell'integrità, della disponibilità e della tracciabilità delle informazioni. Spesso vengono menzionati ulteriori criteri di protezione che però, in linea di principio, vengono coperti dai criteri indica-

ti nel capoverso 2 o eventualmente da una combinazione degli stessi, ad esempio l'autenticità (inclusa nell'«integrità»), l'imputabilità o l'incontestabilità (derivati dai criteri di «integrità» e di «tracciabilità»).

- Confidenzialità: questo principio viene concretato nel senso che le informazioni devono essere accessibili solamente alle persone autorizzate. La cerchia delle persone autorizzate risulta dal contesto dell'adempimento dei rispettivi compiti legali, nonché dal contenuto e dalla rilevanza dell'informazione. Di conseguenza, la cerchia delle persone autorizzate può essere limitata a poche persone o molto ampia.
- Disponibilità: per la capacità di decisione e d'azione delle autorità e organizzazioni è indispensabile che nell'ambito dell'adempimento dei compiti legali esse possano accedere tempestivamente alle informazioni necessarie. I requisiti posti alla disponibilità di informazioni sono più elevati se queste devono essere disponibili senza interruzioni per l'adempimento di compiti essenziali.
- Integrità: la salvaguardia dell'inalterabilità e dell'esattezza delle informazioni è, tra l'altro, rilevante per informazioni destinate a essere pubblicate o riutilizzate (v. n. 1.1.1, OGD). Anche dati personali (art. 5 LPD) o informazioni della contabilità (art. 38 LFC) devono essere corretti. La salvaguardia dell'integrità è inoltre decisiva per il corretto funzionamento di determinati mezzi informatici.
- Tracciabilità: la tracciabilità del trattamento delle informazioni è di notevole rilevanza in particolare per tutte le procedure pubbliche (procedimenti penali, procedure di ricorso ecc.), ma anche per l'adempimento dei compiti di controllo e di vigilanza e per la procedura in caso di abusi.

Secondo i capoversi 1 e 2, le autorità e le organizzazioni assoggettate devono dunque procedere a una valutazione della necessità di protezione di informazioni e stabilire per quale aspetto e in che misura le informazioni devono essere protette. La protezione della confidenzialità, ad esempio, è necessaria solamente se tale confidenzialità deve essere garantita per una ragione giuridica. Determinate informazioni possono avere requisiti più elevati per la protezione della loro integrità o disponibilità, senza che questi particolari requisiti siano stabiliti per legge, per esempio se le relative informazioni devono essere necessariamente corrette o disponibili affinché un'autorità possa adempiere i propri compiti. Ciò riguarda in particolare le informazioni e i mezzi informatici che supportano processi aziendali critici.

Sebbene in linea di massima il requisito di una protezione adeguata dei mezzi informatici dall'utilizzazione abusiva e dai disturbi risulti già dal capoverso 2 lettere b e c, esso viene ancora menzionato esplicitamente perché il supporto ai processi aziendali da parte della tecnica assume una rilevanza sempre maggiore. Il loro buon funzionamento rappresenta oggi un presupposto indispensabile per l'adempimento efficace dei compiti delle autorità federali.

Rimane inteso che una sicurezza assoluta costituisce un ideale irraggiungibile e che l'onere per eliminare le esigue lacune di sicurezza rimanenti può diventare eccessivamente elevato. Le autorità e le organizzazioni competenti devono perciò badare a che le loro misure siano adeguate ed economiche. Di conseguenza, nel definire le

misure di protezione gli organi superiori devono procedere a una ponderazione degli interessi tra i costi legati alla sicurezza e i benefici derivanti da essa. Se le misure di sicurezza rendono troppo difficile ai collaboratori adempiere i propri compiti, è grande la probabilità che non vengano rispettate oppure che vengano addirittura eluse di proposito.

Art. 7 Responsabilità direttiva suprema

La sicurezza è di competenza dei capi. Perciò le autorità assoggettate vengono anzitutto invitate a organizzare, applicare e verificare secondo lo stato della scienza e della tecnica la sicurezza delle informazioni nel loro ambito. Varie norme tecniche formulano corrispondenti migliori prassi (*best practices)* e stabiliscono requisiti per l'applicazione di misure di sicurezza che possono essere adeguati ai bisogni delle rispettive autorità od organizzazioni o di parti di esse. La legge non esige che le autorità, ad esempio, realizzino un ISMS secondo la norma DIN ISO/IEC 27001. La loro organizzazione dovrebbe però per lo meno orientarvisi. Le autorità con un effettivo di personale esiguo non potranno ovviamente costituire una propria siffatta organizzazione. La legge consente perciò, ad esempio, ai tribunali della Confederazione di decidere di costituire un'unica organizzazione comune che nel contempo tuteli l'autonomia dei vari tribunali. Per un'applicazione uniforme della legge è necessario che le autorità optino per un modello organizzativo comune. Poiché la realizzazione della sicurezza delle informazioni concerne molti ambiti specialistici (le finanze, i servizi del personale, il diritto, l'informatica, la gestione dei rischi ecc.), gli ambiti specialistici interessati devono condividere gli obiettivi della sicurezza delle informazioni e partecipare al processo decisionale.

Alle autorità si chiede anche di disciplinare la verifica della sicurezza delle informazioni. In linea di principio, tale controllo incombe ai superiori gerarchici. Anche gli incaricati della sicurezza delle informazioni effettueranno verifiche su mandato dell'autorità da cui dipendono (v. art. 82 cpv. 2 lett. c). Ciò potrà avvenire ad esempio proponendo un piano annuale di audit che motivi le priorità in materia di audit e definisca le risorse necessarie a tal fine. Gli standard impongono inoltre un controllo periodico dell'efficacia dell'organizzazione e delle misure da parte di un organo esterno (indipendente). La decisione in merito alla periodicità e all'organo a cui affidare il controllo spetta all'autorità interessata. Nell'Amministrazione federale gli audit di questo tipo possono essere effettuati sia dalle strutture di vigilanza interne ai Dipartimenti, sia dal CDF – che si occupa già delle revisioni in ambito informatico – o da una ditta esterna.

Nel capoverso 2 le autorità assoggettate vengono invitate a stabilire determinati principi:

– gli obiettivi delle autorità assoggettate indicano il livello di sicurezza che deve essere raggiunto (stato auspicato della sicurezza delle informazioni). Essi presuppongono un'analisi costi-benefici (qual è il livello di sicurezza di cui vuole beneficiare l'autorità e quanto può costare) e sono determinanti per l'attribuzione delle necessarie risorse. L'efficacia delle misure volte a tutelare la sicurezza delle informazioni deve corrispondere al livello di sicurezza perseguito da questi obiettivi;

- le autorità devono anche determinare come le organizzazioni a loro subordinate devono gestire i rischi, quali rischi possono senz'altro accettare e quali rischi devono essere riferiti all'autorità (accettazione del rischio). Anche se la maggior parte dei rischi nel campo della sicurezza delle informazioni possono essere trattati e accettati a livello operativo (dipartimento, ufficio o addirittura unità subordinata), determinati rischi possono avere un carattere strategico. Simili rischi vanno comunicati per lo meno all'autorità interessata. Ciò è in particolare il caso per i rischi connessi con mezzi informatici del livello di sicurezza «protezione molto elevata» (art. 17 cpv. 3);
- in ogni organizzazione ci sono sempre persone che non considerano con la dovuta serietà la sicurezza delle informazioni e gestiscono informazioni o mezzi informatici in maniera contraria alle prescrizioni o senza la debita cura. Molto spesso simili infrazioni vengono scusate *a priori* e, di conseguenza, non vengono analizzate. Esse possono tuttavia avere, quale conseguenza, considerevoli ripercussioni. Le autorità assoggettate devono perciò imporre in maniera coerente l'applicazione delle prescrizioni, definendo e spiegando le conseguenze in caso di inosservanza.

Art. 8 Gestione dei rischi

La gestione efficace dei rischi è un presupposto indefettibile per garantire una sicurezza funzionale ed economica delle informazioni. L'accento va posto precisamente sui rischi maggiori, sui quali devono concentrarsi misure della massima efficienza. Le autorità e organizzazioni federali sono pertanto invitate a tenere sotto controllo i rischi, non solo nel rispettivo ambito di competenza ma anche nell'ambito della collaborazione con terzi. La valutazione dei rischi presuppone approfondite conoscenze dei compiti legali e dei corrispondenti processi aziendali, la valutazione periodica delle minacce, l'analisi dei punti deboli, nonché la stima della probabilità che si verifichi un evento e della potenziale portata dei danni che possono risultare da taluni pericoli. Benché la gestione dei rischi richiesta da questa disposizione sia di natura tecnico-specialistica e debba pertanto essere pilotata ed esercitata costantemente da professionisti, la sicurezza delle informazioni è nondimeno un'esigenza che riguarda la gestione dei comuni rischi operativi. Pertanto, essa deve essere integrata nella gestione generale dei rischi dell'autorità o organizzazione interessata.

Un importante obiettivo della gestione dei rischi consiste nel poter adottare le misure più idonee per evitare o ridurre i rischi. I rischi possono essere evitati rinunciando del tutto a una determinata attività troppo rischiosa (p. es. si rinuncia a un progetto informatico per il quale l'applicazione di misure in funzione dei rischi non è economicamente sostenibile). Ovviamente, i rischi possono anche essere accettati o sostenuti, ma non dovrebbero essere ignorati. I rischi che permangono dopo l'attuazione delle previste misure di sicurezza (cosiddetti rischi residui), o i rischi che non possono essere ridotti, devono essere chiaramente indicati. Affinché possano procedere alla pertinente ponderazione degli interessi, ai responsabili vanno segnalati in forma documentata questi rischi e le potenziali ripercussioni. I rischi rimanenti devono essere accettati in maniera comprovata e, di conseguenza, essere sostenuti.

Nell'ambito della sicurezza delle informazioni, vengono periodicamente sviluppate misure organizzative che sono più efficaci o più economiche. I nuovi sviluppi tecnici si susseguono ancor più rapidamente, in particolare nel campo dei mezzi informatici, ma anche della tecnologia dei sensori (p. es. rivelatori di incendi, calore o movimento) o della tecnica di chiusura (p. es. sistemi di chiusura delle porte). È molto importante che le misure di sicurezza non si basino su tecnologie obsolete, bensì siano efficaci contro le minacce attuali. Le autorità e organizzazioni assoggettate devono applicare metodi possibilmente uniformi. A tal fine occorre definire requisiti standard secondo lo stato della scienza e della tecnica (v. art. 86), sapendo che le varie autorità assoggettate definiscono i criteri relativi all'accettazione dei rischi, determinanti per la valutazione dei rischi stessi, in funzione delle loro proprie necessità in materia di sicurezza delle informazioni.

Art. 9 Collaborazione con terzi

Sono considerati terzi secondo la presente legge tutte le autorità, organizzazioni e persone di diritto pubblico o privato che non sono né un'autorità né un'organizzazione assoggettata (Cantoni compresi) e che perciò, in linea di principio, agiscono indipendentemente da queste autorità e organizzazioni. Per adempiere i propri compiti, le autorità federali sovente dipendono dalla collaborazione dell'economia privata o di altri servizi. In questo caso, le autorità e le organizzazioni che conferiscono i mandati devono provvedere affinché in occasione del conferimento e dell'esecuzione dei mandati vengano rispettate le misure previste dalla legge. Le misure di sicurezza da rispettare vengono disciplinate contrattualmente. In linea di massima, i terzi dovrebbero ottenere l'accesso a informazioni o a mezzi informatici della Confederazione solamente se hanno attuato le misure necessarie. La LSIn richiede anche alle autorità e alle organizzazioni assoggettate che verifichino adeguatamente (ossia in funzione dei rischi) l'applicazione delle misure. Tale verifica può avvenire ad esempio per mezzo di un sopralluogo o mediante conferma scritta da parte del terzo in questione. Se il mandato include l'esercizio di un'attività sensibile sotto il profilo della sicurezza, le autorità e le organizzazioni assoggettate devono avviare il necessario CSP (v. art. 28 segg.) o richiedere l'esecuzione di una PSA (v. art. 50 segg.).

Art. 10 Procedura in caso di violazioni della sicurezza delle informazioni

Incidenti nell'ambito della sicurezza delle informazioni si verificheranno anche in futuro. È perciò necessario procedere con un approccio uniforme ed effettivo per la gestione di simili incidenti. Le autorità e le organizzazioni assoggettate devono adottare le misure necessarie per identificare tempestivamente incidenti riguardanti la sicurezza delle informazioni (p. es. controlli periodici, sensori, impianti d'allarme, sorveglianza della rete, valutazione periodica di *log-file*). Esse devono definire una procedura in base alla quale agire se vengono identificati incidenti o punti deboli, nonché attribuire chiare competenze per il trattamento degli incidenti. Collaboratori interni ed esterni devono inoltre sapere come occorre reagire al verificarsi di un evento affinché le sue ripercussioni possano essere ridotte al minimo. Affinché si impari dagli incidenti, le autorità e le organizzazioni assoggettate devono fare in modo che le cause di un incidente vengano chiarite e analizzate.

Per di più, le autorità federali, e in particolare il Consiglio federale, devono adottare tutti i provvedimenti necessari affinché possano adempiere i loro compiti fondamentali entro i termini stabiliti persino in situazioni straordinarie (*business continuity management*, cfr. art. 6 cpv. 3 LOGA). Oggi si può presupporre che l'adempimento di tutti i compiti più critici della Confederazione dipenda dall'impiego affidabile di mezzi informatici. La LSIn richiede perciò che le autorità assoggettate identifichino i compiti irrinunciabili dal loro punto di vista strategico e, nel caso di una violazione grave della sicurezza delle informazioni (p. es. mancato funzionamento di un sistema), allestiscano pianificazioni preventive e facciano svolgere esercitazioni in tale ambito. Per i mezzi informatici che vengono impiegati ai fini dell'adempimento di simili compiti irrinunciabili, si applica il livello di sicurezza «protezione molto elevata» (art. 17 cpv. 3).

Sezione 2: Classificazione delle informazioni

Art. 11 Principi della classificazione

La classificazione è obbligatoria purché siano soddisfatti i relativi criteri. In considerazione del principio di trasparenza e dell'onere connesso con la classificazione, essa deve tuttavia costituire un'eccezione. Spesso, con il passare del tempo, si riduce la necessità di protezione delle informazioni o essa diventa superflua dopo un determinato evento (p. es. pubblicazione di un rapporto o fine di una determinata misura). La classificazione di siffatte informazioni (p. es. non più attuali) non si giustifica allora più: causerebbe semplicemente un onere inutile. Le informazioni che devono rimanere classificate per un lungo periodo necessitano inoltre di provvedimenti di protezione tecnici diversi rispetto a quelle che sono degne di protezione solamente per un periodo limitato. Sempre che non sia possibile stabilire preliminarmente una classificazione temporanea, occorre garantire che le informazioni non rimangano classificate inutilmente. Una verifica della necessità di protezione deve avvenire almeno nel quadro dell'obbligo di offerta all'Archivio federale.

La protezione di informazioni classificate deve essere garantita per l'intero periodo durante il quale le informazioni in questione necessitano di essere protette. Le corrispondenti misure vengono definite a livello di ordinanza. Se la Svizzera ha concluso con un determinato Paese o una determinata organizzazione internazionale un trattato internazionale sullo scambio di informazioni classificate (v. art. 88 lett. b), il trattamento delle informazioni assoggettate al trattato è disciplinato dalle disposizioni speciali di quest'ultimo. In assenza di un simile trattato, il trattamento di informazioni classificate è retto dalle disposizioni della LSIn e dei suoi atti normativi d'esecuzione.

La classificazione può anche riguardare un determinato *materiale* (v. commento all'art. 5 lett. b n. 1). La classificazione di materiale è un caso d'applicazione della classificazione di informazioni al quale si applicano in linea di principio gli stessi metodi di valutazione e le stesse misure di protezione (CSP e PSA compresi).

Art. 12 Competenze

Nell'Amministrazione federale, la competenza in materia di classificazione è attualmente assegnata all'autore di un documento perché conosce meglio di chiunque altro la necessità di protezione delle informazioni ed è in grado di stimare eventuali rischi. Le autorità assoggettate possono però anche decidere che la classificazione, ad esempio, deve essere fatta dalla direzione dell'autorità, da un organo competente centrale o esclusivamente dalla linea gerarchica. La classificazione è in linea di principio vincolante. Se un'informazione è classificata, viene per così dire «accompagnata» da questa classificazione per tutto il suo iter. Chi ottiene l'accesso a una simile informazione deve rispettare le direttive connesse con la classificazione. Una modifica o una soppressione della classificazione può, in linea di massima, essere eseguita solamente dal servizio che ha stabilito la classificazione. Rimane inteso che anche qui sono fatte salve la via di servizio, la vigilanza gerarchica e la relativa facoltà di emanare istruzioni dei servizi o delle autorità di vigilanza gerarchicamente superiori. Queste ultime possono, se del caso, correggere decisioni del servizio incaricato della classificazione. Il disciplinamento delle competenze previsto all'articolo 12 non esclude che nei sistemi di informazione (quali p. es. GEVER) l'attuazione delle disposizioni in materia di classificazione e declassificazione venga automatizzata.

Il capoverso 3 consente al Consiglio federale di disciplinare la declassificazione dei documenti in vista della loro archiviazione, così come la declassificazione di fondi di archivio classificati. Non conferisce al Consiglio federale una competenza generale in materia di declassificazione delle informazioni; l'articolo 85 capoverso 1 conferisce questa competenza a ogni autorità soggetta alla presente legge, per il proprio ambito.

Da un lato, questa disposizione è volta ad assicurare che soltanto le informazioni che necessitano durevolmente di una protezione elevata siano classificate negli archivi (archivi classificati). Per quanto possibile, le informazioni classificate devono essere declassificate prima del loro versamento all'Archivio federale (cfr. commento all'art. 11 cpv. 3). Il bisogno di protezione deve pertanto essere verificato al più tardi quando i documenti sono offerti all'Archivio federale. D'altro lato questa disposizione è volta a evitare che gli archivi rimangano classificati indefinitamente. I documenti classificati dovrebbero in linea di massima essere automaticamente declassificati alla scadenza del termine di protezione previsto nella LAr. Nell'emanazione delle disposizioni di esecuzione, il Consiglio federale si adopererà affinché i meccanismi di declassificazione non impongano oneri sproporzionati né all'Archivio federale né ai servizi che offrono documenti.

Questa disposizione mostra implicitamente che tra la LSIn e la LAr vi sono delle intersezioni. Entrambe si applicano infatti alle informazioni per le quali le autorità federali sono competenti. Occorre pertanto evitare conflitti in materia di obiettivi e di competenze nel quadro di queste due leggi. In linea di massima i rapporti tra i due sistemi sono semplici: la LAr disciplina in modo uniforme l'archiviazione dei documenti della Confederazione nonché l'accesso agli stessi, mentre la LSIn si applica alle misure usuali di protezione delle informazioni e dei mezzi informatici, ossia alle misure non specifiche alla tecnica di archiviazione. Se per ragioni di sicurezza sono necessarie regolamentazioni speciali per documenti archiviati, tali norme sono

stabilite nella LSIn (v. art. 14 cpv. 2 LSIn). Sotto il profilo giuridico l'esecuzione di questa regolamentazione non pone problemi poiché il Consiglio federale è competente per l'esecuzione della LAr e, nella misura in cui è interessata l'Amministrazione federale, anche per la legislazione d'esecuzione della LSIn.

Nella prassi la tutela di documenti cartacei archiviati con un elevato bisogno di protezione non pone problemi. L'incremento dell'archiviazione elettronica di documenti sensibili pone tuttavia nuove sfide sia ai servizi che offrono documenti che all'Archivio federale. Gli organi incaricati della pianificazione dell'attuazione della LSIn esamineranno in collaborazione con l'Archivio federale se le misure organizzative e tecniche di protezione previste attualmente dalla LAr sono sufficienti o se devono essere adeguate. Se del caso, il Consiglio federale chiederà un aumento dell'importo del limite di spesa dell'Archivio federale per il personale e le risorse necessarie.

Art. 13 Livelli di classificazione

L'articolo 13 disciplina i presupposti materiali per la classificazione di informazioni per tutte le autorità e le organizzazioni assoggettate e stabilisce i livelli di classificazione. Il testo proposto si limita a criteri piuttosto generali e si riferisce direttamente agli interessi pubblici da proteggere definiti nell'articolo 1 capoverso 2 lettere a–d. Il rimando a questi interessi è tuttavia circoscritto: la protezione degli interessi pubblici ai sensi della lettera e non rappresenta un motivo proprio per la classificazione. Con la protezione di questo interesse si intende infatti garantire il trattamento conforme al diritto di informazioni la cui protezione è prevista in altre leggi o viene convenuta contrattualmente con terzi. I dati personali ai sensi della LPD o i segreti d'affari, di fabbricazione o professionali non vengono quindi, in linea di principio, classificati, a meno che singole informazioni debbano essere classificate per proteggere un interesse di cui all'articolo 1 capoverso 2 lettere a–d. Lo stesso dicasi per informazioni che vengono trattate presso i tribunali o i ministeri pubblici nell'ambito dei loro procedimenti ordinari. La maggior parte di queste informazioni sono dati personali che, pur essendo degni di protezione, non devono però essere classificati in virtù della presente legge. Le particolari misure che vengono adottate per proteggere simili informazioni possono invece essere classificate (ad es. un ' piano in materia di sicurezza delle informazioni).

Per il livello di classificazione stesso è determinante il *grado di pregiudizio* che una conoscenza da parte di persone non autorizzate può arrecare agli interessi di cui all'articolo 1 capoverso 2 lettere a–d. Per l'assegnazione a un livello di classificazione è determinante se la conoscenza da parte di persone non autorizzate:

- *può pregiudicare* tali interessi: livello di classificazione «ad uso interno»;
- *può pregiudicare considerevolmente* gli interessi in questione: livello di classificazione «confidenziale»;
- *può pregiudicare gravemente* gli interessi in questione: livello di classificazione «segreto».

Queste qualificazioni rappresentano nozioni giuridiche indeterminate che vanno ancora rese concrete tenendo conto della politica in materia di gestione dei rischi.

Sebbene il criterio della gravità del potenziale pregiudizio per gli interessi di cui all'articolo 1 capoverso 2 lettere a–d sia determinante per la classificazione, da solo non è sufficiente. Occorre anche un nesso causale ragionevole tra la conoscenza non autorizzata dell'informazione e il potenziale pregiudizio per gli interessi protetti. È quindi indispensabile che venga considerata anche la probabilità che si verifichi il danno. La classificazione di un'informazione corrisponde dunque al risultato di una valutazione dei rischi e deve quindi rispecchiare l'effettiva *necessità di protezione* di questa informazione.

Nel valutare la necessità di protezione di informazioni *di natura politica* è indispensabile usare particolare prudenza. Anche se la protezione della libera formazione dell'opinione e della volontà delle autorità e delle organizzazioni assoggettate viene contemplata dall'articolo 1 capoverso 2 lettera a (capacità di decisione), in una moderna democrazia appartiene però alla normale attività del Governo che idee politiche, proposte, piani e decisioni vengano discussi dall'opinione pubblica ed eventualmente (anche aspramente) criticati. La classificazione non deve dunque servire a sottrarre al pubblico dibattito determinati argomenti se non sussiste alcun interesse pubblico preponderante in tal senso.

Capoverso 1: quale criterio delimitatore per distinguere tra «non classificato» e «classificato» occorre, anche per un «pregiudizio» per gli interessi in questione non ulteriormente qualificato dalla legge, che vi siano indizi qualificati atti a giustificare la classificazione «ad uso interno». Il danno potenziale non può essere semplicemente trascurabile: il pregiudizio per gli interessi di cui all'articolo 1 capoverso 2 lettere a–d deve piuttosto essere sensibile. Rispetto all'attuale articolo 7 OPrI, che menziona semplicemente la possibilità di un «pregiudizio», la nuova normativa è quindi considerevolmente più restrittiva. Quando si tratta di *informazioni rilevanti per la sicurezza* ai sensi dell'articolo 1 capoverso 2 lettera b, la soglia per la classificazione «ad uso interno» può essere raggiunta relativamente in fretta. Tale classificazione è anche utilizzata molto spesso per siffatti casi. Così, singole documentazioni di sicurezza relative a mezzi informatici o semplici piani d'intervento di forze di sicurezza sono, di regola, classificate «ad uso interno».

Capoverso 2: rispetto al disciplinamento attuale, in virtù del quale è richiesto semplicemente un *danno* non qualificato (art. 6 OPrI), la nuova normativa proposta rappresenta un innalzamento dei requisiti per la classificazione. Con l'espressione scelta è richiesto un danno chiaro e importante, ad esempio:

- la libera formazione dell'opinione e della volontà delle autorità assoggettate è temporaneamente resa più difficile in maniera illecita;
- un'organizzazione assoggettata è temporaneamente incapace di agire;
- l'adempimento di taluni compiti di un'autorità o di un'organizzazione è reso considerevolmente più difficile su un lungo periodo;
- determinate risorse dell'esercito o degli organi di sicurezza della Confederazione non sono temporaneamente impiegabili;
- la posizione della Svizzera nell'ambito di negoziati internazionali è resa considerevolmente più difficile;

- la sicurezza di persone o gruppi di persone è minacciata;
- alla Confederazione deriva un considerevole danno finanziario.

Capoverso 3: con la formulazione scelta è richiesto un danno catastrofico particolarmente consistente per la Confederazione, ad esempio:

- un'autorità assoggettata è temporaneamente incapace di decidere o di agire o la sua capacità di decisione e d'azione è seriamente ostacolata su un lungo periodo;
- l'adempimento di compiti irrinunciabili di un'organizzazione assoggettata è temporaneamente impedito o reso seriamente più difficile su un lungo periodo;
- risorse essenziali dell'esercito o degli organi di sicurezza della Confederazione non sono impiegabili;
- la vita e l'integrità fisica di gruppi della popolazione sono minacciate;
- la fornitura di prestazioni di servizi irrinunciabili da parte di infrastrutture critiche è interrotta;
- le funzioni di un impianto nucleare particolarmente sensibili sotto il profilo della sicurezza sono sabotate;
- la Confederazione subisce un grave danno finanziario.

La classificazione deve essere di immediata evidenza e non confondibile con altre menzioni. Nell'ambito internazionale si è imposta la regola secondo cui la classificazione va sempre scritta in lettere maiuscole e in grassetto. Il capoverso 4 è necessario per fare in modo che tale regola sia applicata da tutte le autorità della Confederazione.

Art. 14 Accesso a informazioni classificate

Il capoverso 1 definisce i presupposti per l'accesso a informazioni classificate, il quale è a sua volta il presupposto per il trattamento delle corrispondenti informazioni. Il principio «conoscere soltanto se necessario» si applica a ogni singola informazione classificata. Non vi è dunque un diritto generale all'accesso a tutte le informazioni classificate. Ciò vale anche per gli organi di verifica, di controllo o di vigilanza che, certo, beneficiano, se del caso, di un diritto d'informazione generale, ma che per ogni singola informazione classificata devono fornire la prova che per adempiere il proprio mandato devono effettivamente conoscere le informazioni in questione. Nel caso di un diritto di accesso convenuto contrattualmente, i relativi contratti devono prevedere l'accesso a informazioni classificate e disciplinarne il trattamento. «Offrire la garanzia» di un trattamento appropriato presuppone che le persone che devono trattare informazioni classificate siano state adeguatamente formate. Devono poi, eventualmente, fornire la prova della capacità di poter rispettare le necessarie misure di sicurezza tecniche e fisiche. Per le informazioni classificate «confidenziale» o «segreto», l'esecuzione di un CSP può inoltre costituire un ulteriore presupposto per il trattamento.

Capoverso 2: il disciplinamento dell'accesso agli archivi (art. 9–16 LAr) si è dimostrato valido anche in relazione agli archivi classificati e va pertanto mantenuto (v. anche commento all'art. 12).

Capoverso 3: la maggioranza dei Paesi e delle organizzazioni internazionali con i quali la Svizzera ha concluso un trattato internazionale per lo scambio di informazioni classificate richiede che le loro informazioni classificate siano trattate esclusivamente da persone in possesso della cittadinanza del Paese in questione o della cittadinanza svizzera (cosiddetta *clausola dell'esclusione degli Stati terzi*). Siffatte informazioni non sono dunque, in linea di massima, accessibili a persone di altra nazionalità. È fatta salva un'autorizzazione preliminare dell'autore delle informazioni.

Art. 15 Accesso a informazioni classificate disciplinate da procedure particolari

È fatto salvo il diritto procedurale dell'Assemblea federale e quello dei tribunali e dei ministeri pubblici. All'accesso a informazioni classificate (p. es. nell'ambito dell'utilizzazione delle stesse come base decisionale o come mezzo di prova) va applicato il rispettivo diritto procedurale. Le leggi di procedura federali contengono norme che stabiliscono in quale misura simili informazioni possono essere rese accessibili, per consultazione, ai partecipanti alla procedura, in quale misura possono essere rese note nell'ambito di procedure pubbliche o in quale misura i testimoni possono rifiutare di deporre adducendo obblighi legali di mantenere il segreto (v. p. es. art. 47, 150, 153 e 154 LParl, art. 56 cpv. 2 e 59 cpv. 2 LTF, art. 16 cpv. 2, 18 cpv. 2, 27 e 28 PA, art. 40 cpv. 3 LTAF o art. 70, 170, 173 cpv. 2 e 194 cpv. 2 CPP, nonché art. 45, 48 cpv. 2 e 77 PPM; v. anche art. 58 dell'ordinanza del 24 ottobre 1979[27] concernente la giustizia penale militare). Prima di decidere in merito alla comunicazione di informazioni classificate è possibile dare al servizio incaricato della classificazione l'opportunità di esprimersi quanto ai motivi della classificazione e consultarlo in merito alle eventuali ripercussioni di una comunicazione. Alla luce delle circostanze, l'organo o il tribunale competenti decideranno poi come procedere ulteriormente.

Sezione 3: Sicurezza in occasione dell'impiego di mezzi informatici

Art. 16 Procedura di sicurezza

Sono ormai lontani i tempi in cui ad esempio gli uffici federali e i tribunali gestivano i loro mezzi informatici per conto proprio. Oggi le autorità e le organizzazioni della Confederazione acquistano in genere i servizi informatici che occorrono loro presso fornitori di prestazioni esterni altamente specializzati. Si è così creata una separazione organizzativa tra impiego e gestione dei mezzi informatici, la quale esercita profonde ripercussioni anche sulla sicurezza, ad esempio per il fatto che la sicurezza delle informazioni viene perlopiù considerata una questione prettamente tecnica che

27 RS **322.2**

rientra nella responsabilità dei fornitori di prestazioni. La legge definisce in linea di principio i compiti che le autorità e organizzazioni beneficiarie di prestazioni devono adempiere per assumere la loro responsabilità per quanto riguarda la sicurezza. Le autorità assoggettate (ma non le organizzazioni) devono precisare questi compiti nell'ambito di una cosiddetta procedura di sicurezza. Tutte le autorità federali utilizzano già oggi una simile procedura. Le procedure esistenti devono tuttavia essere sistematizzate e, dove necessario, completate. Le più importanti fasi procedurali dovranno essere uniformate a livello di ordinanza applicabili a tutte le autorità. La procedura di sicurezza deve in particolare stabilire compiti, competenze e responsabilità inerenti alla sicurezza dei servizi che pianificano e decidono l'impiego di mezzi informatici. Il capoverso 2 indica alcuni punti cardine della procedura:

– lettera a: i mezzi informatici vengono impiegati per determinati scopi e per una durata pianificata. La prima fase in relazione all'attuazione della sicurezza delle informazioni consiste, in occasione della definizione della finalità d'impiego del mezzo informatico, nel determinare i processi aziendali che vanno supportati con il mezzo informatico da impiegare e nell'identificare le informazioni che vanno trattate con esso. A quel momento, dunque nella fase di pianificazione, il beneficiario di prestazioni deve rilevare la necessità di protezione delle informazioni secondo l'articolo 6 capoverso 1 e valutare le potenziali ripercussioni – sugli interessi di cui all'articolo 1 capoverso 2 – di disturbi o di un'utilizzazione abusiva del mezzo informatico da impiegare. Si tratta, sostanzialmente, di una cosiddetta *Business Impact Analysis*, che deve essere imperativamente svolta dal servizio responsabile del processo aziendale. Nella valutazione della necessità di protezione occorre anche considerare che, di regola, i mezzi informatici per lo più vengono messi in rete e gestiti in un determinato ambiente tecnico e logico (cosiddetta architettura). L'identificazione tempestiva delle interconnessioni e dipendenze contribuisce anche ad attuare le misure là dove sono più efficaci. Dall'analisi delle necessità di protezione risultano i requisiti per la protezione delle informazioni e il livello di sicurezza del mezzo informatico di cui all'articolo 17;
– lettera b: le autorità assoggettate devono stabilire quali misure devono essere applicate (v. anche art. 18) e come va verificata l'applicazione di tali misure. In linea di principio, vanno applicate misure standardizzate (v. art. 86). In tale contesto è particolarmente importante la verifica dell'applicazione delle misure. Prima di impiegare un mezzo informatico, l'autorità o l'organizzazione competente dovrebbe avere una prova che la procedura di sicurezza è avvenuta conformemente al diritto e che sono state effettivamente attuate le misure necessarie (conformità);
– lettera c: i mezzi informatici vengono spesso messi in funzione senza che sia coperto il fabbisogno in materia di sicurezza delle informazioni. Con il nullaosta di sicurezza si intende garantire che, prima di impiegare un mezzo informatico, l'autorità o l'organizzazione competente conosca i rischi residui identificati e sia anche disposta a sostenerli. Se ritiene che i rischi residui siano ancora troppo elevati, può rifiutare il nullaosta e richiedere l'applicazione di misure aggiuntive atte a ridurre i rischi;

– lettera d: la sicurezza delle informazioni cambia in modo continuo. Le autorità devono perciò stabilire una procedura al fine di tenere conto di un mutamento dei rischi in mezzi informatici già impiegati.

Secondo il capoverso 3, la competenza per l'esecuzione della procedura di sicurezza spetta all'autorità o all'organizzazione che decide l'impiego di mezzi informatici (beneficiario di prestazioni). Il beneficiario di prestazioni è infatti responsabile dei processi aziendali e dell'attuazione dei requisiti di sicurezza. Deve perciò comunicare chiaramente le proprie esigenze aziendali e di sicurezza al suo fornitore di prestazioni, che gestisce i mezzi informatici.

Art. 17 Livelli di sicurezza

L'assegnazione a un livello di sicurezza serve a identificare la criticità di un determinato mezzo informatico rispetto agli interessi pubblici di cui all'articolo 1 capoverso 2. Tale criticità dipende dalla gravità del pregiudizio che può essere causato dall'utilizzazione abusiva o dal sovvertimento delle informazioni trattate con il mezzo informatico in questione oppure dall'utilizzazione abusiva o dal disturbo del mezzo informatico stesso. Il livello di sicurezza di un mezzo informatico è dunque determinato tanto dalla necessità di proteggere la confidenzialità, la disponibilità, l'integrità e la tracciabilità delle informazioni quanto dalla criticità dell'immediato e corretto svolgimento dei processi aziendali da esso supportati. Per quanto riguarda la valutazione della gravità del pregiudizio ci si può riferire, *mutatis mutandis*, a quanto esposto nel commento all'articolo 13.

Le vigenti prescrizioni dell'Amministrazione federale prevedono soltanto due livelli: una necessità di protezione generale e una necessità di protezione elevata. Il nuovo modello di classificazione a tre livelli si rifà allo standard del *Bundesamt für Sicherheit in der Informationstechnik* tedesco:

– il livello di sicurezza «protezione di base» si applica a tutti i mezzi informatici che non presentano requisiti di protezione particolari. La larga maggioranza dei sistemi della Confederazione sarà classificata a questo livello. Dati personali, informazioni classificate «ad uso interno» e ulteriori informazioni che, pur dovendo essere protette quanto alla loro confidenzialità non necessitano però di una protezione elevata, possono essere trattate con mezzi così classificati;

– un mezzo informatico rientra nel livello di sicurezza «protezione elevata» se un'utilizzazione abusiva delle informazioni trattate con esso o del mezzo informatico stesso può causare un danno considerevole. I mezzi informatici destinati a trattare le informazioni classificate «confidenziale» rientrano in questo livello. Ciò si applica anche ai mezzi informatici utilizzati per il trattamento di dati personali degni di particolare protezione o di segreti d'affari o di fabbricazione, sempre che il danno potenziale in caso di abuso di tali dati sia considerevole. Vanno classificati in questo livello anche i mezzi informatici che supportano processi aziendali la cui interruzione o il cui disturbo può compromettere considerevolmente la capacità di agire di un'autorità;

– un mezzo informatico rientra nel livello di sicurezza «protezione molto elevata» se un'utilizzazione abusiva delle informazioni trattate con esso o del mezzo informatico stesso può causare un danno *grave*. Si tratta di mezzi informatici il cui mancato funzionamento o il cui disturbo può pregiudicare gravemente gli interessi di cui all'articolo 1 capoverso 2 (v. anche art. 10 cpv. 2) o di quelli con i quali vengono trattate informazioni «segrete».

L'assegnazione a un livello di sicurezza evidenzia al tempo stesso quali sono i requisiti applicabili in materia di sicurezza e quali misure di protezione devono essere definite. Per ogni livello di sicurezza si applicano requisiti e misure di sicurezza standard per proteggere la confidenzialità, la disponibilità, l'integrità e la tracciabilità (art. 86). La standardizzazione è assolutamente necessaria per garantire uno scambio di informazioni efficiente e sicuro tra tutte le autorità e comporta importanti vantaggi: anzitutto alle autorità responsabili dello sviluppo e ai servizi incaricati degli acquisti vengono indicati chiari requisiti da adempiere in materia di sicurezza, sui quali potranno fondarsi nell'implementazione della sicurezza nei mezzi informatici; in secondo luogo consente di prevedere e pianificare in modo più trasparente e semplice i costi della sicurezza nell'ambito dei progetti.

Per ora non è possibile allestire una tavola di concordanza (mapping) che definisca il livello di sicurezza corrispondente a ogni tipo di informazione e di processo aziendale. I criteri di classificazione previsti all'articolo 17 sono nuovi e quindi mai applicati prima d'ora nella prassi. Inoltre, non tutte le autorità e organizzazioni trattano le stesse informazioni, ragion per cui è impossibile valutare *in abstracto* l'effettiva necessità di protezione corrispondente alle varie informazioni. Nell'ambito dell'esecuzione le informazioni e i dati saranno comunque assegnati in funzione delle necessità di protezione, a un determinato *livello di protezione* relativo alla confidenzialità, disponibilità, integrità e tracciabilità. I livelli di protezione, indicati per mezzo di tavole di concordanza, serviranno per la necessaria standardizzazione delle misure.

Art. 18 Misure di sicurezza

A seconda del livello di sicurezza le autorità assoggettate devono stabilire quali requisiti di sicurezza devono soddisfare i loro mezzi informatici. La prassi ha mostrato che con un adeguato numero di requisiti e misure determinati e predefiniti i rischi per la maggior parte dei mezzi informatici possono essere ridotti a un'entità accettabile. La totalità di tutti questi requisiti e misure costituisce la *protezione di base*. Il vantaggio di una protezione di base definita e standardizzata consiste nel fatto che, per i mezzi informatici di questo livello, le autorità e le organizzazioni non devono eseguire valutazioni dei rischi dettagliate e onerose. La protezione di base viene quindi anche definita come un presupposto del quale devono tener conto i mezzi informatici dei livelli di sicurezza «protezione elevata» e «protezione molto elevata». Le misure della protezione di base devono essere configurate in maniera relativamente flessibile e modulare. Se determinate misure non sono attuabili per un particolare mezzo informatico, vanno applicate altre misure che consentono una protezione equivalente.

Per i livelli di sicurezza «protezione elevata» e «protezione molto elevata» spesso non bastano i requisiti e le misure della protezione di base. Oggigiorno per simili

mezzi viene quindi dapprima svolta un'analisi dei rischi specifica all'oggetto, dando la massima importanza alla protezione di quei criteri che hanno requisiti di protezione elevati. Se, a motivo di requisiti elevati posti alla disponibilità, a un mezzo informatico viene attribuito il livello «protezione elevata», ma nel contempo non presenta requisiti elevati quanto alla protezione della confidenzialità, allora devono venire valutati in primo luogo i rischi per la disponibilità. Sulla base di tale analisi dei rischi viene allestito un piano per la sicurezza dell'informazione e la protezione dei dati che attesta l'applicazione delle misure di protezione di base e descrive le ulteriori misure di sicurezza.

Per i mezzi informatici dei due livelli di sicurezza più elevati occorre attenersi al sistema attuale (analisi dei rischi e piano in materia di sicurezza). Tuttavia, ciò non è prescritto dalla legge e un'altra soluzione è quindi possibile.

La verifica dell'efficacia ai sensi del capoverso 3 è l'unico provvedimento con il quale è possibile misurare la sicurezza delle informazioni garantita. Il mezzo informatico viene sottoposto a un audit dettagliato. Possono inoltre essere eseguiti attacchi reali, così da identificare eventuali falle nella sicurezza e punti deboli che qualcuno potrebbe sfruttare a proprio vantaggio (p. es. mediante il test di penetrazione). La verifica dell'efficacia viene richiesta solamente per i mezzi informatici più critici, perché è connessa a un onere finanziario non indifferente (dallo 0,5 al 2 % del totale dei costi di investimento).

Art. 19 Sicurezza durante l'esercizio

Secondo gli articoli 16–18, la responsabilità principale della sicurezza in occasione dell'impiego di mezzi informatici incombe ai beneficiari delle prestazioni. Dal canto loro, i fornitori di prestazioni sono competenti per garantire la sicurezza secondo lo stato della scienza e della tecnica nell'esercizio di questi mezzi informatici. Devono considerare e attuare sia i requisiti e le misure previsti dalla LSIn sia i requisiti aggiuntivi convenuti con i beneficiari di prestazioni. I fornitori di prestazioni interni rientrano tutti nel campo d'applicazione della presente legge e devono perciò applicarla alle proprie attività. I fornitori di prestazioni esterni sono per contro considerati terzi ai sensi dell'articolo 9 e devono essere obbligati contrattualmente a osservare le misure della presente legge.

Ogni fornitore di prestazioni è tenuto a sorvegliare le proprie reti. Anomalie, attacchi o disturbi devono essere scoperti e valutati tempestivamente al fine di poterli contrastare. In caso di sospetto di minaccia o di violazione concreta della sicurezza delle informazioni può succedere che le attività elettroniche di determinati collaboratori (o macchine) interni o esterni debbano essere esaminate in maniera dettagliata. Se in questo contesto è necessaria l'identificazione nominale di una persona, si applicano allora per analogia le disposizioni della LOGA sul trattamento dei dati personali che si presentano nell'ambito dell'utilizzazione dell'infrastruttura informatica. Già oggi le cosiddette *procedure forensi* dell'Amministrazione federale poggiano su tali disposizioni, quando è necessaria una valutazione dei dati riferita alle persone.

Sezione 4: Misure in materia di personale

Art. 20 Condizioni per l'accesso a informazioni e ai mezzi informatici della Confederazione

Le persone che hanno accesso a informazioni, mezzi informatici o infrastrutture della Confederazione devono soddisfare determinati requisiti. Spetta al datore di lavoro o al mandante provvedere affinché i lavoratori o i mandatari adempiano questi requisiti.

- In occasione della scelta delle persone da assumere o a cui affidare un mandato, i criteri di selezione devono corrispondere alla necessità di protezione delle informazioni o alla criticità dei mezzi informatici. I datori di lavoro sono responsabili delle loro decisioni in materia di personale. L'assoggettamento di una persona al CSP non li dispensa da questa responsabilità;
- l'amministrazione dell'accesso a sistemi d'informazione, locali e infrastrutture avviene sempre di più elettronicamente. Le persone che vogliono servirsi di risorse della Confederazione devono lasciarsi identificare elettronicamente (autenticazione) affinché si possa decidere in merito alla loro autorizzazione d'accesso. A seconda della criticità dell'accesso vengono impiegati sistemi di autenticazione più o meno forti. Ad esempio, oltre a una password, si richiede una smart card o la verifica di una caratteristica biologica (impronta digitale, scannerizzazione dell'occhio ecc.);
- le autorità e le organizzazioni assoggettate devono formare a sufficienza i propri impiegati e mandatari. Nell'ambito della sicurezza delle informazioni non basta fornire una formazione *una tantum*. I lavoratori e i mandatari devono essere istruiti e sensibilizzati periodicamente. Occorre prestare particolare attenzione all'istruzione dei superiori e delle persone che esercitano un'attività sensibile sotto il profilo della sicurezza;
- in virtù degli articoli 22 LPers e 320 CP, gli impiegati della Confederazione devono tutelare il segreto d'ufficio. Per i terzi che eseguono mandati per la Confederazione, il contratto deve prevedere per scritto l'obbligo di tutela del segreto connesso a chiare conseguenze in caso di inosservanza, poiché questi terzi non ricadono nel campo d'applicazione dell'articolo 320 CP. Va menzionato anche il fatto che l'obbligo di tutela del segreto pattuito per contratto non libera il funzionario che dovesse fare delle rivelazioni senza disporre internamente del consenso scritto dell'autorità superiore secondo l'articolo 320 capoverso 2 CP. Per quanto riguarda la violazione del segreto d'ufficio: vedi il commento alla modifica dell'articolo 320 CP.

L'utilizzo di metodi di verifica biometrici ai fini dell'autenticazione di persone può portare sicurezza supplementare. Non si tratta di identificare una persona tra un gruppo qualsiasi di persone, bensì solamente di verificare se una determinata persona, che richiede l'accesso a risorse della Confederazione, è davvero chi afferma di essere. Le autorità assoggettate devono poter fare uso di questa possibilità per l'accesso alle proprie risorse. Oggi questi metodi vengono già impiegati in taluni settori. Per ragioni di protezione dei dati, al decadere dell'autorizzazione all'accesso i dati biometrici vanno assolutamente distrutti.

Art. 21 Rilascio restrittivo di autorizzazioni

L'articolo 21 enuncia un principio centrale della sicurezza delle informazioni. Chi lavora o esegue un mandato per un'autorità federale necessita eventualmente, per adempiere i compiti, di un accesso a determinate informazioni, mezzi informatici o locali. I lavoratori e i mandatari devono ricevere soltanto le autorizzazioni di cui effettivamente necessitano per adempiere i propri compiti. Il rischio di un'utilizzazione abusiva può essere ridotto considerevolmente se una persona non può trattare senza motivo informazioni di un altro settore. Succede che, al termine del rapporto di lavoro, scaduto il contratto o ultimato un compito particolare, ex impiegati o mandatari non vengano invitati a restituire la propria chiave o il proprio *badge*, oppure che il loro conto di utente non venga bloccato. Simili autorizzazioni «*scadute*» possono in seguito venire utilizzate per agire contro gli interessi del datore di lavoro o del mandante. Quando un impiego, un contratto o un compito è terminato, le pertinenti autorizzazioni devono essere revocate. Se vi è motivo di supporre di essere in presenza di una minaccia per la sicurezza delle informazioni, le autorizzazioni devono essere bloccate o revocate immediatamente. Entrambe le misure devono, in particolare, contribuire a ridurre il rischio di un reato dall'interno.

Sezione 5: Protezione fisica

Art. 22 Principio

Con le misure di protezione fisica si tratta di ridurre i rischi dovuti a minacce fisiche, tra le quali rientrano atti umani (p. es. spionaggio, furto, vandalismo o sabotaggio), ma anche i danni causati da elementi naturali (p. es. calore, fuoco, acqua, polvere, vibrazioni ecc.). L'articolo 22 stabilisce il principio che le autorità e le organizzazioni assoggettate devono garantire la protezione fisica delle loro informazioni e dei loro mezzi informatici. Occorre in particolare impedire l'accesso non autorizzato a informazioni o mezzi informatici, ad esempio mediante controlli dell'accesso, videocamere, sistemi di chiusura, contenitori di sicurezza, apparecchi di distruzione di documenti eccetera. Contro i danni causati da elementi naturali vengono ad esempio impiegati impianti di rivelazione e di segnalazione di incendi e impianti di spegnimento automatici. Le misure di protezione fisica riguardano sia informazioni e mezzi informatici situati nei locali dell'autorità o organizzazione interessata, sia quelli accessibili pubblicamente. Nel secondo caso si tratta di informazioni e mezzi informatici che vengono portati lontano dal loro posto abituale (ufficio) – e che in seguito devono essere protetti al di fuori del perimetro di sicurezza abituale – ma anche di informazioni e installazioni, cavi e condotte di alimentazione che non sono sotto il costante controllo dell'autorità o dell'organizzazione. Occorre prestare particolare attenzione, ad esempio, ai punti di accesso quali le zone di consegna e di carico.

Art. 23 Zone di sicurezza

La delimitazione di questi locali o settori quali zone di sicurezza rappresenta una misura fisica di sicurezza delle informazioni che già oggi viene parzialmente adottata presso la Confederazione, in particolare per proteggere i locali dei server o deter-

minati locali di condotta. Una zona di sicurezza deve essere predefinita, identificabile ed essere protetta di conseguenza. La normativa d'esecuzione del Consiglio federale definirà probabilmente due generi di zone di sicurezza, secondo la criticità delle informazioni o dei mezzi informatici. Le misure nelle zone di sicurezza dei rispettivi livelli dovranno essere impostate in funzione dei rischi. Contrariamente alla legislazione di altri Paesi o di organizzazioni internazionali e alla legislazione in materia di protezione di impianti militari (v. anche cpv. 4), per le autorità e le organizzazioni assoggettate non sussiste però alcun obbligo di designare simili settori quali zone di sicurezza. In merito al loro effettivo allestimento decide l'autorità o l'organizzazione dopo una valutazione dei rischi.

I capoversi 2 e 3 disciplinano i poteri particolari dell'autorità o dell'organizzazione che allestisce una zona di sicurezza:

- la possibilità di prendere con sé determinati oggetti in una zona di sicurezza può essere limitata. Di regola, prendere con sé apparecchi per registrazioni audiovisive (incl. smartphone o notebook con pertinenti funzioni) è consentito soltanto con un'autorizzazione particolare;
- settori della zona di sicurezza che sono particolarmente importanti per la sicurezza delle informazioni (p. es. la zona d'accesso a un particolare locale server, il posto di lavoro dell'amministratore del sistema o il locale archivio con informazioni classificate «segreto»), possono essere controllati mediante apparecchi di registrazione video;
- all'entrata o all'uscita, l'autorità o l'organizzazione può far eseguire perquisizioni di borse e persone. In questo modo si intende impedire che persone portino con sé senza autorizzazione apparecchi nella zona di sicurezza o sottraggano informazioni (p. es. con una chiavetta USB);
- per applicare le prescrizioni devono essere possibili controlli degli uffici. Nei controlli degli uffici sarà fra l'altro verificato il rispetto della cosiddetta *Clean Desk Policy* (informazioni degne di protezione non devono trovarsi né sulla scrivania né in altro luogo, il PC deve essere bloccato o spento, i supporti di dati devono essere tenuti sotto chiave, i cassetti devono essere chiusi a chiave, il cestino dei rifiuti non deve contenere informazioni classificate ecc.). Il controllo può avere luogo anche in assenza delle persone interessate, ad esempio durante la notte.
- Se la zona di sicurezza è particolarmente critica, l'autorità o l'organizzazione può esercitare un impianto di telecomunicazione che provoca interferenze. L'effettiva necessità e le condizioni per l'esercizio di un simile impianto vengono valutate in virtù della LTC.

Sezione 6: Sistemi di gestione delle identità

Art. 24 Impiego di sistemi di gestione delle identità

Al centro di un sistema globale di gestione delle identità vi sono sistemi di gestione delle identità centralizzati. I capoversi 1 e 2 descrivono a grandi linee lo scopo e il funzionamento dei sistemi di gestione delle identità centralizzati, al fine di costituire una base per le restanti normative. Le autorità assoggettate avranno la competenza di gestire siffatti sistemi per il controllo centralizzato di persone, macchine e sistemi che richiedono l'accesso a sistemi d'informazione e altre risorse. Si rinuncia consapevolmente a indicare il numero di sistemi di gestione delle identità centralizzati che saranno impiegati. Per l'Amministrazione federale, sarà il Consiglio federale a decidere quali servizi o unità amministrative gestiscono simili sistemi. È ad esempio ipotizzabile che per l'Amministrazione federale vengano dapprima costituite diverse di queste cerchie di gestione delle identità e che con il tempo esse vengano parzialmente consolidate. Per ogni sistema deve essere designato un servizio responsabile. Poiché spetta alle autorità assoggettate scegliere quanti di tali sistemi gestire e come organizzare le relative cerchie, nella legge non possono essere menzionati i servizi responsabili.

Art. 25 Scambio e armonizzazione dei dati

Vi sono tre casi chiaramente distinguibili nei quali un sistema di gestione delle identità scambia dati personali con altri sistemi:

- alla creazione di un nuovo sistema di gestione delle identità esso acquisisce i necessari dati sull'identità dei collaboratori del settore da coprire dai relativi registri dei collaboratori e degli utenti. Nell'esercizio successivo devono essere comunicate periodicamente al sistema di gestione delle identità le mutazioni di questi sistemi;
- un'ulteriore occasione è il collegamento di un'applicazione tecnica che finora ha eseguito autonomamente l'autenticazione degli utenti. In questo caso, i dati utilizzati a tale scopo vengono trasmessi al sistema di gestione delle identità centralizzato e lì registrati nei dati esistenti. A quel momento verranno anche verificati i requisiti di cui al capoverso 2. Normalmente, le ulteriori mutazioni dei dati degli utenti vengono comunicate dall'applicazione tecnica al sistema di gestione delle identità. A seconda dell'impostazione organizzativa concreta, per determinate cerchie di utenti è però ipotizzabile anche una gestione degli utenti centralizzata;
- durante il funzionamento corrente, la trasmissione di dati più frequente avviene in occasione di ogni accesso (login) di un utente. Il sistema di gestione delle identità autentica l'utente, completa i dati sull'identità richiesti dall'applicazione tecnica ricorrendo al suo registro (p. es. l'appartenenza a un servizio) o a fonti esterne (p. es. la funzione di pubblico ufficiale o medico) e mette a disposizione dell'applicazione tecnica questi dati sotto forma di conferme, affinché essa possa decidere in merito alle autorizzazioni d'accesso concrete.

Art. 26 Utilizzo del numero d'assicurato AVS

Per un sistema di gestione delle identità è indispensabile che le persone da registrare vengano identificate senza errori. Nessuna persona può essere confusa con un'altra a causa della coincidenza di criteri di identificazione né può essere consentito che i dati di persone diverse vengano fusi. Nessuna persona può figurare due volte a causa di una coincidenza non riconosciuta. Tale problema si pone sia per la creazione e l'aggiornamento del registro degli utenti, sia nel singolo accesso o nell'ulteriore comunicazione dal sistema di gestione delle identità all'applicazione tecnica dei dati della persona che accede. Il migliore identificatore di persone disponibile per una siffatta identificazione esente da errori è il numero d'assicurato AVS di cui all'articolo 50*c* LAVS. Quasi tutte le persone registrate nei sistemi di gestione delle identità previsti nel presente caso dispongono di tale numero. Per un utilizzo sistematico del numero d'assicurato al di fuori delle assicurazioni sociali della Confederazione, l'articolo 50*e* capoverso 1 LAVS chiede un disciplinamento formale dello scopo d'utilizzazione e degli aventi diritto in una legge federale.

Per la comunicazione tra il sistema di gestione delle identità e le applicazioni tecniche o altre risorse, si rinuncia all'utilizzo del numero d'assicurato AVS. Nel presente caso, il numero può essere sostituito senza limitazioni esagerate o costi supplementari da identificatori di persone settoriali. In occasione dell'aggiornamento del registro degli utenti dei sistemi di gestione delle identità, sia che si tratti della ripresa dei dati dai registri dei collaboratori e degli utenti, del collegamento di applicazioni tecniche finora autonome o dell'immissione diretta di nuovi utenti, il numero d'assicurato AVS sarà invece utilizzato *temporaneamente* per garantire un'attribuzione senza errori. Per questo confronto, con una procedura irreversibile, dal numero d'assicurato AVS sarà formato un identificatore di persone settoriale specifico al sistema di gestione delle identità. Questo identificatore di persone sarà utilizzato per il confronto e memorizzato nel sistema di gestione delle identità per successive armonizzazioni dei dati. Con questa procedura è possibile mantenere a un livello elevato la qualità dei dati dei sistemi di gestione delle identità, cosa che altrimenti sarebbe possibile solamente con un onere sproporzionato. Inoltre, l'utilizzo del numero d'assicurato AVS è limitato in vari modi:

- l'utilizzo è ammesso unicamente se il sistema che fornisce i dati contiene esso stesso il numero d'assicurato AVS o quest'ultimo può figurarvi;
- il numero d'assicurato AVS viene utilizzato soltanto per breve tempo per generare il nuovo identificatore e non è memorizzato nel sistema di gestione delle identità;
- il numero d'assicurato AVS viene utilizzato soltanto nella ripresa o nella registrazione di nuove persone, quindi, per così dire, solamente al di fuori del sistema di gestione delle identità.

Se in un caso concreto si presenta un modo più semplice per un'armonizzazione sicura dei dati, ad esempio un numero personale interno, ovviamente si rinuncia a utilizzare il numero d'assicurato AVS. Se necessario, simili casi possono essere stabiliti a livello di ordinanza.

Art. 27 Disposizioni esecutive

Alle autorità assoggettate sarà conferito il mandato e accordata la competenza di disciplinare in modo esaustivo, in disposizioni esecutive, l'impiego dei sistemi di gestione delle identità.

Capitolo 3: Controllo di sicurezza relativo alle persone

Sezione 1: Disposizioni generali

Art. 28 Scopo e contenuto del controllo

Il CSP è una misura preventiva per la protezione contro i reati commessi da «elementi interni». Il suo obiettivo è quello di *identificare* l'eventuale rischio che, in seguito all'esercizio di un'attività sensibile sotto il profilo della sicurezza da parte di una determinata persona, vengano pregiudicati interessi ai sensi dell'articolo 1 capoverso 2. Si tratta dunque di stimare la probabilità che una determinata persona possa, intenzionalmente o per negligenza, pregiudicare la sicurezza delle informazioni della Confederazione. A tale scopo vengono acquisiti dati sulla condotta di vita di questa persona. Su tale base si procede a una valutazione del rischio, ossia a un pronostico relativo a fattispecie future incerte. La considerazione del rischio non si basa unicamente su fatti *assodati*, ma data la natura della questione le conclusioni tratte dai dati rilevati possono anche basarsi su ipotesi e supposizioni (v. anche sentenza del Tribunale amministrativo federale A-5617/2013 del 25.3.2013, consid. 3.4). Dopo avere preso atto della valutazione del rischio da parte del servizio specializzato CSP competente, spetta unicamente all'autorità o organizzazione assoggettata decidere se vuole assumersi un eventuale rischio elevato, se vuole ridurlo mediante determinate condizioni o se vuole evitarlo non assumendo o licenziando la persona in questione.

I capoversi 2 e 3 definiscono in generale il contenuto del controllo e i relativi limiti, ossia i dati che possono essere trattati per la valutazione del rischio e, per garantire il rispetto dei diritti della personalità delle persone sottoposte al controllo, quelli che non possono in linea di principio essere trattati. La prassi ha evidenziato che un catalogo esemplificativo di dati *rilevanti per la sicurezza* rappresenta un prezioso strumento interpretativo per quanto riguarda il contenuto materiale del CSP. Spesso, la messa in pericolo o la violazione della sicurezza delle informazioni da parte di una determinata persona ha radici nel passato ed è riconducibile a determinate circostanze personali. Difficoltà personali, in particolare finanziarie, o relazioni collegate a viaggi all'estero ma taciute dalla persona interessata in Svizzera possono, a seconda delle circostanze, creare situazioni gravemente pregiudizievoli per lo Stato. Nell'ambito del CSP viene pertanto puntata l'attenzione sulla *condotta di vita* della persona sottoposta al controllo. Il catalogo di dati sulla condotta di vita, elencato al capoverso 2, non è esaustivo e corrisponde nel contenuto al primo periodo dell'articolo 20 capoverso 1 LMSI. Il rimando figurante in quest'ultimo articolo ad «attività atte a minacciare in maniera illegale la sicurezza interna ed esterna» viene però cancellato: anzitutto, simili attività sono già contemplate nell'espressione generale *condotta di vita* e secondariamente il rilevamento di questi dati viene anche

subordinato a una condizione (che tali attività possano minacciare in maniera illegale la sicurezza) che può essere stabilita soltanto nell'ambito della valutazione del rischio per la sicurezza. Rispetto al diritto vigente, questa cancellazione non restringe ulteriormente i diritti di rilevamento dei dati dei servizi specializzati CSP. I limiti fissati dai vigenti articoli 3 capoverso 1 secondo periodo e 20 capoverso 1 LMSI rimangono comunque validi.

Art. 29 Elenco delle funzioni

L'articolo 29 disciplina, in combinato disposto con l'articolo 30, per quali persone deve essere eseguito un CPS. Le autorità assoggettate (ma non le organizzazioni) devono emanare per il loro ambito un elenco delle funzioni che *esigono* l'esercizio di un'attività sensibile sotto il profilo della sicurezza e i cui titolari devono per tanto essere sottoposti al controllo. Per i presupposti materiali per iscrivere una funzione nell'elenco delle funzioni non viene però semplicemente ripreso l'attuale sistema. Si prescinde dal criterio della *periodicità*, in particolare nel trattamento di informazioni classificate (v. n. 1.2.5). È invece decisiva per l'assoggettamento degli impiegati federali e dei militari al CSP la questione di sapere se il titolare di una determinata funzione *deve,* per l'adempimento dei propri compiti, esercitare un'attività sensibile sotto il profilo della sicurezza. Se una simile attività è *necessaria* per l'adempimento dei compiti inerenti alla funzione, allora e soltanto allora, la funzione deve essere inserita nell'elenco delle funzioni da sottoporre al controllo.

Alcuni esempi fittizi sono utili per spiegare l'applicazione del principio:

- nell'ambito dei suoi compiti, una collaboratrice dell'Ufficio federale dell'ambiente è competente per l'esame dell'impatto sull'ambiente delle costruzioni e degli impianti militari. Nell'adempimento di tali compiti deve trattare informazioni classificate a partire dal livello «confidenziale» e talvolta avere accesso a zone di protezione 2 di impianti militari. La sua funzione deve essere inserita nell'elenco delle funzioni;
- un collaboratore dell'Amministrazione federale delle finanze (AFF) deve eccezionalmente valutare le ripercussioni di una proposta classificata «confidenziale» all'attenzione del Consiglio federale. Questo genere di affari compete di regola ad altri collaboratori, che però sono assenti per ferie o malattia. In linea di principio, questo compito non rientra nella sua funzione, la quale di conseguenza non deve essere annoverata nell'elenco delle funzioni;
- il personale di pulizia di un'autorità ha talvolta, involontariamente, accesso a informazioni classificate quando, nell'ambito dei suoi compiti ordinari, pulisce gli uffici degli impiegati federali e questi ultimi non conservano o smaltiscono i supporti d'informazione conformemente alle prescrizioni. Tuttavia non fa parte del settore di compiti del personale di pulizia trattare informazioni classificate. Non può perciò essere compreso nell'elenco, a meno che non sia competente per la pulizia all'interno di una zona di sicurezza.

Il criterio della *periodicità*, anche se *de facto* sarà quasi sempre soddisfatto, *de iure* è irrilevante. Pure se, nella descrizione del posto, soltanto il cinque per cento del grado d'occupazione è previsto per l'adempimento di compiti sensibili sotto il profilo della sicurezza, la funzione va inserita nell'elenco. Anche se magari la titolare della

funzione interessata durante un lungo periodo non deve affatto adempiere simili compiti. L'*eventualità* dell'esercizio, inerente alla funzione, di un'attività sensibile sotto il profilo della sicurezza non è invece un motivo per inserire una funzione nell'elenco delle funzioni.

L'applicazione di questo approccio restrittivo presuppone che le autorità e le organizzazioni assoggettate abbiano una chiara panoramica dei processi aziendali interni e intersettoriali come pure dei compiti necessariamente connessi con attività sensibili sotto il profilo della sicurezza. Acquisire e mantenere una visione d'insieme in questo campo rappresenta nel contempo una misura fondamentale nel quadro della gestione dei rischi della sicurezza delle informazioni. I motivi per iscrivere una funzione nell'elenco delle funzioni devono essere dimostrabili: le descrizioni dei posti delle rispettive funzioni devono contenere un'esatta definizione dei compiti che implicano l'esercizio di un'attività sensibile sotto il profilo della sicurezza. Inoltre, indipendentemente da un eventuale assoggettamento al controllo di sicurezza relativo alle persone, le autorità e le organizzazioni assoggettate devono adottare le necessarie misure per limitare al minimo necessario la cerchia delle persone che devono esercitare attività sensibili sotto il profilo della sicurezza.

Il verbo utilizzato (*emanano*) chiarisce che si tratta di una formale delega di legiferare alle autorità assoggettate. Gli elenchi delle funzioni si troveranno quindi in ordinanze o regolamenti. Riguardo all'Amministrazione federale occorre, in linea di principio, mantenere l'attuale sistema. In virtù dei disciplinamenti delle competenze in conformità con la LOGA, il Consiglio federale può continuare ad autorizzare i dipartimenti e la Cancelleria federale a emanare i propri elenchi dettagliati.

Capoverso 2: soltanto le autorità assoggettate sono responsabili, secondo il capoverso 1, della valutazione della sensibilità delle funzioni sotto il profilo della sicurezza. Per i servizi specializzati CSP, gli elenchi delle funzioni sono in linea di principio vincolanti. Essi non possono verificare per ogni CSP avviato se la funzione è effettivamente sensibile sotto il profilo della sicurezza. Se così fosse, l'onere richiesto sarebbe sproporzionato. Occorre dunque assicurarsi che le autorità assoggettate garantiscano l'aggiornamento degli elenchi delle funzioni, e quindi la corrispondenza delle funzioni elencate con il loro grado effettivo di sensibilità sotto il profilo della sicurezza.

Art. 30 Persone da controllare

I capoversi 1 e 3 stabiliscono chi deve essere sottoposto al controllo. I presupposti per l'esecuzione del CSP in ambito internazionale sono disciplinati dai pertinenti trattati internazionali. Il principio definito al capoverso 1 lettera c si applica anche alle persone chiamate a esercitare un'attività sensibile sotto il profilo della sicurezza su incarico di un'autorità estera o di un'organizzazione internazionale. Nel caso in cui una funzione, pur adempiendo i criteri di cui all'articolo 29, non figurasse ancora nel relativo elenco, il controllo potrebbe comunque essere eseguito, sempre che l'autorità assoggettata vi acconsenta. Per l'Amministrazione federale, il Consiglio federale può delegare la competenza decisionale per il controllo eccezionale al capodipartimento interessato. L'elenco dovrà poi essere adeguato di conseguenza. I membri di autorità eletti dal Popolo o i magistrati eletti dall'Assemblea federale non

vengono in linea di principio sottoposti a un controllo per l'esercizio di tale funzione, anche se queste persone spesso esercitano le attività più sensibili sotto il profilo della sicurezza. Questa eccezione si riferisce tuttavia soltanto alla funzione e deve di conseguenza essere considerata relativa: se ad esempio un membro dell'Assemblea federale è soggetto all'obbligo di prestare servizio militare e nel contesto della propria funzione militare esercita un'attività sensibile sotto il profilo della sicurezza, occorre allora eseguire un CSP. Benché non vengano menzionati espressamente, sono escluse dal controllo anche le persone che nei Cantoni esercitano la funzione di cancelliere dello Stato.

Art. 31 Livelli di controllo

Riguardo ai livelli di controllo, la LMSI non contiene alcuna normativa precisa. Il principio di legalità richiede però, a motivo della profonda ingerenza nei diritti fondamentali delle persone connessa con l'esecuzione del CSP, che le più importanti modalità dell'ingerenza vengano stabilite a livello di legge. Poiché i livelli di controllo sono determinanti per la gravità dell'ingerenza, devono essere disciplinati nella legge. Il disegno prevede ora (v. n. 1.2.5) i due livelli di controllo seguenti:

– il controllo di sicurezza di base si applica alle attività sensibili sotto il profilo della sicurezza il cui esercizio contrario alle prescrizioni o non appropriato può pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2. Si tratta dunque implicitamente, in base al potenziale di danno menzionato, di quanto segue: (a) trattamento di informazioni classificate «confidenziale»; (b) amministrazione, esercizio, verifica o manutenzione di mezzi informatici del livello di sicurezza «protezione elevata»; e (c) accesso a zone di sicurezza nelle quali vengono esercitate attività di cui ad (a) e (b). Per l'accesso a zone di protezione 2 di un impianto militare è parimenti necessario un CSP di questo livello;
– il CSP ampliato si applica di conseguenza: (a) al trattamento di informazioni classificate «segreto»; (b) all'amministrazione, all'esercizio, alla verifica o alla manutenzione di mezzi informatici del livello di sicurezza «protezione molto elevata»; e (c) all'accesso a zone di sicurezza nelle quali vengono esercitate attività di cui ad (a) e (b). Per l'accesso a zone di protezione 3 di un impianto militare è parimenti necessario un CSP di questo livello.

Per la determinazione del livello di controllo è determinante soltanto l'effettiva sensibilità sotto il profilo della sicurezza della funzione in questione. Spetta alle autorità assoggettate definire i livelli di controllo e provvedere affinché nel caso dell'esercizio di funzioni di uguale sensibilità sotto il profilo della sicurezza i collaboratori esterni ed interni della Confederazione vengano sottoposti a un controllo di sicurezza dello stesso livello (v. n. 1.1.4). La valutazione operata dalla linea gerarchica è in linea di massima vincolante per i servizi specializzati CSP. Questi acquisiscono i dati per il livello di controllo richiesto (art. 35) e per la valutazione del rischio applicano i parametri del livello corrispondente. Siccome il danno potenziale che può giustificare l'esecuzione di un CSP ampliato è molto più importante rispetto a quello di un CSP di base, uno stesso evento può più facilmente giustificare un rischio per la sicurezza in caso di CSP ampliato che non nel caso di un CSP di base.

Sezione 2: Esecuzione

Art. 32 Servizi competenti

Il capoverso 1 conferisce formalmente alle autorità assoggettate e ai Cantoni la competenza formale per la definizione delle competenze relative all'avvio della procedura di controllo e alla decisione in merito all'esercizio delle attività sensibili sotto il profilo della sicurezza:

- i servizi specializzati CSP non possono avviare ed eseguire un CSP di propria iniziativa; necessitano sempre di un pertinente mandato. Le autorità assoggettate devono perciò designare, per il proprio ambito di competenza, i servizi autorizzati ad avviare il controllo e a conferire il relativo mandato ai servizi specializzati CSP. Di regola questa competenza è assegnata al servizio del personale, ma in talune unità amministrative è stata assegnata ai titolari di altre funzioni (p. es. agli incaricati della sicurezza delle informazioni). Se lo reputa opportuno, il Consiglio federale può anche autorizzare determinati terzi ad avviare CSP. Si tratta in particolare di aziende che esercitano frequentemente attività sensibili sotto il profilo della sicurezza per conto della Confederazione e sono in possesso di una dichiarazione di sicurezza aziendale ai sensi dell'articolo 62;
- la competenza a decidere in merito all'esercizio di un'attività sensibile sotto il profilo della sicurezza è necessariamente connessa anche alla responsabilità di gestire un eventuale rischio. Si tratta dunque, in linea di principio, di un affare del personale, che sottostà alle regole del diritto del personale. Sono possibili deroghe, in particolare se si tratta di attribuire l'esercizio di un'attività sensibile sotto il profilo della sicurezza a esterni. A questo riguardo occorre rilevare che spesso il servizio competente per la decisione è un servizio diverso da quello cui compete l'avvio del controllo.

Per l'esecuzione dei controlli, il Consiglio federale ricorre attualmente a due servizi specializzati CSP: uno, aggregato al DDPS, è competente per la maggior parte dei controlli; l'altro, subordinato alla Cancelleria federale dal profilo amministrativo, esegue i controlli relativi ai quadri del massimo livello dell'Amministrazione federale e agli impiegati dell'altro servizio specializzato CPS. In linea di massima, occorrerebbe mantenere il sistema attuale. Tuttavia, la competenza di decidere in merito all'organizzazione e alla subordinazione dei servizi specializzati appartiene al Consiglio federale (v. anche art. 49 lett. b nonché il parere del Consiglio federale del 22 aprile 2009 concernente il rapporto della CdG-N del 28 novembre 2008[28] sulle circostanze della nomina di Roland Nef a capo dell'esercito, ad raccomandazione 3, pag. 2941). I servizi specializzati CSP devono poter valutare il rischio per la sicurezza delle informazioni con la massima obiettività possibile, ossia sulla base dei dati rilevati, e secondo lo stato della scienza e della giurisprudenza. Di conseguenza, la linea gerarchica non deve immischiarsi nella procedura di controllo, altrimenti si corre il rischio che si abusi del CSP per fini personali o politici. La LSIn stabilisce pertanto che i servizi specializzati CSP effettuano la loro valutazione in modo indi-

28 FF **2009** 2937

pendente (non sono vincolati da istruzioni). Ciò corrisponde al diritto vigente (v. art. 21 cpv. 1 LMSI).

Art. 33 Consenso e collaborazione

L'esecuzione del CSP richiede, in linea di principio, il consenso espresso della persona interessata. Sotto questo aspetto i servizi specializzati CSP soggiacciono implicitamente a un obbligo di informare. Nella prassi tale obbligo viene espletato mediante consegna alla persona interessata, prima del controllo, di un promemoria che riporta le basi legali del CSP (anche per quanto riguarda l'acquisizione dei dati) e spiega la procedura seguita per il controllo. Unicamente nell'ambito dell'esercito o della protezione civile possono essere eseguiti CSP senza il consenso della persona interessata. Questa eccezione è necessaria perché altrimenti, rifiutando il consenso, i militari e i militi della protezione civile impedirebbero l'esecuzione del controllo e quindi potrebbero sottrarsi al proprio obbligo di prestare servizio.

Il capoverso 3 rimanda implicitamente all'articolo 13 capoverso 1 lettera c PA. La giurisprudenza e la dottrina in materia sono dunque applicabili. Nell'ambito dell'obbligo di collaborazione, la persona sottoposta al controllo è tenuta a cooperare all'accertamento dei fatti. Tale obbligo comprende, oltre all'obbligo di fornire informazioni durante l'audizione, anche quello di presentare documenti più ampi, utili ai fini del CSP. In particolare, è necessario che la persona interessata cooperi all'accertamento delle circostanze e relazioni personali delle quali i servizi specializzati CSP non hanno alcun indizio e che non sono direttamente individuabili. La persona interrogata è tenuta a dare risposte veritiere. Se vi fosse la possibilità di eludere domande sull'abuso di alcol o stupefacenti, su debiti personali, su occupazioni accessorie o simili facendo appello ai diritti fondamentali, e grazie a questo espediente le corrispondenti informazioni non potessero confluire nella valutazione del rischio per la sicurezza, ciò renderebbe illusorio l'intero controllo di sicurezza (v. anche messaggio LMSI, FF *1994* II 1004, in particolare pag. 1070). La persona sottoposta al controllo ha certo il diritto di dichiarare durante l'audizione che non vuole rispondere a determinate domande. I servizi specializzati avranno però poi il compito di valutare il rifiuto di informare o anche di presentare altri documenti, poiché per le domande sulla sfera segreta personale occorre pur concedere un certo margine. Ma se la persona sottoposta al controllo si rifiuta di cooperare in una misura tale da impedire una corretta valutazione, il servizio specializzato CSP emana una dichiarazione di constatazione (art. 40 cpv. 1 lett. d).

Art. 34 Momento del controllo di sicurezza relativo alle persone

Il diritto vigente (art. 19 cpv. 3 LMSI) richiede che il CSP venga eseguito prima di attribuire la carica o la funzione o conferire il mandato. L'applicazione della normativa vigente (di per sé opportuna), in pratica non può tuttavia avvenire senza un sostanziale aumento delle risorse di personale dei servizi specializzati CSP. Perciò, nel capoverso 1 viene attenuata la norma per gli impiegati delle autorità e delle organizzazioni assoggettate nonché dei Cantoni: si richiede ancora che soltanto per il gruppo di persone in questione il CSP venga avviato prima dell'attribuzione della funzione. I datori di lavoro continuano ovviamente a essere liberi di attendere la

dichiarazione del servizio specializzato CSP prima di permettere alla persona interessata di esercitare la funzione sensibile sotto il profilo della sicurezza. In pratica, di regola, essi inseriranno probabilmente nel contratto di lavoro una clausola in virtù della quale il rilascio di una dichiarazione di sicurezza con riserva, di una dichiarazione di rischio o di una dichiarazione di constatazione (v. art. 40 cpv. 1 lett. b–d) può costituire un motivo per revocare l'autorizzazione a esercitare l'attività sensibile sotto il profilo della sicurezza o addirittura per sciogliere immediatamente il rapporto di lavoro. Quanto alla temporanea riduzione dei rischi, i datori di lavoro possono richiedere un estratto del casellario giudiziale o del registro delle esecuzioni (art. 20*a* LPers).

Per le persone nominate dal Consiglio federale, il disciplinamento corrisponde al diritto vigente (art. 19 cpv. 3 LMSI). Lo stesso dicasi per i terzi destinati a eseguire un mandato sensibile sotto il profilo della sicurezza: il CSP deve essere concluso prima che alla persona possa essere affidato l'esercizio di un'attività sensibile sotto il profilo della sicurezza (v. anche n. 1.1.4: rapporto della CdG-S concernente i collaboratori esterni dell'Amministrazione federale, raccomandazione 6). Il motivo della differenza di trattamento sul piano giuridico tra gli impiegati interni e i terzi risiede nel particolare rapporto degli impiegati federali con la Confederazione, per i quali si può, in linea di principio, presupporre un elevato grado di lealtà nei confronti degli interessi della Confederazione. Inoltre, gli impiegati della Confederazione lavorano per lo più direttamente presso il datore di lavoro, il che consente un controllo più semplice.

Anche se non è disciplinato esplicitamente nel corrispondente trattato, in ambito internazionale si richiede sempre che il CPS sia concluso prima di consentire l'esercizio di un'attività sensibile sotto il profilo della sicurezza.

Art. 35 Acquisizione dei dati

L'acquisizione dei dati si ispira ampiamente alla legislazione attuale (v. art. 20 LMSI). I capoversi 1 e 2 disciplinano l'acquisizione dettagliata dei dati, la quale è stata reimpostata in seguito alla riduzione da tre a due livelli di controllo. Entrambi i capoversi contengono disposizioni *potestative*. I servizi specializzati, per valutare il rischio, non devono dunque necessariamente servirsi di tutti i mezzi disponibili. Ciò è importante in particolare nel controllo ampliato, perché la riduzione dei livelli di controllo non deve causare un aumento spropositato dei costi del CSP. Il Consiglio federale, nelle sue disposizioni esecutive, potrà anche stabilire quali dati e quando *devono* essere acquisiti.

Per il controllo di base possono venire consultate le seguenti fonti:

– il casellario giudiziale, gli atti delle autorità penali (v. art. 12 CPP), comprese le autorità penali minorili, e le raccolte di dati del Servizio delle attività informative della Confederazione (SIC) e delle autorità di polizia e di sicurezza della Confederazione e dei Cantoni possono contenere indicazioni sull'affidabilità e sugli eventuali precedenti di una persona. Nella LSIP, ai servizi specializzati CSP viene accordato il diritto all'accesso in linea al Registro nazionale di polizia. I dati degli organi di polizia cantonali collegati saranno quindi loro accessibili in maniera semplice ed efficiente. Ovviamen-

te, eventuali risultati vanno ponderati nell'ottica della prevista attività della persona sottoposta al controllo e posti nel giusto contesto. Non spetta alle autorità penali decidere quali siano i documenti necessari per un CSP. Il servizio specializzato CSP deve ricevere tutti gli atti disponibili per potersi fare un quadro esaustivo della persona da sottoporre al controllo;

- le informazioni dai registri delle autorità di esecuzione e fallimento sono necessarie per poter valutare la situazione finanziaria delle persone sottoposte al controllo nell'ottica di un eventuale rischio per la sicurezza come, ad esempio, la corruttibilità;
- ora potranno essere addotti anche gli atti e i risultati di controlli di sicurezza effettuati in precedenza. Da un lato, il servizio specializzato deve valutare in modo coerente gli stessi fatti. In linea di principio, ad esempio, una determinata persona non dovrebbe essere valutata diversamente, in base agli stessi fatti, rispetto a un controllo dello stesso livello già eseguito in passato. D'altro lato, questa disposizione facilita l'acquisizione dei dati, poiché determinati eventi sono già stati accertati nell'ambito di controlli precedenti. A causa dei termini previsti per la ripetizione dei controlli può succedere che una dichiarazione precedente contenga dati non più disponibili nel sistema in quanto distrutti in applicazione dell'articolo 48. Ovviamente, questi dati non devono più essere trattati;
- le informazioni dai social network che non sono rivolte alla collettività, bensì sono destinate soltanto a cerchie di persone chiuse, non sono considerate pubblicamente accessibili e non possono essere acquisite.

Per il controllo di sicurezza ampliato, oltre ai dati delle fonti appena menzionate possono essere consultate anche le fonti seguenti:

- i dati dei registri fiscali federali e cantonali possono fornire ulteriori informazioni sulla situazione economica della persona sottoposta al controllo, ad esempio in caso di discrepanza tra lo stile di vita e la dichiarazione fiscale;
- i dati dei registri dei controlli degli abitanti non vengono sempre acquisiti, poiché spesso presentano soltanto un valore aggiunto relativo. Tuttavia, in certe situazioni possono fornire importanti indizi per la valutazione della situazione personale;
- nell'ambito del controllo ampliato, la situazione finanziaria della persona sottoposta al controllo viene esaminata nei dettagli. Perciò possono essere sistematicamente acquisiti dati presso istituti finanziari e banche con le quali la persona interessata intrattiene relazioni d'affari;
- l'audizione della persona interessata serve a discutere di fatti che non risultano, o risultano soltanto in modo poco chiaro, dalla consultazione dei registri. L'audizione personale non va confusa con l'audizione di cui al capoverso 3. L'audizione di cui al capoverso 2 lettera d può essere eseguita anche in assenza di indizi relativi all'esistenza di un rischio per la sicurezza e non è limitata quanto alla sua portata.

Il capoverso 3 prevede che prevede che i servizi specializzati CSP possono sentire personalmente la persona sottoposta al controllo indipendentemente dal livello di

controllo se nell'ambito dell'acquisizione dei dati emergono circostanze rilevanti in materia di sicurezza. Tale audizione personale è limitata nella sua portata ai dati che possono essere acquisiti nell'ambito del livello di controllo in questione. L'audizione può essere effettuata anche nel caso in cui il servizio specializzato CSP non ha potuto acquisire una quantità sufficiente di dati relativi a un periodo di tempo adeguato. Questo caso può presentarsi, ad esempio, se prima del controllo la persona interessata ha soggiornato per un lungo periodo in un Paese nel quale non è possibile acquisire dati, o comunque non dati affidabili. L'espressione *periodo di tempo adeguato* è stata consapevolmente formulata in modo generico. L'attuale normativa dell'articolo 19 capoverso 3 OCSP, in virtù della quale i servizi specializzati CSP devono disporre almeno di dati concernenti un periodo di tempo di cinque anni precedente l'avvio del controllo di base e di dieci anni precedente l'avvio del controllo ampliato, è stata in parte giudicata sproporzionata e troppo assoluta. Sono perciò ipotizzabili due approcci di soluzione: o il Consiglio federale precisa la pertinente espressione nell'ambito delle sue disposizioni d'esecuzione oppure l'interpretazione di questa espressione rimane a discrezione dei servizi specializzati CSP. Per il chiarimento di particolari circostanze rilevanti per la sicurezza o per ottenere dati supplementari su un periodo di tempo più lungo, il servizio specializzato CSP può anche sentire terzi. Simili audizioni possono avvenire soltanto con il consenso della persona sottoposta al controllo e dei terzi interessati, ma il consenso del terzo interessato non comporta l'obbligo di fornire informazioni. Quindi, anche se consente all'audizione, il terzo interessato può sempre rifiutare di fornire qualsiasi informazione.

Il fatto che nell'ambito delle audizioni ai sensi del capoverso 2 lettera d o del capoverso 3 possano essere poste domande di carattere altamente personale fa parte della natura della questione. La rilevanza delle domande risulta sempre dal contesto dell'audizione o della funzione, del compito o della situazione personale della persona interessata. Ad esempio, determinate domande possono mirare a aspetti imprescindibili per la valutazione del rischio. Altre servono invece a strutturare il colloquio o a creare un'atmosfera favorevole al dialogo. Tuttavia, si rinuncia a domande senza alcun legame con il mandato. In linea di principio, in questo contesto non si può mai escludere completamente che l'audizione risulti penosa per la persona sottoposta al controllo. Pertanto, alla luce di ciò, le audizioni vengono condotte in modo da mettere a proprio agio la persona interessata, per quanto consentito dal loro scopo. Ciò nondimeno, vanno comunque acquisite tutte le informazioni necessarie alla valutazione.

È possibile che i dati necessari per la valutazione non riguardino soltanto le persone sottoposte al controllo, bensì anche terzi. Ciò può, ad esempio, essere il caso degli estratti conto bancari di una persona coniugata. Il capoverso 4 prevede perciò che anche questi dati personali devono poter essere trattati, sempre che siano inseparabilmente connessi con i dati sulla persona sottoposta al controllo e indispensabili per la valutazione del rischio. L'onere connesso con l'ottenimento del rispettivo consenso della persona terza per il trattamento dei dati sarebbe sproporzionatamente elevato per i servizi specializzati CSP. Per ragioni di trasparenza, i servizi specializzati CSP devono però informare questi terzi sul trattamento dei dati. Se l'informazione non è possibile o lo è soltanto con un onere sproporzionato, si applica l'articolo 18*a* capoverso 4 lett. b LPD.

Art. 36 Assistenza amministrativa

I servizi specializzati CSP non acquisiscono tutti i dati in modo autonomo. Ciò riguarda in particolare l'acquisizione di dati all'estero, che in linea di principio vengono acquisiti per il tramite di fedpol e del SIC. La legge deve pertanto autorizzare, rispettivamente obbligare le autorità incaricate di acquisire i dati a garantire l'assistenza amministrativa a favore dei servizi specializzati CSP. Il capoverso 2 disciplina le modalità specifiche dell'assistenza amministrativa di fedpol per i dati esteri in ambito di perseguimento penale. Secondo il diritto internazionale, i canali d'informazione della polizia (sistema d'informazione Schengen e di Europol) sono a disposizione unicamente per lo scambio di informazioni tra autorità di perseguimento penale. Lo stesso limite è previsto anche per il canale Interpol. Siccome i servizi specializzati CSP, anche interpretando largamente la nozione, non possono essere annoverati tra le autorità di perseguimento penale e i loro compiti non possono essere qualificati come attività in ambito di perseguimento penale, ma sono considerati esclusivamente quali attività di polizia di sicurezza, i canali di polizia non sono in linea di principio utilizzabili per richieste internazionali nell'ambito dei CSP in assenza di sospetti. Questi canali possono tuttavia essere utilizzati se dai primi accertamenti del servizio specializzato CSP nei sistemi d'informazione disponibili (in particolare con la consultazione automatica dei registri secondo l'art. 46 cpv. 6) emergono indizi di reati che rientrano dell'ambito di competenza della polizia giudiziaria federale quale ufficio centrale. In tal caso l'ufficio centrale competente (fedpol) controlla se i dati sono rilevanti sotto il profilo della sicurezza e possono quindi essere trasmessi. Il capoverso 2 è stato dunque inserito per dotare di una base legale concreta le richieste dei servizi specializzati CSP e i relativi lavori dei servizi d'analisi di fedpol.

Art. 37 Assunzione dei costi

La collaborazione da parte di autorità alla procedura deve essere fornita gratuitamente. Questo principio corrisponde sostanzialmente alla vigente prassi, salvo nel caso degli estratti degli uffici di esecuzione e fallimento cantonali, che sinora erano forniti a pagamento. I terzi, ad esempio banche o istituti di credito, ai quali si ricorre affinché collaborino, devono essere indennizzati se l'onere causato è considerevole. Un siffatto onere diventa considerevole in particolare se va oltre l'allestimento di estratti conto e simili e richiede ricerche particolarmente intense da parte dei terzi interpellati. Il Consiglio federale disciplinerà i presupposti e l'ammontare di simili indennizzi nelle disposizioni d'esecuzione.

Art. 38 Abbandono della procedura

Una procedura di controllo già avviata viene abbandonata se la persona sottoposta al controllo revoca il suo consenso nel corso della procedura, oppure se per un altro motivo essa non entra più in considerazione per la funzione prevista o il mandato in questione (p. es. perché la persona sottoposta al controllo ha disdetto il contratto di lavoro oppure in caso di insolvenza della ditta per la quale avrebbe dovuto lavorare). In tal caso occorre informare in merito all'abbandono della procedura sia la persona sottoposta al controllo sia il servizio che l'ha avviato e i dati già acquisiti dal servi-

zio specializzato PSP devono essere distrutti. Di conseguenza, la persona interessata non sarà considerata «persona già controllata» e non potrà esercitare l'attività sensibile sotto il profilo della sicurezza in questione o assumere la relativa funzione. L'abbandono della procedura è un atto materiale ai sensi dell'articolo 25*a* PA.

Sezione 3: Valutazione del rischio per la sicurezza

Art. 39 Rischio per la sicurezza

In passato si è deplorato che la normativa vigente della LMSI non menzioni esplicitamente che cosa va considerato come rischio per la sicurezza (v. n. 1.1.4: rapporto della CdG-N sulla verifica riguardante l'ispezione sulle circostanze della nomina di Roland Nef a capo dell'esercito, raccomandazione 1). Perciò ora sarà inserita una corrispondente norma che renda, per analogia, il senso della giurisprudenza del Tribunale amministrativo federale e del Tribunale federale. Rimane inteso che non vi è alcun metodo di valutazione puramente quantitativo quando si tratta di stimare il rischio in relazione alle azioni o alle omissioni umane. Si applica perciò un metodo qualitativo con il quale vengono valutati la presenza e il concorso di fattori di rischio.

Il rischio è, nella dottrina, il prodotto della probabilità che si verifichi un evento e delle ripercussioni di tale evento. L'espressione *attività sensibile sotto il profilo della sicurezza*, determinante per l'assoggettamento al CSP, contiene nella sua definizione le ripercussioni delle quali va impedito il verificarsi. Si tratta di un o *grave pregiudizio considerevole per gli interessi di cui all'articolo 1 capoverso 2*. Se la persona da sottoporre al controllo adempie in maniera appropriata e conforme alle prescrizioni i compiti che si prevede di assegnarle, il danno non può allora verificarsi per causa sua. L'evento da evitare è dunque *e contrario* l'esercizio non conforme alle prescrizioni o non appropriato, da parte della persona interessata, dell'attività sensibile sotto il profilo della sicurezza. Un rischio per la sicurezza nel senso del capoverso 1 deve quindi venire presunto se è elevata la probabilità che la persona sottoposta al controllo eserciterà l'attività sensibile sotto il profilo della sicurezza in maniera contraria alle prescrizioni o non appropriata e che così pregiudicherà almeno considerevolmente gli interessi di cui all'articolo 1 capoverso 2.

I servizi specializzati CSP devono focalizzarsi unicamente sulla probabilità che si verifichi l'evento. Nella valutazione di una simile probabilità si tratterà inevitabilmente sempre di una previsione associata a eventi futuri incerti; questa previsione è caratterizzata da incertezze, poiché per sua natura non può basarsi esclusivamente su fatti *assodati* e poiché le conclusioni tratte dai dati acquisiti possono anche basarsi su ipotesi e supposizioni. La base per questa previsione è costituita dalla totalità di tutte le circostanze, ad esempio la personalità della persona interessata, il suo passato e le sue condizioni di vita, nella misura in cui da esse sia possibile dedurre il suo futuro comportamento. Nel capoverso 2 vengono perciò resi concreti i fattori di rischio che portano a supporre un'elevata probabilità di un pregiudizio, in quanto vi sono definite caratteristiche personali che sono particolarmente ad alto rischio. L'enumerazione si rifà dal profilo materiale all'attuale prassi dei servizi specializzati CSP, nonché alla giurisprudenza del Tribunale amministrativo federale e del Tribu-

nale federale. Anche se le definizioni mirano, in linea di principio, a caratteristiche accertabili nella maniera più obiettiva possibile, sovente queste possono essere dedotte solamente da indizi o dal contesto e in parte si sovrappongono. Con integrità e affidabilità si mira primariamente al carattere, alle abitudini e alle relazioni di una persona con il suo ambiente. Queste caratteristiche sono i requisiti di idoneità per antonomasia nell'esercizio di un'attività sensibile sotto il profilo della sicurezza. In presenza di queste caratteristiche, si può considerare con elevata probabilità che la persona alla quale è stata affidata una simile attività è leale rispetto al suo compito e tutela gli interessi in materia di sicurezza del datore di lavoro o dell'istituzione. Quali indizi e nessi dimostrano la mancanza di affidabilità di una persona, la sua presunta ricattabilità o la sua pregiudicata capacità di giudizio e di decisione, non può essere specificato a livello di legge, bensì deve, in ultima analisi, essere accertato e illustrato in ogni singola valutazione.

Secondo il capoverso 3 il CSP si fonda su una minaccia obiettiva, e non su un comportamento colpevole. Ciò contrariamente, ad esempio, al diritto penale, nel quale la colpa è sempre il presupposto per una pena. Diversamente dal diritto penale (*in dubio pro reo*), nel dubbio la sicurezza dello Stato o l'interesse del Paese prevalgono quindi sugli interessi della persona in questione. La presunzione di un rischio per la sicurezza deve essere fondata su fatti e circostanze effettive riguardo alla persona da sottoporre al controllo. Non sono ammesse mere supposizioni, in particolare se riguardano l'orientamento politico della persona da sottoporre al controllo.

Art. 40 Risultato della valutazione

Il capoverso 1 disciplina le varie dichiarazioni dei servizi specializzati CSP nelle quali viene registrato il risultato della valutazione. Se a motivo dell'insufficienza dei dati acquisti di cui all'articolo 35 capoverso 3 una persona non può essere valutata secondo le norme, il servizio specializzato CSP rilascia una dichiarazione di constatazione. Se del caso si procede dapprima all'audizione della persona interessata.

Sotto il profilo giuridico, le dichiarazioni dei servizi specializzati CSP non costituiscono decisioni, bensì atti materiali ai sensi dell'articolo 25*a* capoverso 1 PA. Analogamente all'attuale LMSI (v. art. 21 cpv. 3 LMSI) la LSIn instaura una tutela giurisdizionale diretta per le persone sottoposte al controllo (v. art. 95). Il rimedio previsto all'articolo 25*a* capoverso 2 PA (emanazione di una decisione) non è applicabile. Il capoverso 2 riconosce perciò un diritto formale di essere sentiti. In pratica, di fronte a un progetto di dichiarazione secondo le lettere b–d, occorre informare adeguatamente la persona interessata in merito al contenuto del progetto e accordarle un termine adeguato per esprimersi al riguardo.

Art. 41 Comunicazione

I capoversi 1 e 2 corrispondono sostanzialmente al diritto vigente (art. 21 cpv. 2–4 LMSI). La decisione in forma integrale è comunicata anche al servizio decidente, il quale altrimenti non potrebbe decidere con cognizione di causa.

Il capoverso 3 disciplina il caso in cui viene avviato un CSP, ma la persona interessata è soggetta a un controllo anche in relazione con un'altra attività di cui alle lettere a–c (p. es. secondo l'art. 20*b* LPers). In questo caso il servizio specializzato

CSP deve poter comunicare al rispettivo servizio decidente la dichiarazione relativa al controllo principale. Il disciplinamento dell'esame dell'affidabilità di cui all'articolo 20*b* LPers, nonché di cui all'articolo 113 LM, esige che le due procedure vengano riunite se, in virtù della presente legge, una persona deve parimenti essere sottoposta a un CSP. Con il termine *soggetta* non si esige che sia stato avviato un altro controllo o che un controllo debba essere immediatamente ripetuto. Questo è particolarmente importante per i controlli secondo l'articolo 113 LM a cui sono soggetti tutti i militari. Se nell'ambito di un CSP si constata un rischio in relazione all'arma militare, i servizi specializzati CPS possono comunicare la dichiarazione alla competente autorità militare.

Nel caso di una riserva motivata riguardo alla sicurezza e se vi è urgenza, nell'ottica della prevenzione dai pericoli i servizi specializzati CSP possono informare in merito alle loro constatazioni i servizi competenti già prima che la procedura sia conclusa. In seguito a ciò, il servizio competente può adottare misure di sicurezza preventive.

Sezione 4: Conseguenze della dichiarazione

Art. 42 Esercizio dell'attività sensibile sotto il profilo della sicurezza

Il capoverso 1 corrisponde al vigente articolo 21 capoverso 4 LMSI. Non spetta ai servizi specializzati CSP adottare o limitare la responsabilità della linea gerarchica per le decisioni in materia di personale, bensì unicamente informare l'autorità decidente in merito al rischio eventuale. Prima della sua decisione, il servizio decidente deve prendere conoscenza della dichiarazione del servizio specializzato CSP, poiché soltanto allora potrà decidere tenendo conto degli eventuali rischi.

Le condizioni di cui al capoverso 3 rappresentano misure atte a ridurre i rischi che per lo più riguardano il diritto in materia di personale. Il servizio decidente può, ad esempio, esigere che la persona interessata renda nota periodicamente la sua situazione finanziaria o si sottoponga a test antidroga. Queste condizioni riguardano esclusivamente l'esercizio dell'attività sensibile sotto il profilo della sicurezza; non riguardano l'esercizio di altri compiti. Di regola, le condizioni più idonee vengono raccomandate dal servizio specializzato CSP. Il servizio decidente non è però vincolato a queste condizioni e può stabilire autonomamente condizioni diverse.

La comunicazione della decisione secondo il capoverso 4 avviene all'interno del sistema d'informazione di cui all'articolo 46 ed è determinante soprattutto per la concessione dell'accesso a determinate zone di sicurezza. I servizi specializzati CSP non traggono conclusioni dalle decisioni, né si lasciano condizionare da esse nella propria prassi.

Art. 43 Utilizzo molteplice di una dichiarazione

Se per la persona interessata è già stata rilasciata una dichiarazione ancora valida ed equivalente, per motivi di economia procedurale non deve di norma essere eseguito un nuovo controllo. La condizione per poter rinunciare a una nuova procedura di

controllo quando esiste una dichiarazione ancora valida ed equivalente consiste nel procedere in modo strutturato all'esecuzione del controllo e alla valutazione del rischio (v. commento all'art. 31). Nella prassi questa normativa non rappresenta alcun problema se è stata rilasciata una dichiarazione di sicurezza per lo stesso livello di controllo o uno superiore. Problemi possono però risultare, ad esempio, se per un livello di controllo superiore a una determinata persona è stata rilasciata una dichiarazione di sicurezza con riserva o una dichiarazione di rischio. È infatti senz'altro possibile che per il trattamento di informazioni classificate «segreto» sussista un rischio per la sicurezza, ma che questo rischio sia sostenibile se riferito al trattamento di informazioni classificate «confidenziale». Il Consiglio federale dovrà rendere concreta questa prescrizione *potestativa* a livello di ordinanza.

Art. 44 Ripetizione

La LSIn rinuncia a prescrivere intervalli fissi per la ripetizione ordinaria. A questo riguardo essa fissa unicamente principi generali. Il motivo è che in futuro la ripetizione dovrà avvenire sempre più in conformità con l'effettiva esigenza di sicurezza. Le disposizioni d'esecuzione disciplineranno in dettaglio le ripetizioni. Per quanto riguarda i militari o i militi della protezione civile, il Consiglio federale dovrebbe poter rinunciare a una ripetizione di un controllo se, ad esempio, la ripetizione appare sproporzionata rispetto al periodo di servizio residuo.

Il capoverso 3 disciplina la ripetizione straordinaria. Il motivo di una simile ripetizione anticipata è l'insorgere di nuovi rischi inerenti alla persona in questione, ad esempio l'apertura nei confronti di tale persona di un procedimento penale che presenta un rapporto con l'attività sensibile sotto il profilo della sicurezza.

Art. 45 Tutela giurisdizionale

Nonostante gli adeguamenti redazionali, i capoversi 1 e 2 corrispondono al diritto vigente (v. art. 21 cpv. 2 LMSI). Il termine per l'esercizio dei diritti di consultazione e rettifica viene esteso, rispetto al diritto vigente, da 10 a 30 giorni. Dato che in virtù del capoverso 3 la persona sottoposta al controllo ha 30 giorni di tempo per interporre ricorso presso il Tribunale amministrativo federale, durante questo periodo deve poter esercitare tutti i diritti previsti al capoverso 1.

Anche il capoverso 3 corrisponde in linea di principio al diritto vigente (v. art. 21 cpv. 3 LMSI), sebbene inizi precisando che le dichiarazioni dei servizi specializzati CSP rappresentano un atto materiale ai sensi dell'articolo 25*a* PA. L'attuale articolo 22 OCSP definisce le dichiarazioni dei servizi specializzati CSP quali decisioni ai sensi dell'articolo 5 PA. Questa qualificazione è però materialmente errata, poiché tali dichiarazioni hanno soltanto carattere di raccomandazione (v. art. 21 cpv. 4 LMSI nonché art. 42 LSIn). Data la gravità dell'ingerenza nei diritti della personalità delle persone sottoposte a controllo, si rinuncia tuttavia alla tutela giurisdizionale ordinaria per gli atti materiali secondo l'articolo 25*a* PA, creando in luogo e vece un rimedio giuridico che permette di appellarsi direttamente al Tribunale amministrativo federale.

Con l'adozione della LSIn, il Tribunale amministrativo federale e il Tribunale federale potranno avviare un CSP per i propri impiegati o per i terzi ai quali affidano

mandati. In questi casi saranno competenti anche per la decisione riguardante l'esercizio dell'attività sensibile sotto il profilo della sicurezza e al tempo stesso per un'eventuale procedura di ricorso. Di conseguenza emerge, come per i litigi in materia di diritto del lavoro, un conflitto di interessi che sarà impedito grazie alla collaudata norma dell'articolo 36 LPers.

Sezione 5: Trattamento di dati personali

Art. 46 Sistema d'informazione per i controlli di sicurezza relativi alle persone

L'articolo 46 corrisponde sostanzialmente al diritto vigente (v. art. 144–149 LSIM). Entrambi i servizi specializzati utilizzano un sistema (Sistema informatizzato per i controlli di sicurezza relativi alle persone, SIBAD) impiegato e gestito dal DDPS. I dati acquisiti e in particolare le valutazioni dei rischi costituiscono dati personali degni di particolare protezione e profili della personalità secondo l'articolo 3 lettere c e d LPD. Ovviamente, il sistema non è impiegato solo per i CSP ai sensi della LSIn, ma anche per l'esecuzione delle verifiche dell'affidabilità secondo la legislazione speciale e per le valutazioni del potenziale di violenza secondo la LM. Il Consiglio federale definirà le competenze per la protezione dei dati (v. art. 49 lett. d).

Per l'identificazione delle persone, il sistema utilizza un numero di registrazione proprio. Il numero d'assicurato AVS viene utilizzato soltanto se è utilizzato sistematicamente anche da un altro sistema. Questo caso si presenta principalmente nel sistema d'informazione PISA dell'Aggruppamento Difesa. Il sistema PISA utilizza sistematicamente i numeri AVS e quindi questi numeri vengono ripresi nel sistema SIBAD in occasione dell'avvio di CSP dell'esercito. In seguito, all'interno del sistema SIBAD, viene utilizzato unicamente il numero di registrazione SIBAD. Tuttavia, dopo il controllo, per l'armonizzazione dei dati con il sistema PISA la concordanza con il numero AVS deve essere ristabilita.

Capoverso 6: secondo l'articolo 19 capoverso 3 LPD, i dati personali degni di particolare protezione possono essere resi accessibili attraverso una procedura automatizzata soltanto qualora lo preveda esplicitamente una legge in senso formale. La possibilità di consultare mediante procedura di richiamo automatica i sistemi d'informazione della Confederazione ai quali i servizi specializzati CSP hanno legalmente accesso può incrementare l'efficienza della procedura di controllo. Le basi legali formali dei tre sistemi d'informazione menzionati nel presente messaggio prevedono già l'accesso da parte dei servizi specializzati CSP. Con questo capoverso non vengono dunque garantiti a questi ultimi diritti d'accesso nuovi o più estesi. Finora, tuttavia, ogni sistema doveva essere consultato singolarmente e ancora manualmente dai collaboratori dei servizi specializzati CSP. In futuro sarà necessario consultare manualmente un sistema soltanto se la consultazione automatica avrà prodotto un risultato, ossia una registrazione (v. anche art. 36 cpv. 2). Questo modo di procedere, i cui dettagli saranno definiti a livello di ordinanza, riduce inoltre considerevolmente le fonti di errore in occasione dell'immissione manuale. Natu-

ralmente, anche i Cantoni, nel loro diritto interno, possono concedere ai servizi specializzati CSP un analogo accesso automatico alle loro banche dati.

Art. 47 Diritti d'accesso e comunicazione dei dati

L'articolo 47 capoversi 1–3 corrisponde al diritto vigente (v. art. 144–149 LSIM), che però viene formulato in modo più esaustivo in virtù dell'articolo 19 capoverso 3 LPD. Gli elenchi di cui al capoverso 4 vengono forniti soltanto in caso di comprovata necessità. La fornitura avviene al di fuori del sistema d'informazione.

Art. 48 Conservazione, archiviazione e distruzione dei dati

L'articolo 48 corrisponde sostanzialmente al diritto vigente (v. art. 144–149 LSIM nonché OCSP). Il capoverso 1 costituisce il fondamento giuridico per la registrazione audio delle audizioni. Secondo il capoverso 2, la durata di conservazione dei dati non deve superare dieci anni. Qualora una persona sia già stata sottoposta a più controlli, vanno cancellati i dati riguardanti controlli che risalgono a oltre dieci anni prima. L'Archivio federale valuta quali dati del sistema d'informazione hanno valore archivistico (cpv. 3). Si tratta in particolare delle statistiche sui casi di rischio e sul numero di CSP eseguiti. In caso di abbandono della procedura secondo l'articolo 38 esiste la possibilità (quantunque assai improbabile) che la persona interessata chieda l'emanazione di una decisione e che in seguito inoltri ricorso presso il Tribunale amministrativo federale. Ai servizi specializzati non è dunque consentito cancellare subito i dati.

Sezione 6: Disposizioni del Consiglio federale

Art. 49

Il Consiglio federale deve poter emanare normative completive e suppletive. Non si tratta dunque semplicemente di disposizioni d'esecuzione, per le quali il Consiglio federale è senz'altro competente sulla base dell'articolo 182 Cost. Il motivo risiede nel disciplinamento previsto all'articolo 85 capoverso 1, secondo il quale tutte le autorità ai sensi dell'articolo 2 capoverso 1 sono incaricate dell'esecuzione della legge e dell'emanazione delle opportune disposizioni esecutive.

- Lettera c: le autorità di sicurezza estere accordano esclusivamente a persone che sono state sottoposte al CSP l'accesso a informazioni e materiale classificati o a zone di sicurezza. L'autorità svizzera competente (verosimilmente il servizio specializzato della Confederazione per la sicurezza delle informazioni ai sensi dell'art. 84) deve poter rilasciare la necessaria attestazione di sicurezza relativa alle persone. Determinante non è l'attestazione, bensì la decisione del servizio decidente.
- Lettere d–f: in applicazione dell'articolo 16 capoverso 2 LPD, il Consiglio federale deve emanare normative completive sull'organizzazione delle competenze e responsabilità per la protezione dei dati (incl. la sicurezza dei dati) in relazione con il sistema d'informazione di cui all'articolo 46. Siccome i

dati trattati nell'ambito dei CSP sono particolarmente sensibili, la legalità del loro trattamento deve essere controllata periodicamente da un organo indipendente dai servizi specializzati CSP.

Capitolo 4: Procedura di sicurezza relativa alle aziende

Sezione 1: Disposizioni generali

Art. 50 Scopo della procedura

In merito allo scopo della PSA, si rimanda al numero 1.2.6.

Art. 51 Aziende interessate

Quale *azienda* ai sensi della legge non si considera necessariamente l'intera impresa. Si tratta piuttosto soltanto di quelle parti e persone dell'impresa alle quali è effettivamente affidato il mandato sensibile sotto il profilo della sicurezza.

– La lettera a menziona il caso di applicazione principale: l'intenzione di un'autorità o di un'organizzazione assoggettata di conferire un mandato sensibile sotto il profilo della sicurezza a un'impresa che si candida per tale mandato. La PSA costituisce, in linea di principio, una questione di carattere nazionale. Perciò, le aziende con sede all'estero che si candidano per un mandato proveniente dalla Svizzera devono farsi controllare dallo Stato nel quale si trova la loro sede. Le competenze e le modalità di controllo sono parte integrante dei trattati internazionali di cui all'articolo 88.

– La lettera b considera, inversamente, il caso di aziende con sede in Svizzera che vogliono candidarsi per un mandato dall'estero e devono presentare alle autorità del Paese interessato una dichiarazione di sicurezza delle autorità dello Stato in cui si trova la loro sede. Questa procedura e la corrispondente certificazione rappresentano un'attività ufficiale che non può essere delegata all'economia privata perché le autorità estere esigono, senza eccezioni, un «sigillo di sicurezza» ufficiale dello Stato in cui ha sede l'azienda. Poiché in questo caso, la Confederazione non ha alcun interesse proprio diretto all'esecuzione della procedura, i costi della procedura sono a carico delle aziende (cpv. 3). Il Consiglio federale disciplinerà la questione dei costi a livello di ordinanza.

Nella prassi il necessario consenso dell'azienda non rappresenta mai un problema, poiché le aziende hanno un interesse finanziario al conferimento del mandato.

Art. 52 Abbandono della procedura

La PSA viene eseguita soltanto se vengono soddisfatti determinati criteri e presupposti (p. es. il consenso). Se nel corso della PSA l'azienda non soddisfa più questi criteri, la procedura viene abbandonata e tutti i dati e atti in rapporto con essa vengono distrutti. Secondo la lettera c, ciò può anche avvenire, ad esempio, se l'azienda, nel caso del proprio fallimento o della distruzione dello stabilimento in seguito a un

incendio, non è assolutamente più in grado di adempiere il mandato. Il capoverso 2 stabilisce che le PSA vengono eseguite da un *servizio specializzato per la sicurezza aziendale* (servizio specializzato SA). In seno alla Confederazione (come finora) un unico servizio si occuperà dunque di questa procedura. Il servizio specializzato SA deve comunicare l'abbandono della procedura all'azienda e al mandante.

Sezione 2: Avvio della procedura di sicurezza relativa alle aziende

Art. 53 Domanda di avvio della procedura

Il servizio specializzato SA si attiva soltanto su domanda (e non su mandato) di un'autorità o organizzazione assoggettata. Queste ultime sono però tenute a presentare una domanda in tal senso se vogliono conferire a un'azienda un mandato sensibile sotto il profilo della sicurezza. Le autorità assoggettate devono stabilire quali servizi sono competenti per la presentazione della domanda. A seconda delle loro necessità organizzative, può trattarsi di un servizio centrale o di qualsiasi servizio che dispone della competenza di conferire mandati sensibili sotto il profilo della sicurezza a imprese dell'economia privata (v. anche l'ordinanza del 24 ottobre 2012[29] concernente l'organizzazione degli acquisti pubblici dell'Amministrazione federale).

In ambito internazionale, la procedura è di regola avviata mediante una domanda da parte dell'autorità di sicurezza estera (*Facility Security Clearance Information Sheet, FSCIS*) all'autorità di sicurezza locale e una conferma dell'azienda interessata. Alla domanda si risponde secondo una procedura standardizzata i cui dettagli vanno disciplinati mediante ordinanza.

Art. 54 Esame della domanda

Una volta ricevuta la domanda, il servizio specializzato SA verifica dapprima se vi è un mandato sensibile sotto il profilo della sicurezza e se del caso avvia la PSA. Se, nel caso concreto, i rischi per la sicurezza delle informazioni possono essere ridotti al minimo mediante altre misure, il servizio specializzato SA, dopo aver consultato il mandante, può rinunciare all'esecuzione della PSA. Ciò consente di evitare in questi casi oneri antieconomici e burocratici. Se il mandato è svolto sotto la vigilanza del mandante e nei suoi locali, e al mandatario (azienda) non è consegnata alcuna documentazione, bastano ad esempio, eventualmente, i corrispondenti CSP. Se il servizio specializzato SA rinuncia alla PSA, allora raccomanda anche le misure di sicurezza che reputa opportune. In questo caso il servizio specializzato SA non dispone più di alcuna competenza di attuazione.

Art. 55 Definizione dei requisiti di sicurezza

Dopo l'avvio della procedura, il servizio specializzato SA definisce, d'intesa con il mandante, i requisiti in materia di sicurezza delle informazioni per l'adempimento del mandato. Se l'esercizio di un'attività sensibile sotto il profilo della sicurezza è

29 RS **172.056.15**

necessario già nell'ambito della procedura di aggiudicazione, anche per questa fase vengono stabiliti i requisiti. In particolare, ciò si verifica spesso quando per l'allestimento di un'offerta durante la procedura di aggiudicazione è necessario conoscere informazioni classificate o accedere a zone di sicurezza.

Sezione 3: Valutazione delle aziende

Art. 56 Idoneità

La nozione di *idoneità* va intesa nel senso della sistematica del diritto in materia di acquisti pubblici. Anche se la garanzia della sicurezza delle informazioni non rappresenta un esplicito criterio di idoneità di cui all'articolo 9 LAPub, il presente disegno la introduce però per l'esecuzione di mandati sensibili sotto il profilo della sicurezza. La valutazione dell'idoneità sotto il profilo della sicurezza equivale a una valutazione del rischio. Per ragioni di economicità e di protezione dei dati, tale valutazione non deve essere eseguita per tutti gli offerenti, ma soltanto per quelli che entrano in considerazione per l'aggiudicazione. Se sussiste un rischio per la sicurezza delle informazioni ai sensi dell'articolo 58, l'azienda interessata non è idonea. Il servizio specializzato SA non deve essere vincolato a istruzioni per valutare l'idoneità. Qui si tratta di eseguire la valutazione senza farsi condizionare da interessi di politica economica (v. art. 32 cpv. 2).

Art. 57 Acquisizione dei dati

L'articolo 57 costituisce la base legale formale per l'acquisizione dei dati in vista della valutazione dell'idoneità delle aziende. Il capoverso 1 elenca quali dati può rilevare il servizio specializzato SA per la valutazione dell'idoneità. Sostanzialmente, i dati necessari vengono acquisiti presso l'azienda stessa con il suo consenso. Sono particolarmente importanti anche i risultati degli accertamenti presso il SIC. Infine, il servizio specializzato SA può acquisire dati sulla ditta anche dal registro di commercio o da Internet. Simili ricerche possono fornire importanti informazioni sull'affidabilità della ditta (v. l'art. 35 cpv. 1 lett. g per il CSP). Dato che molte aziende hanno legami con l'estero, è indispensabile poter acquisire i corrispondenti dati. In particolare le informazioni di intelligence acquisite dal SIC all'estero possono fornire preziosi indizi sull'esistenza di un rischio per la sicurezza. Le modalità per simili domande e per le informazioni che vengono fornite di conseguenza vanno disciplinate a livello di ordinanza.

Art. 58 Rischio per la sicurezza

Questa disposizione è simmetrica alla valutazione del rischio per la sicurezza effettuata nell'ambito del CSP. I meccanismi di valutazione del rischio sono, in linea di principio, identici (v. commento all'art. 39). Sussiste dunque un rischio per la sicurezza quando vi sono indizi concreti che l'azienda con elevata probabilità eserciterà l'attività sensibile in materia di sicurezza in maniera contraria alle prescrizioni o non appropriata. Ciò può essere il caso, ad esempio, se i dati acquisiti mostrano che l'azienda ha commesso reati rilevanti per la sicurezza delle informazioni oppure se

l'azienda è costituita da una singola persona (ditta individuale) o se per l'adempimento del mandato sono indispensabili determinate persone (p. es. perché queste persone sono specialisti che non possono essere sostituiti o perché dirigono l'azienda e il mandato non può essere eseguito senza il loro impiego). Il rilascio di una dichiarazione di rischio nell'ambito del CSP per queste persone appartenenti all'azienda può avere quale conseguenza che l'azienda nella sua totalità debba essere valutata come un rischio per la sicurezza. Le PSA sono tuttavia volte soprattutto a impedire che informazioni sensibili sotto il profilo della sicurezza o vettori di attacco pratici a mezzi informatici sensibili della Confederazione siano resi accessibili a aziende che per i loro rapporti di proprietà, i loro rapporti giuridici, le loro strutture organizzative o le loro relazioni d'affari vengono ad esempio dirette o influenzate in maniera determinante da servizi informazioni esteri o da organizzazioni di stampo criminale (*Foreign Ownership, Control or Influence*) (v. anche n. 1.2.6).

Il capoverso 3 sancisce che il rischio menzionato deve essere motivato dalle circostanze effettive. In tale contesto, è irrilevante se all'azienda stessa o ai suoi collaboratori è imputabile una qualsivoglia colpa, ad esempio se la ditta cui appartiene l'azienda è diretta da persone legate a servizi informazioni o alla criminalità (v. commento all'art. 39 cpv. 3).

Art. 59 Notifica della valutazione ed esclusione dalla procedura di aggiudicazione

Il servizio specializzato SA notifica all'azienda interessata la propria valutazione quanto all'idoneità. Se essa non è d'accordo con la valutazione del rischio, può presentare ricorso contro questa decisione dinanzi al Tribunale amministrativo federale (art. 70 cpv. 1 lett. d). Il mandante può continuare la procedura di aggiudicazione o le sue trattative con tutte le aziende nelle quali non è individuabile alcun rischio per la sicurezza. Esso non è autorizzato a presentare ricorso e perciò viene soltanto informato sulla valutazione. Se il servizio specializzato SA individua rischi insostenibili per la sicurezza in relazione a un'azienda, il mandante non può invece né aggiudicare il mandato a tale azienda né stipulare il contratto con essa. Esso esclude dalla procedura di aggiudicazione l'azienda in questione in quanto non idonea sotto il profilo della sicurezza. Contrariamente al caso del CSP, nel caso della PSA il mandante è in linea di principio vincolato alla valutazione del servizio specializzato SA. Un'impresa o un'azienda alla quale viene rilasciata una DSA riceve un «sigillo di sicurezza» statale. L'integrità di questo sigillo può essere assicurata soltanto se la decisione sull'idoneità viene presa da specialisti. Per questo motivo il servizio specializzato SA emana una decisione impugnabile.

Al capoverso 3 è concessa una deroga al principio di cui al capoverso 2 nel caso in cui per l'esecuzione del mandato non esiste una reale alternativa a un'azienda che rappresenta un rischio per la sicurezza delle informazioni della Confederazione. Questa ipotesi riguarda soprattutto le prestazioni di servizi in ambito informatico, dove alcune ditte occupano una posizione di quasi monopolio sul mercato. Se a causa della mancanza di alternative una simile azienda dovesse comunque essere presa in considerazione per l'esecuzione del mandato, non sarà consentito in alcun caso rilasciarle una dichiarazione di sicurezza svizzera. Di conseguenza, la PSA sarebbe abbandonata e la responsabilità del controllo delle misure di sicurezza

sarebbe delegata al mandante, il quale per forza di legge vanta diritti di imposizione analoghi a quelli del servizio specializzato SA nell'ambito della PSA.

Sezione 4: Piano in materia di sicurezza

Art. 60 Aggiudicazione e piano in materia di sicurezza

Appena il mandante ha aggiudicato il mandato, informa il servizio specializzato SA, che avvia le ulteriori fasi della procedura. Per garantire la sicurezza delle informazioni nell'azienda occorre adottare pertinenti misure organizzative, in materia di personale, tecniche e fisiche. Perciò, l'azienda in questione descriverà in un piano in materia di sicurezza come devono essere applicati i requisiti in materia di sicurezza delle informazioni definiti dal servizio specializzato SA (v. anche l'art. 55). Di regola, le aziende hanno già adottato nei più svariati ambiti misure di sicurezza che devono soltanto essere ancora verificate dal servizio specializzato SA e, ove necessario, completate. Tutte le misure sono sancite nel piano in materia di sicurezza. Il servizio specializzato SA acquisisce direttamente presso l'azienda i dati necessari per il controllo e l'approvazione del piano in materia di sicurezza.

Art. 61 Controlli di sicurezza relativi alle persone

Il personale dell'azienda viene controllato in virtù dell'articolo 30 capoverso 1 lettera c o capoverso 2. Il livello del controllo è stabilito in base all'articolo 31 senza distinguere tra collaboratori interni ed esterni. Al termine del CSP, il servizio specializzato SA decide in modo vincolante se alla persona controllata può essere affidata l'attività sensibile sotto il profilo della sicurezza. Se la PSA viene abbandonata in applicazione dell'articolo 59 capoverso 3, la competenza spetta al mandante.

Sezione 5: Dichiarazione di sicurezza aziendale

Art. 62 Rilascio della dichiarazione di sicurezza aziendale

Diversamente dalla dichiarazione di sicurezza nell'ambito del CSP, il rilascio o il mancato rilascio della DSA costituisce una decisione ai sensi dell'articolo 5 PA, perché produce effetti giuridici diretti per i partecipanti. Nella prassi sinora applicata è successo soltanto di rado che un'azienda non abbia attuato le misure di sicurezza o che la DSA non sia stata rilasciata. Ma se dovesse effettivamente verificarsi un caso del genere, prima di poter decidere di rifiutare la DSA, il servizio specializzato SA deve concedere un termine di grazia all'azienda affinché questa possa adempiere i suoi obblighi. Se non è d'accordo con la decisione del servizio specializzato SA, l'azienda può presentare ricorso al Tribunale amministrativo federale (art. 70 cpv. 1 lett. d). La decisione è comunicata anche al mandante, poiché quest'ultimo non può affidare il mandato sensibile all'azienda cui viene rifiutata la DSA (vedi art. 63). A questo stadio il mandante avrà probabilmente già investito molto denaro nel progetto in questione. Pertanto, viene riconosciuto anche al mandante (contrariamente al caso previsto all'art. 59 cpv. 1) il diritto di ricorrere.

Limitando a cinque anni la durata di validità della DSA si intende garantire che si proceda periodicamente a una nuova valutazione dell'idoneità sotto il profilo della sicurezza. Grazie a essa sarà possibile tenere conto delle modifiche fondamentali nell'azienda che influiscono sulla sicurezza delle informazioni.

Art. 63 Esecuzione del mandato sensibile

Il mandante è vincolato alla decisione del servizio specializzato SA. Esso non può più affidare un mandato sensibile sotto il profilo della sicurezza all'azienda alla quale è stata rifiutata la DSA (vedi l'art. 62 cpv. 2). Viceversa, le aziende con una DSA valida sono autorizzate a eseguire mandati sensibili sotto il profilo della sicurezza se è stato aggiudicato loro il pertinente mandato e il contratto si concretizza. La DSA deve essere rilasciata prima che il mandante faccia eseguire il mandato all'azienda. Questa norma corrisponde al principio dell'articolo 34 capoverso 3 nell'ambito del CSP.

Art. 64 Obblighi dell'azienda

Le aziende titolari di una DSA sono tenute a cooperare e collaborare. Il loro obbligo più importante consiste nell'applicare in permanenza le misure del piano in materia di sicurezza. Queste aziende devono inoltre annunciare al servizio specializzato SA tutti i cambiamenti fondamentali per la salvaguardia della sicurezza delle informazioni nell'adempimento del mandato sensibile sotto il profilo della sicurezza. Ad esempio, vanno annunciati i nuovi collaboratori ai quali devono essere affidate attività sensibili sotto il profilo della sicurezza affinché nei loro confronti venga eseguito un CSP. L'azienda deve poi annunciare senza indugio se si è verificato un incidente rilevante sotto il profilo della sicurezza.

Art. 65 Controlli e misure di protezione

Il servizio specializzato SA deve sorvegliare il rispetto, nell'azienda, delle misure di sicurezza previste nel piano in materia di sicurezza. Per sua stessa natura, l'ispezione può anche avvenire senza preavviso. Può essere eseguita soltanto con l'accompagnamento o in presenza di una persona appartenente all'azienda, di regola l'incaricato della sicurezza. Quando vi sono indizi concreti di una minaccia per la sicurezza delle informazioni il servizio specializzato SA può adottare le necessarie misure di protezione. Può, ad esempio, disporre l'immediata messa sotto chiave o restituzione di taluni documenti o materiali. Qualora la sicurezza delle informazioni non possa essere garantita diversamente, è persino autorizzato a sequestrare determinati documenti o materiali. Ciò si applica anche nei casi in cui, dopo il fallimento di un'azienda, documenti o mezzi informatici ancora presenti devono essere separati rapidamente dalla massa fallimentare.

Art. 66 Procedura semplificata in caso di aggiudicazione di altri mandati sensibili

Le aziende titolari di una DSA sono in linea di principio considerate sicure. La loro idoneità non è oggetto di una nuova valutazione. In casi simili occorre tuttavia verificare se occorre adeguare il piano in materia di sicurezza vigente. Un adeguamento sarebbe ad esempio necessario se l'azienda interessata avesse sinora dovuto trattare «soltanto» informazioni classificate «confidenziale», ma dovesse in futuro trattare anche informazioni classificate «segreto». In questi casi si applica una procedura semplificata, che il Consiglio federale disciplinerà a livello di ordinanza.

Art. 67 Attestazione di sicurezza aziendale internazionale

Le aziende con sede in Svizzera che si candidano per un mandato estero sensibile sotto il profilo della sicurezza, devono sempre più spesso presentare alle autorità del Paese in questione una dichiarazione di sicurezza delle autorità svizzere. L'articolo 67 costituisce la base necessaria per il rilascio di questo tipo di attestazioni, che consentono alle ditte svizzere di accedere a mandati all'estero.

Art. 68 Revoca della dichiarazione di sicurezza aziendale

La revoca della DSA durante l'esecuzione di un mandato è un evento estremamente raro. Se si verifica, viene emanata una relativa decisione, che può essere impugnata dinanzi al Tribunale amministrativo federale. Il diritto di ricorrere è riconosciuto anche al mandante, poiché una revoca può essere svantaggiosa anche per esso. Ad esempio, può avere un interesse finanziario rilevante a evitare la revoca della DSA. Tuttavia, per scongiurare il rischio, il mandante deve esonerare senza indugio l'azienda dall'esecuzione del mandato. L'azienda non ha diritto ad alcun indennizzo di carattere finanziario. Il lavoro già prestato deve però essere remunerato. È fatta salva l'applicazione dell'articolo 59 capoverso 3 (assegnazione del mandato a un'azienda inidonea), poiché è possibile che il mandante non abbia alcuna alternativa economicamente sostenibile rispetto all'azienda in questione. In tal caso, le facoltà di controllo e imposizione di cui gode il servizio specializzato SA vengono delegate al mandante.

Sezione 6: Ripetizione della procedura e tutela giurisdizionale

Art. 69 Ripetizione della procedura

Durante la ripetizione della procedura l'adempimento del mandato non viene interrotto. Se il mandato è quasi adempiuto e all'azienda non sono stati assegnati nuovi mandati, per motivi di economia procedurale il servizio specializzato SA non ripeterà la procedura. Se sussiste un motivo concreto per presumere che in seguito a cambiamenti sostanziali in seno all'azienda siano emersi nuovi rischi per la sicurezza, la procedura va ripetuta.

Art. 70 Tutela giurisdizionale

Agli organi dell'azienda vengono concessi in linea di principio gli stessi diritti concessi nell'ambito del CSP (v. art. 45). Contro le decisioni del servizio specializzato SA è ammesso il ricorso al Tribunale amministrativo federale. Con questa norma si stabilisce implicitamente che, nel presente caso, non si applica la disposizione derogatoria dell'articolo 32 capoverso 1 lettera a della legge sul Tribunale amministrativo federale (sostanziale inammissibilità del ricorso contro le decisioni in materia di sicurezza interna o esterna del Paese). Se tuttavia una decisione del servizio specializzato SA si fonda su informazioni di intelligence che non devono giungere all'azienda o all'opinione pubblica, allora trovano applicazione le corrispondenti disposizioni procedurali (art. 27 e 28 PA).

Sezione 7: Trattamento dei dati personali

Art. 71 Sistema d'informazione per la procedura di sicurezza relativa alle aziende

Per ragioni di sistematica, l'attuale base giuridica relativa al sistema (art. 150 segg. LSIM), esistente da anni, va spostata nella LSIn. Siccome il sistema può contenere dati personali degni di particolare protezione, necessita di una base legale formale (art. 17 cpv. 2 LPD).

Art. 72 Diritti d'accesso e comunicazione dei dati

I mandanti hanno accesso ai dati che li riguardano e all'elenco di tutte le aziende titolari di una DSA. Ciò consente loro di vedere rapidamente se un'azienda è già titolare di una DSA. Nell'ambito delle proprie disposizioni esecutive, il Consiglio federale può autorizzare determinate aziende ad avviare autonomamente CSP per il rispettivo ambito di competenza. In questo caso tali aziende devono ottenere l'accesso a determinati dati del sistema d'informazione. Già con l'attuale sistema gli incaricati della sicurezza di talune aziende possono consultare la decisione in merito al controllo e il livello di controllo dei collaboratori della loro azienda.

Art. 73 *Conservazione, archiviazione e distruzione dei dati*

Il disciplinamento della conservazione, dell'archiviazione e della distruzione dei dati corrisponde, *mutatis mutandis,* a quello proposto per il CSP (vedi art. 48).

Sezione 8: Disposizioni del Consiglio federale

Art. 74

Il commento all'articolo 49 relativo al CSP vale anche per la PSA.

Capitolo 5: Infrastrutture critiche

Gli articoli 75–81 disciplinano i compiti e le competenze della Confederazione per quanto riguarda il sostegno ai gestori di infrastrutture critiche nel campo della sicurezza delle informazioni. La partecipazione dei gestori di infrastrutture critiche al partenariato pubblico-privato con la Confederazione e l'acquisizione delle prestazioni della Confederazione avvengono su base volontaria. In merito alla SNPC, v. i numeri 1.1.2 e 1.2.7.

Art. 75 Compiti della Confederazione

L'interesse dell'intera società per un funzionamento affidabile delle infrastrutture critiche si riflette nella prima disposizione di questo capitolo: la Confederazione, sostenendo i gestori di infrastrutture critiche, intende garantire che le interruzioni di reti e di sistemi e gli abusi siano rari, di breve durata, gestibili e poco dannosi. Si tratta di assicurare la funzionalità tecnica delle infrastrutture dell'informazione, Internet compresa, e di fare in modo che i mezzi informatici non vengano utilizzati all'insaputa degli utenti autorizzati. Il suddetto sostegno comprende in particolare le prestazioni menzionate al capoverso 2. Per contro, non può essere invocato per combattere abusi relativi ai contenuti, quali le violazioni del diritto d'autore o i delitti contro l'onore.

Secondo il capoverso 3, la Confederazione, da un lato, gestisce un servizio nazionale di preallerta che analizza costantemente la situazione di minaccia nell'ambito della sicurezza delle informazioni e rielabora le informazioni riguardanti minacce e pericoli identificati all'attenzione dei gestori di infrastrutture critiche, per sostenerne il processo di sicurezza delle informazioni e di gestione dei rischi. Dall'altro, gestisce un punto di contatto per misure preventive e reattive nell'ambito della sicurezza tecnica delle informazioni, che può procedere ad analisi tecniche, ad esempio su software nocivi, ed emanare raccomandazioni per misure tecniche concrete volte a rendere sicuri i mezzi informatici, sventare pericoli o individuare incidenti. Per acquisire conoscenze, i servizi ai quali vengono assegnati compiti di cui al capoverso 3 possono per esempio gestire mezzi informatici vulnerabili (honeypots) in reti nonché lasciar funzionare, sotto osservazione, mezzi informatici infettati, per analizzare il funzionamento e il comportamento di software nocivi e di aggressori.

Secondo il capoverso 4, il Consiglio federale provvede affinché possa avere luogo uno scambio di informazioni sicuro tra la Confederazione e i gestori di infrastrutture critiche e tra gli stessi gestori di infrastrutture critiche. Questo capoverso non istituisce alcuna competenza autonoma per il trattamento dei dati, ma offre la base legale per allestire una piattaforma sicura per lo scambio di informazioni. Sovente minacce, pericoli e vulnerabilità riguardano non soltanto un singolo obiettivo, bensì varie organizzazioni operanti in un determinato settore, forse anche tutti i gestori di infrastrutture critiche di vari settori. Tuttavia, il ricorso alle prestazioni di cui all'articolo 75 e la partecipazione al partenariato pubblico-privato poggiano completamente sulla volontarietà. Il principio secondo il quale le infrastrutture critiche assumono la responsabilità del proprio operato viene dunque implicitamente ripetuto. Mediante uno scambio di informazioni permanente si intende creare trasparenza e fiducia. In questo modo, non acquisiscono know-how soltanto i gestori di infrastrutture critiche,

bensì anche le autorità federali nella loro qualità di proprietari e gestori di infrastrutture critiche. Esse possono ottenere importanti informazioni per valutare i propri rischi e per sventare pericoli.

L'espressione «servizi della Confederazione competenti» designa attualmente MELANI, che l'ODIC gestisce congiuntamente al SIC. In considerazione dell'autonomia organizzativa del Consiglio federale, i servizi competenti non vanno designati nel testo della legge, ma a livello di ordinanza (cpv. 5). Anche in futuro tali servizi si presenteranno in maniera omogenea nei confronti dei gestori di infrastrutture critiche. Per contro, il posizionamento nell'organigramma e l'organizzazione interna di tali servizi possono essere liberamente stabiliti dal Consiglio federale.

Art. 76 Trattamento di dati personali

Per l'adempimento dei compiti secondo l'articolo 75, i servizi competenti della Confederazione devono poter trattare e scambiare con i gestori di infrastrutture critiche informazioni riguardo a minacce e pericoli nonché indicatori relativi a incidenti nell'ambito della sicurezza delle informazioni. Simili informazioni consistono soprattutto in elementi d'indirizzo secondo l'articolo 3 lettera f LTC (p. es. indirizzi IP, indirizzi e-mail, nomi di dominio). Questi elementi d'indirizzo sono accomunati dal fatto che si riferiscono a persone e apparecchi o collegamenti di telecomunicazione determinati o determinabili, che a loro volta possono essere attribuiti a una persona determinata o determinabile. Inoltre i clienti finali acquistano elementi d'indirizzo per lo più da fornitori di servizi di telecomunicazione o altri fornitori di servizi, che a loro volta possono essere determinati sulla base dell'elemento d'indirizzo – di regola consultando elenchi pubblici. Di conseguenza, gli elementi d'indirizzo possono essere considerati dati personali il cui trattamento da parte di organi della Confederazione necessita di una base legale (art. 4 cpv. 3 e 17 cpv. 1 LPD). La qualificazione di elementi d'indirizzo è controversa nella dottrina e nella prassi e in casi concreti può essere giudicata in maniera molto differente, non da ultimo a causa delle procedure amministrative di assegnazione e degli obblighi in materia di registri in parte assai divergenti per quanto riguarda gli elementi d'indirizzo esteri. Per questo motivo nella LSIn l'interpretazione se gli elementi d'indirizzo siano o meno dati personali è consapevolmente ampia, allo scopo di garantire la legalità del trattamento dei dati e offrire certezza giuridica ai servizi incaricati del trattamento.

Il capoverso 1 prevede di conseguenza che i servizi secondo l'articolo 75 capoverso 5 possano trattare gli elementi d'indirizzo necessari e i relativi dati personali. Il trattamento di dati secondo il presente capitolo non è comparabile alle misure segrete di sorveglianza relative a persone e al contenuto di colloqui secondo il CPP o la LSCPT. Per quanto riguarda i dati qui menzionati si tratta tipicamente di istruzioni di programmi sotto forma di codici (nocivi) destinati ai computer e di elementi d'indirizzo comparsi in relazione con un incidente (ad es. utilizzazione abusiva di un servizio informatico o infezione di un mezzo informatico con software nocivi) e annunciati a MELANI. Scambiando simili dati sarà possibile stabilire se i sistemi degni di protezione dei gestori di infrastrutture critiche hanno avuto collegamenti con tali elementi d'indirizzo (confronto con dati di log delle reti interne di gestori di infrastrutture critiche), poiché ciò funge da *indizio* (e non da *prova*) di una viola-

zione della sicurezza delle informazioni. Occorre quindi esaminare simili indizi effettuando ulteriori accertamenti nei propri sistemi per scoprire ad esempio infezioni con software nocivi nella propria rete.

Ai sensi dell'articolo 17 capoverso 2 LPD, nel capoverso 2 è accordata ai servizi competenti la competenza per il trattamento di elementi d'indirizzo e dei relativi dati personali che possono essere considerati degni di particolare protezione.

– Lettera a: gli attacchi a mezzi e sistemi informatici avvengono prevalentemente per moventi di ordine finanziario. Spesso tuttavia non sono pianificati o perpetrati principalmente a scopo di lucro, ma per motivi religiosi, ideologici o politici. Simili motivi sono all'origine, per esempio, degli attacchi commessi da hackers militanti, che interrompono servizi forniti per via informatica, provocano danni finanziari o pubblicano dati confidenziali delle vittime dell'attacco al fine di attirare l'attenzione dell'opinione pubblica sui propri obiettivi politici. Poiché l'intenzione all'origine di un attacco può essere essenziale per la valutazione di una minaccia e dei conseguenti pericoli, MELANI deve poter trattare anche dati concernenti opinioni personali se ciò risulta necessario per la valutazione di minacce e pericoli concreti.

– Lettera b: gli attacchi a mezzi e infrastrutture informatici sono di regola perseguiti penalmente. Secondo l'articolo 3 lettera c numero 4 LPD, se dati personali concernono procedimenti penali, sono considerati dati personali degni di particolare protezione il cui trattamento da parte degli organi della Confederazione necessita di una base legale formale. Tuttavia poiché unicamente con una denuncia il pericolo per lo meno a breve termine non è scongiurato, informare i gestori delle infrastrutture critiche per quanto riguarda questi vettori d'attacco è essenziale, affinché questi possano proteggere i loro sistemi ed eventualmente individuare attacchi già avvenuti. Anche se non viene comunicato il fatto che è stato avviato un procedimento riguardante un elemento d'indirizzo o che è stata inflitta una sanzione, dall'indicazione che un elemento d'indirizzo è stato utilizzato per scopi criminali la persona che riceve l'informazione può dedurre che è in corso un procedimento in tal senso. Con la competenza stabilita in questo capoverso s'intende impedire che questo scambio non possa più avere luogo appena viene sporta denuncia riguardo a un elemento d'indirizzo o viene avviata una procedura amministrativa.

Il capoverso 3 consente il trattamento dei dati senza che le persone interessate ne siano informate. In molti casi il regime dell'assegnazione di elementi d'indirizzo consta di più livelli. Nell'assegnazione di nomi di dominio Internet sono ad esempio coinvolte numerose persone che di norma possono essere determinate consultando registri pubblici («richieste WHOIS»): centro di registrazione, *registrar*, *registrant*, contatto tecnico, contatto amministrativo. Se il dominio Internet è attivo, è inoltre correlato a un indirizzo IP e a determinate persone individuabili sulla base di tale indirizzo (consultando nuovamente registri pubblici). Non è proporzionale, per ogni trattamento di un nome di dominio, informare tutte le persone fisiche e giuridiche correlate e determinabili – tuttavia spesso alcune persone interessate vengono contattate in maniera mirata, affinché possano adottare misure atte a prevenire i pericoli, impedire ulteriori abusi e ristabilire lo stato legale. Per contro l'identificazione

dell'utente (finale) non è di norma possibile, o comporta un onere notevole, in particolare per gli elementi d'indirizzo registrati all'estero. Non è neppure necessaria per la prevenzione dei pericoli mediante misure di protezione passive. Se non avviene alcuna identificazione, il trattamento dei dati non può né essere reso noto alle persone interessate, né esse possono essere informate in merito al trattamento.

Se invece, ai sensi del capoverso 4, sussiste il sospetto che un elemento d'indirizzo (svizzero) o un apparecchio che utilizza questo elemento d'indirizzo è utilizzato abusivamente da persone non autorizzate, l'utente legittimo sarà identificato e informato in merito all'utilizzazione abusiva. L'identificazione e l'informazione non devono tuttavia avvenire per forza da parte delle autorità competenti: ad esempio, nel caso di indirizzi IP dinamici, può venire informato il fornitore di servizi di telecomunicazione affinché possa inoltrare le relative indicazioni ai clienti interessati, consentendo loro così di adottare misure per impedire ulteriori abusi e, in presenza di reati, di denunciarli ed eventualmente sporgere querela.

La presente disposizione va quindi vista come *lex specialis* rispetto all'articolo 4 capoverso 4 e all'articolo 18*a* LPD.

Art. 77 Collaborazione in Svizzera

L'articolo 77 autorizza i servizi competenti a comunicare, per l'adempimento dei propri compiti, i generi di dati definiti ai gestori di infrastrutture critiche, affinché quest'ultimi possano proteggersi. I servizi competenti possono inoltre comunicare dati a fornitori e a gestori di servizi informatici affinché questi, dopo un abuso dei loro sistemi e di quelli dei rispettivi clienti, siano in grado di impedire ulteriori abusi.

Il capoverso 3 concede ai gestori di infrastrutture critiche nonché ai fornitori e ai gestori di servizi informatici e di servizi di comunicazione il diritto di comunicare volontariamente ai servizi di cui all'articolo 75 informazioni connesse con pericoli e incidenti nell'ambito della sicurezza delle informazioni. Possono dare indicazioni in merito alle prestazioni di servizi, alle trasmissioni e ad altre operazioni effettuate per sventare pericoli e di conseguenza per impedire danni. Questa disposizione consente il trattamento conforme al diritto dei dati personali e di altre indicazioni pertinenti. Un caso di applicazione di questa disposizione lo si ha quando da un hosting provider viene accertata la presenza di un server di gestione (command & control server) con cui è gestita una rete di computer privati (rete bot) infettati da software nocivi. In casi del genere l'hosting provider potrebbe fornire a MELANI file di archivio da cui sono individuabili gli indirizzi IP dei computer privati infettati. Questi verrebbero poi trasmessi ai rispettivi fornitori di servizi di telecomunicazione affinché possano avvisare i propri clienti. Inoltre l'hosting provider potrebbe fornire file di configurazione e modelli di comunicazione del server di gestione che consentono l'individuazione di altre reti bot. Alle indagini di polizia e ai procedimenti giudiziari continuano ad applicarsi le rispettive norme per l'assunzione delle prove. Le autorità di perseguimento penale non sono autorizzate a procurarsi dati presso MELANI, ma devono farne richiesta in maniera probatoria al titolare originario dei dati. Se il fornitore di dati autorizza esplicitamente un inoltro, MELANI può comunicare autonomamente i dati alle competenti autorità di perseguimento penale.

Art. 78 Cooperazione internazionale

La protezione di infrastrutture critiche da pericoli nel settore della sicurezza delle informazioni è un compito che nessuna impresa né nessun Paese può portare a termine agendo in maniera solitaria. Il carattere globale della rete internet fa sì che di regola gli incidenti non hanno ripercussioni soltanto a livello locale o nazionale, ma concernono gestori di infrastrutture critiche in diversi Paesi. Avendo al riguardo un interesse comune, molti Stati cooperano già attualmente su base volontaria per individuare e fronteggiare gli incidenti. Non sussiste alcun obbligo di fornire determinati dati. La presente legge non comporta cambiamenti in materia. All'articolo 78 è attribuita a MELANI unicamente una competenza esplicita per la cooperazione internazionale e per il relativo scambio di dati. Anche se nel quadro della cooperazione internazionale sono regolarmente scambiati dati, in ogni singolo caso è possibile rinunciare alla comunicazione di dati se giudicata incompatibile con l'articolo 6 LPD o sproporzionata. I servizi esteri devono garantire che i dati ricevuti saranno impiegati esclusivamente in maniera conforme alle pertinenti disposizioni. In ambito internazionale si è affermato il cosiddetto *«traffic light protocol»*, conformemente al quale lo scambio di dati è accompagnato da indicazioni sui destinatari ai quali è autorizzato un inoltro dei dati (per es. unicamente al settore dell'energia).

Lo scambio di informazioni tra autorità comprende in primo luogo elementi d'indirizzo. Al riguardo va tuttavia osservato che MELANI comunica soltanto in casi molto rari ai suoi partner internazionali elementi d'indirizzo relativi a persone, ditte o mezzi informatici ubicati in Svizzera. Minacce e pericoli che emanano dalla Svizzera sono infatti trattati nel quadro della collaborazione nazionale. Lo scambio di informazioni comprende inoltre ulteriori informazioni essenziali per garantire la sicurezza delle informazioni presso le infrastrutture critiche (per es.: descrizioni e valutazioni di minacce; disposizioni per l'individuazione e l'eliminazione tecniche di incidenti; analisi di incidenti e raccomandazioni di sicurezza concrete; analisi concernenti lacune della sicurezza e vulnerabilità). Considerato che la cooperazione internazionale serve alla protezione e alla prevenzione dei pericoli, al capoverso 3 è precisato che ai procedimenti giudiziari si applicano le disposizioni in materia di assistenza amministrativa e giudiziaria. È pertanto stabilito che la presente legge non può essere impiegata per aggirare i presupposti in materia.

Art. 79 Sistema d'informazione per il sostegno alle infrastrutture critiche

Per garantire la massima sicurezza possibile nonché la tracciabilità del trattamento dei dati, è indicato l'impiego di un sistema d'informazione specifico. Lo scambio di informazioni può tuttavia avvenire anche tramite altri canali, ad esempio attraverso la posta elettronica crittata o in occasione di incontri personali. L'elenco delle informazioni contenute nel sistema d'informazione illustra che non si tratta necessariamente di dati personali e anche gli elementi d'indirizzo non sono di norma resi accessibili in base alle persone. Tuttavia in particolare le disposizioni per l'individuazione tecnica di incidenti possono contenere elementi d'indirizzo grazie ai quali, consultando registri pubblici, possono essere individuate persone in relazione con detti elementi d'indirizzo. Sebbene queste persone spesso non siano gli utenti finali degli elementi d'indirizzo, sono determinabili sulla base di tali elementi e di conseguenza questi ultimi sono da qualificare come dati personali.

Art. 80 Conservazione e archiviazione dei dati

I dati personali sono conservati soltanto per la durata necessaria all'individuazione di incidenti e alla prevenzione dei pericoli. La definizione nella legge di una durata massima di conservazione di cinque anni sancisce un orizzonte temporale fondamentale. Nella maggior parte dei casi i dati trattati hanno durata molto breve e possono essere di nuovo cancellati poco dopo che sono stati trattati. Per contro singole indicazioni in merito a vettori d'attacco possono mantenere la loro validità per diversi anni. L'adeguatezza di un trattamento costante dei dati può essere verificato di volta in volta durante i controlli di cui all'articolo 81 lettera d da parte di un organo esterno.

Art. 81 Disposizioni del Consiglio federale

Il Consiglio federale disciplinerà a livello di ordinanza la ripartizione dei compiti e la collaborazione tra i servizi secondo l'articolo 75 capoverso 5. Nella LAIn sono previste competenze del SIC nel campo della protezione delle infrastrutture critiche. Il Consiglio federale dovrà stabilire nel dettaglio la ripartizione dei compiti, la collaborazione e lo scambio di informazioni. Per creare trasparenza e garantire la certezza del diritto, il Consiglio federale disciplinerà il trattamento e lo scambio di dati tra questi servizi, la loro comunicazione ai gestori di infrastrutture critiche nonché a servizi esteri e internazionali, come pure la sicurezza dei dati da considerare in tale ambito. Provvederà anche a un controllo esterno periodico della legalità del trattamento dei dati. L'organo di controllo può essere liberamente scelto dal Consiglio federale, sempre che tale organo disponga della necessaria indipendenza nei confronti di MELANI.

Capitolo 6: Organizzazione ed esecuzione

Sezione 1: Organizzazione

Art. 82 Incaricati della sicurezza delle informazioni

In merito al ruolo degli incaricati della sicurezza delle informazioni si rinvia al numero 1.2.9. Considerata la necessità preponderante di una direzione integrale dell'attuazione della legge, la LSIn interviene nell'autonomia organizzativa delle autorità: chiede che, per il rispettivo ambito di competenza, le autorità, i dipartimenti e la CaF provvedano a designare un incaricato della sicurezza delle informazioni e un supplente. Poiché, da un lato, un'efficace direzione integrale della sicurezza delle informazioni presuppone conoscenze politiche, giuridiche, organizzative e anche tecniche e, dall'altro, gli incaricati della sicurezza delle informazioni devono assumere moltissimi compiti, l'attuazione pratica esige che almeno due persone per autorità assumano questi compiti. Non viene tuttavia richiesto che entrambe le persone siano impiegate a tempo pieno per tale scopo.

Il Consiglio federale stesso deve, parimenti, designare un incaricato della sicurezza delle informazioni. Per contro, a motivo del suo limitato effettivo di personale, l'autorità di vigilanza sul Ministero pubblico della Confederazione non va obbligata

in tal senso. I tribunali della Confederazione non vengono indicati singolarmente perché sarebbe sproporzionato esigere simili servizi dai tribunali con un effettivo di personale relativamente esiguo. La LSIn ammette dunque che, ad esempio, i tribunali della Confederazione possano designare un organo unico per tutti i tribunali oppure scelgano un approccio diverso che preservi l'autonomia delle autorità. Anche gli Uffici federali e l'Amministrazione federale decentralizzata non vengono obbligati dalla legge a designare un incaricato. Nell'ambito dell'adempimento del suo obbligo in materia di organizzazione, il Consiglio federale deve decidere a livello di ordinanza come sarà organizzata e diretta la sicurezza delle informazioni fino a questo livello.

Il capoverso 2 definisce in forma generale il settore di compiti e le competenze degli incaricati della sicurezza delle informazioni:

- la lettera a sottolinea che le competenze decisionali e la responsabilità delle decisioni nell'ambito della sicurezza tecnica delle informazioni devono continuare a rimanere presso la linea gerarchica, dunque presso le autorità competenti e i loro servizi subordinati. Gli incaricati della sicurezza delle informazioni devono però, sotto il profilo tecnico, consigliare e assistere la linea gerarchica;
- la lettera b stabilisce che, per incarico della propria autorità o organizzazione, gli incaricati della sicurezza delle informazioni devono dirigere sotto il profilo tecnico la sicurezza delle informazioni e la corrispondente gestione dei rischi;
- la lettera c prevede che gli incaricati della sicurezza delle informazioni abbiano un obbligo generale di verificare regolarmente il rispetto delle prescrizioni della presente legge, che redigano rapporti all'attenzione della propria autorità e che, in caso di necessità di agire, debbano presentare una richiesta in tal senso. Ciò include anche l'elenco delle funzioni che comportano attività sensibili sotto il profilo della sicurezza. Gli audit e i controlli rappresentano sempre un tema delicato. Il loro svolgimento deve essere in linea di principio ordinato dalla linea gerarchica. A tale scopo gli incaricati della sicurezza delle informazioni presentano annualmente alle proprie autorità o organizzazioni un piano degli audit, in cui sono indicate le priorità e le risorse necessarie al riguardo.
- la lettera d rileva che gli incaricati della sicurezza delle informazioni possono annunciare incidenti rilevanti sotto il profilo della sicurezza al servizio specializzato della Confederazione per la sicurezza delle informazioni, alla Conferenza degli incaricati della sicurezza delle informazioni e ai servizi che assumono i compiti in materia di sicurezza delle informazioni presso le infrastrutture critiche. A causa dell'autonomia delle autorità si rinuncia quindi a *un obbligo generale di annuncio* applicabile a tutte le autorità. Se lo ritiene necessario, il Consiglio federale può prevedere a livello di ordinanza un obbligo di annuncio per l'Amministrazione federale e l'esercito.

Gli incaricati della sicurezza delle informazioni devono essere indipendenti nella loro posizione e nell'adempimento dei loro compiti e non possono essere esposti ad alcun conflitto di interessi materiale. Nella pratica, la mancanza di una separazione delle

funzioni comporta di continuo problemi nell'esecuzione delle direttive di sicurezza. Oggi, ad esempio, la maggioranza degli incaricati della sicurezza informatica è ancora subordinata ai responsabili dell'informatica. Spesso i responsabili dell'informatica perseguono priorità diverse dalla sicurezza e, in ragione dell'urgenza e/o dei costi, nei progetti si rinuncia periodicamente ad attuare le necessarie misure di sicurezza. Agli incaricati della sicurezza delle informazioni non andrebbe neanche affidato l'esercizio diretto di mezzi informatici, né essi andrebbero impiegati quali responsabili di progetti non riguardanti in primo luogo la sicurezza delle informazioni, poiché proprio in questo accumularsi di compiti gli altri requisiti dell'azienda collidono periodicamente con una valutazione per quanto possibile obiettiva dei rischi. Con questa normativa si tiene conto anche della raccomandazione 7 del rapporto della DelCG sulla sicurezza informatica in seno al SIC (v. n. 1.1.4).

L'esatta collocazione della funzione è affidata alle autorità, ai dipartimenti e alla CaF. La prassi mostra tuttavia che gli incaricati della sicurezza delle informazioni sono più efficaci se vengono collocati relativamente vicino alla direzione dell'autorità perché così possono avere una migliore visione d'insieme dei processi aziendali e valutare le esigenze aziendali. Sarebbe inoltre auspicabile collocare gli incaricati della sicurezza delle informazioni in modo che possano assicurare uno stretto coordinamento con i gestori dei rischi, i consulenti per la protezione dei dati, gli incaricati della sicurezza (sicurezza degli oggetti) e i consulenti in materia di trasparenza già presenti.

Art. 83 Conferenza degli incaricati della sicurezza delle informazioni

In merito al ruolo della Conferenza si rimanda al numero 1.2.9. Oltre alle autorità assoggettate saranno rappresentati anche i dipartimenti, la CaF e i Cantoni. In tal modo sarà possibile assicurare che l'esecuzione della legge sia il più possibile uniforme anche all'interno dell'Amministrazione federale e nel quadro della collaborazione con i Cantoni. La Conferenza comprenderà anche l'IFPDT, al fine di garantire in modo sistematico il necessario coordinamento con la protezione dei dati già al momento dell'allestimento delle direttive. La Conferenza si occuperà in particolare di valutare l'attuabilità, l'efficacia e l'economicità delle misure standardizzate proposte (art. 86). Soltanto così sarà possibile trovare soluzioni unitarie e creare il necessario consenso. Il servizio specializzato della Confederazione per la sicurezza delle informazioni coinvolgerà la Conferenza in tutte le questioni importanti relative alla sicurezza delle informazioni (ad es. nelle questioni riguardanti la strategia in materia di sicurezza delle informazioni). La Conferenza servirà anche a individuare tendenze e rischi e a concepire preventivamente misure appropriate. Per i suoi accertamenti e la formazione di una propria opinione, la Conferenza potrà ricorrere anche a esperti indipendenti.

Art. 84 Servizio specializzato della Confederazione per la sicurezza delle informazioni

In merito al ruolo del servizio specializzato della Confederazione per la sicurezza delle informazioni si rimanda al n. 1.2.9. A livello inter-autorità il servizio specializzato non dispone di poteri decisionali e d'attuazione, poiché simili competenze

violerebbero l'autonomia a livello di esecuzione di cui godono le autorità assoggettate, che va rigorosamente rispettata.

- Lettera a: i servizi menzionati nella legge possono richiedere l'assistenza tecnica del servizio specializzato per tutte le questioni correlate all'esecuzione (compresi i CSP). Il servizio specializzato è quindi considerato un «centro di competenza» per la sicurezza delle informazioni;
- lettera b: in caso di nuovi pericoli e minacce nonché di scoperta di nuovi punti deboli e lacune, l'informazione di tutte le persone interessate avverrà in maniera tempestiva e mirata. Per quanto riguarda le minacce operative in ambito tecnico, MELANI assume questo compito per la propria cerchia di clienti;
- lettera c: gli audit e i controlli spettano in linea di principio alle autorità e alle organizzazioni. In particolare per audit di sicurezza tecnici negli ambiti critici sono tuttavia necessarie elevate conoscenze specialistiche che non tutte le autorità assoggettate dovrebbero procurarsi per sé: approntare un pool di esperti è più economico. Il servizio specializzato non può eseguire spontaneamente simili verifiche, ma unicamente su richiesta di un'autorità. Dopo aver consultato la Conferenza, il servizio specializzato allestirà o adeguerà annualmente un piano strategico dei controlli e lo sottoporrà per approvazione alle autorità competenti. Nel piano saranno indicate le priorità degli audit e, se del caso, le risorse necessarie al riguardo;
- lettera d: in ambito tecnico vengono impiegate regolarmente nuove tecnologie. I rischi correlati all'impiego di nuovi mezzi (hardware e software) sono spesso poco chiari. Per le tecnologie particolarmente importanti o che possono avere un ampio campo d'applicazione, le autorità potranno chiedere al servizio specializzato di eseguire un'analisi dei rischi. La Conferenza verificherà successivamente i risultati;
- lettera e: in questo caso si tratta di una misura operativa volta alla standardizzazione di processi, mezzi, installazioni, oggetti e prestazioni di servizi. In ambito informatico i fornitori di prestazioni sono ad esempio interessati a sapere se le soluzioni tecniche che sviluppano soddisfano i requisiti stabiliti dalla Confederazione. Se ciò è il caso, allora possono impiegarli molto più semplicemente per altri progetti o mezzi informatici. Lo stesso dicasi per oggetti o prestazioni di servizi che servono alla protezione fisica. Anche se i requisiti sono soddisfatti, la responsabilità rimane tuttavia sempre dell'autorità o dell'organizzazione che impiega simili mezzi. Questa competenza è necessaria anche in ambito internazionale: il servizio specializzato assumerà il ruolo (oggi mancante), usuale a livello internazionale, di *National Accreditation Authority* (v. il n. 5.2). Il servizio specializzato potrà in tal modo certificare ufficialmente che i mezzi impiegati soddisfano ad esempio i requisiti dell'UE;
- lettera f: nel caso di progetti trasversali la responsabilità sarà affidata a una determinata autorità o organizzazione. Poiché gli interessi e le esigenze in materia di sicurezza delle autorità e delle organizzazioni interessate sono spesso diversi, occorre garantire che le questioni relative alla sicurezza delle

informazioni siano coordinate in maniera professionale. Il servizio specializzato potrà assumersi questo compito in occasione di progetti importanti che coinvolgono più autorità e hanno un sostanziale rapporto con la sicurezza delle informazioni;

– lettera g: poiché le corrispondenti conoscenze specialistiche vanno raggruppate a livello di Confederazione nel previsto servizio specializzato, quest'ultimo sarà anche l'interlocutore della Confederazione per i servizi svizzeri, esteri e internazionali nell'ambito della sicurezza delle informazioni. Esso assumerà anche i necessari ruoli nell'ambito dei contatti internazionali tra autorità (v. n. 5.2). Altre autorità o organizzazioni (per es. DFAE, SIC o UFCOM) potranno però continuare a intrattenere contatti specialistici in questo settore.
– lettera h: il Consiglio federale deve essere informato regolarmente dello stato della sicurezza delle informazioni in modo tale da consentirgli di valutare la loro efficacia ed economicità e di conseguenza informare gli organi di vigilanza dell'Assemblea federale (v. art. 89 cpv. 2).

Capoversi 2–3: il Consiglio federale impiegherà anche un incaricato per la sicurezza delle informazioni. Per evitare eventuali conflitti di competenza, questa persona sarà contemporaneamente capo del servizio specializzato. Il Consiglio federale stabilirà inoltre quali compiti il servizio specializzato deve esercitare autonomamente o in collaborazione con altri servizi federali. Dovrà ovviamente decidere anche sulla questione della sua collocazione. Il Consiglio federale deciderà infine se intenderà assegnare al servizio specializzato compiti supplementari o poteri di attuazione per l'Amministrazione federale e l'esercito.

Sezione 2: Esecuzione

Art. 85 Disposizioni esecutive

In merito all'esecuzione si rimanda anche al numero 1.2.8. Le autorità non sono assoggettate alle disposizioni esecutive del Consiglio federale. Devono però emanare per il proprio ambito le disposizioni necessarie per l'esecuzione. Il secondo periodo del capoverso 1 disciplina il rapporto con l'articolo 15 capoverso 2 LOGA. Il capoverso 2, in relazione con l'articolo 70 LParl, provvede a una chiara competenza esecutiva in seno all'Assemblea federale. Nel capoverso 3 viene stabilito il cosiddetto *opting out*. Le disposizioni esecutive sono preparate in collaborazione con la Conferenza degli incaricati della sicurezza delle informazioni. Il Consiglio federale consulta inoltre le altre autorità e i Cantoni prima di emanare le sue disposizioni esecutive.

Art. 86 Requisiti e misure standardizzati

Uno degli obiettivi principali della presente legge è conseguire standard di sicurezza il più possibile uniformi per tutte le autorità: il Consiglio federale è pertanto incaricato di stabilire, secondo lo stato della scienza e della tecnica, requisiti e misure

standardizzati. Non si tratta di requisiti e misure organizzative fondamentali stabilite a livello di ordinanza, bensì, in primo luogo, di requisiti di natura tecnica o di carattere secondario, ad esempio:

- standard per rilevare le necessità di protezione di informazioni in relazione ai quattro criteri dell'articolo 6 capoverso 2;
- metodo standard per valutare i rischi nonché standard per misure organizzative, in materia di personale, tecniche ed edili (art. 8);
- standard per determinati processi e mezzi volti a proteggere informazioni classificate (art. 11–15);
- standard per la protezione di base, per l'allestimento di piani in materia di sicurezza delle informazioni e per la sicurezza di mezzi informatici dei livelli di sicurezza «protezione elevata» e «protezione molto elevata» (art. 16–19).

Molti altri Paesi e organizzazioni internazionali hanno già stabilito standard per il loro ambito. Le autorità federali non dovranno quindi reinventare la ruota. In questo contesto è anche importante che la Svizzera partecipi attivamente a simili processi di standardizzazione.

Se necessario, il Consiglio federale potrà delegare a servizi subordinati l'elaborazione e l'adozione degli standard per non essere gravato del compito di stabilire misure di sicurezza di livello tecnico-operativo. Poiché le misure di sicurezza devono per principio essere decise dalla linea gerarchica, una soluzione particolarmente adeguata potrebbe consistere in una delega alla Conferenza dei segretari generali (art. 53 LOGA). Il compito potrebbe inoltre essere delegato anche al servizio specializzato della Confederazione per la sicurezza delle informazioni o a fedpol nell'ambito della protezione degli oggetti. I fornitori di prestazioni della Confederazione dovrebbero, parimenti, poter elaborare standard di sicurezza tecnici ed eventualmente, ai fini della standardizzazione, farli esaminare dal servizio specializzato quanto alla loro idoneità per la Confederazione (v. art. 84 cpv. 1 lett. e). Una simile delega da parte del Consiglio federale non deve però avvenire in modo globale. Determinate misure tecniche possono comportare notevoli conseguenze finanziarie che non dovrebbero essere decise da servizi subordinati. Anche nel caso di un'eventuale delega, il Consiglio federale deve dunque garantire che deciderà esso stesso le misure di ampia portata e più costose.

Gli standard non sono vincolanti per le altre autorità assoggettate, poiché sono stati stabiliti dal Consiglio federale. In considerazione del fatto che la Conferenza parteciperà in modo determinante all'elaborazione degli standard, il semplice carattere di raccomandazione degli standard nella prassi non dovrebbe impedire l'applicazione delle stesse da parte delle altre autorità e dei Cantoni.

Art. 87 Cantoni

In merito alla collaborazione tra Confederazione e Cantoni si rimanda al numero 1.2.2. Secondo l'articolo 3 i Cantoni sono tenuti a garantire una protezione equivalente quando trattano informazioni classificate della Confederazione o accedono a mezzi informatici appartenenti a quest'ultima. Devono di conseguenza garantire che

le proprie misure siano effettivamente appropriate per raggiungere il necessario livello di sicurezza. La portata di questa verifica è limitata alla sicurezza del trattamento di informazioni classificate e all'accesso a mezzi informatici della Confederazione. I Cantoni stessi sono competenti per detti controlli. Tuttavia si richiede loro di informare il servizio specializzato della Confederazione per la sicurezza delle informazioni in merito ai risultati delle loro verifiche. Occorre inoltre garantire che lo scambio di informazioni tra i Cantoni e la Confederazione avvenga in modo sistematico ed efficiente e che l'applicazione delle misure secondo la presente legge avvenga in modo coordinato. Dai Cantoni non ci si aspetta che si riorganizzino o che creino nuove strutture. Collaboreranno inoltre direttamente all'elaborazione degli atti esecutivi relativi alla legge nonché degli standard di cui all'articolo 86.

Nonostante i Cantoni siano direttamente competenti per la sicurezza delle proprie informazioni, la Confederazione dispone di particolari strumenti e capacità ai quali i Cantoni possono ricorrere per le proprie necessità. Lo sviluppo di corrispondenti strumenti e capacità a livello cantonale non sarebbe sensato dal profilo economico. Ciò riguarda in particolare i CSP. Gli impiegati dei Cantoni che svolgono attività sensibili sotto il profilo della sicurezza sono sottoposti a un controllo di sicurezza relativo alle persone sulla base dell'articolo 30 capoverso 1 lettera b. I relativi costi continueranno a essere assunti dalla Confederazione. La procedura di sicurezza relativa alle aziende nonché le previste capacità di svolgere audit del servizio specializzato della Confederazione per la sicurezza delle informazioni suscitano a loro volta interesse nei Cantoni. Il Consiglio federale sarà perciò autorizzato a stabilire, in collaborazione con i Cantoni, in quale misura e a quali risorse della Confederazione possono far ricorso i Cantoni. Se i Cantoni ricorrono alle prestazioni della Confederazione per le proprie necessità, saranno tenuti a rimborsare alla Confederazione le relative spese.

Art. 88 Trattati internazionali

I trattati internazionali nel campo della sicurezza delle informazioni contengono prevalentemente normative tecniche sul riconoscimento reciproco di prescrizioni e procedure nazionali (p. es. la procedura CSP e la PSA), elenchi di concordanza sull'applicazione di classificazioni, standard di sicurezza nell'ambito dell'informatica o della sicurezza delle comunicazioni nonché normative sull'esecuzione di controlli reciproci. Per proteggere informazioni messe a disposizione della Confederazione da altri Stati o organizzazioni internazionali, può inoltre essere necessario adottare trattati che in singoli punti (p. es. presupposti per la classificazione, per l'accesso a informazioni classificate o il trattamento di informazioni classificate o per il rilascio delle dichiarazioni di sicurezza) derogano alle prescrizioni legali. In simili casi, il fornitore delle informazioni può chiedere di convenire con le autorità federali riceventi una più o meno rigida protezione delle sue informazioni. Per motivi di economia amministrativa, il Consiglio federale sarà autorizzato a concludere direttamente simili trattati in materia di sicurezza delle informazioni.

L'interconnessione e la collaborazione crescenti sul piano internazionale sono necessarie per minimizzare i rischi connessi alla sicurezza delle informazioni. L'applicazione della SNPC richiede perciò che vengano rafforzati gli scambi per quanto riguarda le esperienze, i lavori di ricerca e sviluppo, le informazioni riferite a inci-

denti, le attività di formazione e le esercitazioni (v. anche il n. 1.1.2). Il Consiglio federale sarà perciò autorizzato anche a concludere trattati internazionali per lo scambio di informazioni su pericoli, punti deboli e incidenti, in particolare per quanto riguarda le infrastrutture critiche. Si tratta soprattutto di questioni organizzative e tecniche secondarie (p. es. collaborazione con altri CERT statali, v. art. 78).

Art. 89 Valutazione

Cinque anni dopo l'entrata in vigore della legge avrà luogo una valutazione. I rapporti periodici (a ritmo annuale) si fonderanno sui rapporti allestiti dal servizio specializzato della Confederazione (vedi art. 84 cpv. 1 lett. h). L'Assemblea federale dovrà designare la commissione incaricata di trattare i rapporti del Consiglio federale.

Capitolo 7: Disposizioni finali

Art. 90 *Modifica di altri atti normativi*

Si rimanda al numero 2.3.

Art. 91 Disposizioni transitorie

Il passaggio al nuovo diritto deve essere strutturato in maniera tale che avvenga nel modo più economico possibile e secondo le priorità. Sarebbe infatti sproporzionato esigere che la classificazione di tutte le informazioni sia verificata entro una determinata scadenza. Questo vale anche in ambito informatico: un adeguamento immediato di tutti i sistemi alle nuove prescrizioni sarebbe certamente da raccomandare per ragioni di sicurezza. L'onere finanziario e di personale correlato sarebbe tuttavia assolutamente sproporzionato. Per tale motivo la legge stabilisce che in un primo momento è necessaria l'attribuzione di ogni mezzo informatico a un determinato livello di sicurezza. Questa misura deve essere attuata entro due anni per consentire la rapida identificazione dei mezzi informatici della massima criticità. L'ammodernamento dei mezzi informatici è spesso oneroso e nettamente più caro che non l'implementazione della sicurezza fatta sin dall'inizio. Se l'onere per il miglioramento di un sistema è sproporzionato rispetto alla sicurezza delle informazioni richiesta, i rischi devono essere indicati e sostenuti in maniera trasparente. Altri quattro anni sono sufficienti per effettuare, se del caso, gli adeguamenti necessari ai sistemi stessi o agli esistenti piani per la sicurezza dell'informazione e la protezione dei dati, ma i sistemi della massima criticità vanno trattati per primi. La premessa per questi adeguamenti è l'esistenza degli standard secondo l'articolo 86, che di conseguenza vanno stabiliti per primi.

La regolamentazione transitoria per i CSP e la PSA è finalizzata in primo luogo alla trasparenza nei confronti di persone e aziende in possesso di una corrispondente dichiarazione nonché, in secondo luogo, a un passaggio ordinato e commisurato ai rischi al nuovo diritto. La durata di validità delle dichiarazioni di sicurezza aziendale è già attualmente di cinque anni. La situazione è leggermente più complicata

nell'ambito dei CSP poiché le dichiarazioni non hanno un termine di scadenza formale (il controllo è semplicemente ripetuto dopo un determinato periodo). La regolamentazione proposta offre continuità sia ai servizi promotori sia ai servizi specializzati CSP. Inoltre concede al Consiglio federale un margine di manovra sufficiente per sottoporre a un nuovo controllo dapprima le funzioni della massima criticità.

2.2 Coordinamento con altri atti normativi

Il presente disegno di legge deve essere coordinato con i seguenti disegni di legge pendenti:

Legge federale sulle attività informative

Se l'entrata in vigore della LAIn è antecedente a quella della presente legge, al momento dell'entrata in vigore della presente legge l'articolo 51 capoverso 4 LAIn deve essere modificato secondo la presente legge.

Se l'entrata in vigore della LAIn è successiva a quella della presente legge, la modifica dell'articolo 51 capoverso 4 LAIn secondo la presente legge entra in vigore solo in quel momento.

Indipendentemente dal fatto che entri prima in vigore la LAIn o la presente legge, alla seconda di queste entrate in vigore o in caso di entrata in vigore simultanea delle due modifiche, l'articolo 367 capoversi 2 lettera i, 2bis lettera b nonché 4 del Codice penale avrà il seguente tenore:

Art. 367 cpv. 2 lett. i, 2bis lett. b e 4

2 Le autorità seguenti possono, mediante procedura di richiamo, accedere ai dati personali concernenti le sentenze di cui all'articolo 366 capoversi 1, 2 e 3 lettere a e b:

i. i servizi specializzati di cui all'articolo 32 capoverso 2 LSIn[30] (servizi specializzati CSP) competenti per l'esecuzione dei controlli di sicurezza relativi alle persone;

2bis Le autorità seguenti possono, mediante procedura di richiamo, accedere anche ai dati personali concernenti le sentenze di cui all'articolo 366 capoverso 3 lettera c:

b. i servizi specializzati CSP;

4 I dati personali concernenti procedimenti penali pendenti possono essere trattati soltanto dalle autorità di cui al capoverso 2 lettere a–e, i, j, l e m.

30 RS …; FF **2017** 2563 2711

Legge sul casellario giudiziale

Se l'entrata in vigore della legge sul casellario giudiziale (LCaGi) è antecedente a quella della presente legge, decadono le modifiche dell'articolo 365 capoverso 2 lettera d nonché articolo 367 capoversi 2 lettera i, 2bis lettera b nonché capoverso 4 del Codice penale previste dalla presente legge. Per contro, con l'entrata in vigore della presente legge l'articolo 46 capoverso 6 lettera a LSIn nonché l'articolo 46 lettera e e l'articolo 51 lettera f LCaGi sono modificati come segue:

Art. 46 cpv. 6 lett. a LSIn

6 I dati secondo il capoverso 4 possono essere acquisiti automaticamente e sistematicamente mediante interrogazione dei seguenti sistemi d'informazione:

a. casellario giudiziale informatizzato VOSTRA conformemente alla legge del 17 giugno 2016[31] sul casellario giudiziale;

Art. 46 cpv. e LCaGi

Le seguenti autorità collegate possono consultare mediante procedura di richiamo tutti i dati figuranti nell'estratto 2 per autorità (art. 38), nella misura necessaria per adempiere i compiti elencati qui appresso:

e.	i servizi specializzati per i controlli di sicurezza relativi alle persone di cui all'articolo 32 capoverso 2 della legge del …[32] sulla sicurezza delle informazioni (LSIn):	1. per la valutazione del rischio nel quadro dei controlli di sicurezza relativi alle persone secondo la LSIn, 2. per valutazioni del potenziale di pericolo o di abuso secondo la legge militare del 3 febbraio 1995[33], 3. per ulteriori valutazioni del rischio nel quadro delle verifiche previste dalla legislazione speciale;

Art. 51 lett. f LCaGi

Abrogato

Se l'entrata in vigore della legge sul casellario giudiziale è successiva alla presente legge, l'articolo 46 capoverso 6 lettera a LSIn nonché l'articolo 46 lettera e e l'articolo 51 lettera f LCaGi devono essere modificati secondo il tenore di cui sopra. Per contro, decade la modifica dell'articolo 20*a* LPers prevista dalla legge sul casellario giudiziale; ciò significa che la modifica dell'articolo 20*a* LPers prevista dalla presente legge rimane in vigore.

31 RS …; FF **2016** 4315
32 RS …; FF **2017** 2563 2711
33 RS **510.10**

Legge federale sull'energia

Se l'entrata in vigore della legge federale sull'energia è antecedente a quella della presente legge, con l'entrata in vigore della presente legge l'articolo 20a LAEl riceve il tenore secondo la presente legge.

Se l'entrata in vigore della legge federale sull'energia è successiva a quella della presente legge, decade la modifica dell'articolo 20a LAEl prevista dalla legge federale sull'energia; ciò significa che la modifica dell'articolo 20a LAEl prevista dalla presente legge rimane in vigore.

2.3 Modifica di altri atti normativi

Legge federale sulle misure per la salvaguardia della sicurezza interna

Art. 2 cpv. 4 lett. c nonché art. 19–21

Il CSP sarà disciplinato principalmente nella LSIn. Le corrispondenti disposizioni della LMSI devono pertanto essere abrogate.

Art. 24a cpv. 7, primo periodo

Per la valutazione dei rischi per la sicurezza nell'ambito di un CSP secondo la LSIn, per una verifica dell'affidabilità in virtù della legislazione speciale nonché per la valutazione del potenziale di violenza ai sensi dell'articolo 113 LM i servizi specializzati CSP devono avere accesso ai dati della banca dati sulla tifoseria violenta di fedpol.

Legge sulle attività informative

Art. 51 cpv. 4 lett. d

I servizi specializzati CSP possono acquisire dati presso il SIC (art. 35 cpv. 1 lett. c). INDEX SIC serve ad accertare se il SIC tratta dati concernenti una determinata persona, un'organizzazione, un oggetto o un evento. In tale sistema sono consultabili tutte le persone registrate in IASA SIC e IASA-GEX SIC (vedi art. 49 e 50 LAIn). In pratica, nell'INDEX SIC vengono inseriti i principali dati di identificazione, per le persone ad esempio il nome, la data di nascita, la nazionalità ecc. INDEX SIC serve dunque a coordinare le attività di intelligence di Confederazione e Cantoni, ma è volto anche al coordinamento tra attività in ambito di intelligence e attività in materia di polizia di sicurezza e giudiziaria. I servizi specializzati CSP sono autorizzati ad accedere soltanto ai dati di identificazione e non al resto delle informazioni. Se una determinata persona è registrata nell'INDEX SIC, il servizio specializzato CSP competente deve chiedere al SIC di fornirgli i dati necessari (v. art. 46 cpv. 6 LSIn nonché art. 49 segg. LAIn).

Legge sul personale federale

Art. 20a

L'innalzamento della soglia per l'esecuzione di CSP secondo la LSIn ha lo scopo di fare in modo che questa misura sia impiegata solo per le attività che presentano effettivamente una maggiore sensibilità sotto il profilo della sicurezza. Esiste comunque il rischio che nella prassi la soglia per i CSP venga abbassata o che le esigenze per un CSP vengano ridotte, qualora le autorità e organizzazioni assoggettate alla LSIn non abbiano a disposizione alcun altro strumento per verificare l'affidabilità di candidati e impiegati. Il nuovo articolo 20*a* LPers intende offrire ai datori di lavoro strumenti adeguati. Essi devono poter avere la possibilità di esigere dai candidati e dagli impiegati la presentazione di un estratto del casellario giudiziale e del registro delle esecuzioni. Tale richiesta non dovrebbe tuttavia essere sistematica, ma essere limitata ai soli casi in cui ciò sia necessario per la tutela degli interessi del datore di lavoro. Il Consiglio federale emanerà le relative disposizioni d'esecuzione.

Art. 20b

I CSP secondo la LSIn possono essere eseguiti unicamente per individuare rischi considerevoli in materia di sicurezza delle informazioni. Nel settore di compiti delle autorità federali vi sono tuttavia ulteriori attività nel cui quadro interessi importanti della Confederazione possono essere considerevolmente pregiudicati anche se non vi è un rapporto diretto con la sicurezza delle informazioni. Le persone che svolgono questo genere di attività devono essere sottoposte a una verifica dell'affidabilità. Con l'introduzione di una nuova disposizione sulla verifica dell'affidabilità nell'articolo 20*b* LPers, si intende coprire un fabbisogno di verifica individuato per determinati impiegati della Confederazione.

- Si tratta in primo luogo del personale diplomatico e consolare del DFAE. Si può però anche trattare del personale di altri dipartimenti che assume funzioni simili (ad es. presso la SECO.
- La verifica può essere applicata a direttori di uffici, ma anche ad esempio a impiegati con competenze decisionali nell'aggiudicazione di mandati importanti o persone che svolgono compiti particolarmente sensibili in relazione alle finanze pubbliche.

La disposizione non contempla tutti i datori di lavoro ai sensi dell'articolo 3 LPers. Non è ad esempio menzionata l'autorità di vigilanza sul Ministero pubblico della Confederazione, poiché nessun impiegato dell'autorità di vigilanza adempie le condizioni dell'articolo 20*b* capoverso 1 LPers. Per le unità amministrative decentralizzate e i tribunali della Confederazione, il Consiglio federale, dopo aver consultato le organizzazioni interessate, deciderà a livello di ordinanza se e in quale misura il loro personale possa essere sottoposto a una verifica dell'affidabilità (v. rinvio alla competenza del Consiglio federale nell'art. 3 cpv. 3 e 3 LPers). Inoltre, la verifica è ordinata soltanto in caso di bisogno comprovato, vale a dire se vi è la possibilità di un danno considerevole. La presente disposizione non deve servire ad aggirare la riduzione richiesta dal Consiglio federale del numero di CSP eseguiti. Non è ragionevole introdurre una procedura particolare o istituire altri servizi specializzati per la verifica dell'affidabilità, dato che le questioni da chiarire sono in linea di principio

analoghe a quelle della sicurezza delle informazioni. Per la verifica sarà pertanto ripresa la regolamentazione della LSIn. La procedura sarà ripresa in particolare per quanto riguarda l'applicazione del principio del consenso della persona interessata, dei principi inerenti all'acquisizione dei dati, degli elenchi delle funzioni, dei livelli di controllo e delle normative sulle conseguenze della valutazione. Gli elenchi delle funzioni necessari per questa verifica saranno allestiti e aggiornati dal servizio specializzato della Confederazione per la sicurezza delle informazioni in collaborazione con l'UFPER (per l'Amministrazione federale) e con i servizi competenti delle altre autorità federali.

Codice di procedura civile

Per la modifica dell'articolo 166 capoverso 1 del Codice di procedura civile si rimanda al commento all'articolo 320 numero 1 CP.

Legge di procedura civile federale

Per la modifica dell'articolo 42 capoverso 3 della legge di procedura civile federale si rimanda al commento all'articolo 320 numero 1 CP.

Codice penale

Art. 320 n. 1

Al giorno d'oggi, in molti settori delle tecnologie dell'informazione e della comunicazione (TIC), l'*outsourcing* non è soltanto un fenomeno abituale e generalizzato ma anche necessario perché ricorrere al *know-how* specializzato dei produttori di hardware e software è spesso indispensabile. Nell'ambito delle TIC anche la Confederazione e i Cantoni ricorrono a numerosi fornitori esterni di prestazioni (v. al riguardo l'art. 10*a* LPD). Nelle banche dati sono frequentemente memorizzate quantità difficili da determinare di informazioni diverse protette da segreto. Anche se il principio della minimizzazione dei dati e altre misure tecniche e organizzative (anonimizzazione dei dati, controllo dei collaboratori ecc.) sono rispettati, le persone incaricate di compiti tecnici ricevono (spesso inevitabilmente) *accesso a informazioni protette dal segreto d'ufficio*.

L'*articolo 320 CP* non obbliga *gli ausiliari esterni* che forniscono prestazioni all'Amministrazione *nel settore TIC* (p. es. manutenzione di banche dati) a osservare il segreto d'ufficio per quanto concerne le informazioni di cui vengono a conoscenza svolgendo la loro attività. Essenzialmente questi collaboratori TIC esterni all'Amministrazione non soddisfano *i requisiti della nozione materiale di funzionario* secondo l'articolo 110 capoverso 3 CP[34] e quindi non sono compresi nella cerchia dei possi-

34 Weber Rolf H., Outsourcing von Informatik-Dienstleistungen in der Verwaltung, in: Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht, 100. Jahrgang (1999), pag. 97 segg., n. 2.2.1. Cfr. anche (e contrario) DTF **135** IV 198, consid. 3.3.

bili autori del reato previsto nell'*articolo 320 numero 1 CP* (reato speciale)[35]. Il diritto penale entra in linea di conto soltanto se gli ausiliari esterni partecipano in qualità di complici o istigatori al reato speciale del funzionario o trasmettono le informazioni commettendo così un altro reato; si può trattare di atti compiuti senza autorizzazione per uno Stato terzo (art. 271 CP) o di spionaggio politico o economico (art. 272 o 273 CP). Diversamente dalla tutela del segreto professionale secondo l'articolo 321 CP, che comprende anche gli ausiliari del detentore del segreto, *nell'ambito dei segreti d'ufficio* sussiste quindi una *lacuna nella tutela e nella punibilità* che riguarda i soli ausiliari esterni.

Secondo l'*articolo 320 numero 2 CP* la rivelazione di segreti d'ufficio[36] non è punibile se è fatta col *consenso* scritto dell'autorità superiore. Poiché l'articolo 320 non concerne soltanto i *segreti di servizio* ma anche i *segreti privati*[37] (p. es. i dati sanitari di un incarto personale o i segreti di fabbricazione o di affari nelle gare d'appalto pubbliche), prima di fornire il proprio consenso l'autorità competente deve eseguire un'attenta ponderazione degli interessi toccati dalla rivelazione. A seconda del genere e dell'importanza dell'interesse a conservare il segreto in questione l'autorità acconsente o rifiuta il consenso[38]. Se l'interesse a mantenere il segreto non ha natura almeno in parte pubblica, ma è di natura esclusivamente privata, il consenso dell'autorità superiore secondo l'articolo 320 numero 2 CP non costituisce in via di principio un motivo giustificativo[39]. Nell'ambito delle TIC vi sono motivi pratici (numero indeterminato di detentori o titolari del segreto) che impediscono di ottenere i consensi necessari, ad esempio se occorre fare immediatamente ricorso al supporto tecnico esterno dopo il crash di una banca dati. Tuttavia, in assenza di un consenso valido, i collaboratori interni dell'Amministrazione sono punibili se permettono a fornitori esterni di prestazioni di accedere a segreti d'ufficio. *De lege lata*, vi è dunque anche un pericolo di *potenziale punibilità* dei collaboratori interni dell'Amministrazione.

35 Oberholzer Niklaus in: Niggli/Wiprächtiger (a c. di.), Basler Kommentar Strafrecht I, Basilea 2013, Art. 110 Abs. 3 N 13 segg. Ricca casistica in Trechsel Stefan/Vest Hans in Trechsel/Pieth (a c. di.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurigo/San Gallo 2013, Art. 110 Abs. 3 N 13.

36 È sufficiente concedere una possibilità di prendere conoscenza del segreto, cfr. Oberholzer Niklaus in: Niggli/Wiprächtiger (a c. di), Basler Kommentar Strafrecht II, Basilea 2013, Art. 320 N 10.

37 Oberholzer Niklaus in: Niggli/Wiprächtiger (a c. di), Basler Kommentar Strafrecht II, Basilea 2013, Art. 320 N 3 e 8.

38 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (a c. di), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurigo/San Gallo 2013, Art. 320 N 11. Sull'analoga struttura del consenso dell'autorità superiore in materia di segreto professionale cfr. Stratenwerth Günter/Bommer Felix, Schweizerisches Strafrecht Besonderer Teil II, Berna 2013, § 61 N 23. Quanto al corrispettivo processuale della norma penale materiale cfr. art. 170 cpv. 3 CPP, e in proposito cfr. Donatsch Andreas in: Donatsch/Hansjakob/Lieber (a c. di), Kommentar zur Schweizerischen Strafprozessordnung, Zurigo ecc. 2014, Art. 170 N 14. Per una ponderazione speculare degli interessi nel diritto di accesso ai documenti ufficiali cfr. art. 7 (in particolare cpv. 3) della legge federale del 17 dicembre 2004 sul principio di trasparenza dell'amministrazione (LTras; RS **152.3**).

39 Sulla portata del consenso cfr. Stratenwerth Günter, Schweizerisches Strafrecht Allgemeiner Teil I, Berna 2011, § 10 N 5, 13 e Stratenwerth Günter/Bommer Felix, Schweizerisches Strafrecht Besonderer Teil II, Berna 2013, § 61 N 10 seg.

Il nostro Consiglio ritiene che il legislatore debba risolvere rapidamente questi problemi. Rinuncia tuttavia a estendere per legge ai segreti di natura puramente privata la necessità del *consenso* dell'autorità superiore. Anche in un tal caso, come nel diritto vigente, l'obbligo dei fornitori esterni di prestazioni di mantenere il segreto d'ufficio potrebbe essere garantito solo in modo indiretto per via contrattuale (mediante pene convenzionali). Inoltre, la situazione giuridica dei privati verrebbe tendenzialmente indebolita. Non pare nemmeno appropriato estendere la *definizione legale* della nozione di funzionario secondo l'articolo 110 capoverso 3 CP, poiché ciò avrebbe ripercussioni su tutti i reati contro i doveri d'ufficio. Gli ausiliari esterni che non soddisfano la definizione materiale di funzionari non svolgono alcuna funzione al servizio del pubblico né sono identificati all'esterno come rappresentanti dell'Amministrazione. Non devono pertanto poter essere chiamati a rispondere in generale di tutti i reati contro i doveri d'ufficio.

Il nostro Consiglio preferisce *estendere la cerchia degli autori del reato punito dall'articolo 320 capoverso 1 CP* agli ausiliari, *rafforzando* di conseguenza *la tutela del segreto d'ufficio*. Appare opportuno che il diritto penale obblighi anche gli ausiliari a mantenere il segreto d'ufficio (art. 321 CP), non da ultimo in considerazione della vigente normativa sul segreto professionale[40]. È così possibile eliminare anche il pericolo della potenziale punibilità dei collaboratori interni nel caso in cui, per motivi di servizio, permettono ad ausiliari esterni di accedere a segreti d'ufficio senza aver ottenuto l'apposito consenso.

Se un ausiliario esterno va liberato dal segreto d'ufficio secondo l'articolo 320 numero 2 CP, l'autorità superiore del mandante interno all'Amministrazione deve acconsentire per scritto. La situazione è quindi paragonabile a quella degli ausiliari del detentore del segreto professionale secondo l'articolo 321 CP. Soltanto l'autorità amministrativa superiore può tenere conto dei criteri decisivi per compiere adeguatamente la ponderazione degli interessi necessaria al consenso.

Le precedenti considerazioni valgono per analogia per la violazione del segreto di servizio secondo l'*articolo 77 PPM*. In conseguenza della modifica del diritto materiale, deve essere ampliata anche la cerchia delle persone con *facoltà di non deporre in base al segreto d'ufficio* negli articoli 170 CPP, 77 PPM, 166 del *Codice di procedura civile*[41] e 42 della *legge di procedura civile federale*[42] (in virtù del rimando dell'articolo 16 capoverso 1 PA).

Art. 365 cpv. 2 lett. d

Poiché i CPS non saranno più disciplinati nella LMSI bensì nella LSIn, le disposizioni riguardanti i servizi che beneficiano dell'autorizzazione di accesso nonché lo scopo dell'acquisizione dei dati devono essere adeguati.

40 Sugli ausiliari del detentore del segreto professionale cfr. Oberholzer Niklaus in: Niggli/Wiprächtiger (a c. di), Basler Kommentar Strafrecht II, Basilea 2013, Art. 321 N 10.
41 RS **272**
42 RS **273**

Art. 367 cpv. 2 lett. i, 2bis lett. b e 4

Per i capoversi 2 e 2bis, vedi il commento all'articolo 365 capoverso 2 lettera d. Benché non siano compresi nell'elenco di cui all'articolo 367 capoverso 4 CP, conformemente alla prassi attuale i servizi specializzati CSP hanno accesso anche a dati concernenti procedimenti penali pendenti. Come già esposto nel messaggio concernente la legge sul casellario giudiziale[43], ciò è dovuto a «una svista normativa che occorre rettificare poiché l'articolo 20 capoverso 2 lettera d LMSI autorizza già attualmente» i suddetti servizi specializzati «a chiedere informazioni sui procedimenti penali in corso alle competenti autorità di perseguimento penale. Sono però in grado di chiedere tali informazioni soltanto se possono sapere che un procedimento penale è pendente, ossia consultando VOSTRA». Per questa ragione si impone un aggiornamento dell'articolo 367 capoverso 4 CP (mediante l'aggiunta della lett. i).

Codice di procedura penale

Per la modifica dell'articolo 170 capoverso 1 CPP si rimanda al commento all'articolo 320 numero 1 CP.

Codice penale militare

Per la modifica dell'articolo 177 capoverso 1 CPM si rimanda al commento all'articolo 320 numero 1 CP.

Procedura penale militare

Per la modifica dell'articolo 77 capoverso 1 PPM si rimanda al commento all'articolo 320 numero 1 CP.

Legge federale sui sistemi d'informazione di polizia della Confederazione

Art. 15 cpv. 4 lett. f e art. 17 cpv. 4 lett. l

Contrariamente al passato, i servizi specializzati CSP avranno accesso unicamente al registro nazionale di polizia (v. art. 46 cpv. 6 LSIn). La disposizione che consente l'accesso al sistema RIPOL (art. 15 LSIP) può essere abrogata.

43 FF **2014** 4929, in particolare pag. 5025

Legge militare

Art. 14

Secondo l'articolo 20*b* LPers proposto, la LSIn prevede che nel quadro delle sue disposizioni d'esecuzione relative alla LM il Consiglio federale possa assoggettare a una verifica dell'affidabilità due settori di compiti:

- alla lettera a si tratta soprattutto di militari che rappresentano la Svizzera in occasione di impieghi all'estero o che adempiono compiti nel settore della diplomazia militare;
- la lettera b riguarda soltanto i militari che nel quadro del loro obbligo di prestare servizio potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione.

La presente disposizione non deve servire ad aggirare la riduzione richiesta dal Consiglio federale del numero di CSP eseguiti. Nella prassi dovrebbe quindi trovare applicazione soltanto a titolo eccezionale.

Art. 113 cpv. 6

Si tratta di una modifica formale del capoverso 6, il quale deve ora rinviare alla presente legge e non alla LMSI.

Art. 150 cpv. 4

La competenza di concludere trattati internazionali destinati a garantire la tutela del segreto militare è ora contemplata dall'articolo 88 LSIn.

Legge federale sui sistemi d'informazione militari

Art. 14 cpv. 1 lett. i

In seguito all'introduzione della verifica dell'affidabilità secondo l'articolo 14 LM deve essere creata una base legale per il trattamento dei risultati delle verifiche nel sistema PISA. Nel PISA dovranno essere trattati esclusivamente il risultato e la data della verifica nonché la relativa decisione.

Capitolo 5, sezioni 1 e 2 (art. 144–155)

I sistemi d'informazione per il CSP e la procedura di sicurezza relativa alle aziende sono ora disciplinati nella LSIn.

Legge federale sull'energia nucleare

Art. 5 cpv. 3 e cpv. 3bis

Già oggi il vigente articolo 5 capoverso 3 LENu prevede che i provvedimenti di sicurezza debbano essere classificati nella misura del necessario. La modifica intende garantire che la classificazione di questi provvedimenti e il trattamento delle corrispondenti informazioni classificate si orienti alla LSIn.

Legge sull'approvvigionamento elettrico

Art. 20a

Nel nostro messaggio del 4 settembre 2013[44] concernente il primo pacchetto di misure della Strategia energetica 2050 (Revisione del diritto in materia di energia) e l'iniziativa popolare «Per un abbandono pianificato dell'energia nucleare (Iniziativa per l'abbandono del nucleare)» abbiamo proposto l'introduzione di un CSP per determinati impiegati della società nazionale di rete. La presente modifica ha unicamente l'obiettivo di adeguare questa proposta alla terminologia e alla sistematica della LSIn.

Legge sulla banca nazionale

Art. 16, rubrica e cpv. 5

In virtù dei suoi compiti di politica monetaria la Banca nazionale va considerata come un'autorità assoggettata.

3 Ripercussioni

3.1 Ripercussioni per la Confederazione

La Confederazione investe ogni anno complessivamente più di 800 milioni di franchi per il proprio settore informatico. Con l'evoluzione in atto verso una società dell'informazione, i pericoli che incombono sulle informazioni e sui mezzi informatici sono diventati sempre più complessi e dinamici. Di conseguenza, l'entità dei danni che possono essere provocati dall'interruzione o dai disturbi dei mezzi informatici oppure dal furto o dall'utilizzazione abusiva di informazioni è aumentata. La sicurezza delle informazioni ha lo scopo di ridurre in modo possibilmente efficace ed economico la probabilità che subentri un danno simile, anche finanziario, come pure le eventuali ripercussioni di tale danno. La legge e le sue disposizioni d'esecuzione comporteranno un miglioramento duraturo della sicurezza delle informazioni in seno alla Confederazione. La LSIn disciplina principalmente la gestione della sicurezza delle informazioni aumentandone l'efficienza. Per esperienza, una gestione efficiente migliora la sicurezza in modo più efficace, economico e duraturo rispetto a puri investimenti in misure tecniche. Inoltre, la prassi ha mostrato che un'ottimizzazione della gestione della sicurezza delle informazioni – in particolare quando quest'ultima è fondata su una gestione dei rischi efficace – può, a medio termine, contribuire a risparmi sui costi.

Il disegno prevede anche diverse misure organizzative che, rispetto a oggi, oltre a una migliore protezione, comporteranno risparmi in termini di costi, sempre che vengano attuate coerentemente. L'innalzamento della soglia per la classificazione, per esempio, dovrebbe ridurre il numero di informazioni classificate e quindi il

44 FF **2013** 6489

relativo onere. Per quanto riguarda i CSP, i criteri di assoggettamento saranno resi più severi e nel contempo sarà ridotto il numero di attività per il cui esercizio è necessario e ammesso un CSP. In futuro i CSP dovrebbero pertanto diminuire sensibilmente. Inoltre, la standardizzazione, il miglioramento dello scambio di informazioni tra autorità federali e il sostegno a tali autorità da parte del servizio specializzato della Confederazione per la sicurezza delle informazioni contribuiranno a fare in modo che non si debba «reinventare la ruota» in occasione di ogni progetto. Infine, la nuova regolamentazione agevolerà la cooperazione internazionale nel settore della sicurezza e migliorerà la protezione dei dati in seno alla Confederazione.

Di conseguenza, vanno sempre ponderate, da un lato, le ripercussioni finanziarie e in materia di personale del disegno e, dall'altro, la corrispondente riduzione dei rischi menzionati nonché degli oneri.

3.1.1 Ripercussioni finanziarie

Le ripercussioni finanziarie della legge dipendono quasi integralmente dal livello di sicurezza che le autorità intendono raggiungere (art. 7 cpv. 2) e di conseguenza potranno essere valutate soltanto durante l'elaborazione del diritto d'esecuzione. La legge in sé ha scarso influsso su questi costi.

I costi della nuova organizzazione secondo lo stato della scienza e della tecnica (art. 7 cpv. 1) variano fortemente a dipendenza del modello di organizzazione. La decisione sul modello di organizzazione sarà presa dalle autorità assoggettate sulla base di un'analisi costi-benefici nell'ambito dell'esecuzione. Una variante minima, nell'ambito della quale si verifica se i processi esistenti comportano importanti lacune e se tra le autorità e le organizzazioni tali processi sono armonizzati tra loro, potrebbe in linea di principio essere attuata con le risorse disponibili. Una variante massima, con la realizzazione di un ISMS conformemente alla norma DIN ISO/IEC 27001 da parte delle autorità e organizzazioni assoggettate comporterebbe, secondo le stime di esperti, costi di progetto (spese di consulenza) tra gli 8 e i 12 milioni di franchi. Tra queste le due varianti esistono altre soluzioni d'attuazione che, a seconda dell'entità e delle esigenze di sicurezza, implicherebbero maggiori o minori spese di consulenza. Per la gestione e l'esercizio dell'organizzazione sono competenti gli incaricati della sicurezza delle informazioni. Eventuali costi per gli audit devono essere pianificati e assunti nel quadro del preventivo ordinario.

Le verifiche dell'efficacia (art. 18 cpv. 3) potrebbero comportare, a seconda del modello di organizzazione (v. n. 3.1.2), costi annui di 1,5 a 1,8 milioni di franchi per audit esterni. In base all'esperienza, i costi per gli audit ammontano di regola dallo 0,5 per cento al 2 per cento delle spese totali per investimenti destinati ai sistemi sottoposti all'audit.

Con decisione del 12 dicembre 2013 il Parlamento ha approvato un credito d'impegno per il Programma IAM Confederazione (art. 24–27). Le risorse sono comprese nel preventivo e nel piano finanziario della Confederazione.

Per l'acquisizione dei dati presso gli istituti finanziari e le banche nel quadro di CSP ampliati (art. 35 cpv. 2 lett. c in combinato disposto con l'art. 37 cpv. 2) occorre considerare costi di 10 000 a 20 000 franchi.

3.1.2 Ripercussioni in materia di personale

Complessivamente, per gli organi specialistici in materia di sicurezza delle informazioni potrebbero risultare necessari tra 13,5 e 14,5 posti supplementari. Il Consiglio federale deciderà in occasione dell'emanazione delle disposizione d'esecuzione in merito alle ulteriori risorse di personale. Tuttavia, questi posti supplementari saranno compensati in gran parte a medio termine con una corrispondente riduzione nel settore dei CSP. Al momento non è ancora possibile procedere a una stima oggettiva del fabbisogno supplementare di personale per gli incaricati della sicurezza delle informazioni, poiché dipende dal disciplinamento dell'organizzazione interna (approccio centralizzato o decentralizzato). Sono tuttavia ipotizzabili spese supplementari per due a sette posti di lavoro, che, a dipendenza del modello di organizzazione, potranno essere più o meno compensate internamente. Tali ripercussioni in materia di personale possono essere illustrate come segue.

Servizi specializzati CSP

I servizi specializzati CSP eseguono ogni anno da 75 000 a 80 000 controlli. Sono compresi non solo i CSP secondo la LMSI, ma anche i controlli secondo la LENu (500 controlli) e le valutazioni del potenziale di violenza delle persone soggette all'obbligo di prestare servizio militare secondo l'articolo 113 LM (40 500 controlli). A tal fine attualmente il nostro Collegio impiega complessivamente 61 posti: 27 a tempo indeterminato e 30 a tempo determinato (fino alla fine del 2017) presso il DDPS nonché quattro posti a tempo indeterminato presso la CaF. La maggior parte dei posti a tempo determinato presso il DDPS (16 posti) sono stati autorizzati alla fine del 2012 per ridurre i casi di potenziale rischio pendenti. Alla fine del 2015 il DDPS ha inoltre autorizzato 10 nuovi posti limitati a due anni. Tuttavia, già oggi risulta evidente che, nonostante tali posti supplementari, le risorse del Servizio specializzato CSP del DDPS non bastano per espletare tutti i controlli. I costi complessivi dei CSP (costi complessivi amministrativi e per il personale nonché per il sistema d'informazione) per il 2015 ammontano a 12,5 milioni di franchi. Inoltre, l'onere amministrativo per l'avvio dei CSP nonché per l'allestimento e l'adattamento degli elenchi delle funzioni secondo le indicazioni dei dipartimenti e della CaF corrispondono complessivamente a dieci posti a tempo pieno. Il nostro Collegio intende diminuire sensibilmente il numero dei CSP e ridurre a medio termine il relativo onere amministrativo e di personale di almeno 12 posti rispetto a oggi. Per contro, il disegno non ha alcun influsso sul numero di controlli secondo la LENu, la LAEI e l'articolo 113 LM.

Servizio specializzato SA

Oggi circa 550 aziende con sede in Svizzera dispongono di una DSA. Per l'esecuzione della PSA connessa a mandati militari classificati, il DDPS impiega 2,2 posti (due posti per specialisti della sicurezza e 0,2 posti per l'avvio dei CSP).

L'estensione della PSA al settore civile e alle altre autorità federali comporterà probabilmente un aumento del 30 per cento delle aziende di cui occorre occuparsi. Inoltre, gli adeguamenti alla procedura odierna genereranno un leggero aumento del fabbisogno di personale. Si prevede che per la PSA saranno complessivamente necessari 1,5 posti supplementari. Senza queste risorse occorrerà rinunciare a una PSA uniforme.

MELANI

Le risorse di MELANI sono state trattate nel quadro della pianificazione dell'attuazione della SNPC. Non sono necessarie risorse supplementari di personale.

Incaricati della sicurezza delle informazioni

Il ruolo degli incaricati della sicurezza delle informazioni raggrupperà i ruoli finora ricoperti dagli incaricati della protezione delle informazioni e dagli incaricati della sicurezza informatica. Inoltre, gli incaricati della sicurezza delle informazioni riceveranno competenze supplementari nell'ambito dei CSP e delle PSA nonché altri compiti (p. es. direzione della sicurezza delle informazioni e della corrispondente gestione dei rischi nonché esecuzione di audit). Per valutare le risorse di personale necessarie a tal fine saranno determinanti le disposizioni esecutive. L'organizzazione specialistica interna ai dipartimenti (approccio centralizzato o decentralizzato) può altresì influenzare in modo determinante la situazione in materia di risorse disponibili. In base all'esperienza, potrebbe essere necessario un fabbisogno supplementare di personale di due fino a otto posti che potrà essere più o meno compensato internamente a dipendenza del modello di organizzazione. Le autorità assoggettate decideranno in merito a tali risorse nell'ambito dell'esecuzione.

Servizio specializzato della Confederazione per la sicurezza delle informazioni

In base alla valutazione degli esperti, per un adempimento minimo dei suoi compiti secondo l'articolo 84 e l'elaborazione degli standard secondo l'articolo 86, il servizio specializzato della Confederazione per la sicurezza delle informazioni necessiterà complessivamente di 22 posti, ripartiti come segue: direzione del servizio specializzato (supplenza compresa): 1,2 posti; segretariato: 1,1 posti; coordinamento degli organi specializzati: 1 posto; formazione e sensibilizzazione: 1 posto; gestione dei rischi e dei requisiti: 4 posti; audit e reporting: 2 posti; audit tecnici: 5 posti; crittologia: 3,5 posti; diritto e affari politici: 2 posti; relazioni internazionali: 1,2 posti. Questi posti saranno compensati e occupati gradualmente (11 posti nel primo anno e 11 posti tra il secondo e il terzo anno). Di questi 22 posti, 7,2 posti saranno compensati con risorse che già oggi sono impiegate dal DFF e dal DDPS per la gestione della sicurezza informatica a livello interdipartimentale e l'applicazione coordinata dell'OPrI. Da 2 a 3 altri posti (in particolare nel settore diritto e relazioni internazionali) saranno trasferiti dal DDPS al dipartimento competente. Complessivamente saranno quindi necessari circa 12–13 posti supplementari. Il nostro Collegio si adopererà, per quanto possibile, per compensare internamente tale eventuale bisogno di personale oppure mediante miglioramenti sotto il profilo dell'efficienza.

Questi posti supplementari saranno impiegati principalmente per tre compiti nuovi o ampliati, motivati come segue:

- *gestione dei rischi e dei requisiti:* da una parte, si tratta di elaborare gli standard e successivamente di applicarli. Requisiti e misure standardizzati possono consentire risparmi nell'ambito di progetti e sono altresì importanti per un'esecuzione uniforme. D'altra parte, occorre garantire l'assistenza alle autorità (e ai Cantoni) nella direzione della sicurezza delle informazioni e nella relativa gestione dei rischi. Senza i quattro posti supplementari occorrerebbe rinunciare alla standardizzazione.

- *Audit tecnici:* si tratta segnatamente di un nuovo compito che comprende sia la verifica dell'idoneità (art. 84 cpv. 2 lett. e), sia le verifiche periodiche dell'efficacia (art. 18 cpv. 3). La verifica dell'idoneità è necessaria nel contesto internazionale (v. n. 5.2.) e per la standardizzazione operativa presso i fornitori di prestazioni (v. commento all'art. 84 cpv. 1 lett. e). La verifica dell'efficacia è l'unica misura che può dimostrare lo stato effettivo della sicurezza tecnica delle informazioni. Le basi legali attualmente in vigore non prevedono il nuovo livello di sicurezza «protezione molto elevata» a cui è riservata questa verifica. Gli esperti stimano tuttavia che la Confederazione impiega da 10 a 20 sistemi con un'elevata necessità di protezione. Siffatti sistemi sono spesso molto complessi. Pertanto, il relativo onere a livello di audit risulta elevato. La modellizzazione si è basata su 12 a 16 sistemi sottoposti ad audit quadriennali secondo lo stato della dottrina. A tale scopo, la Confederazione necessita di 11 posti supplementari (1 posto per la direzione degli audit, 1 posto per l'amministrazione e tre gruppi di 3 auditori ciascuno), o di 8 posti (direzione degli audit, amministrazione e due gruppi di auditori) con un budget di 750 000 a 900 000 franchi per esperti esterni, o di 5 posti (direzione dell'audit, esecuzione e un gruppo di auditori) con un budget di 1,5 a 1,8 milioni di franchi per esperti esterni, o di 2 posti (soltanto direzione degli audit e amministrazione) con un budget di 2,25 a 2,7 milioni di franchi per esperti esterni. Per la realizzazione si propone la variante con 5 posti, poiché essa garantisce che la Confederazione disponga internamente delle necessarie conoscenze specialistiche e che le autorità federali possano decidere regolarmente sull'onere a livello di audit, dato che vanno richieste le relative risorse. Inoltre, non è certo che la Confederazione possa trovare un numero maggiore di esperti.

  Senza questi 5 posti supplementari si dovrebbe scegliere la variante con soltanto 2 posti supplementari e il relativo budget o rinunciare a questi compiti. In tal caso i requisiti non sarebbero soddisfatti rispetto al contesto internazionale e la standardizzazione operativa presso i fornitori di prestazioni potrebbe essere raggiunta unicamente con un onere esterno supplementare. Inoltre, lo stato della sicurezza delle informazioni nell'ambito dei mezzi informatici di massima criticità della Confederazione non potrebbe essere valutato in maniera corretta.

- *Crittologia:* l'impiego di misure crittologiche costituisce una misura di sicurezza irrinunciabile per le informazioni con un'elevata necessità di protezione a livello di confidenzialità e di integrità. L'impiego della crittologia

richiede la disponibilità di requisiti chiari, ma anche l'accompagnamento del processo d'acquisto, la verifica dei piani in materia di crittologia nonché la cura periodica delle componenti crittografiche. Sia i requisiti sia le capacità menzionate mancano ampiamente presso la Confederazione. Il DDPS, invece, impiega 7,5 posti (4,5 presso la BAC e 3 presso armasuisse) per l'adempimento di questi compiti a favore del dipartimento e dell'esercito. Gli esperti stimano che per adempiere tali compiti nel caso di tutti i mezzi informatici con un grado di protezione molto elevato e dei mezzi informatici con un grado di protezione elevato comuni a tutte le autorità sono necessari 3,5 posti supplementari. Senza queste risorse supplementari si dovrebbe rinunciare all'accompagnamento e alla verifica delle misure crittologiche al di fuori del DDPS.

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

Le ripercussioni sui Cantoni potranno essere valutate definitivamente solo al momento dell'emanazione delle disposizioni esecutive. Tuttavia, l'applicazione della LSIn ai Cantoni è limitata e avverrà principalmente in funzione di progetti o applicazioni. I Cantoni saranno altresì coinvolti strettamente nell'impostazione delle disposizioni esecutive e degli standard, affinché possano valutare tempestivamente l'economicità delle misure ed esercitare un influsso in merito. La Confederazione continuerà ad assumersi i costi per i CSP degli impiegati dei Cantoni che svolgono compiti della Confederazione sensibili sotto il profilo della sicurezza. Si tratta di circa 400 CSP l'anno. I Cantoni beneficeranno anche dell'assistenza del servizio specializzato della Confederazione per la sicurezza delle informazioni. Per contro saranno tenuti a verificare periodicamente l'efficacia delle misure di protezione adottate. Tuttavia, al riguardo non dovrebbero costituire nuove organizzazioni, bensì utilizzare le loro attuali strutture di vigilanza. Nell'ambito dei CSP in futuro l'acquisizione di estratti dei registri esecuzioni e fallimenti dei Cantoni avverrà gratuitamente (attualmente alla Confederazione costano 250 000 franchi l'anno). Tuttavia, poiché in futuro nel quadro del progetto e-LEF[45] questi dati saranno acquisiti elettronicamente tramite un'interfaccia, per i Cantoni il relativo onere verrà a cadere. Complessivamente è prevedibile che la nuova regolamentazione comporterà un moderato onere supplementare per i Cantoni che sarà in parte compensato dalle efficaci misure di sostegno della Confederazione.

In linea di principio la legge non comporta ripercussioni per i centri urbani, gli agglomerati e le regioni di montagna.

45 Per infomazioni sul progetto e-LEF consultare: www.bj.admin.ch > Stato & cittadino > Informatica giuridica > Progetto e-LEF

3.3 Ripercussioni per l'economia

I terzi sono interessati dalla legge solo se nel quadro di un contratto sono destinati a gestire informazioni o mezzi informatici della Confederazione. Le aziende che si candidano per mandati civili della Confederazione che comportano attività sensibili sotto il profilo della sicurezza saranno d'ora in poi soggette alla PSA. L'assoggettamento è connesso a un lieve onere amministrativo supplementare, tuttavia la concorrenzialità delle imprese svizzere sarà migliorata poiché la legge crea la base per il rilascio di dichiarazioni di sicurezza delle autorità a favore di privati che si candidano per mandati classificati esteri o internazionali per la cui esecuzione è necessaria un'attestazione nazionale di sicurezza.

I terzi, per esempio banche o istituti di credito, di cui si richiede la collaborazione nell'ambito dei CSP, devono essere indennizzati unicamente se l'onere così causato è considerevole. Un siffatto onere diventa considerevole in particolare se, per esempio, va oltre l'allestimento di estratti conto e richiede ricerche particolarmente intense. Questo tipo di collaborazione è previsto soltanto per il livello di controllo più elevato. Il relativo onere rimarrà pertanto limitato.

3.4 Ripercussioni per la società

La società è interessata sotto due aspetti. In primo luogo la protezione dei dati e la sicurezza dei dati vengono migliorate. In secondo luogo, sono resi noti i principi della classificazione e si inaspriscono i criteri allo scopo di ridurre globalmente il volume di informazioni e mezzi informatici da classificare. Ciò è particolarmente importante in relazione al principio della trasparenza, la cui efficacia non può essere assolutamente pregiudicata dalla legge.

3.5 Ripercussioni per l'ambiente

La legge non ha ripercussioni sull'ambiente.

3.6 Altre ripercussioni

Dal punto di vista formale, il disegno non attua alcun impegno internazionale diretto. A livello pratico la cooperazione internazionale sarà facilitata, in quanto la legge definisce chiaramente le competenze usuali nel contesto internazionale (v. n. 5.2).

4 Programma di legislatura e strategie nazionali del Consiglio federale

4.1 Rapporto con il programma di legislatura

Il presente disegno è una conseguenza della misura «Aggiornamento e attuazione della Strategia per una società dell'informazione» in Svizzera annunciata nel messaggio del 25 gennaio 2012[46] sul programma di legislatura 2011–2015 e nel decreto federale del 15 giugno 2012[47] sul programma di legislatura 2011–2015.

4.2 Rapporto con le strategie nazionali del Consiglio federale

4.2.1 Strategia per una società dell'informazione in Svizzera

Riguardo alla strategia: v. numero 1.1.1; la LSIn è menzionata nel Catalogo dei progetti società dell'informazione 2011–2015 (stato: novembre 2013) sotto l'ambito d'intervento «Sicurezza e fiducia». La legge creerà una base chiara per i requisiti in materia di sicurezza nei progetti gestiti dalla Confederazione.

4.2.2 Strategia nazionale per la protezione della Svizzera contro i cyber-rischi

Riguardo alla Strategia nazionale per la protezione della Svizzera contro i cyber-rischi: v. numero 1.1.2; per quanto riguarda il rapporto tra tale strategia e la LSIn: v. il numero 1.2.7; per il sostegno ai gestori di infrastrutture critiche: v. gli articoli 75–81.

4.2.3 Strategia nazionale per la protezione delle infrastrutture critiche

La strategia nazionale del 27 giugno 2012[48] per la protezione delle infrastrutture critiche (strategia PIC) si prefigge di rafforzare la resilienza della Svizzera a livello di infrastrutture critiche. A questo scopo la strategia definisce diverse misure suddivise in due campi d'azione. L'autoprotezione viene migliorata grazie all'allestimento e all'applicazione, da parte degli organi competenti, di piani di protezione integrali volti a identificare e ridurre i rischi specifici. A livello intersettoriale viene migliorata la collaborazione fra gli attori coinvolti (autorità, gestori) di tutti i settori delle infrastrutture critiche e ridotta la vulnerabilità della società, dell'economia e dello Stato nei confronti di interruzioni importanti. A tal fine vengono elaborate

46 FF **2012** 305, in particolare pagg. 367, 423 e 430
47 FF **2012** 6413, in particolare pag. 6415
48 FF **2012** 6875

pianificazioni volte a limitare i danni e a sostenere in modo sussidiario i gestori di infrastrutture critiche in caso di simili eventi. Il Consiglio federale intende sostenere i gestori di infrastrutture critiche nei loro sforzi di protezione. Al riguardo si mira a raggiungere la maggior resilienza possibile dal profilo della sicurezza delle informazioni. La misura 7 della strategia PIC, ad esempio, prevede di creare una base legale formale che permetta di sottoporre determinate categorie di personale dei gestori di infrastrutture critiche a controlli di sicurezza. La LSIn sostiene pertanto anche la concretizzazione della strategia PIC.

5 Aspetti giuridici

5.1 Costituzionalità e legalità

Secondo l'articolo 42 Cost. per le sue normative il legislatore federale necessita di una base costituzionale (esplicita o implicita). Per il progetto legislativo esistono sufficienti basi costituzionali. Sotto il profilo formale, nel caso del presente atto normativo si tratta principalmente di disposizioni organizzative per le autorità federali. Il diritto federale in materia di organizzazione non è espressamente menzionato come competenza legislativa nel catalogo della Cost. inerente alla ripartizione delle competenze tra Confederazione e Cantoni, tuttavia l'articolo 164 capoverso 1 lettera g Cost. annovera nell'ambito delle competenze dell'Assemblea federale l'«organizzazione e [la] procedura delle autorità federali» tra le materie le cui disposizioni sono emanate sotto forma di legge federale (v. l'ingresso della LParl). Inoltre, nella legislazione vigente in materia di organizzazione si rinvia anche all'articolo 173 capoverso 2 Cost. che assegna all'Assemblea federale il trattamento di tutte le questioni che rientrano nella competenza della Confederazione e non sono attribuite ad altre autorità (v. l'ingresso [con la nota a piè di pagina 1] della LOGA o della LTras).

Sotto l'aspetto dei contenuti, la normativa è in primo luogo destinata alla salvaguardia della sicurezza interna ed esterna della Svizzera nonché a proteggere la libera formazione dell'opinione e la capacità di agire delle autorità. In questo contesto, essa si fonda anche sull'articolo 54 capoversi 1 e 2 Cost. (Relazioni con l'estero e salvaguardia della sicurezza esterna) nonché sull'articolo 57 capoverso 1 Cost. secondo il quale «nell'ambito delle loro competenze, la Confederazione e i Cantoni provvedono alla sicurezza del Paese […]».

Non rientrano tra gli obiettivi menzionati in precedenza le disposizioni sulla PSA, nella misura in cui è prevista per aziende che necessitano di una dichiarazione di sicurezza aziendale allo scopo di potersi candidare per mandati di autorità estere o internazionali. Questa regolamentazione è coperta dall'articolo 101 Cost., che rappresenta la base per la promozione dell'economia esterna. Le disposizioni inerenti alla protezione delle infrastrutture critiche possono fondarsi tanto sulle basi nell'ambito della sicurezza interna ed esterna quanto sulle competenze della Confederazione per l'approvvigionamento del Paese (art. 102 Cost.). Per l'esercito si può rinviare all'articolo 60 Cost. che dichiara l'organizzazione dell'esercito di competenza della Confederazione.

5.2 Compatibilità con gli impegni internazionali della Svizzera

La Svizzera ha firmato con diversi Stati e organizzazioni internazionali accordi sulla protezione delle informazioni (v. RS *0.514.XXX*). Con questi accordi internazionali, la Svizzera si è impegnata a rispettare determinati standard in materia di protezione di informazioni classificate di questi Stati e organizzazioni. Oltre che con l'UE, la Svizzera ha concluso anche accordi in materia di protezione delle informazioni con l'ESA (European Space Agency) e la NATO. Questi accordi contengono meccanismi di protezione uniformi per il trattamento di informazioni classificate o il riconoscimento reciproco di attestazioni di sicurezza. Menzionano ad esempio di volta in volta l'organo competente per l'applicazione delle misure di sicurezza (*National Security Authority*). Nell'ambito della sicurezza delle comunicazioni sono richieste autorità nazionali (*Security Accreditation Authority*) che definiscono standard unitari e confermano l'idoneità dei sistemi. Il servizio specializzato della Confederazione per la sicurezza delle informazioni assumerà questi compiti per la Svizzera.

Gli impegni internazionali della Svizzera nell'ambito della sicurezza delle informazioni non sono in contrasto con la presente legge.

5.3 Forma dell'atto

Già nella sua decisione del 12 maggio 2010 (v. n. 1.1.4) il Consiglio federale riteneva che la normativa essenziale sulla sicurezza delle informazioni avrebbe dovuto presentare la forma di una legge federale. Da un lato si tratta di disposizioni in materia di organizzazione e di procedura per le autorità federali (art. 164 cpv. 1 lett. g Cost.), che in conseguenza della necessità del loro carattere unitario devono esplicare effetti su tutte le autorità; anche ai Cantoni vengono imposti degli obblighi in materia di sicurezza delle informazioni. Dall'altro, si tratta di disposizioni che, in particolare nell'ambito dei CSP e delle PSA, comportano considerevoli ingerenze in ambiti protetti dalla Costituzione (art. 164 cpv. 1 lett. b e c Cost.) o per le quali è indispensabile, per ragioni inerenti alla protezione dei dati, una base a livello di legge formale (art. 17 cpv. 2 LPD). Riguardo agli svantaggi del campo d'applicazione unitario a livello legislativo si rimanda al numero 1.3.

5.4 Subordinazione al freno alle spese

Il progetto legislativo non sottostà al freno delle spese di cui all'articolo 159 capoverso 3 lettera b Cost., poiché non contiene né disposizioni in materia di sussidi né le basi per costituire un credito d'impegno o un limite di spesa.

5.5 Conformità alla legge sui sussidi

Il presente progetto legislativo non prevede aiuti finanziari o indennità ai sensi della legge del 5 ottobre 1990[49] sui sussidi.

5.6 Delega di competenze normative

Le competenze normative possono essere delegate mediante legge federale, sempre che la Costituzione non lo escluda (art. 164 cpv. 2 Cost.). In base al campo d'applicazione che contempla tutte le autorità federali, l'esecuzione della legge non avviene secondo lo schema «ordinario» in virtù del quale il Consiglio federale ha, in linea di principio, la competenza esclusiva per il diritto d'esecuzione. Per tutelare l'autonomia esecutiva delle autorità assoggettate, il disegno prevede che tali autorità emanino loro stesse le disposizioni necessarie (art. 85 cpv. 1). Questa delega si applica all'intera legge, sempre che la competenza normativa non sia espressamente delegata al Consiglio federale. Il disegno delega al Consiglio federale le seguenti competenze normative:

- articolo 2 capoversi 3 e 4: il Consiglio federale stabilisce quali unità dell'Amministrazione federale decentralizzata e quali organizzazioni di cui all'articolo 2 capoverso 4 LOGA devono applicare la legge;
- articolo 12 capoverso 3: il Consiglio federale disciplina la declassificazione degli archivi;
- articolo 32 capoverso 2: il Consiglio federale deve istituire i servizi specializzati CSP;
- articolo 44 capoverso 2: il Consiglio federale può rinunciare alla ripetizione del CSP per funzioni dell'esercito e della protezione civile;
- articolo 49: il Consiglio federale emana normative completive concernenti i CSP e la protezione dei dati;
- articolo 74: il Consiglio federale emana normative completive concernenti la PSA nonché la relativa protezione dei dati e disciplina l'organizzazione del servizio specializzato SA;
- articolo 75 capoverso 5: il Consiglio federale designa i servizi competenti per i compiti di sostegno alle infrastrutture critiche nell'ambito della sicurezza delle informazioni;
- articolo 81: il Consiglio federale emana normative completive concernenti la sicurezza delle informazioni nelle infrastrutture critiche e la relativa protezione dei dati;
- articolo 84 capoverso 3: il Consiglio federale disciplina l'organizzazione del servizio specializzato della Confederazione per la sicurezza delle informazioni e può assegnargli ulteriori incarichi;

49 RS **616.1**

- articolo 85 capoverso 1: il Consiglio federale può delegare alla Cancelleria federale l'emanazione di disposizioni esecutive per gli affari del Consiglio federale;
- articolo 86: il Consiglio federale stabilisce misure standard secondo lo stato della scienza e della tecnica. Esso può delegare tale compito;
- articolo 87 capoverso 4: il Consiglio federale decide a quali risorse della Confederazione possono ricorrere i Cantoni per le loro necessità e fissa gli emolumenti;
- articolo 88: il Consiglio federale può concludere autonomamente trattati internazionali;
- articolo 14 capoverso 2 LM: il Consiglio federale stabilisce le funzioni soggette alla verifica;
- articolo 20*a* capoverso 2 LAEl: il Consiglio federale stabilisce quali gruppi di persone sono soggetti alla verifica dell'affidabilità.

5.7 Protezione dei dati

Per l'adempimento dei compiti secondo il presente progetto legislativo è indispensabile trattare dati personali negli ambiti seguenti:

- articolo 19 capoverso 2: il trattamento di dati personali nell'ambito della sorveglianza delle reti da parte dei fornitori di prestazioni si fonda sul diritto vigente (art. 57*i*–57*q* LOGA);
- articolo 20 capoverso 2: per l'utilizzo di dati biometrici ai fini della verifica dell'identità di persone che necessitano di un accesso a informazioni, mezzi informatici e locali della Confederazione, è creata una base legale formale ai sensi dell'articolo 17 capoverso 2 LPD;
- articoli 24–27: per l'impiego di sistemi d'informazione ai fini del controllo centralizzato delle identità sono create basi legali formali dettagliate ai sensi dell'articolo 17 capoverso 2 LPD. Poiché la responsabilità della protezione dei dati sarà probabilmente ripartita, le autorità assoggettate (in particolare il Consiglio federale) disciplineranno la responsabilità della protezione dei dati sulla base dell'articolo 16 capoverso 2 LPD. L'impiego di simili sistemi migliorerà la protezione dei dati operativa e la loro sicurezza;
- articoli 28–49: per i CSP è necessario il trattamento di dati personali degni di particolare protezione (art. 3 lettera c LPD). Il risultato del CSP corrisponde inoltre a un profilo della personalità (art. 3 lett. d LPD). Per il trattamento di tali dati la LSIn crea una base legale formale dettagliata ai sensi dell'articolo 17 capoverso 2 LPD. Poiché il Consiglio federale intende istituire almeno due servizi specializzati CSP, esso dovrà ancora disciplinare nei dettagli la responsabilità per la protezione dei dati (art. 16 cpv. 2 LPD). Globalmente, il nuovo disciplinamento sarà nettamente migliore per quanto concerne la protezione dei dati e più proporzionato rispetto al diritto vigente (art. 19–21 LMSI e art. 144–149 LSIM). Inoltre, il Consiglio federale inten-

de ridurre il numero di persone sottoposte ai CSP, ciò che diminuirà proporzionalmente il trattamento di dati personali;

- articoli 50–74: per l'esecuzione di PSA è indispensabile il trattamento di dati personali degni di particolare protezione (art. 3 lett. c LPD). Per il trattamento di tali dati la LSIn crea una base legale formale dettagliata ai sensi dell'articolo 17 capoverso 2 LPD;
- articoli 75–81: per il sostegno nell'ambito della sicurezza delle informazioni alle infrastrutture critiche, MELANI deve trattare regolarmente dati personali (elementi d'indirizzo) che, in determinati casi, possono essere considerati dati personali degni di particolare protezione. A tal fine viene creata una base legale formale;
- modifica di altri atti normativi: alcune disposizioni di altri atti normativi disciplinano il trattamento di dati personali in relazione con il CSP secondo gli articoli 28–49. Al riguardo si applicano per analogia i relativi commenti.

Ai sensi della LSIn, i dati personali sono considerati informazioni di cui è necessario tutelare la confidenzialità, la disponibilità, l'integrità e la tracciabilità. Il progetto legislativo crea la base per processi, misure e capacità uniformi per tutte le autorità allo scopo di proteggere le informazioni di competenza della Confederazione. Nell'ambito dell'esecuzione e in particolare dell'elaborazione di misure standardizzate sarà coinvolto l'IFPDT. L'applicazione integrativa della legge ai dati personali migliorerà pertanto l'attuazione della protezione dei dati e in particolare la loro sicurezza.

Abbreviazioni

AFS	Archivio federale svizzero
BAC	Base d'aiuto alla condotta dell'esercito
BLEs	Base logistica dell'esercito
BSI	Bundesamt für Sicherheit in der Informationstechnik (D)
CaF	Cancelleria federale
CDF	Controllo federale delle finanze
CdG-N	Commissione della gestione del Consiglio nazionale
CdG-S	Commissione della gestione del Consiglio degli Stati
CERT	Computer Emergency Response Team
Cost.	Costituzione federale; RS *101*
CP	Codice penale svizzero del 21 dicembre 1937; RS *311.0*
CPA	Controllo parlamentare dell'amministrazione
CPM	Codice penale militare del 13 giugno 1927; RS *321.0*
CPP	Codice di diritto processuale svizzero del 5 ottobre 2007, Codice di procedura penale; RS *312.0*
CSI	Conferenza svizzera sull'informatica
CSP	Controllo/i di sicurezza relativo/i alle persone
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DelCG	Delegazione delle Commissioni della gestione
DFAE	Dipartimento federale degli affari esteri
DFF	Dipartimento federale delle finanze
DFGP	Dipartimento federale di giustizia e polizia
DFI	Dipartimento federale dell'interno
DSA	Dichiarazione di sicurezza aziendale
e-LEF	Denominazione di uno standard per lo scambio di dati elettronici riguardanti le pratiche di esecuzione e fallimento sviluppato dall'Ufficio federale di giustizia
fedpol	Ufficio federale di polizia
GLID	Gruppo di lavoro interdipartimentale
GovCERT	Governmental CERT

IAM	Identity and Access Management
IC	Infrastrutture critiche
IFPDT	Incaricato federale della protezione dei dati e della trasparenza
ISMS	Information Security Management Systems
ISA CH-EU	Accordo del 28 aprile 2008 tra la Confederazione Svizzera e l'Unione europea sulle procedure di sicurezza per lo scambio di informazioni classificate; RS *0.514.126.81*
IT	Information technology
LAEI	Legge federale del 23 marzo 2007 sull'approvvigionamento elettrico; RS *734.7*
LAIn	Legge federale del 25 settembre 2015 sulle attività informative; FF *2015* 5925
LAPub	Legge federale del 16 dicembre 1994 sugli acquisti pubblici; RS *172.056.1*
LAr	Legge federale del 26 giugno 1998 sull'archiviazione, Legge sull'archiviazione; RS *152.1*
LAVS	Legge federale del 20 dicembre 1946 su l'assicurazione per la vecchiaia e per i superstiti; RS *831.10*
LBN	Legge federale del 3 ottobre 2003 sulla Banca nazionale svizzera, Legge sulla Banca nazionale; RS *951.11*
LEF	Legge federale dell'11 aprile 1889 sulla esecuzione e sul fallimento; RS *281.1*
LENu	Legge federale del 21 marzo 2003 sull'energia nucleare; RS *732.1*
LFC	Legge federale del 7 ottobre 2005 sulle finanze della Confederazione; RS *611.0*
LM	Legge federale del 3 febbraio 1995 sull'esercito e sull'amministrazione militare, Legge militare; RS *510.10*
LMSI	Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna; RS *120*
LOGA	Legge del 21 marzo 1997 sull'organizzazione del Governo e dell'Amministrazione; RS *172.010*
LParl	Legge federale del 13 dicembre 2002 sull'Assemblea federale, Legge sul Parlamento; RS *171.10*
LPD	Legge federale del 19 giugno 1992 sulla protezione dei dati; RS *235.1*
LPers	Legge del 24 marzo 2000 sul personale federale; RS *172.220.1*

LResp	Legge federale del 14 marzo 1958 su la responsabilità della Confederazione, dei membri delle autorità federali e dei funzionari federali, Legge sulla responsabilità; RS *170.32*
LSIM	Legge federale del 3 ottobre 2008 sui sistemi d'informazione militari; RS *510.91*
LSIn	Legge federale sulla sicurezza delle informazioni in seno alla Confederazione, Legge sulla sicurezza delle informazioni
LSIP	Legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione; RS *361*
LTAF	Legge del 17 giugno 2005 sul Tribunale amministrativo federale; RS *173.32*
LTC	Legge del 30 aprile 1997 sulle telecomunicazioni; RS *784.10*
LTF	Legge del 17 giugno 2005 sul Tribunale federale; RS *173.110*
LTras	Legge federale del 17 dicembre 2004 sul principio di trasparenza dell'amministrazione, Legge sulla trasparenza; RS *152.3*
MELANI	Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
Messaggio LTras	Messaggio del 12 febbraio 2003 concernente la legge federale sulla trasparenza dell'amministrazione (Legge sulla trasparenza, LTras) (FF *2003* 1783)
OCSP	Ordinanza del 4 marzo 2011 sui controlli di sicurezza relativi alle persone; RS *120.4*
ODIC	Organo direzione informatica della Confederazione
OGD	Open Government Data
OIAF	Ordinanza del 9 dicembre 2011 concernente l'informatica e la telecomunicazione nell'Amministrazione federale, Ordinanza sull'informatica nell'Amministrazione federale; RS *172.010.58*
OLPD	Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati; RS *235.11*
OPrI	Ordinanza del 4 luglio 2007 sulla protezione delle informazioni della Confederazione, Ordinanza sulla protezione delle informazioni; RS *510.411*
PA	Legge federale del 20 dicembre 1968 sulla procedura amministrativa; RS *172.021*
PIC	Prior Informed Consent
PISA	Sistema di gestione del personale dell'esercito
PPM	Procedura penale militare del 23 marzo 1979; RS *322.1*
PSA	Procedura di sicurezza relativa alle aziende

Servizio specializzato SA	Servizio specializzato per la sicurezza aziendale
SG	Segreteria generale
SIC	Servizio delle attività informative della Confederazione
SIO	Sicurezza delle informazioni e degli oggetti
SNPC	Strategia nazionale del 27 giugno 2012 per la protezione della Svizzera contro i cyber-rischi (FF *2013* 499, all'epoca denominata «Strategia nazionale del 27 giugno 2012 per la protezione della Svizzera contro i rischi informatici»)
TIC	Tecnologie dell'informazione e della comunicazione
UFCOM	Ufficio federale delle comunicazioni
UFG	Ufficio federale di giustizia
UFIT	Ufficio federale dell'informatica e della telecomunicazione
UFPER	Ufficio federale del personale