Avamprogetto di legge federale sulla sicurezza delle informazioni (LSIn)

Rapporto esplicativo

Progetto del 26 marzo 2014

Compendio

Le informazioni sono il mezzo di scambio della società dell'informazione. Le autorità federali sono responsabili della gestione sicura delle informazioni trattate da loro stesse o dai rispettivi collaboratori per incarico e in nome della Svizzera e, per poter adempiere a tale responsabilità, devono disporre di strumenti moderni. L'evoluzione verso una società dell'informazione ha reso più complessi e dinamici i pericoli e le minacce che incombono sulle informazioni. Per quanto concerne la protezione delle informazioni, diversi attacchi sferrati ai sistemi d'informazione della Confederazione hanno evidenziato la presenza di lacune che, in particolare in ambito organizzativo, possono tra l'altro essere ricondotte all'anacronismo o all'incoerenza delle basi legali.

Ispirandosi a standard internazionalmente riconosciuti, il presente avamprogetto di legge crea basi legali formali uniformi per la gestione della sicurezza delle informazioni nell'ambito di responsabilità della Confederazione. Lo scopo è quello di adeguare la protezione delle informazioni e la sicurezza nell'impiego di tecnologie dell'informazione e della comunicazione (TIC) alle esigenze di una società dell'informazione moderna e interconnessa, nonché di eliminare le lacune e i punti deboli del diritto vigente.

Punti essenziali dell'avamprogetto

Sicurezza delle informazioni

Per «sicurezza delle informazioni» si intende la totalità dei requisiti e delle misure destinati a proteggere la confidenzialità, la disponibilità, l'integrità e la tracciabilità delle informazioni indipendentemente dal fatto che esse siano trattate in forma elettronica, orale o cartacea.

In seno alla Confederazione, le basi legali esistenti per la definizione di tali requisiti e per l'attuazione delle misure sono impostate in modo molto settoriale e risultano scarsamente coordinate nonché, spesso, lacunose. Lo stesso dicasi per le competenze organizzative. Attualmente, infatti, la Confederazione gestisce organizzazioni parallele, sia a livello organizzativo che sul piano giuridico, per la protezione dei dati, la protezione delle informazioni (protezione di informazioni classificate), la sicurezza informatica, la sicurezza delle persone, la sicurezza fisica e la gestione dei rischi. L'esperienza pratica ha dimostrato l'inefficienza di questo orientamento settoriale. L'avamprogetto riassume pertanto le misure più importanti per la protezione delle informazioni in un unico disciplinamento uniforme e prevede inoltre un'unica struttura per gestire ed esaminare in modo integrale, dal punto di vista giuridico e organizzativo, le questioni legate alla sicurezza delle informazioni.

Campo d'applicazione istituzionale

Gli scambi di informazioni tra le autorità e tra autorità e privati (compreso il settore economico) sono fortemente aumentati e avvengono sempre più spesso in formato elettronico. Il fatto che un'informazione sia degna di protezione o meno, tuttavia, non dipende dal servizio o dalla persona da cui essa viene trattata. Inoltre, poiché le infrastrutture e i sistemi TIC sono sempre più interconnessi tra loro, cresce il rischio che eventuali attacchi e minacce contro un'autorità possano estendersi anche agli ambiti di competenza di altre autorità coinvolte. È pertanto necessario fissare un livello di sicurezza uniforme per tutte le autorità al fine di garantire la fiducia reciproca tra le autorità federali nel quadro del trattamento delle informazioni nonché di ridurre il rischio per tutte le autorità coinvolte.

Rientreranno quindi nel campo d'applicazione principale del presente avamprogetto tutte le autorità federali (l'Assemblea federale, i tribunali della Confederazione, il Consiglio federale, il Ministero pubblico della Confederazione, l'autorità di vigilanza sul Ministero pubblico della Confederazione e la Banca nazionale) e le organizzazioni ad esse subordinate (i Servizi del Parlamento, le amministrazioni dei tribunali della Confederazione, l'Amministrazione federale e l'esercito). Le direttive della Confederazione devono essere vincolanti anche per i Cantoni o i terzi a cui viene affidato il trattamento di informazioni della Confederazione o che hanno accesso ai suoi mezzi TIC.

Gestione dei rischi

La complessità e la dinamica delle minacce esigono inoltre che le autorità federali si focalizzino maggiormente su una valutazione sistematica delle necessità di protezione delle informazioni e sull'analisi dei relativi rischi. Ciò presuppone una gestione dei rischi efficace nel campo della sicurezza delle informazioni e una verifica periodica dell'attuazione delle misure di riduzione dei rischi. Queste due condizioni sono oggi quasi completamente inadempiute. Con il presente avamprogetto viene pertanto avviato anche un processo destinato a garantire in maniera duratura ed economica la sicurezza delle informazioni.

Classificazione delle informazioni

Tenendo conto delle maggiori aspettative dei cittadini per quanto concerne la trasparenza dell'operato delle autorità federali, l'avamprogetto fissa in modo trasparente i criteri per la classificazione delle informazioni della Confederazione e innalza inoltre i valori soglia per tale classificazione. Il principio di trasparenza dell'Amministrazione federale non viene in alcun modo limitato dalle disposizioni sulla classificazione.

Sicurezza nell'impiego delle TIC

L'avamprogetto tiene conto del fatto che, da qualche anno a questa parte, è considerevolmente aumentata l'importanza della sicurezza delle informazioni nell'impiego delle TIC. In particolare, viene fissato un meccanismo per la valutazione della criticità dei mezzi TIC, associando tale valutazione all'attuazione delle relative misure di sicurezza. In quest'ambito occorre concentrarsi principalmente sulla sicurezza dei sistemi e mezzi TIC più critici. L'avamprogetto rafforza sia il ruolo strategico e operativo delle autorità nell'attuazione delle misure sia il sistema degli audit.

Controlli di sicurezza relativi alle persone (CSP)

I CSP rappresentano in primo luogo una misura volta a garantire la sicurezza delle informazioni. Per questo il loro disciplinamento viene trasferito dalla LMSI alla nuova legge sulla sicurezza delle informazioni. Al contempo vengono inoltre eliminate le lacune esistenti nel disciplinamento in vigore, mirando anche a semplificare i CSP. I motivi del controllo vengono adeguati alle esigenze attuali in materia di sicurezza delle informazioni e i livelli di controllo vengono ridotti da tre a due. Anche la raccolta dei dati viene adeguata in funzione dei due livelli di controllo. In futuro i controlli saranno meno numerosi, ma terranno maggiormente conto dei rischi.

Procedura di sicurezza relativa alle aziende

La procedura di sicurezza relativa alle aziende è applicabile alle imprese che, nel quadro di un acquisto pubblico della Confederazione, devono essere incaricate di svolgere attività sensibili sotto il profilo della sicurezza. Tale procedura serve, da un lato, a verificare l'affidabilità di tali imprese e, dall'altro, a controllare e imporre la sicurezza delle informazioni durante l'adempimento del mandato. Il campo d'applicazione dell'attuale procedura di tutela del segreto è limitato ai mandati classificati provenienti dall'ambito militare. Con il presente avamprogetto viene invece introdotta una procedura di sicurezza relativa alle aziende unitaria e viene al contempo creata una base per il rilascio di dichiarazioni di sicurezza da parte delle autorità a favore delle imprese svizzere che concorrono per mandati esteri o internazionali e che, a tal fine, necessitano di una dichiarazione di sicurezza. Ciò rafforza la competitività delle imprese in questione.

Appoggio alle infrastrutture critiche

Nella sua Strategia nazionale del 27 giugno 2012 per la protezione della Svizzera contro i rischi informatici (FF 2013 499), il Consiglio federale ha sancito il principio dell'appoggio da parte della Confederazione ai gestori di infrastrutture critiche nel campo della sicurezza delle informazioni. Nell'ambito della collaborazione tra i gestori di infrastrutture critiche e la Confederazione, i servizi competenti devono potersi scambiare dati personali (elementi d'indirizzo nel settore delle telecomunicazioni) su sanzioni o perseguimenti amministrativi o penali. Il presente avamprogetto crea la base legale formale necessaria per il trattamento di tali dati personali.

Esecuzione

L'esecuzione della presente legge deve essere il più possibile uniforme. Inoltre, occorre garantire l'indipendenza e l'autonomia organizzativa delle autorità federali interessate. L'avamprogetto prende in considerazione tali esigenze, di per sé contraddittorie, con i tre meccanismi seguenti:

- *clausola di esenzione («opting out») per l'esecuzione: ogni autorità esegue autonomamente l'atto normativo nel proprio ambito ed emana il relativo disciplinamento a livello di ordinanza. Le disposizioni esecutive del Consiglio federale devono tuttavia essere applicate per analogia anche alle altre autorità federali fintanto che e nella misura in cui queste ultime non emanano disciplinamenti propri;*
- *requisiti e misure standard: il Consiglio federale è abilitato a fissare requisiti e misure standard, conformi allo stato della dottrina e della tecnica, che fungeranno da raccomandazioni per le altre autorità federali;*
- *istituzione di uno specifico organo di coordinamento inter-autorità: quest'organo (Conferenza degli incaricati della sicurezza delle informazioni) ha come obiettivo principale un'esecuzione della legge uni-*

forme, valida per tutte le autorità e basata sul rischio. La conferenza viene coinvolta anche nella definizione dei requisiti e delle misure standard.

La soluzione proposta garantisce l'indipendenza delle autorità federali nell'ambito dell'esecuzione. Poiché le autorità federali non possono essere assoggettate alle disposizioni esecutive del Consiglio federale, tutte le misure e tutti i requisiti minimi vincolanti per tutte le autorità devono essere fissati nella legge stessa. Di conseguenza, l'avamprogetto contiene anche numerose disposizioni che, dal punto di vista della gerarchia normativa, avrebbero potuto essere definite in un'ordinanza. L'avamprogetto garantisce anche una sufficiente autonomia a livello di esecuzione per i Cantoni e per determinate organizzazioni assoggettate alla legge e alle disposizioni esecutive del Consiglio federale. Inoltre, crea la necessaria base legale formale, attualmente mancante, per la conclusione di trattati internazionali da parte del Consiglio federale nel campo della sicurezza delle informazioni.

Organizzazione della sicurezza delle informazioni

Nel presente avamprogetto, l'organizzazione specialistica della sicurezza delle informazioni viene adeguata a questa nuova realtà complessa e dinamica. Ciò avviene su due livelli organizzativi:

- *organizzazione interna:*
  - *gestione della sicurezza delle informazioni: nell'ambito della gestione della sicurezza delle informazioni, le autorità federali devono basarsi su norme tecniche riconosciute a livello internazionale e consolidate nella pratica (per es. le norme DIN ISO/IEC 27001 e 27002);*
  - *incaricati della sicurezza delle informazioni: le autorità federali devono designare un incaricato della sicurezza delle informazioni che si occuperà della gestione di tutte le questioni relative alla sicurezza delle informazioni, nonché un suo sostituto;*
- *organizzazione inter-autorità:*
  - *servizio specializzato della Confederazione per la sicurezza delle informazioni: determinati organi esistenti devono essere raggruppati in un nuovo servizio specializzato per trovare una soluzione sistematica ai problemi di competenza riconosciuti e accumulare maggiori conoscenze specialistiche interdisciplinari. Data l'indipendenza delle singole autorità federali, questo servizio specializzato, con compiti di assistenza e consulenza, non dispone della facoltà di impartire istruzioni a tutte le autorità. Nelle sue disposizioni esecutive, il Consiglio federale disciplinerà la collocazione e i compiti dettagliati del servizio specializzato;*
  - *Conferenza degli incaricati della sicurezza delle informazioni: quest'organo serve principalmente a garantire un'esecuzione della legge uniforme e valida per tutte le autorità. All'occorrenza saranno consultati anche esperti provenienti dai Cantoni, dal mondo scientifico o dall'economia privata;*
  - *servizi specializzati per i controlli di sicurezza relativi alle persone: per garantire l'indipendenza dei controlli, il Consiglio federale impiegherà come finora almeno due servizi specializzati;*
  - *servizio specializzato per la sicurezza aziendale: per lo svolgimento della procedura di sicurezza relativa alle aziende, il Consiglio federale deve impiegare un servizio specializzato.*

<u>Ripercussioni</u>

La legge consentirà di migliorare in modo sostanziale la gestione della sicurezza delle informazioni in seno alla Confederazione e, pertanto, di ridurre i relativi rischi, in parte anche di natura finanziaria. L'esperienza insegna che, a medio termine, una gestione efficiente della sicurezza delle informazioni può addirittura consentire risparmi in termini di costi. Per la Confederazione, tuttavia, la legge avrà anche ripercussioni dirette a livello finanziario e di personale. Al momento non è ancora possibile procedere a una stima esatta del fabbisogno supplementare, che sarà illustrato in maniera trasparente nel messaggio. I principali fattori di costo sono i seguenti:

- *l'organizzazione, la gestione e il controllo della sicurezza delle informazioni;*
- *il rafforzamento dei controlli e degli audit;*
- *i controlli di sicurezza relativi alle persone;*
- *la procedura di sicurezza relativa alle aziende;*
- *l'istituzione di un servizio specializzato della Confederazione per la sicurezza delle informazioni e i relativi compiti.*

Va osservato che la legge stessa non fissa quasi nessuna misura dettagliata e che, pertanto, non è direttamente attuabile. Le autorità federali interessate devono emanare le proprie disposizioni esecutive. Per valu-

tare i costi d'esecuzione saranno quindi determinanti il livello di sicurezza, che dovrà essere definito dalle autorità stesse, e le conseguenti misure organizzative, in materia di personale, tecniche ed edili decise dalle autorità federali a livello di ordinanze, istruzioni o progetti sulla base di adeguate analisi «costi-benefici».

Le ripercussioni sui Cantoni saranno esigue, mentre l'economia e la società non verranno praticamente toccate dall'avamprogetto.

Indice

Atti normativi citati con l'abbreviazione

Cost.	Costituzione federale della Confederazione Svizzera del 18 aprile 1999; RS **101**
CP	Codice penale svizzero del 13 giugno 1937; RS **311.0**
CPM	Codice penale militare del 13 giugno 1927; RS **321.0**
CPP	Codice di diritto processuale svizzero del 5 ottobre 2007; RS **312.0**
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**
LAEI	Legge federale del 23 marzo 2007 sull'approvvigionamento elettrico; RS **734.7**
LAPub	Legge federale del 16 dicembre 1994 sugli acquisti pubblici; RS **172.056.1**
LAr	Legge federale del 26 giugno 1998 sull'archiviazione; RS **152.1**
LATer	Legge federale del 15 dicembre 2000 sui medicamenti e i dispositivi medici, Legge sugli agenti terapeutici; RS **812.21**
LBN	Legge federale del 3 ottobre 2003 sulla Banca nazionale svizzera, Legge sulla Banca nazionale; RS **951.11**
LENu	Legge federale del 21 marzo 2003 sull'energia nucleare; RS **732.1**
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**
LSIC	Legge federale del 3 ottobre 2008 sul servizio informazioni civile; RS **121**
LSIM	Legge federale del 3 ottobre 2008 sui sistemi d'informazione militari; RS **510.91**
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**
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**
OCSP	Ordinanza del 19 dicembre 2001 sui controlli di sicurezza relativi alle persone; RS **120.4**
OCSPN	Ordinanza del 9 giugno 2006 sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari; RS **732.143.3**
OIAF	Ordinanza del 9 dicembre 2011concernente l'informatica e la telecomunicazione nell'Amministrazione federale, Ordinanza sull'informatica nell'Amministrazione federale; RS **172.010.58**
OPrl	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**
PPM	Procedura penale militare del 23 marzo 1979; RS **322.1**
	Legge federale del 23 giugno 1950 concernente la protezione delle opere militari; RS **510.518**
	Legge federale del 7 ottobre 2005 sulle finanze della Confederazione; RS **611.0**
	Ordinanza del 29 agosto 1990 sulla procedura di tutela del segreto in occasione di mandati con contenuto classificato dal punto di vista militare, Ordinanza sulla tutela del segreto; RS **510.413**
	Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati; RS **235.11**

1 Parte generale

1.1 Situazione iniziale

1.1.1 Evoluzione della Svizzera verso una società dell'informazione

Da alcuni decenni, il mondo sta vivendo un profondo mutamento sociale, indotto dallo sviluppo, tuttora in fase di accelerazione, delle tecnologie dell'informazione e della comunicazione (TIC). 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 ecc. Questi sviluppi sono contemporaneamente un'ineluttabile manifestazione collaterale e una condizione imprescindibile dell'incalzante globalizzazione. Tutte le società odierne sono più interconnesse, mobili e 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 alle TIC 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 come mezzo di scambio della società dell'informazione. La perdita, il furto, la divulgazione e l'abuso di informazioni o la perturbazione dei mezzi che servono a trattarle possono pregiudicare gravemente interessi pubblici essenziali o i diritti di terzi, comportare pesanti conseguenze finanziarie e addirittura compromettere l'adempimento di compiti critici della Confederazione. Inoltre, se incidenti gravi o ripetuti mettono in dubbio la diligenza della Confederazione nel proteggere le proprie informazioni, può risentirne in modo duraturo anche la fiducia che la popolazione e i partner esteri della Svizzera ripongono nelle autorità federali.

1.1.1.1 Strategia per una società dell'informazione in Svizzera

Il Consiglio federale è consapevole della fondamentale importanza delle TIC per la Svizzera in quanto piazza economica e ambiente di vita. Già nel 1998 aveva adottato una Strategia per una società dell'informazione in Svizzera, che è stata successivamente aggiornata nel 2006 e nel 2012 (FF 2012 3353). Intendendo sfruttare le opportunità derivanti dall'applicazione delle TIC, il Consiglio federale ha stabilito che tali tecnologie devono essere impiegate in modo tale da rafforzare il benessere comune, lo sviluppo sostenibile, la coesione interna e la diversità culturale del Paese. La strategia definisce i settori d'intervento nei quali il potenziale innovatore delle TIC può dare i migliori frutti e gli ambiti d'intervento prioritari della Confederazione.

Con la suddetta strategia, il Consiglio federale persegue due obiettivi strategici generali:

- le TIC rendono la piazza economica svizzera innovativa e competitiva sul piano internazionale;
- le TIC sono impiegate a favore di tutti e rendono attrattivo l'ambiente di vita in Svizzera.

In relazione con la trasformazione sociale in atto, il Consiglio federale ha commissionato numerosi progetti (per es. e-government, e-justice, e-health, Gestione elettronica degli affari [GEVER] ecc.). Inoltre, ha impartito al Dipartimento federale di giustizia e polizia (DFGP) diversi mandati per l'elaborazione delle basi legali necessarie nell'ambito della Strategia per una società dell'informazione in Svizzera. 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.

1.1.1.2 Principio di trasparenza dell'Amministrazione federale

Nel suo messaggio del 12 febbraio 2003 concernente la legge federale sulla trasparenza dell'amministrazione (messaggio LTras; FF 2003 1783), il Consiglio federale aveva riconosciuto che il principio 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, il 17 dicembre 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 possiede 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.

1.1.1.3 Open Government Data (OGD)

La nozione di OGD (dati liberamente accessibili dell'amministrazione pubblica) è strettamente legata al principio di trasparenza e 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.

Nel suo rapporto del 13 settembre 2013 in adempimento del postulato Wasserfallen 11.3884 del 29 settembre 2011 («Il libero accesso ai dati governativi, priorità strategica nell'ambito del governo elettronico»), il Consiglio federale ha sottolineato come, dalla ponderazione delle opportunità e dei rischi legati agli OGD, emerga un interessante potenziale di efficienza e trasparenza nella gestione dell'amministrazione nonché di creazione di valore aggiunto a livello economico. Ha inoltre incaricato l'Organo direzione informatica della Confederazione (ODIC) di assumere, in collaborazione con l'Archivio federale svizzero (AFS), la responsabilità e il coordinamento delle attività relative all'ulteriore sviluppo degli OGD come pure di formulare una strategia OGD svizzera.

1.1.2 Rischi della società dell'informazione

Il Consiglio federale intende ridurre il rischio che la trasformazione sociale avvenga ai danni della popolazione e dell'economia o che porti alla violazione dei diritti della personalità. In particolare, esistono rischi che non riguardano primariamente le ripercussioni della trasformazione sociale (per 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'abuso 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 TIC 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 criticità aziendale, comportare pesanti conseguenze finanziarie. Se riguarda il gestore di un'infrastruttura che fornisce servizi indispensabili per il funzionamento della società, dell'economia o della Confederazione (infrastruttura critica), un simile mancato funzionamento può avere, nel caso peggiore, conseguenze catastrofiche, compresa la perdita di vite umane.

1.1.2.1 Pericoli per informazioni e mezzi TIC

I media riportano pressoché quotidianamente notizie di spionaggio, attentati, mancato funzionamento di servizi TIC e altri eventi nell'ambito della sicurezza delle informazioni. Tali pericoli vengono descritti anche nella Strategia nazionale del 27 giugno 2012 per la protezione della Svizzera contro i rischi informatici (FF 2013 499, denominata Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) nell'apposito sito Internet della Confederazione; cfr. n. 1.1.2.2). 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 del settore tendono spesso a esagerare 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 online (in particolare carte bancarie e di credito) o ricattare privati cittadini, ma si tratta di mezzi minimi in confronto 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 l'ulteriore sviluppo della propria economia o per la modernizzazione delle loro forze armate.

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 o privati è infatti minacciata a causa della dipendenza di tali infrastrutture e servizi dalle TIC. Sebbene, a questo proposito, tra gli ipotetici pericoli vengano citate soprattutto le azioni di sabotaggio, come l'attacco scoperto nel giugno del 2010 contro gli impianti iraniani di arricchimento dell'uranio mediante il software dannoso (malware) *Stuxnet*, i problemi di funzionamento causati da guasti tecnici, manipolazioni inappropriate o fenomeni atmosferici, come per esempio un'interruzione di corrente o un incendio, sono molto più frequenti e possono avere conseguenze altrettanto gravi.

Non va infine dimenticata la sorveglianza di massa del traffico Internet, in particolare tramite la compromissione di servizi TIC e applicazioni di ampia diffusione nonché mediante la corruzione sistematica di standard di cifratura. Le ultime rivelazioni in merito a tali pratiche dimostrano che le ipotesi di fondo sull'integrità di

Internet e dei servizi di base, sostenute da molti in relazione al trattamento sicuro delle informazioni, non corrispondono a verità.

Si sta verificando una «corsa agli armamenti digitali». La maggior parte dei Paesi sviluppati è consapevole della propria dipendenza dalle infrastrutture di informazione e di comunicazione e, pertanto, dell'esposizione alle relative minacce. Per questo attuano apposite misure di protezione. Tuttavia, non tutti gli Stati perseguono strategie puramente *difensive*. Al contrario, molti di essi stanno sviluppando capacità *offensive* a livello militare e nell'ambito dei servizi informazioni. 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 non sempre si tratta di attività particolarmente complicate e costose o che richiedono impianti di grandi dimensioni, sono molti gli informatici, i matematici e gli altri esperti in campo tecnologico che lavorano instancabilmente per sviluppare nuovi programmi di protezione o malware. Visti i mezzi impiegati 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 al trattamento elettronico delle informazioni 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 TIC 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 in larga misura 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 tra le persone o trattate su carta. I rischi legati a tale procedura non dovrebbero essere ignorati se si vuole garantire la sicurezza delle informazioni.

1.1.2.2 Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)

Il Consiglio federale, in collaborazione con le autorità, l'economia privata e i gestori di infrastrutture critiche, intende 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.

Il Consiglio federale persegue i seguenti obiettivi:

- individuazione precoce delle minacce e dei pericoli nel cyberspazio;
- incremento della resistenza delle infrastrutture critiche agli attacchi;
- riduzione efficace dei cyber-rischi, segnatamente per quanto concerne la cyber-criminalità, il cyber-spionaggio e il cyber-sabotaggio.

Il Consiglio federale intende approfondire la collaborazione tra le autorità e l'economia nel campo del cyberspazio e rafforzare ulteriormente le fondamenta già poste. Fa dunque leva sulle strutture esistenti e rinuncia a istituire un organo centrale di gestione e coordinamento nazionale sul modello di quelli che vengono attualmente creati in altri Paesi. La SNPC enuncia le misure e i settori d'intervento previsti per ridurre i cyber-rischi sul piano nazionale. A tale scopo è stata potenziata la 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. Il Consiglio federale ha inoltre dato incarico ai dipartimenti di procedere, sia a livello dipartimentale 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 TIC critiche fino a una migliore tutela degli interessi svizzeri sul piano internazionale. Il coordinamento e l'attuazione della SNPC sono stati affidati a un organo di coordinamento istituito in seno al Dipartimento federale delle finanze (DFF). La Strategia nazionale per la protezione delle infrastrutture critiche è illustrata al numero 3.5.3.

1.1.2.3 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. Nell'ambito dei propri compiti legali, la Confederazione tratta quotidianamente grandi quantità

di informazioni, tra cui anche informazioni che risultano particolarmente sensibili 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 riguardava principalmente l'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 e così via. 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 conforme alla legge, adeguato allo scopo e proporzionato, nonché protetti con misure organizzative e tecniche. In caso di abuso in materia di dati personali, i diritti della personalità degli interessati possono essere gravemente violati. Certi dati personali sono ricercati tanto quanto le informazioni tecnologiche dell'industria. Il loro valore finanziario non dovrebbe essere sottovalutato. L'acquisizione e la rivelazione di dati riferiti alle persone sono infatti oggetto di un fiorente mercato.

Il verificarsi di incidenti gravi o ripetuti può pregiudicare seriamente la fiducia riposta nelle autorità federali. Questa sfiducia può inoltre addirittura privare la Confederazione di importanti informazioni fintanto che non comprovi di poter garantire in modo affidabile la loro protezione.

Questi rischi per la Confederazione non sono ipotesi astratte e improbabili. Nel mese di ottobre del 2009, nel Dipartimento federale degli affari esteri (DFAE) è stato per esempio individuato un malware finalizzato ad attività di spionaggio e rimasto occultato per molto tempo dopo essere giunto nella rete attraverso la posta elettronica. Negli anni precedenti, anche l'impresa parastatale d'armamento RUAG e la ditta Mowag avevano subito un attacco simile. Non vanno inoltre dimenticate le minacce derivanti da collaboratori della Confederazione. A tale proposito, nel maggio del 2012 è stato scoperto un grave furto di dati presso il Servizio delle attività informative della Confederazione (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 Servizio. Prima di essere arrestato, il collaboratore in questione aveva già tentato di vendere i dati sottratti.

Spesso si verificano inoltre fatti meno gravi quali il furto o lo smarrimento di computer portatili o smartphone nonché la perdita di supporti di informazioni classificati, la divulgazione non autorizzata, perlopiù a scopo politico, di informazioni degne di protezione, 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 comunicata agli organi specializzati affinché possano effettuare una valutazione, è difficile stimare i danni complessivi subiti dalla Confederazione.

1.1.3 Mandati del Consiglio federale

Durante l'elaborazione dell'avamprogetto si è dovuto tenere conto di numerose proposte formulate dal Consiglio federale in merito alla sicurezza delle informazioni. Qui di seguito sono riportate soltanto le proposte che hanno influito in maniera sostanziale sull'avamprogetto di legge.

1.1.3.1 Adozione dell'ordinanza sulla protezione delle informazioni e mandato d'esame del Consiglio federale

A metà del 2007 il Consiglio federale ha adottato la nuova ordinanza sulla protezione delle informazioni (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. Il terzo livello di classificazione introdotto dall'OPrI, vale a dire il livello AD USO INTERNO, ha inoltre consentito di semplificare il trattamento di gran parte delle informazioni classificate, facilitando al tempo stesso anche la collaborazione internazionale, in particolare con l'Unione europea.

L'OPrI è stata concepita come atto normativo transitorio e, di conseguenza, la sua validità temporale è limitata. Contemporaneamente all'adozione di questa ordinanza, il Consiglio federale ha incaricato il Dipartimento federale della difesa, della protezione della popolazione e dello sport (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.

1.1.3.2 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.

Il Consiglio 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 trasmesso per conoscenza ai membri del Consiglio federale il 2 dicembre 2011[1].

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

Il rapporto sull'esecuzione e sull'efficacia dell'OPrI nonché sui costi occasionati dalla sua attuazione, richiesto dal Consiglio federale contemporaneamente all'adozione dell'ordinanza in questione, ha evidenziato che, nella maggior parte dei casi, il periodo transitorio in essa previsto per la realizzazione degli adeguamenti tecnici necessari a garantire la protezione delle informazioni, ossia fine 2009, non era stato rispettato. Sussistevano dunque considerevoli lacune, soprattutto riguardo alla protezione elettronica delle 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 della Confederazione. Il nuovo disciplinamento doveva in particolare:

- estendere il campo d'applicazione delle norme sulla protezione delle informazioni a tutte le persone che la Confederazione incarica di trattare informazioni protette;
- creare basi legali formali unitarie per lo svolgimento di procedure 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, durante l'elaborazione dell'avamprogetto, se e in quale misura sussistessero, in materia di protezione delle informazioni, altri problemi materiali da includere in una base legale formale e se le competenze e le responsabilità nell'ambito della sicurezza delle informazioni fossero conformi ai requisiti attuali.

1.1.3.4 Decisione del Consiglio federale concernente la raccomandazione 12 della Commissione della gestione del Consiglio degli Stati (CdG-S) in relazione con la crisi diplomatica tra la Svizzera e la Libia

Nell'ambito della verifica della gestione della crisi diplomatica tra la Svizzera e la Libia, la CdG-S ha riscontrato una serie di problemi a livello di protezione delle informazioni. Nel suo rapporto del 3 dicembre 2010, 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 fede-*

1 www.efk.admin.ch/images/stories/efk_dokumente/publikationen/querschnittspruefungen/QP%20%2816%29/11387BE_Publikation.pdf (*testo in tedesco con riassunto in italiano*)

rale veglierà con la dovuta attenzione anche agli aspetti tecnici degli apparecchi messi a disposizione dei collaboratori[2]*.»*
Il Consiglio federale ha quindi deciso di prendere misure per ovviare alle carenze di carattere organizzativo e tecnico riscontrate[3].

1.1.3.5 Completamento del mandato del Consiglio federale

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 da porre direttamente in consultazione. 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 delle informazioni alla sicurezza delle informazioni. Ha inoltre incaricato il DDPS di coordinare i lavori legislativi con i mandati inerenti all'elaborazione di una strategia in materia di «cyber defense» e alla Strategia per una società dell'informazione in Svizzera.
In seguito all'estensione del campo oggetto della normativa e all'esigenza di un coordinamento con i progetti summenzionati, è stato ampliato il gruppo di esperti, formato ora da rappresentanti di: CaF, DFAE, DFGP (SG, UFG, fedpol), DDPS (SG, Stato maggiore dell'esercito), DFF (SG, ODIC, UFIT), DATEC (UFCOM), IFPDT, Servizi del Parlamento, tribunali della Confederazione e Cantoni (CSI). Occasionalmente è stato interpellato anche il Servizio delle attività informative della Confederazione (SIC).

1.1.3.6 Mandato del Consiglio federale per l'armonizzazione e lo snellimento dei controlli di sicurezza relativi alle persone

Il 1° febbraio 2012 il Consiglio federale ha incaricato il DDPS di prendere in esame 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 gruppo di lavoro interdipartimentale istituito a tal fine (GLID CSP), il 29 novembre 2013 il Consiglio federale ha tra l'altro incaricato il gruppo di lavoro responsabile dell'elaborazione della legge sulla sicurezza delle informazioni (GLID LSIn) di tenere conto delle raccomandazioni del rapporto nei propri lavori e, laddove opportuno, di farle confluire nell'avamprogetto di legge (cfr. numero 1.2.4).

1.1.3.7 Mandato aggiuntivo e trasformazione del gruppo di esperti in gruppo di lavoro interdipartimentale (GLID LSIn)

In seguito alla scoperta di un increscioso episodio avvenuto in seno al SIC, il 24 ottobre 2012 il gruppo di esperti è stato incaricato dal Consiglio federale di elaborare un rapporto su rischi e lacune nella sicurezza delle informazioni dell'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 ampliato con rappresentanti del DFI e del 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).

1.2 Punti essenziali del nuovo disciplinamento proposto

Qui di seguito vengono riportati il fabbisogno normativo e le soluzioni suggerite per i punti essenziali del nuovo disciplinamento. Il nuovo disciplinamento proposto per l'organizzazione della sicurezza delle informazioni è commentato separatamente (n. 1.3).

Sono in primo luogo necessarie due osservazioni:

- il fabbisogno normativo è dato dalle lacune e dai punti deboli riscontrati dal punto di vista materiale e giuridico nell'ambito della sicurezza delle informazioni. Il fatto di concentrarsi su queste lacune potrebbe far pensare che le direttive, le misure e i processi vigenti finora non siano efficaci, il che non corrisponde assolutamente a verità;

2 Gestione della crisi diplomatica tra la Svizzera e la Libia da parte delle autorità federali, Rapporto della Commissione della gestione del Consiglio degli Stati del 3 dicembre 2010, FF **2011** 3859.

3 Gestione della crisi diplomatica tra la Svizzera e la Libia da parte delle autorità federali, Rapporto della Commissione della gestione del Consiglio degli Stati del 3 dicembre 2010, Parere del Consiglio federale del 20 aprile 2011, FF **2011** 3949-3950.

- di regola, i rapporti dettagliati riguardanti le lacune e i punti deboli nell'ambito della sicurezza delle informazioni sono classificati. Per questo nel presente rapporto non è possibile trattare in maniera più approfondita tutte le lacune e tutti i punti deboli.

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 dalla sicurezza delle procedure e dei mezzi elettronici utilizzati per trattarle. Attualmente, il trattamento elettronico di informazioni di ogni genere degne di protezione presenta importanti lacune in materia di sicurezza.

1.2.1.1 Lacune tecniche

In un rapporto sull'esecuzione e sull'efficacia dell'ordinanza sulla protezione delle informazioni nonché sui costi occasionati dalla sua attuazione (cfr. n. 1.1.3.3), il DDPS ha dimostrato al Consiglio federale come gli obiettivi perseguiti dall'OPrI nel campo del trattamento elettronico di informazioni classificate, per quanto piuttosto modesti se confrontati con la realtà internazionale, nella maggior parte dei casi non possano essere rispettati in quanto le soluzioni e le prestazioni di servizi in materia di sicurezza necessari a tal fine non sono attualmente disponibili o, per ragioni di varia natura, finanziaria in particolare, non vengono utilizzate o proposte. Da questo stato di cose deriva una situazione paradossale: in certe circostanze, collaboratori della Confederazione che nella vita privata non utilizzerebbero mai un servizio di e-banking senza i prodotti e le procedure di sicurezza richiesti dallo stato della tecnica, memorizzano o trasmettono spensieratamente nel loro ambiente di lavoro informazioni classificate CONFIDENZIALE o SEGRETO senza preoccuparsi di cifrarle.

Tale riscontro non riguarda soltanto le informazioni classificate, che già oggi rappresentano soltanto una piccola parte di tutte le informazioni della Confederazione degne di protezione. Lacune simili sono presenti anche nell'ambito della protezione di dati personali, di segreti professionali, d'affari e di fabbricazione nonché di altre informazioni di cui è necessario tutelare la confidenzialità, la disponibilità, l'integrità o la tracciabilità. In caso di accresciute esigenze di protezione, devono essere adottate misure tecniche di sicurezza particolari. Queste misure presuppongono che sia preliminarmente garantita una solida protezione di base a livello di sicurezza informatica. Se non poggiano su un simile fondamento, i provvedimenti tecnici supplementari possono essere facilmente elusi. Le verifiche effettuate dall'UFIT hanno però evidenziato frequenti carenze nell'attuazione delle misure minime previste in tale ambito.

In uno scenario caratterizzato da importanti lacune a livello di protezione elettronica delle informazioni, 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. Questa evoluzione è da ricondurre in particolare alle continue innovazioni tecnologiche, ai nuovi pericoli e punti deboli ad esse legati e alla scarsità delle risorse finanziarie e di personale.

1.2.1.2 Carenze organizzative

Di fronte all'emergere delle suddette sfide in ambito tecnico, la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) aveva annunciato già nel 2008, in occasione del 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[4].»

Queste affermazioni rivestono un'importanza centrale ai fini della comprensione del nuovo disciplinamento proposto. La sicurezza TIC 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 nella gestione della sicurezza delle informazioni e nelle basi legali.

Nell'economia privata, il fatto che la sicurezza sia un affare dei capi e che risulti utile anche dal punto di vista economico viene compreso al più tardi quando si verificano danni e occorre adottare misure atte a contenerli. Spesso, tuttavia, nelle pubbliche amministrazioni 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

4 MELANI Rapporto semestrale 2008/1, http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=it

TIC, non viene in genere né analizzata né ponderata con i costi dell'attuazione di eventuali misure volte a ridurre i rischi.

Per quanto concerne la protezione delle informazioni, si osserva una situazione simile anche a livello di Confederazione. Spesso, per esempio, la sicurezza TIC 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 di sicurezza e le comuni attività direttive (per 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 procedere a 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.

Sussistono carenze anche nel quadro giuridico. In seno alla Confederazione, le basi legali per la protezione delle informazioni sono impostate in modo molto settoriale e risultano scarsamente coordinate nonché, spesso, lacunose. Attualmente, per esempio, la Confederazione gestisce sistemi paralleli, a livello giuridico e organizzativo, per la protezione dei dati, la protezione delle informazioni (protezione di informazioni classificate), la sicurezza informatica, la sicurezza fisica e la gestione dei rischi. Inoltre, i controlli di sicurezza relativi alle persone (cfr. n. 1.2.4) e le procedure di sicurezza relative alle aziende (cfr. n. 1.2.5) si applicano prevalentemente alle persone e alle imprese che trattano informazioni classificate della Confederazione ma non alle persone che amministrano o gestiscono i suoi mezzi TIC critici.

Va altresì osservato che non sempre le basi legali sono in linea con le esigenze pratiche legate al trattamento elettronico delle informazioni. A titolo di esempio:

- i segreti d'affari e di fabbricazione sono protetti prevalentemente da un obbligo di discrezione (segreto d'ufficio) imposto alle persone incaricate di trattare questo tipo di informazioni. In una società dell'informazione, tuttavia, la tutela del segreto d'ufficio richiede qualcosa di più di un semplice obbligo personale di discrezione. Se vengono registrati elettronicamente, i segreti d'affari e di fabbricazione devono essere protetti anche sul piano organizzativo e tecnico conformemente alle rispettive necessità di protezione. Nella maggior parte dei casi, tuttavia, mancano direttive sul modo di definire, impostare, attuare e verificare questa protezione;
- per quanto riguarda la protezione di dati personali esiste invece un'alta densità normativa. Per le autorità federali, l'accento è posto tuttavia sull'esistenza delle basi giuridiche necessarie per il trattamento legale, appropriato e proporzionato dei dati personali piuttosto che sull'effettiva e concreta gestione di tali dati da parte dei collaboratori (per es. trasmissione, conservazione, distruzione, cifratura ecc.);
- le direttive concernenti la protezione di informazioni classificate contengono numerose contraddizioni rispetto alle prescrizioni in materia di informatica, tra l'altro per quanto concerne il disciplinamento delle competenze e determinate procedure.

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, è necessaria una percezione più chiara dei propri compiti da parte della linea gerarchica e le basi legali devono essere obbligatoriamente armonizzate con le esigenze legate al trattamento elettronico delle informazioni.

1.2.1.3 Nuovo orientamento a una sicurezza integrale delle informazioni

Il Consiglio federale è consapevole delle crescenti interdipendenze tra la protezione tecnica e la protezione organizzativa delle informazioni, come pure delle carenze organizzative summenzionate. Quale misura immediata, ha pertanto deciso di introdurre, per i quadri dell'Amministrazione federale, una formazione sugli aspetti relativi alla sicurezza delle informazioni (cfr. n. 1.1.3.7). In occasione della seduta del 30 novembre 2011, il Consiglio federale ha inoltre affermato che limitare il campo d'applicazione materiale del presente avamprogetto di legge al ristretto ambito della protezione delle informazioni non sarebbe sufficiente a soddisfare il fabbisogno normativo riscontrato. Di conseguenza, ha incaricato il DDPS di impostare secondo un nuovo orientamento i lavori legislativi, mirando a una *sicurezza delle informazioni* completa che tenga conto anche degli aspetti organizzativi e tecnici e fondando il nuovo disciplinamento dell'organizzazione su *standard internazionali riconosciuti*.

Il nuovo orientamento verso una *sicurezza integrale delle informazioni*, richiesto dal Consiglio federale, corrisponde a ciò che, nell'economia privata e in molte pubbliche amministrazioni a livello mondiale, rappresenta già da alcuni anni la *regola dell'arte*. La sicurezza delle informazioni è codificata da alcuni standard internazionali, tra cui in particolare le norme ISO/IEC 27001/27002. Questi standard hanno poco a che vede-

re 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 pratiche (*best practices*), concrete e di provata efficacia, per l'attuazione di misure in materia di personale, tecniche ed edili.

Il presente avamprogetto crea una base legale formale uniforme per la gestione della sicurezza delle informazioni in seno alla Confederazione. Il contenuto e la struttura del presente avamprogetto si basano in larga misura su dette norme e ne perseguono l'attuazione in funzione delle esigenze specifiche. In tale ambito, la sicurezza delle informazioni viene considerata *in base a un approccio integrale*, secondo cui tutte le questioni che la riguardano sono, per quanto possibile, gestite, concretizzate, verificate e migliorate congiuntamente. Per questo l'avamprogetto concentra in un'unico atto normativo le misure organizzative più importanti volte a garantire la protezione delle informazioni e la sicurezza nell'impiego delle TIC. Rispetto all'attuale impostazione settoriale delle strutture giuridiche e organizzative della Confederazione, questo approccio in materia di sicurezza delle informazioni rappresenta un orientamento nuovo e integrale.

1.2.2 Campo d'applicazione

1.2.2.1 Campo d'applicazione materiale

Il campo d'applicazione materiale si evince, di principio, dalla nozione stessa di sicurezza delle informazioni. La protezione deve concentrarsi su tutte le informazioni di competenza delle autorità federali. La legge si applica alle informazioni di qualsiasi genere (per es. non solo a testi, ma anche a rappresentazioni grafiche) e in qualsiasi forma, ossia non soltanto a informazioni elettroniche, ma anche a informazioni su supporto fisico (documenti cartacei). Si tratta principalmente di informazioni prodotte dalle autorità federali stesse, ma sono comprese anche le informazioni che queste ultime ricevono da terzi, assumendosi pertanto anche la responsabilità del loro trattamento sicuro e conforme al diritto. L'avamprogetto riguarda inoltre le informazioni di cui le autorità federali affidano il trattamento a terzi. Limitare il campo d'applicazione materiale implicito alle informazioni sensibili non sarebbe opportuno. Per valutare se un'informazione è sensibile o degna di protezione sono indispensabili criteri e meccanismi di valutazione che, *inevitabilmente*, devono essere applicati a tutte le informazioni.

L'avamprogetto comprende tutti i mezzi TIC che vengono impiegati dalla Confederazione o il cui esercizio viene commissionato da quest'ultima. 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 TIC sono annoverati tra gli *oggetti da proteggere*, vengono anch'essi inclusi espressamente nella LSIn.

1.2.2.2 Campo d'applicazione istituzionale

Per ampi tratti, il presente avamprogetto 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. Nella legge vanno inoltre incluse altre organizzazioni di diritto pubblico o privato che esercitano attività sensibili sotto il profilo della sicurezza su incarico della Confederazione. Ciò corrisponde al mandato del Consiglio federale di estendere il campo d'applicazione delle norme sulla protezione delle informazioni a tutte le persone che la Confederazione incarica di trattare 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 compiti previsti dalla Costituzione e dalla legge, le autorità federali si scambiano regolarmente informazioni, comprese le informazioni classificate o altre informazioni degne di protezione. Attualmente, tuttavia, non applicano un sistema di classificazione uniforme. Inoltre, le misure adottate dalle singole autorità per proteggere tali informazioni sono molto diverse e scarsamente coordinate tra loro. Per questo, in passato, è spesso accaduto che informazioni della Confederazione classificate che erano state trasmesse ad altre autorità federali venissero trattate violando alcune fondamentali prescrizioni di protezione del Consiglio federale. 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. Uno degli obiettivi del Consiglio federale è quello di puntare maggiormente e con più decisione sullo scambio elettronico delle informazioni e sui servizi elettronici (e-government). Saranno quindi sempre più numerose le interfacce comuni tra i sistemi delle diverse autorità federali e aumenterà il rischio che eventuali attacchi e minacce contro una determinata autorità si estendano anche agli ambiti di competenza di altre au-

torità interessate. Per questo è indispensabile che le autorità federali coinvolte applichino criteri e metodi equivalenti per la valutazione del rischio e che nell'impiego delle TIC le rispettive misure di sicurezza organizzative, in materia di personale, tecniche e fisiche siano coordinate tra loro.

Il campo d'applicazione istituzionale non deve limitare l'indipendenza delle autorità interessate, prevista dalla Costituzione. Le autorità federali devono eseguire la legge in maniera autonoma e si rinuncia pertanto all'istituzione di un organo di controllo con la facoltà di impartire istruzioni a tutte le autorità. Lo svantaggio rappresentato dall'esecuzione autonoma è che i requisiti minimi relativi all'organizzazione per la sicurezza delle informazioni, che tutte le autorità federali sono tenute a rispettare, devono obbligatoriamente essere fissati a livello di legge. Di conseguenza, l'avamprogetto contiene anche numerose disposizioni che, dal punto di vista della gerarchia normativa, corrispondono piuttosto al livello di un'ordinanza.

1.2.3 Misure generali in materia di sicurezza delle informazioni

1.2.3.1 Gestione della sicurezza delle informazioni

La sicurezza delle informazioni è affare dei capi. La relativa responsabilità incombe alla direzione dell'autorità in questione e non può essere delegata. In tale ambito, l'avamprogetto fissa determinati obblighi che possono essere adempiuti esclusivamente dalle singole autorità coinvolte. Le massime autorità dovranno per esempio:

- emanare le disposizioni esecutive necessarie per l'esecuzione della presente legge (cfr. art. 87);
- organizzare, dirigere, attuare e verificare la sicurezza delle informazioni secondo lo stato della dottrina (per es. secondo la norma ISO 27001), fissando tra l'altro in modo chiaro i compiti, le competenze e le responsabilità (cfr. art. 5 cpv. 1 lett. a e cpv. 2);
- fissare i loro obiettivi in materia di sicurezza delle informazioni nonché il livello di sicurezza da raggiungere (cfr. art. 5 cpv. 3 lett. a);
- fissare i parametri per la gestione dei rischi (cfr. art. 5 cpv. 3 lett. b);
- stabilire e spiegare le conseguenze in caso di inosservanza delle prescrizioni (cfr. art. 5 cpv. 3 lett. c);
- ordinare la verifica periodica dell'attuazione e dell'efficacia delle misure (cfr. art. 11);
- emanare un elenco delle funzioni da sottoporre al controllo di sicurezza relativo alle persone (cfr. art. 33).

Infine, l'avamprogetto rafforza il ruolo operativo della linea gerarchica nell'ambito dell'impiego delle TIC (cfr. art. 23-26).

1.2.3.2 Gestione dei rischi

Con l'evoluzione in atto verso una società dell'informazione, le minacce e i pericoli che incombono sulle informazioni e sui mezzi TIC sono diventati sempre più complessi e dinamici. Il contesto descritto esige inoltre che le autorità federali si focalizzino maggiormente su una valutazione sistematica delle necessità di protezione delle informazioni e su un'analisi continua dei relativi rischi. Ciò presuppone però una gestione dei rischi efficace nel campo della sicurezza delle informazioni e una verifica periodica dell'attuazione delle misure di riduzione dei rischi. Queste due condizioni sono oggi quasi completamente inadempiute. Viene pertanto avviato anche un processo destinato a garantire in maniera duratura ed economica la sicurezza delle informazioni.

Per le autorità federali, la gestione dei rischi è un'esigenza sia politica che economica. Nell'avamprogetto, le autorità assoggettate sono esortate a stabilire il livello di sicurezza delle informazioni che intendono raggiungere (obiettivi in materia di sicurezza delle informazioni). Tale livello è determinante per la definizione delle misure di sicurezza e per la valutazione della relativa efficacia. In relazione alle gestione dei rischi, le autorità assoggettate devono inoltre stabilire chi può sostenere quali rischi e che cosa accade in caso di rischi residui troppo elevati.

La gestione dei rischi nell'ambito della sicurezza delle informazioni è una questione che presenta specificità proprie al singolo settore, ma deve essere comunque integrata nel processo generale di gestione dei rischi per tutte le autorità assoggettate, poiché, naturalmente, anche i rischi per la sicurezza delle informazioni sono da annoverare tra i rischi commerciali generali.

Nell'ambito della gestione dei rischi vengono valutate le necessità di protezione delle informazioni (riguardo a confidenzialità, integrità, disponibilità e tracciabilità) e si procede all'analisi dei pericoli di origine umana, tecnica o naturale nonché dei corrispondenti punti deboli. La valutazione del rischio deve essere effettuata nel modo più obiettivo e sistematico possibile e le misure necessarie al raggiungimento del livello di sicurezza determinante devono essere fissate dalla linea gerarchica. Infine, occorre garantire la sorveglianza dei rischi identificati.

Strettamente collegata alla gestione dei rischi è anche la cosiddetta gestione della continuità operativa («Business Continuity Management», BCM), volta a garantire l'adempimento dei compiti fondamentali da parte delle autorità entro i termini previsti anche in situazioni straordinarie. Vista la crescente dipendenza dell'adempimento dei compiti dall'impiego delle TIC, i rischi nell'ambito della sicurezza delle informazioni possono mettere a repentaglio l'adempimento di compiti legali critici (cfr. anche art. 6 cpv. 3 LOGA). Di conseguenza, le autorità federali vengono esortate ad allestire appositi piani per la prevenzione di incidenti in materia di sicurezza delle informazioni che possono minacciare l'adempimento di compiti irrinunciabili e a svolgere esercitazioni in tale ambito.

1.2.3.3 Controlli e audit

Ogni singola misura ordinata nel settore della sicurezza delle informazioni deve essere verificabile e verificata. Soltanto grazie a controlli adeguati le autorità e le organizzazioni possono comprendere lo stato della sicurezza delle proprie informazioni, come pure i rischi esistenti e le eventuali misure correttive necessarie. Oggi i controlli 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. Inoltre, data la pressoché totale assenza di controlli, attualmente mancano il know-how e il personale necessari per il loro svolgimento. Occorre pertanto partire dal presupposto che, per adempiere tale compito, le autorità e le organizzazioni assoggettate non potranno fare a meno di impiegare risorse supplementari.

I meccanismi e gli strumenti di controllo devono necessariamente essere rafforzati per tutti i settori della sicurezza delle informazioni. Per questo l'avamprogetto prevede un obbligo di controllo generale (art. 11). Nei casi in cui sono necessari controlli, verifiche e audit mirati, questi ultimi vengono espressamente richiesti (per le TIC: cfr. n. 1.2.3.5). In linea di principio, i controlli e gli audit nell'ambito delle attività correnti dovranno rimanere nella sfera di competenza della linea gerarchica. L'attuazione delle misure ordinate figura tra i compiti fondamentali a livello direttivo. L'avamprogetto rafforza tuttavia anche gli strumenti a disposizione della linea gerarchica per lo svolgimento di audit e controlli nell'ambito della sicurezza delle informazioni. Gli incaricati della sicurezza delle informazioni devono per esempio poter svolgere controlli su mandato della rispettiva autorità. In caso di audit complessi o di controlli indipendenti, le autorità devono inoltre poter affidare il relativo mandato al servizio specializzato della Confederazione per la sicurezza delle informazioni o al Controllo federale delle finanze (CDF).

1.2.3.4 Classificazione delle informazioni

La classificazione è una misura che viene da sempre impiegata da qualsiasi organizzazione per proteggere informazioni interne la cui conoscenza da parte di persone non autorizzate può pregiudicare gli obiettivi perseguiti o addirittura danneggiare l'organizzazione stessa. Attualmente la classificazione delle informazioni viene disciplinata dall'OPrI soltanto per l'Amministrazione federale e l'esercito. Uno degli obiettivi del presente avamprogetto è quello di introdurre un sistema di classificazione valido per tutte le autorità e attuato secondo principi uniformi tenendo conto delle maggiori aspettative dei cittadini per quanto concerne la trasparenza dell'operato delle autorità federali. La classificazione deve pertanto essere concepita come un'eccezione da motivare. È inoltre necessario un parziale innalzamento degli attuali valori soglia per la classificazione.

Il sistema a tre livelli consente di garantire una protezione delle informazioni adeguata ai rischi: quanto maggiore è il rischio per gli interessi pubblici da proteggere, tanto più onerose e costose risulteranno le misure di sicurezza. Il livello di classificazione AD USO INTERNO consente un trattamento più semplice e poco oneroso di informazioni che, pur essendo degne di protezione, non presentano un fabbisogno di protezione tale da giustificare l'onere necessario per il trattamento di informazioni classificate CONFIDENZIALE. Il livello di classificazione AD USO INTERNO garantira un livello di sicurezza uniforme anche nel contesto internazionale. La maggior parte degli Stati utilizza un sistema a quattro livelli (per es. nell'UE: RESTRICTED, CONFIDENTIAL, SECRET e TOP SECRET).

1.2.3.5 Sicurezza nell'impiego delle TIC

Le disposizioni in materia di sicurezza nell'impiego delle TIC sono oggi disciplinate a livello di ordinanza oppure, nella maggior parte dei casi, a livello di istruzioni. A causa della crescente interconnessione dei sistemi TIC e della sempre maggiore dipendenza delle autorità federali da questi mezzi per l'adempimento dei loro compiti legali, da qualche anno a questa parte l'importanza della sicurezza dei mezzi TIC è notevolmente aumentata. Numerosi incidenti avvenuti all'estero o in Svizzera dimostrano la vulnerabilità dei mezzi TIC e le potenziali conseguenze di simili episodi. Oggi è impossibile fare a meno di prevedere a livello di legge formale determinati parametri della sicurezza TIC, in particolare perché l'interconnessione di questi mezzi tra tutte le autorità e lo scambio di informazioni per via elettronica sono destinati a intensificarsi ulteriormente ed esigono pertanto soluzioni e processi comuni a tutte le autorità. Tuttavia, considerata la rapidità

dell'evoluzione tecnologica, la maggior parte delle misure concrete di protezione dovrà continuare a essere definita e fissata a livello di ordinanza o addirittura di istruzioni.

Di regola, i rapporti dettagliati riguardanti le lacune e i punti deboli nell'ambito delle TIC sono classificati. Nonostante la portata limitata del controllo, il primo rapporto di revisione del CDF dopo la decisione del Consiglio federale del 16 dicembre 2009 concernente le misure per aumentare la sicurezza delle informazioni nell'Amministrazione federale fornisce una buona panoramica della necessità d'intervento nel campo dell'impiego delle TIC (cfr. n. 1.1.3.2).

Spesso la sicurezza delle informazioni nell'ambito dell'impiego delle TIC è considerata una questione tecnica. In realtà, l'aspetto tecnico è solo marginale, in quanto la stragrande maggioranza delle misure di sicurezza relative alle TIC è di natura organizzativa. La responsabilità in tale ambito spetta prevalentemente alle autorità e alle organizzazioni che decidono di impiegare le TIC (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.

Il disciplinamento proposto si fonda su processi e procedure che esistono già e che vengono adeguati in funzione del fabbisogno riconosciuto. Oltre al rafforzamento della gestione dei rischi (cfr. n. 1.2.3.2), ciò comprende principalmente quattro aspetti essenziali:

- *chiaro disciplinamento delle competenze e delle responsabilità tra i beneficiari e i fornitori di prestazioni TIC:* la responsabilità principale della sicurezza nell'impiego dei mezzi TIC incombe ai beneficiari di prestazioni, che sono competenti per lo svolgimento della procedura di sicurezza. I fornitori di prestazioni hanno invece la responsabilità di garantire la sicurezza dei mezzi TIC 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;
- *valutazione della criticità dei mezzi TIC da impiegare dal punto di vista delle informazioni che devono essere trattate con tali mezzi e dell'adempimento dei compiti dell'autorità o dell'organizzazione in questione (livelli di sicurezza):* da un lato, l'attribuzione di un mezzo TIC a un determinato livello di sicurezza serve a rendere consapevoli le autorità della criticità delle loro informazioni e dei loro mezzi TIC 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 TIC;
- *rafforzamento del ruolo operativo della direzione dell'autorità o dell'organizzazione assoggettata:* la direzione dell'autorità o dell'organizzazione deve essere coinvolta nella procedura di sicurezza nonché informata tempestivamente sui rischi affinché possa decidere le relative misure. Per questo l'avamprogetto prevede che la messa in esercizio di tutti i mezzi TIC da impiegare venga autorizzata, *sotto il profilo della sicurezza,* dall'autorità o dall'organizzazione in questione. Nel caso in cui la criticità di un mezzo TIC renda necessaria l'elaborazione di un concetto in materia di sicurezza delle informazioni, tale concetto deve essere approvato dall'autorità o dall'organizzazione interessata;
- *rafforzamento dei controlli e delle verifiche:* oltre ai controlli generali (art. 11), l'avamprogetto prevede tre ulteriori verifiche nell'ambito dei mezzi TIC, ossia:
  - *una verifica della conformità:* per ogni mezzo TIC da impiegare occorre verificare se la procedura di sicurezza è stata eseguita conformemente al diritto e se le misure decise sono state attuate. Si tratta pertanto di un controllo della qualità;
  - *una verifica dei concetti in materia di sicurezza delle informazioni:* gli incaricati della sicurezza delle informazioni devono effettuare una verifica di tutti i concetti in materia di sicurezza delle informazioni prima che questi ultimi vengano sottoposti alla direzione per approvazione;
  - *una verifica dell'efficacia per i mezzi TIC maggiormente critici:* prima di autorizzare mezzi TIC per i quali è richiesto il massimo livello di sicurezza («protezione molto elevata») occorre esaminare l'effettiva efficacia delle misure attuate. L'esecuzione di tali verifiche deve essere affidata esclusivamente a revisori qualificati e certificati. Questa verifica dell'efficacia è l'unica misura in grado di fornire un riscontro sull'effettiva sicurezza delle informazioni.

1.2.3.6 Misure riguardanti il personale

Nell'ambito della gestione delle informazioni e dei mezzi TIC, i collaboratori e i terzi incaricati di trattare informazioni della Confederazione 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 settore in cui si registra una particolare necessità d'intervento.

Ai fini della tutela della sicurezza delle informazioni è inoltre di fondamentale importanza prevedere un rilascio restrittivo delle autorizzazioni. Secondo questo principio, per il trattamento delle informazioni e l'accesso a queste ultime, come pure per l'accesso a determinati locali e aree, devono essere concesse esclusivamente le autorizzazioni di cui le persone in questione necessitano effettivamente per adempiere i propri compiti. Le autorizzazioni devono inoltre essere oggetto di verifiche periodiche. Attualmente questa regola, volta in particolare a scongiurare il pericolo di attacchi interni, non viene impiegata e attuata ovunque.

L'avamprogetto fissa pertanto entrambi i principi (formazione e rilascio restrittivo di autorizzazioni) come requisiti minimi riguardanti il personale. Nell'ambito dell'elaborazione delle rispettive disposizioni esecutive, le autorità e le organizzazioni assoggettate dovranno emanare direttive dettagliate.

1.2.3.7 Protezione fisica di informazioni e mezzi TIC

Troppo spesso ci si dimentica di quanto i controlli all'entrata e altre misure di protezione fisica siano efficaci per garantire la sicurezza delle informazioni. In tale ambito, l'avamprogetto fissa il requisito minimo necessario per disciplinare questa protezione.

L'avamprogetto 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 TIC del livello di sicurezza «protezione elevata» o «protezione molto elevata» e che sono pertanto protetti in modo particolare. Queste zone di sicurezza sono diffuse a livello internazionale, mentre risultano pressoché sconosciute in seno alla Confederazione. L'allestimento di zone di sicurezza è concepito non come misura vincolante, bensì come norma potestativa. Per allestire tali zone è necessaria una base legale formale, in quanto le zone di sicurezza possono essere associate a misure che rappresentano una profonda ingerenza nei diritti della personalità (per es. metodi di identificazione biometrici o videosorveglianza permanente). Per l'accesso alle zone di sicurezza può anche essere necessario effettuare previamente un controllo di sicurezza relativo alle persone. 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.

1.2.4 Controlli di sicurezza relativi alle persone

Una delle minacce più sensibili e intense per la sicurezza si verifica quando persone che hanno accesso a informazioni con una classificazione di livello elevato o che amministrano o gestiscono mezzi TIC particolarmente critici commettono atti di tradimento o sabotaggio oppure hanno intenzione di modificare illecitamente le istituzioni statali. Le funzioni sensibili devono quindi essere affidate esclusivamente a persone che offrono le più ampie garanzie possibili sul fatto che non abuseranno della fiducia loro concessa. Tali garanzie non sono date in particolare se una persona presenta indizi di ricattabilità o corruttibilità. L'esperienza insegna che queste due caratteristiche sono in molti casi riconducibili a una situazione preesistente, per esempio difficoltà personali o finanziarie. Un controllo di sicurezza relativo alle persone (CSP) può indicare ai superiori gerarchici eventuali rischi legati al passato della persona controllata o al suo ambiente (cfr. anche il Messaggio concernente la legge federale sulle misure per la salvaguardia della sicurezza interna e sull'iniziativa popolare «S.o.S. - per una Svizzera senza polizia ficcanaso» del 7 marzo 1994, FF 1994 II 1004).

Il CSP è una misura preventiva per la protezione contro attacchi 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 intenzionalmente o per negligenza interessi pubblici essenziali. Al termine del controllo, spetta esclusivamente all'autorità o all'organizzazione competente per l'attribuzione del mandato alla persona interessata o per la sua assunzione decidere se assumersi un eventuale rischio più elevato, se ridurlo ponendo determinate condizioni o evitarlo non assumendo o licenziando la persona interessata. Anche in caso di valutazione positiva da parte del servizio specializzato per i controlli di sicurezza relativi alle persone (servizio specializzato CSP), i superiori gerarchici non vengono in alcun modo svincolati dalla propria 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 i datori di lavoro commissionano prima dell'assunzione di persone destinate a ricoprire funzioni dirigenziali o posizioni chiave.

1.2.4.1 Trasferimento del disciplinamento dalla LMSI nella legge sulla sicurezza delle informazioni

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, ma anche la LENu prevede, all'articolo 24, controlli dell'affidabilità per il personale impiegato dagli esercenti di centrali nucleari. Per lo svolgimento dei controlli, il Consiglio federale ha istituito due servizi specializzati CSP: uno è integrato nel DDPS ed è responsabile della maggior parte dei controlli, mentre l'altro è aggregato amministrativamente alla Cancelle-

ria federale (CaF) e si occupa del controllo dei quadri superiori dell'Amministrazione federale nonché degli impiegati dell'altro servizio specializzato CSP.

Con la prevista legge sulle attività informative, la LMSI verrà quasi totalmente abrogata. Saranno mantenuti soltanto i CSP e i compiti il cui adempimento rientra nella competenza di fedpol. Poiché l'attuale disciplinamento dei CSP nella LMSI è finalizzato *esclusivamente* alla protezione di informazioni (cfr. art. 19 cpv. 1 LMSI), è opportuno spostare tale disciplinamento nella presente legge. È stata presa in esame anche la possibilità di elaborare una legge specifica per i CSP (e per la procedura di sicurezza relativa alle aziende; cfr. n. 1.2.5). Questa variante è stata tuttavia respinta in quanto non conforme all'obiettivo di riunire in un unico atto normativo tutte le misure concernenti la sicurezza delle informazioni della Confederazione.

1.2.4.2 Eliminazione di lacune giuridiche

Con il trasferimento delle disposizioni legali formali concernenti i CSP nel presente avamprogetto si mira a colmare alcune carenze del diritto vigente. Il CSP rappresenta una grave ingerenza nei diritti della personalità delle persone da sottoporre al controllo. Secondo il principio di legalità sancito dalla Costituzione, per tali ingerenze 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 dei criteri per la valutazione del rischio (cfr. art. 42).

Sebbene il disciplinamento dei CSP nella LMSI sia finalizzato esclusivamente alla protezione di informazioni, in passato i motivi atti a giustificare lo svolgimento di un CSP sono stati ampliati *contra legem* nell'OCSP. Per questo si propone di fissare in maniera esaustiva i motivi del controllo nella futura legge sulla sicurezza delle informazioni e di limitarli alle esigenze direttamente legate a tale sicurezza. Nell'avamprogetto, questi motivi del controllo, rigorosamente definiti, sono sussunti nell'espressione *attività sensibile sotto il profilo della sicurezza*. Le seguenti attività rientrano in tale categoria:

- il trattamento di informazioni classificate «CONFIDENZIALE» o «SEGRETO» oppure la gestione del materiale classificato in maniera corrispondente;
- l'amministrazione, l'esercizio, la manutenzione o la verifica di mezzi TIC del livello di sicurezza «protezione elevata» oppure «protezione molto elevata»»;
- l'accesso a zone di sicurezza, in particolare alle zone di protezione 2 o 3 di un impianto secondo la legislazione sulla protezione di impianti militari.

Alcuni dei motivi del controllo attualmente in vigore vengono pertanto stralciati senza sostituzione. È in particolare il caso del motivo, applicato finora, dell'accesso regolare a dati personali degni di particolare protezione, la cui divulgazione potrebbe gravemente pregiudicare i diritti individuali delle persone interessate (cfr. art. 19 cpv. 1 lett. e LMSI). Nella prassi è infatti pressoché impossibile determinare quali informazioni rientrino nel campo d'applicazione di tale disposizione.

Qualora, per ragioni di sicurezza, sia necessario svolgere un controllo anche per altre attività, occorrerà disciplinare i motivi del controllo nella legislazione speciale. Per poter garantire una distinzione chiara tra il CSP basato sulla legge sulla sicurezza delle informazioni e quello disciplinato da altri atti normativi è indispensabile utilizzare per quest'ultimo una terminologia diversa, ossia *verifica dell'affidabilità*. Nell'allegato viene pertanto proposta una modifica della legge sul personale federale (LPers) e della legge militare (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.

Una questione controversa è stata quella di stabilire se, ai fini dell'iscrizione di una determinata funzione nell'elenco delle funzioni da sottoporre al controllo, fosse sufficiente anche aver svolto una sola volta un'attività sensibile sotto il profilo della sicurezza o se fosse opportuno mantenere il principio della *regolarità* contemplato dal sistema attuale (cfr. art. 19 cpv. 1 LMSI). Il criterio della regolarità si fonda tra l'altro sulla valutazione del Servizio delle attività informative della Confederazione, 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 anche 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. Ciò può avvenire, per esempio, quando la persona in questione divulga pubblicamente informazioni concernenti la strategia negoziale della Svizzera in questioni di particolare importanza. Il pregiudizio in sé non deriva pertanto unicamente dalla regolarità dell'accesso, ma anche dal contenuto delle informazioni. Inoltre, il termine *regolare* non è univoco e, nell'ambito del diritto vigente, ha spesso dato luogo a interpretazioni non uniformi.

Per tale ragione, nell'avamprogetto i presupposti materiali per l'iscrizione di una funzione nell'elenco delle funzioni da sottoporre al controllo e, di conseguenza, per lo svolgimento di un controllo di sicurezza relativo alle persone sono leggermente diversi rispetto a quelli contemplati dal sistema attuale. A livello di basi legali formali si prevede in particolare di tralasciare il criterio della regolarità, soprattutto per quanto concerne il trattamento di informazioni classificate. Ai fini dell'assoggettamento degli impiegati della Confederazione ai CSP è infatti più importante sapere se, per l'adempimento dei propri compiti, la persona che occupa una determinata funzione *deve* trattare informazioni classificate CONFIDENZIALE o SEGRETO o provvedere all'amministrazione, all'esercizio, alla manutenzione o alla verifica di mezzi TIC 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 previsti dalla funzione in questione, allora (e solo allora) tale funzione va inserita nell'elenco delle funzioni da sottoporre al controllo. Questo approccio corrisponde al principio del rilascio restrittivo di autorizzazioni (art. 29) e al principio della necessità di sapere (*need to know*), applicato per il trattamento delle informazioni classificate (art. 15 cpv. 1).

Per il resto, l'attuale disciplinamento è stato modificato in particolare nei seguenti punti:

- *natura giuridica della dichiarazione rilasciata*: l'articolo 22 OCSP prevede che, una volta concluso il controllo di sicurezza relativo alle persone, i servizi specializzati CSP emanino una decisione secondo l'articolo 5 PA. La valutazione dell'eventuale rischio per la sicurezza da parte dei servizi specializzati CSP non corrisponde però alla definizione giuridica di decisione, poiché non influisce direttamente *in senso giuridico* né sui diritti né sugli obblighi e sullo statuto della persona interessata. In effetti, il servizio competente per l'assegnazione dell'attività sensibile sotto il profilo della sicurezza non è vincolato dalla dichiarazione dei servizi specializzati CSP (cfr. art. 46) e la persona da sottoporre al controllo non ha il diritto di essere assunta, di farsi attribuire una determinata funzione o di farsi aggiudicare un mandato. Dal punto di vista giuridico, le valutazioni dei servizi specializzati CSP configurano pertanto un atto materiale ai sensi dell'articolo 25*a* PA (per quanto concerne la tutela giurisdizionale, cfr. art. 51);
- *dichiarazione di sicurezza con riserva e non vincolata*: se sussiste un rischio relativo per la sicurezza che può essere limitato in misura sufficiente imponendo alla persona interessata determinate misure o condizioni, i servizi specializzati CSP emettono una dichiarazione di sicurezza con riserva (invece che «vincolata» come sinora). Gli stessi servizi specializzati CSP non impongono condizioni, ma formulano proposte in tal senso. La nuova formulazione palesa innanzitutto che i servizi specializzati CSP esprimono una riserva sulla dichiarazione di sicurezza. In secondo luogo, sottolinea chiaramente il puro carattere di raccomandazione che la riserva assume per l'autorità o l'organizzazione competente per l'attribuzione dell'attività o della funzione sensibile sotto il profilo della sicurezza. Incombe a questo servizio definire eventuali condizioni pertinenti;
- *stralcio del divieto di raccogliere dati sull'esercizio dei diritti costituzionali contemplato dall'articolo 20 capoverso 1 LMSI:* anche se il senso e lo scopo di questa disposizione sono chiari e adeguati, il divieto in questione non è applicabile nella pratica. Uno dei diritti costituzionali di ogni persona è, per esempio, il diritto al matrimonio. Nell'ambito della raccolta dei dati, tuttavia, vengono naturalmente rilevati anche dati concernenti lo stato civile, cosa che, in realtà, sarebbe vietata in virtù della suddetta disposizione della LMSI. Con il disciplinamento vigente si intende soltanto impedire che, per quanto concerne la sicurezza, le persone vengano escluse a causa delle proprie opinioni politiche. Per questo l'avamprogetto introduce l'obbligo di motivare sempre l'ipotesi di un rischio per la sicurezza indicando fatti concreti connessi alla situazione personale della persona sottoposta al controllo. L'ipotesi di un rischio per la sicurezza non può pertanto essere motivata né dall'estremismo, di sinistra o di destra, né da altre opinioni politiche o ideologie se, *in tale contesto*, le persone interessate non hanno agito illegalmente (cfr. art. 42);
- *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, è stata sollevata la questione di stabilire quali fossero le informazioni o le attività che, secondo il diritto svizzero, potrebbero 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 secondo l'articolo 11 OCSP. In seno alla Confederazione non esiste tuttavia un livello di classificazione «SEGRETISSIMO» («TOP SECRET») per il quale po-

trebbe eventualmente essere richiesto un controllo secondo l'articolo 12 OCSP. Pertanto, al fine di adeguare il diritto vigente al sistema di classificazione della LSIn e di semplificare le modalità di controllo, 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 tuttavia riorganizzata e se necessario completata per garantire una maggiore efficacia dei CSP (cfr. art. 39).

È stato oggetto di discussioni anche il sistema che prevede un elenco delle funzioni emanato mediante un'apposita base legale e che comporta i seguenti svantaggi: gli elenchi richiedono un allestimento particolarmente oneroso, non sono praticamente armonizzati tra i dipartimenti e la Cancelleria federale e, in seguito a riorganizzazioni e a cambiamenti delle denominazioni delle varie funzioni, devono continuamente essere adeguati. Gli elenchi risultano inoltre problematici per motivi di sicurezza, poiché forniscono una panoramica completa 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. Presentano tuttavia anche 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 di emanare le proprie disposizioni esecutive, il Consiglio federale può eventualmente valutare se sia opportuno pubblicare gli elenchi senza alcuna restrizione.

Nell'ambito dei lavori inerenti alla revisione è sorta infine la questione di sapere se in futuro i servizi specializzati CSP dovessero essere automaticamente avvisati qualora, dopo la conclusione del CSP, nel casellario giudiziale o in altre banche dati rilevanti per i controlli di sicurezza fossero state registrate nuove iscrizioni riguardanti le persone controllate. Tecnicamente, un'informazione automatica di questo tipo sarebbe senz'altro realizzabile, previo adeguamento delle relative basi legali. Inoltre, potrebbe aumentare sensibilmente la sicurezza, poiché consentirebbe di constatare rapidamente nuovi rischi per la sicurezza stessa. Tuttavia, tale informazione automatica significherebbe anche che i servizi specializzati CSP dovrebbero informare il servizio che chiede l'avvio del controllo o il servizio competente per l'attribuzione dell'attività sensibile sotto il profilo della sicurezza affinché essi possano disporre la ripetizione del CSP. Una simile soluzione modificherebbe in modo sostanziale la funzione del CSP stesso, imponendo in un certo senso una sorveglianza permanente della persona controllata. Per questi motivi si è rinunciato a disciplinare l'informazione automatica dei servizi specializzati CSP.

1.2.4.3 Riduzione e armonizzazione dei CSP

Nell'ambito dell'elaborazione del primo elenco di persone da controllare conformemente all'ordinanza del 15 aprile 1992 relativa ai controlli di sicurezza nell'Amministrazione federale, il Consiglio federale aveva deciso, sulla base di riflessioni politiche, di sottoporre al controllo un numero il più possibile ristretto di funzioni, prevedendo un elenco di 1200 funzioni in totale (cfr. messaggio sulla LMSI). Dall'entrata in vigore della LMSI, nel 1998, tuttavia, il numero delle persone controllate ogni anno è progressivamente aumentato. Solo nel 2012 sono stati per esempio effettuati complessivamente più di 75 000 CSP. Di questi, oltre 60 000 sono stati condotti su persone soggette all'obbligo di leva e militari, includendo anche la valutazione del potenziale di violenza recentemente introdotta nell'articolo 113 LM. Ciò ha reso necessario un aumento periodico delle risorse dei servizi specializzati CSP.

L'avamprogetto di legge prevede diverse misure che, nella loro totalità, dovranno contribuire a ridurre il numero dei CSP da effettuare:

- le attività che devono essere sottoposte al controllo sono definite in modo più chiaro rispetto a quanto avviene nella LMSI e i motivi del controllo sono strettamente limitati alle esigenze in materia di sicurezza delle informazioni;
- anche con la riduzione a due livelli di controllo si mira a far sì che il controllo ampliato venga svolto soltanto sulle persone che devono effettivamente trattare informazioni classificate SEGRETO o svolgere attività con un livello di sensibilità corrispondente. Nel 2012 sono stati svolti più di 28 000 CSP ampliati, il che farebbe supporre che oltre 28 000 persone abbiano accesso a informazioni classificate SEGRETO. Ciò non è tuttavia assolutamente possibile, motivo per cui il numero di CSP da effettuare per questo livello dovrebbe risultare nettamente inferiore;
- tra i compiti di controllo degli incaricati della sicurezza delle informazioni (cfr. art. 84) figura anche quello di verificare se l'iscrizione di una funzione nell'elenco delle funzioni da sottoporre al controllo è conforme al diritto.

In seguito all'innalzamento del valore soglia per l'esecuzione di controlli di sicurezza relativi alle persone, che si mira a ottenere con le misure summenzionate, determinate esigenze di sicurezza non saranno più coperte dai CSP. Al fine di evitare che si crei un vuoto in materia di sicurezza è necessario mettere a disposi-

zione dei datori di lavoro altri mezzi più proporzionati per soddisfare le loro più che legittime esigenze in materia di sicurezza. Occorre garantire ai datori di lavoro la facoltà di esigere dai candidati o dagli impiegati un estratto del casellario giudiziale e del registro delle esecuzioni qualora ciò sia indispensabile per la tutela degli interessi dello stesso datore di lavoro. Si propone pertanto una revisione in tal senso della LPers (cfr. art. 20*a* LPers).

1.2.5 Procedura di sicurezza relativa alle aziende

La procedura di sicurezza relativa alle aziende (sinora denominata «procedura di tutela del segreto») mira alla tutela della sicurezza delle informazioni nell'ambito dell'aggiudicazione di mandati da parte delle autorità a terzi (di seguito denominati «aziende») che non sottostanno direttamente alla loro vigilanza. In molti settori, le autorità aggiudicano all'economia privata mandati connessi con attività sensibili sotto il profilo della sicurezza. Nei confronti di determinati mandatari viene svolta una procedura di sicurezza relativa alle aziende allo scopo di garantire la tutela degli interessi secondo l'articolo 1 capoverso 2 anche al di là del campo d'applicazione diretto della legge. La procedura serve, da un lato, a verificare l'affidabilità delle aziende alle quali dovrebbe essere affidato un mandato e, dall'altro, consente di controllare e imporre le misure necessarie alla tutela della sicurezza delle informazioni durante l'esecuzione del mandato. La procedura di sicurezza relativa alle aziende non serve invece a garantire la sicurezza dei prodotti, che spetta ovviamente soltanto al servizio che attribuisce il mandato.
La procedura di sicurezza relativa alle aziende è appropriata e comunemente applicata sul piano internazionale (cfr. per es. l'art. 11 della «decisione del Consiglio, del 31 marzo 2011, sulle norme di sicurezza per la protezione delle informazioni classificate UE[5]» e la sezione VII delle «Regeln und Vorschriften der Europäischen Weltraumorganisation vom 15. Dezember 2011[6]»). In Svizzera viene eseguita sin dalla fine degli anni 1970 per i mandati della Confederazione il cui contenuto è classificato dal punto di vista militare e si fonda sull'ordinanza sulla tutela del segreto. A causa del ristretto campo d'applicazione materiale di questa ordinanza, 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 in settori diversi da quello militare, ma ha anche ripetutamente impedito a imprese svizzere di candidarsi con successo per la partecipazione a progetti classificati non militari all'estero, tra cui per esempio la fabbricazione di documenti d'identità o di mezzi di pagamento per Stati terzi oppure la partecipazione a determinati progetti scientifici. Questa lacuna ha così inciso anche sulla competitività dell'economia svizzera.

A grandi linee, la procedura di sicurezza relativa alle aziende si svolge nel modo seguente: il servizio che attribuisce il mandato 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 (mandante), il servizio specializzato SA fissa innanzitutto i requisiti in materia di sicurezza, dopodiché verifica l'idoneità delle aziende in questione dal punto di vista della sicurezza. Occorre in particolare esaminare 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 servizio che attribuisce il mandato affida quindi l'incarico a un'azienda valutata idonea sotto il profilo della sicurezza. Successivamente, il servizio specializzato SA definisce in un apposito concetto in materia di sicurezza le modalità con cui il mandatario è tenuto ad applicare i requisiti concernenti la sicurezza delle informazioni. Dopo che le misure di sicurezza sono state attuate, al mandatario viene rilasciata la dichiarazione di sicurezza aziendale. Infine, una volta concluso il CSP e in presenza delle necessarie dichiarazioni di sicurezza, il servizio che attribuisce il mandato può mettere a disposizione dell'azienda i mezzi (per es. 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. I dettagli della procedura di sicurezza relativa alle aziende saranno disciplinati dal Consiglio federale mediante ordinanza.

Il disciplinamento presenta in parte un nesso relativamente stretto con il CSP, ma se ne distingue per i seguenti punti essenziali dell'iter procedurale:

- in linea di principio, viene effettuata anche in questo caso una verifica dell'affidabilità dell'azienda. Secondo l'esito della valutazione viene quindi rilasciata una dichiarazione di sicurezza aziendale, la quale

5 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32011D0292:IT:HTML

6 http://esamultimedia.esa.int/docs/eso/esa-reg-004d.pdf (*non disponibili in italiano*)

attesta l'affidabilità dell'azienda e le consente di esercitare in veste di mandatario attività della Confederazione (o di un'autorità estera) sensibili sotto il profilo della sicurezza. La procedura non si limita tuttavia a un «controllo» dell'azienda in senso stretto, ma riguarda anche la definizione delle misure di sicurezza da attuare nell'azienda in relazione al mandato;

- a differenza del CSP, la procedura di sicurezza relativa alle aziende non si conclude semplicemente con il rilascio della dichiarazione di sicurezza, bensì occorre poter verificare in qualsiasi momento il rispetto delle misure stabilite.

1.2.6 Sicurezza delle informazioni nelle infrastrutture critiche

Con decisione del 30 novembre 2011, il Consiglio federale ha incaricato il DDPS di integrare nella presente legge, laddove necessario, il fabbisogno normativo a livello di legge formale derivante dalla Strategia nazionale per la protezione della Svizzera contro i rischi informatici. Poiché in tale Strategia il Consiglio federale ha ribadito il principio del disciplinamento decentralizzato delle infrastrutture critiche (cfr. n. 1.1.2.2), la verifica del fabbisogno normativo a livello di legge formale incombe ai dipartimenti che, nel quadro dell'adempimento dei rispettivi compiti, sono investiti di poteri normativi nei confronti dei gestori di infrastrutture critiche (per es. il DATEC per il settore dell'infrastruttura di comunicazione o per il settore dell'approvvigionamento energetico). Se, in settori specifici, sussiste una necessità d'intervento a livello di legge formale, occorre adeguare la pertinente legislazione speciale.

Vi sono tuttavia determinati compiti che devono essere svolti a livello intersettoriale e che, anche per motivi di efficienza e di costo, non possono essere assunti dai singoli enti regolamentatori decentralizzati. Si tratta in primo luogo dell'appoggio alle varie 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 (nella fattispecie, la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI) è espressamente auspicata dai gestori di infrastrutture critiche. Si è inoltre rivelato particolarmente efficace il partenariato pubblico-privato istituito nel quadro della centrale MELANI, segnatamente grazie alla sua possibilità di accedere alle informazioni del Servizio delle attività informative della Confederazione. Oltre alle informazioni messe a disposizione dalla centrale MELANI, vengono apprezzati soprattutto il mantenimento, da parte dei rispettivi fornitori, del controllo sulle informazioni scambiate in caso di incidente, il carattere volontario della collaborazione nonché l'approccio secondo cui l'appoggio a favore della sicurezza delle informazioni e del processo di gestione dei rischi viene garantito mediante informazioni ed eventualmente raccomandazioni e non prescrivendo misure tramite apposite regolamentazioni.
Questo compito intersettoriale della Confederazione per l'appoggio alle infrastrutture critiche deve essere previsto nella presente «legge trasversale» nella misura in cui sia necessaria al riguardo una base legale formale. Nell'avamprogetto vengono così fissati i compiti fondamentali della centrale MELANI, la quale, per adempierli, deve regolarmente trattare dati personali. Tra questi possono anche figurare (raramente) dati personali degni di particolare protezione. L'avamprogetto crea la base legale formale necessaria per il trattamento di tali dati.

1.2.7 Esecuzione

1.2.7.1 Esecuzione presso le autorità federali

La sfida nel disciplinare l'esecuzione della presente legge consiste nel garantire la sua applicazione secondo criteri il più possibile uniformi. Occorre inoltre applicare costantemente le direttive relative alla sicurezza delle informazioni. Se non si ottiene un'esecuzione uniforme (in particolare nell'ambito della gestione di informazioni classificate o di mezzi TIC), la sicurezza delle informazioni nello scambio di informazioni tra autorità sarà inevitabilmente affetta da lacune. È tuttavia necessario rispettare al tempo stesso l'autonomia delle autorità interessate (Parlamento, Consiglio federale, tribunali della Confederazione, Ministero pubblico della Confederazione, Banca nazionale) 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 (per es. il Consiglio federale).

L'avamprogetto tiene conto di questi requisiti, di per sé contraddittori, con tre meccanismi:

- *clausola di esenzione («opting out») per l'esecuzione:* viene fissato il principio secondo cui ogni autorità esegue autonomamente l'atto normativo nel proprio ambito ed emana il relativo disciplinamento a livello di ordinanza. Le disposizioni esecutive del Consiglio federale devono tuttavia essere applicate per analogia anche alle altre autorità federali fintanto che e nella misura in cui queste ultime non emanano disciplinamenti propri;

- *requisiti e misure standard:* il Consiglio federale sarà abilitato a fissare requisiti e misure standard, conformi allo stato della dottrina e della tecnica, che fungeranno da raccomandazioni per le altre autorità federali. Non si tratta di questioni organizzative di principio, bensì di processi, mezzi e servizi secondari (per es. rilevamento delle necessità di protezione delle informazioni, metodi per la valutazione del rischio, cifratura, requisiti per i contenitori di sicurezza). L'obiettivo è quello di raggiungere un livello di sicurezza uniforme, riducendo però al 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 uno specifico organo di coordinamento inter-autorità:* grazie alla loro posizione, gli incaricati della sicurezza delle informazioni responsabili della direzione tecnica dell'attuazione della legge otterranno una panoramica completa della situazione e dei problemi legati alla sicurezza delle informazioni nel proprio ambito di competenza, in particolare per quanto concerne la realizzabilità e l'efficacia delle prescrizioni e delle misure stabilite. È pertanto opportuno istituzionalizzare a livello di legge, in qualità di organo di coordinamento, una conferenza che riunisca tutti questi incaricati e che abbia come obiettivo principale un'esecuzione della legge uniforme, valida per tutte le autorità e basata sui rischi. A tal fine, la conferenza dovrà essere coinvolta anche nella definizione dei requisiti e delle misure standard.

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 e la consulenza professionali da parte di organi specializzati. Per quanto riguarda gli svantaggi legati a questa soluzione dal punto di vista della tecnica legislativa, si veda il numero 1.2.2.2.

1.2.7.2 Esecuzione in seno all'Amministrazione federale e presso altre organizzazioni assoggettate

L'avamprogetto di legge disciplina principalmente il quadro generale valido per tutte le autorità. L'esecuzione in seno all'Amministrazione e presso le organizzazioni che adempiono compiti amministrativi ai sensi dell'articolo 2 capoverso 4 LOGA spetta al Consiglio federale. La sua autonomia sul piano dell'esecuzione, fatto salvo l'adempimento dei requisiti materiali e organizzativi contemplati dalla legge, è pressoché illimitata. L'avamprogetto prevede due ingerenze nell'autonomia del Consiglio federale, ossia:

- il Consiglio federale, come tutte le altre autorità federali, deve provvedere, nel proprio ambito di competenza, affinché la sicurezza delle informazioni sia organizzata, attuata e verificata secondo lo stato della dottrina e della tecnica (cfr. art. 5 cpv. 1);
- il Consiglio federale, i dipartimenti e la Cancelleria federale devono designare per il rispettivo ambito di competenza un incaricato della sicurezza delle informazioni e un sostituto (cfr. n. 1.3.2 e art. 84).

L'avamprogetto non contempla ulteriori direttive per l'esecuzione in seno all'Amministrazione federale e il relativo disciplinamento a livello di ordinanza. In quest'ambito la legge lascia un ampio margine di manovra al Consiglio federale, il quale può per esempio concedere una maggiore autonomia sul piano dell'esecuzione alle organizzazioni del terzo cerchio o alle organizzazioni di cui all'articolo 2 capoverso 4 LOGA. In tale contesto potrà inoltre decidere se mantenere l'attuale forma di esecuzione, perlopiù decentralizzata, o se centralizzare determinate competenze e responsabilità.

1.2.8 Ambiti per i quali si rinuncia a proporre un disciplinamento

Dall'esame delle possibilità e dell'opportunità di disciplinare a livello di legge le problematiche elencate nel seguito è emerso che l'inclusione di tali ambiti estenderebbe per diversi aspetti il campo d'applicazione materiale della legge sulla sicurezza delle informazioni e presumibilmente incontrerebbe scarso consenso. Si rinuncia pertanto a proporre un disciplinamento di detti ambiti.

1.2.8.1 Disposizioni penali

Pur avendo constatato che le attuali disposizioni del Codice penale e del Codice penale militare relative alla tutela del segreto d'ufficio e alla protezione di informazioni della Confederazione e dei Cantoni classificate o degne di protezione sono poco coerenti e richiedono una revisione sotto molteplici aspetti, occorre considerare che si tratta di una materia facente parte del nucleo essenziale del diritto penale, che non va disciplinato a titolo accessorio in un atto normativo di natura organizzativa, bensì dovrebbe essere rielaborato nell'ambito di una revisione a sé stante del Codice penale. A tempo debito il Consiglio federale attribuirà il relativo mandato.

1.2.8.2 Restrizioni dell'accesso a informazioni classificate fondate sulla nazionalità

Nei primi progetti del gruppo di esperti era previsto che l'accesso a informazioni della Confederazione classificate SEGRETO fosse di principio riservato ai soli cittadini svizzeri. Eccezionalmente sarebbe comunque

stato possibile concedere l'autorizzazione d'accesso a cittadini di Stati con i quali la Svizzera avesse concluso un accordo sulla protezione delle informazioni. Su mandato del Consiglio federale, tuttavia, si deve rinunciare a prevedere restrizioni dell'accesso a informazioni della Confederazione classificate SEGRETO per i cittadini di Stati esteri.

1.2.8.3 Restituzione di informazioni degne di protezione giunte nelle mani di privati

Si è esaminato se, per una rapida realizzazione della protezione delle informazioni, sarebbe stato essenziale che i supporti di informazioni contenenti informazioni degne di protezione giunti nelle mani di terzi senza il consenso dell'autorità competente potessero essere recuperati mediante decisione amministrativa diretta. Questa soluzione avrebbe permesso alle autorità federali interessate di ordinare, nell'ambito della legislazione in materia di procedura amministrativa (vale a dire senza precedente procedimento penale o civile), la restituzione o la distruzione dei supporti di informazioni in questione. Tuttavia, poiché presumibilmente una simile disposizione sarebbe estremamente controversa, in particolare nell'ottica della libertà di stampa, e incontrerebbe una forte opposizione politica, si rinuncia a un disciplinamento in tal senso.

1.2.8.4 Messa in pericolo della sicurezza a causa della diffusione di informazioni da parte di privati

Al di fuori delle fattispecie penali in senso stretto, oggi non esistono basi legali che consentano alle autorità di impedire la diffusione di informazioni private la cui divulgazione può comportare minacce o pericoli rilevanti per la collettività e per lo Stato. Si pensa in particolare ai piani di fabbricazione di determinate armi, ai dati di laboratorio, ai piani di talune infrastrutture ecc. Si è esaminato se fosse il caso di prevedere la facoltà per i servizi federali materialmente competenti di vietare nel caso particolare, nell'ambito di una procedura amministrativa, la pubblicazione di questo tipo di informazioni, o di obbligare i loro detentori ad adottare misure di sicurezza previste dalla legge (classificazione delle informazioni, svolgimento di controlli di sicurezza relativi alle persone o di una procedura di sicurezza relativa alle aziende). Una normativa in tal senso comporterebbe però una sensibile ingerenza nei diritti fondamentali protetti di terzi e si scontrerebbe probabilmente a una consistente opposizione politica.

1.2.8.5 Integrazione di normative esistenti in materia di protezione delle opere

Di per sé, è incontestato che la sicurezza delle informazioni (inclusa la protezione dei mezzi TIC) e i CSP presentino un nesso relativamente stretto con la protezione delle opere, vale a dire con la protezione degli edifici e delle installazioni della Confederazione. Attualmente la materia è disciplinata in vario modo da diverse disposizioni legali di struttura piuttosto disparata (cfr. in ambito militare la legge federale concernente la protezione delle opere militari, in ambito civile per es. gli art. 22-24 LMSI, l'art. 62*f* LOGA, l'art. 69 LParl e l'art. 25*a* LTF). L'esame effettuato ha messo in luce 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 del presente progetto. L'avamprogetto contiene tuttavia due disposizioni sulla protezione fisica delle informazioni e dei mezzi TIC. Le competenze attuali in materia di protezione delle opere non vengono però messe in discussione.

1.3 Organizzazione della sicurezza delle informazioni in seno alla Confederazione

Nella sua decisione del 12 maggio 2010, il Consiglio federale ha incaricato il DDPS di esaminare, in occasione dell'elaborazione dell'avamprogetto, se e in quale misura le competenze e responsabilità esistenti in materia di sicurezza delle informazioni corrispondessero alle odierne esigenze. In particolare, occorreva anche esaminare se convenisse raggruppare i vari comitati interdipartimentali operanti in quest'ambito. Sebbene il mandato d'esame riguardasse, in linea di principio, soltanto l'Amministrazione federale, i risultati ottenuti forniscono tuttavia importanti riscontri in merito all'organizzazione della sicurezza delle informazioni per tutte le autorità.

1.3.1 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 (per 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, sicurezza delle opere e gestione dei rischi). Nel seguito saranno esaminate più da vicino le competenze e le responsabilità nei tre ambiti espressamente menzionati dal Consiglio federale (protezione delle informazioni, protezione dei dati e sicurezza informatica).

1.3.1.1 Organizzazione della protezione delle informazioni

- La protezione delle informazioni nell'Amministrazione federale è disciplinata per l'essenziale nell'OprI. Sono previste disposizioni complementari nei cosiddetti accordi sulla protezione delle informazioni (API; cfr. anche art. 90). L'attuazione della protezione delle informazioni è decentralizzata, ma viene coordinata a livello centrale da organi ai quali non è riconosciuta la facoltà di impartire istruzioni.
- *Conferenza dei segretari generali (CSG):* in virtù degli articoli 8 e 18 OPrI, la CSG è competente per emanare le prescrizioni di dettaglio (catalogo di classificazione e prescrizioni in materia di trattamento) per la protezione delle informazioni. 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 dei mezzi TIC.
- *Incaricati della protezione delle informazioni:* in virtù dell'articolo 19 OPrI, tutti i dipartimenti e la Cancelleria federale designano un incaricato della protezione delle informazioni. Gli incaricati della protezione delle informazioni provvedono all'attuazione della protezione delle informazioni nel proprio ambito di competenza. Sebbene l'OPrI non lo esiga, tutti i dipartimenti hanno designato ulteriori «consulenti per la protezione delle informazioni» a livello di unità amministrativa.
- *Comitato di coordinamento per la protezione delle informazioni in seno alla Confederazione (comitato di coordinamento):* il coordinamento a livello interdipartimentale si svolge nell'ambito del comitato di coordinamento (art. 20 OPrI), il quale provvede a un'esecuzione uniforme della protezione delle informazioni in seno alla Confederazione, prepara i documenti all'attenzione della CSG e presenta a quest'ultima un rapporto ogni due anni. Coordina inoltre le sue attività con il Comitato per la sicurezza informatica (C-SI) dell'ODIC.
- *Organo di coordinamento per la protezione delle informazioni in seno alla Confederazione (organo di coordinamento):* in virtù dell'articolo 20*a* OPrI, l'organo di coordinamento, aggregato alla Protezione delle informazioni e delle opere (PIO) in seno al DDPS, ha il compito di assistere il comitato di coordinamento e gli incaricati della protezione delle informazioni. Allestisce i necessari mezzi didattici e funge da interlocutore centrale per i contatti con organi nazionali, esteri e internazionali nel settore della protezione delle informazioni. Può anche eseguire le ispezioni di sicurezza previste da trattati internazionali e altri controlli d'intesa con i dipartimenti e la Cancelleria federale.

1.3.1.2 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 a livello centrale è sottoposta alla sorveglianza dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) e coordinata dal Gruppo interdipartimentale per la protezione dei dati, organo informale sprovvisto della facoltà di impartire istruzioni.

- *Incaricato federale della protezione dei dati e della trasparenza (IFPDT):* la LPD ha istituito la figura dell'IFPDT, con funzioni di consulenza e di sorveglianza per privati e organi della Confederazione riguardo al rispetto delle disposizioni in materia di protezione dei dati. L'IFPDT vigila sul rispetto della LPD e delle altre disposizioni federali in materia di protezione dei dati da parte degli organi della Confederazione. Dal punto di vista amministrativo è subordinato alla Cancelleria federale.
- *Consulenti per la protezione dei dati:* in virtù dell'articolo 23 OLPD, la Cancelleria federale e i dipartimenti designano ciascuno almeno un consulente per la protezione dei dati. Questi consulenti consigliano gli organi responsabili e gli utenti, promuovono l'informazione e la formazione dei collaboratori e contribuiscono all'applicazione delle prescrizioni sulla protezione dei dati. Gli organi federali comunicano con l'IFPDT tramite il loro consulente per la protezione dei dati. Nella maggior parte dei casi, sono stati designati consulenti per la protezione dei dati anche a livello di unità amministrativa.
- *Gruppo interdipartimentale per la protezione dei dati:* la legislazione in materia di protezione dei dati non prevede un organo competente per il coordinamento a livello interdipartimentale della protezione dei dati in seno alla Confederazione. È stato pertanto istituito un gruppo interdipartimentale informale per la protezione dei dati presieduto dal consulente per la protezione dei dati della Cancelleria federale. Ne fanno parte tutti i consulenti per la protezione dei dati dei dipartimenti, un rappresentante dell'IFPDT e uno dei Servizi del Parlamento. Il gruppo provvede in particolare a un'esecuzione uniforme e coordinata della protezione dei dati in seno alla Confederazione, difende gli interessi della prassi nei confronti dell'IFPDT e si occupa di organizzare manifestazioni formative.

1.3.1.3 Organizzazione specialistica della sicurezza informatica

L'organizzazione della sicurezza informatica è principalmente definita dall'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.). 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) e seguita da un organo consultivo (C-SI).

- *Consiglio federale:* il Consiglio federale svolge un ruolo strategico in materia di sicurezza TIC. Molti dei suoi compiti in questo settore si ricollegano alla sua responsabilità nell'ambito generale delle TIC secondo l'articolo 14 OIAF: stabilisce la strategia TIC della Confederazione, vigila sull'attuazione della strategia TIC della Confederazione e, all'occorrenza, ordina misure, definisce i servizi standard TIC, emana istruzioni in materia di sicurezza TIC e autorizza deroghe alle proprie direttive.
- *ODIC:* in virtù dell'articolo 17 OIAF, nel settore della sicurezza TIC l'ODIC decide in merito alle richieste dei dipartimenti, della Cancelleria federale e delle unità amministrative concernenti disposizioni 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 TIC 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; gestisce la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) in collaborazione con il Servizio delle attività informative della Confederazione; dirige il Comitato per la sicurezza informatica (C-SI), uno degli organi consultivi.
- *Incaricati della sicurezza informatica:* per l'esecuzione decentralizzata i dipartimenti e la Cancelleria federale devono designare ciascuno un incaricato della sicurezza informatica (art. 19 cpv. 1 OIAF). Gli incaricati della sicurezza informatica dei dipartimenti e della Cancelleria federale coordinano tutti gli aspetti riguardanti la sicurezza informatica all'interno del dipartimento e con gli organi interdipartimentali. Anche le unità organizzative sono tenute a designare un proprio incaricato della sicurezza informatica. Gli incaricati a livello di unità organizzativa coordinano tutti gli aspetti riguardanti la sicurezza informatica sia all'interno dell'unità organizzativa sia con i servizi dipartimentali.
- *Comitato per la sicurezza informatica (C-SI):* il C-SI è l'organo consultivo dell'ODIC per tutte le questioni inerenti alla sicurezza TIC (art. 19 OIAF). Si occupa anche del coordinamento a livello interdipartimentale. È formato dagli incaricati della sicurezza informatica dei dipartimenti e della Cancelleria federale. Possono partecipare con voto consultivo un rappresentante ciascuno del Controllo federale delle finanze (CDF), dell'IFPDT e dei Servizi del Parlamento.
- *Consiglio informatico della Confederazione (CIC):* il CIC è l'organo consultivo dell'ODIC per gli affari TIC (compresi quelli relativi alla sicurezza TIC) 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 alla loro applicazione (art. 18 OIAF). È formato dal delegato per la direzione TIC e da un rappresentante nominato appositamente per ciascun dipartimento e per la Cancelleria federale. Possono partecipare con voto consultivo un rappresentante dell'Amministrazione federale delle finanze (AFF), dell'IFPDT, dei fornitori di prestazioni interni e dei servizi del Parlamento.
- *Controllo federale delle finanze (CDF):* dal 1° gennaio 2012 il CDF svolge la revisione informatica in seno all'Amministrazione federale (art. 28 OIAF).

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 TIC. Qui di seguito sono elencati soltanto quelli che esercitano specifiche competenze e responsabilità rilevanti per la sicurezza TIC delle autorità federali, tralasciando tuttavia i servizi incaricati di attività informative, le autorità penali o altri servizi.

- *Protezione delle informazioni e delle opere (PIO):* la Protezione delle informazioni e delle opere, aggregata all'Aggruppamento Difesa, è responsabile delle direttive in materia di sicurezza TIC del DDPS e dell'esercito e della verifica della loro attuazione. Sotto questo aspetto adempie compiti molto simili a quelli dell'ODIC.
- *Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI):* la centrale MELANI, istituita in via definitiva dal Consiglio federale nel 2004, è incaricata di proteggere le infrastrutture critiche dell'informazione in Svizzera. La cooperazione, diretta dall'ODIC (art. 17 cpv. 1 lett. i OIAF), tra DFF, DDPS ed economia privata per la protezione delle infrastrutture critiche si basa sul modello del *par-*

tenariato pubblico-privato. Si tratta di una stretta collaborazione tra pubblica amministrazione e imprese private dei vari settori dell'economia che operano nel campo della sicurezza dei sistemi informatici e della rete Internet nonché della protezione delle infrastrutture critiche svizzere.

- *Stato maggiore speciale per la sicurezza dell'informazione (SONIA):* SONIA si riunisce in caso di crisi provocate da perturbazioni delle infrastrutture di informazione e di comunicazione. È formato da decisori provenienti dagli ambienti dell'Amministrazione, dei Cantoni e dell'economia (infrastrutture critiche) e diretto dal delegato per la direzione informatica della Confederazione (ODIC). La centrale MELANI funge da centro incaricato dell'analisi permanente della situazione a favore di SONIA.
- *Computer Security Incident Response Team (CSIRT):* il CSIRT, aggregato all'UFIT in seno al DFF, si occupa di proteggere le reti civili della Confederazione svolgendo attività di sorveglianza, prevenzione e reazione. Collabora strettamente con altri partner in seno alla Confederazione, per esempio con la centrale MELANI e l'Ufficio federale di polizia (fedpol), e adempie i seguenti compiti fondamentali: osservazione delle minacce attuali e analisi di log file; emanazione di raccomandazioni operative volte a ridurre al minimo i rischi, a garantire rapidamente il contenimento dei danni in caso di incidenti rilevanti per la sicurezza TIC e a proteggere i dati affidati all'UFIT (protezione operativa delle infrastrutture TIC centrali della Confederazione).
- *Computer Emergency Response Team militare (MilCERT):* il MilCERT, corrispettivo nel settore militare del CSIRT dell'UFIT, si occupa di proteggere le reti dell'esercito e del DDPS. È integrato nel Centro operazioni elettroniche (COE) della Base d'aiuto alla condotta (BAC) in modo da poter effettuare, come unità indipendente, indagini sugli incidenti rilevanti per la sicurezza che si verificano nel DDPS e nell'esercito.
- *Sicurezza dell'informazione e Crittologia (SI Critt):* il settore SI Critt è anch'esso aggregato al COE della BAC. I suoi crittologi valutano e sviluppano per conto proprio procedure e sistemi crittologici al fine di garantire la sicurezza delle informazioni dell'esercito, del DDPS e di altre unità dell'Amministrazione federale. Il lavoro di questo settore spazia dalla verifica di concetti crittologici di massima all'analisi di singole funzioni crittologiche e richiede pertanto profonde conoscenze dell'attuale ricerca in materia di crittoanalisi.
- *armasuisse Scienza e tecnologia (S+T):* il settore Informatica e cyberspazio di armasuisse S+T effettua analisi dei rischi, controlli di sicurezza e audit nel campo della sicurezza informatica organizzativa e tecnica. I servizi di armasuisse S+T sono richiesti sempre più spesso anche da organi civili dell'Amministrazione federale, in particolare per la certificazione dell'effettività dei concetti in materia di sicurezza e dell'efficacia protettiva delle misure di sicurezza nonché per la realizzazione di test tecnici di verifica e di penetrazione. In questo campo, armasuisse S+T effettua anche un monitoraggio degli sviluppi tecnologici e delle minacce.

1.3.1.4 Confronto tra le competenze e le responsabilità

Ognuna delle tre organizzazioni specialistiche descritte adempie soltanto un mandato circoscritto nell'ambito della sicurezza delle informazioni. In tutti e tre i settori, la responsabilità per quanto attiene all'attuazione delle direttive è assunta dai dipartimenti e dalla Cancelleria federale. Inoltre, tutti i settori presentano in linea di principio la stessa identica struttura organizzativa, consistente in:

- un ente regolamentatore;
- incaricati a livello di dipartimento / Cancelleria federale e unità amministrativa; e
- un organo di coordinamento interdipartimentale.

Anche i titolari delle varie funzioni svolgono in linea di principio gli stessi compiti nei rispettivi settori specialistici. L'unica eccezione importante è rappresentata dai vari enti regolamentatori, i cui poteri presentano in certi casi importanti differenze. La tabella che segue fornisce una panoramica della situazione e comprende anche gli altri due settori direttamente connessi alla sicurezza delle informazioni, vale a dire la protezione delle opere e la gestione dei rischi.

	Direttive	Dipartimento/CaF	Unità amministrativa	Coordinamento
Protezione delle informazioni	CSG	Incaricati della protezione delle informazioni	Incaricati/consulenti per la protezione delle informazioni	Comitato di coordinamento/organo di coordinamento
Protezione dei dati	IFPDT	Consulenti per la protezione dei dati	Consulenti per la protezione dei dati	GLID Protezione dei dati
Sicurezza TIC	CF/ODIC	Incaricati della sicurezza informatica	Incaricati della sicurezza informatica	Settore specialistico Sicurezza dell'ODIC (ODIC SEC)/C-SI
Protezione delle opere	fedpol/ Servizio federale di sicurezza (SFS)	Incaricati della sicurezza	Incaricati della sicurezza	Comitato di coordinamento Sicurezza
Gestione dei rischi	CF/CSG	Gestore dei rischi	Coach in materia di rischi	Organo di coordinamento AFF

1.3.1.5 Carenze organizzative

L'attuale organizzazione presenta molteplici lacune e punti deboli.

- *Le competenze dei vari settori non sono sempre chiare e l'attenzione dedicata alle interfacce tra i singoli ambiti specialistici della sicurezza informatica non è sufficiente.*

  La mancanza di chiarezza che caratterizza le competenze è evidente a tutti i livelli. Per il trattamento elettronico dei dati personali degni di particolare protezione o di informazioni classificate a partire dal livello di classificazione CONFIDENZIALE, per esempio, è necessario un concetto per la sicurezza delle informazioni e la protezione dei dati (concetto SIPD). Si tratta di una questione di protezione dei dati, di protezione delle informazioni o di sicurezza TIC? Chi è competente per la corretta classificazione delle informazioni e per il controllo dell'attuazione delle misure? La protezione delle linee di rete è una questione di sicurezza informatica oppure di protezione delle opere? La distruzione degli atti è una questione di protezione delle informazioni, di protezione dei dati o di sicurezza fisica e chi definisce i requisiti in materia? Chi li attua? Una penna USB è un supporto di informazioni ai sensi dell'OPrI o un mezzo TIC ai sensi dell'OIAF?

  I problemi evocati hanno ripercussioni dirette anche sul piano internazionale. A causa della mancanza di chiarezza riguardo alla ripartizione di competenze e responsabilità all'interno dell'Amministrazione federale, per esempio, sinora non è stato possibile trovare una soluzione con l'UE per la trasmissione elettronica di informazioni classificate. Di conseguenza, persino le informazioni del livello più basso di classificazione previsto dall'UE vengono tuttora scambiate esclusivamente su carta. Problemi analoghi si riscontrano anche nell'ambito della collaborazione con l'Agenzia spaziale europea (ESA). In tale contesto ci si domanda per esempio chi sia competente per il settore della sicurezza delle comunicazioni (COMSEC)[7]. La questione condiziona pesantemente anche la riuscita della partecipazione di istituzioni e imprese svizzere alle attività dell'ESA, ma sinora è rimasta irrisolta.

  I settori specialistici sono anche tenuti ad attuare misure di formazione e di sensibilizzazione. Spesso, tuttavia, le misure di sensibilizzazione e di formazione dei vari servizi non sono coordinate tra loro, benché abbiano contenuti analoghi.

- *Gli attori sono troppo numerosi e in parte non dispongono di conoscenze specialistiche o risorse di personale sufficienti. Le risorse disponibili sono in parte mal utilizzate. La massa critica non viene mai raggiunta.*

  Nei sottosettori esaminati, oltre ai compiti in materia di sicurezza delle informazioni gli elenchi degli obblighi degli incaricati prevedono in genere anche altri obblighi. Spesso, alle persone incaricate di compiti riguardanti la sicurezza delle informazioni rimangono soltanto ritagli di tempo per tali mansioni e possono quindi dedicarvisi soltanto marginalmente. Di conseguenza, non tutti dispongono delle conoscenze specialistiche richieste, il che penalizza gravemente la sicurezza. Nel campo della sicurezza delle infor-

[7] Per *COMSEC* si intende la sicurezza delle comunicazioni nel senso dell'applicazione di misure di sicurezza alle telecomunicazioni per impedire che persone non autorizzate entrino in possesso di informazioni preziose che possono essere ottenute mediante accesso alle telecomunicazioni e alla loro analisi oppure per garantire l'autenticità, la confidenzialità e liintegrità delle telecomunicazioni.

mazioni e dei dati, inoltre, operano soprattutto giuristi, i quali di regola hanno poca dimestichezza con la sicurezza informatica. Inoltre, i giuristi tendono a considerare la questione facendo prevalere l'aspetto giuridico e spesso non sono in grado di seguire o verificare l'effettiva attuazione dei requisiti di sicurezza nell'ambito dei progetti TIC. Nel caso degli specialisti della sicurezza TIC, invece, la situazione risulta capovolta, in quanto spesso tali specialisti non dispongono di conoscenze sufficienti in materia di protezione delle informazioni o dei dati.

Tali constatazioni si applicano anche ai servizi specializzati. Rispetto alla mole di lavoro, in quasi tutti questi servizi si riscontra una sottodotazione di personale. La massa critica non viene mai raggiunta. Inoltre, talvolta mancano sufficienti conoscenze specialistiche degli altri settori e, soprattutto nel settore della sicurezza informatica, vi sono moltissimi attori che svolgono compiti complementari. Alcuni di questi compiti o servizi non sono però coordinati, oppure i servizi non vengono affatto richiesti (per es. i servizi dei crittologi del DDPS).

Oggi gli specialisti della sicurezza delle informazioni sono più che mai richiesti, sia nell'ambito tecnico sia in quello della gestione. La Confederazione dispone di tali specialisti, ma spesso essi non vengono destinati completamente a compiti nel campo della sicurezza delle informazioni. È dunque legittimo chiedersi se queste scarse risorse vengano impiegate adeguatamente.

- *I poteri di cui dispongono i vari attori sono spesso insufficienti.*

  Una constatazione importante consiste nel fatto che l'attuazione delle misure adottate in materia di sicurezza delle informazioni viene verificata soltanto in casi estremamente rari. Di solito, infatti, né i servizi specializzati né i vari incaricati hanno la facoltà di effettuare controlli. Senza controlli, però, è impossibile valutare se le misure sono efficaci o se esistono invece lacune e punti deboli.

- *Vi è scarsa consapevolezza in materia di sicurezza.*

  In seno ai dipartimenti e alla Cancelleria federale, l'importanza attribuita ai temi della sicurezza informatica varia enormemente. La sensibilizzazione dei collaboratori dipende in primo luogo dall'impegno dei superiori e in particolare delle direzioni.

1.3.1.6 Bilancio della situazione e conseguenze

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

Gli aspetti importanti di cui tenere conto per ottenere un miglioramento della situazione a livello organizzativo sono i seguenti:

- la responsabilità dell'attuazione delle direttive deve essere lasciata alla linea gerarchica, la quale deve però essere consigliata e coadiuvata a tutti i livelli con maggiore competenza;
- la futura organizzazione della sicurezza delle informazioni deve concentrarsi maggiormente sull'identificazione e sul trattamento precoci dei rischi. La realizzazione di questo obiettivo presuppone una gestione sistematica dei rischi nel campo della sicurezza delle informazioni, presupposto che oggi è ancora largamente inadempiuto. È però indispensabile anche un migliore controllo per quanto riguarda l'attuazione delle misure volte a ridurre al minimo i rischi;
- i vari organi specializzati devono essere per quanto possibile raggruppati per sfruttare le sinergie e ottenere effetti di scala. Ciò consentirebbe anche di trovare una soluzione sistematica ai problemi di competenza e di accumulare maggiori conoscenze specialistiche interdisciplinari. Un raggruppamento di tutti gli organi specializzati non risulta possibile, ma per gli organi rimanenti occorre in ogni caso definire con maggiore chiarezza competenze e responsabilità e migliorare il coordinamento e lo scambio di conoscenze;
- 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;
- occorre dedicare un'attenzione particolare alla separazione delle funzioni e al loro inquadramento. Gli incaricati non dovrebbero essere subordinati a un settore specialistico di cui devono valutare i rischi in modo oggettivo e indipendente e non dovrebbero neppure ricevere compiti che potrebbero dare adito a un conflitto di interessi.

In base alle considerazioni che precedono, risulta opportuno fondere i tre comitati. È però evidente che l'auspicata fusione dei comitati non deve portare a un trattamento indifferenziato dei singoli temi (informazioni classificate, protezione dei dati o sicurezza tecnica). Si tratta semplicemente di trattare tutti i temi in seno a un unico organismo consolidato che definisca la propria agenda in funzione delle effettive necessità.

1.3.2 Nuovo disciplinamento dell'organizzazione a livello di Confederazione

L'avamprogetto tiene conto dei risultati del mandato d'esame conferito dal Consiglio federale relativamente all'attuale organizzazione della sicurezza delle informazioni. La soluzione contemplata nell'avamprogetto fornisce la base per il chiarimento e la semplificazione delle corrispondenti competenze e responsabilità. Essa pone inoltre l'accento sullo sviluppo delle competenze dei servizi responsabili dell'esecuzione mediante attività di sostegno e di consulenza da parte di specialisti nonché attraverso un'intensificazione dello scambio di informazioni tra i servizi in questione. L'avamprogetto prevede di conseguenza un'unica figura di incaricato (incaricato della sicurezza delle informazioni), un unico organo di coordinamento e un servizio specializzato della Confederazione per la sicurezza delle informazioni, che assumeranno tutti i compiti trasversali in materia di sicurezza delle informazioni. Con il nuovo disciplinamento proposto si mira a fondere integralmente, in seno all'Amministrazione federale, le strutture di esecuzione appartenenti ai settori della protezione delle informazioni e della sicurezza delle informazioni, finora separati.

1.3.2.1 Incaricati della sicurezza delle informazioni

La nuova figura dell'incaricato della sicurezza delle informazioni assume un ruolo centrale per l'esecuzione dell'avamprogetto di legge. 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 CaF) l'organizzazione specialistica della 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 e adeguata ai rischi, oltre a beneficiare di un chiaro sostegno da parte delle 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 responsabili dell'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 delle informazioni, finora separati. Il Consiglio federale dovrà decidere, a livello di ordinanza, in merito all'opportunità e alla necessità di una simile fusione delle funzioni all'interno delle unità organizzative.

1.3.2.2 Conferenza degli incaricati della sicurezza delle informazioni

Uno degli obiettivi dichiarati della presente legge è quello di raggiungere un livello di sicurezza il più possibile uniforme per le diverse autorità federali e organizzazioni. In virtù dell'indipendenza delle autorità sancita dalla Costituzione federale, questo 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 (art. 84) 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 quindi opportuno istituzionalizzare, come organo di coordinamento, una conferenza di tali incaricati.

La prevista Conferenza degli incaricati della sicurezza delle informazioni si occuperà principalmente del coordinamento dell'esecuzione tra tutte le autorità. In tale ambito, svolgerà un ruolo importante per lo sviluppo di una dottrina uniforme come pure per il necessario scambio di esperienze. Dovranno far parte della Conferenza anche gli incaricati della sicurezza delle informazioni dei dipartimenti e della Cancelleria come pure un rappresentante dell'IFPDT. Per le questioni strategiche legate alla sicurezza delle informazioni, infine, la Conferenza dovrà poter ricorrere anche a esperti provenienti dai Cantoni, dal mondo scientifico o dall'economia.

Per l'Amministrazione federale, questa Conferenza 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.

1.3.2.3 Servizio specializzato della Confederazione per la sicurezza delle informazioni

La sicurezza delle informazioni deve essere organizzata, diretta e controllata mediante un approccio integrale. I compiti già esistenti tra quelli previsti dalla presente legge sono 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, tuttavia, non basterà, di per sé, a realizzare l'approccio integrale alla sicurezza delle informazioni. Nell'avamprogetto, il servizio specializzato è concepito soprattutto come centro di competenza per i compiti comuni a tutte le autorità, motivo per cui è sprovvisto della facoltà di impartire istruzioni. In linea di principio, opera sempre su richiesta o su mandato di un'autorità assoggettata e va inteso come organo con compiti di assistenza e consulenza.

Nella legge vengono fissati in modo esaustivo i compiti concreti del servizio specializzato che concernono tutte le autorità. Oltre a fornire consulenza e assistenza, il servizio specializzato potrà anche essere incaricato di valutare i rischi in occasione dell'impiego di nuove tecnologie o di dirigere e coordinare l'ambito della sicurezza delle informazioni nell'ambito di progetti importanti che coinvolgono più autorità. Un altro compito fondamentale del servizio specializzato sarà 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 di tale esame confermano che i processi, i mezzi o le prestazioni in questione adempiono i requisiti standard 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 essere incaricato di effettuare controlli e audit in materia di sicurezza. Nel contesto internazionale, infine, sarà l'interlocutore per i contatti specializzati nel campo della sicurezza delle informazioni con servizi svizzeri, esteri e internazionali, ruolo necessario per l'attuazione di trattati internazionali (art. 90 e n. 4.2).

Il Consiglio federale disciplinerà a livello di ordinanza l'organizzazione del servizio specializzato della Confederazione per la sicurezza delle informazioni. A tal fine stabilirà quali sono i compiti che il servizio specializzato deve adempiere autonomamente o 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 previsto dalla legge. Il servizio specializzato dovrà per esempio svolgere per l'Amministrazione federale determinati compiti che oggi vengono svolti dall'ODIC SEC e dalla PIO. Di conseguenza, i compiti delle autorità esistenti verranno ridefiniti a livello di ordinanza e sarà necessario verificare alcune interfacce.

In questo contesto, il Consiglio federale dovrà naturalmente anche decidere in merito alla delicata questione dell'inquadramento amministrativo del servizio specializzato. Ai fini dell'autonomia organizzativa del Consiglio federale, tuttavia, tale questione non va risolta a livello di legge formale. La collocazione del servizio specializzato deve essere proposta al Consiglio federale soltanto una volta chiariti i compiti e le competenze di quest'ultimo nonché dopo aver elaborato un concetto dettagliato per l'attuazione delle direttive legali per l'Amministrazione federale e le organizzazioni di diritto pubblico e privato assoggettate a tali direttive.

1.3.3 Nuovo disciplinamento per l'Amministrazione federale e altre organizzazioni assoggettate

A livello inter-autorità, il servizio specializzato della Confederazione per la sicurezza delle informazioni è *volutamente* sprovvisto di poteri esecutivi a livello *giuridico*. Per l'Amministrazione federale e le organizzazioni di diritto pubblico e privato che sottostanno alle disposizioni esecutive del Consiglio federale, invece, quest'ultimo può conferire ulteriori competenze al servizio specializzato e impostare in modo differenziato i rapporti che tale servizio intrattiene con la linea gerarchica e con gli incaricati della sicurezza delle informazioni. Sebbene, in linea di principio, la responsabilità 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 i controlli.

In tale contesto, alcuni servizi chiedono che vengano sin d'ora presentate e attribuite diverse opzioni per l'esecuzione in seno all'Amministrazione federale, con i rispettivi vantaggi e svantaggi, affinché possa essere adottata una decisione in materia. A questo proposito occorrerebbe mettere a confronto due modelli: uno che preveda un'organizzazione dell'esecuzione totalmente decentralizzata e un servizio specializzato con una pura funzione di coordinamento e un altro che contempli invece un servizio specializzato con la facoltà di impartire istruzioni, a livello centrale, agli incaricati della sicurezza delle informazioni dei dipartimenti. Tuttavia, sebbene l'allestimento e la valutazione di simili modelli di attuazione siano assolutamente necessari, sarà possibile fornire una valida risposta a tali questioni soltanto in un secondo momento. Prima di decidere in merito all'attuazione dettagliata in seno all'Amministrazione federale occorre infatti chiarire i principi generali e i contenuti materiali del presente progetto legislativo come pure le relazioni tra le varie autorità.

2 Commento ai singoli articoli

2.1 Legge federale sulla sicurezza delle informazioni

Titolo

Riguardo al titolo dell'atto normativo, sono importanti due precisazioni:

- 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 si servano di informazioni o di mezzi e installazioni delle tecnologie dell'informazione e della comunicazione (mezzi TIC) della Confederazione, tuttavia ciò accade solamente con l'applicazione delle disposizioni rilevanti da parte di un'autorità o di un'organizzazione della Confederazione;
- per la nozione di «*sicurezza delle informazioni*» ci 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 TIC. La sicurezza delle informazioni non può essere ridotta alla sicurezza TIC: comprende infatti tutti i processi di trattamento, dunque anche documenti cartacei e affermazioni orali, e non soltanto il trattamento di informazioni mediante l'infrastruttura elettronica della Confederazione. La nozione include anche l'attuazione dei requisiti di protezione della legislazione in materia di protezione dei dati o di altre leggi che fissano requisiti per la protezione di informazioni.

Ingresso

Vedi numero 4.1.

2.1.1 Disposizioni generali

Art. 1

Questa disposizione riassume in forma generale lo scopo dell'atto normativo.

Il capoverso 1 segnala che sia le informazioni in quanto tali sia le TIC rientrano nel campo d'applicazione della legge. La nozione di «informazione» non viene definita nella presente legge sulla sicurezza delle informazioni (LSIn), poiché nell'atto normativo si rinuncia a definizioni legali e la nozione 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 la nozione di «informazioni». Nella legge, la nozione di «dati» viene utilizzata solamente se sono interessati dati personali ai sensi della LPD. Con la nozione di «*mezzi TIC*», la LSIn include l'insieme delle installazioni, degli apparecchi, dei sistemi e delle applicazioni utilizzati per il trattamento elettronico (incl. memorizzazione e comunicazione) di informazioni. In merito alla menzione esplicita delle TIC nell'articolo concernente lo scopo si veda il numero 1.2.2.1.

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 del presente avamprogetto non sono gli stessi (in merito ai rapporti tra LSIn e LTras, si veda l'art. 3 cpv. 1).

La presente legge protegge i seguenti interessi:

- lett. a: la protezione della capacità di decisione e d'azione delle autorità federali 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 (si veda anche l'art. 7 cpv. 1 lett. a e b LTras e i n. 2.2.2.1.1-2 del messaggio LTras);
- lett. b: vengono in primo luogo protette 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 TIC delle autorità impiegati per sostenere compiti di sicurezza critici devono rimanere sempre di-

sponibili e funzionanti anche in tempi di crisi (si veda anche l'art. 7 cpv. 1 lett. d LTras e il n. 2.2.2.1.3 del messaggio LTras);

- lett. c: insieme alle questioni relative alla sicurezza, le relazioni estere sono fra i settori più 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 condurre la politica estera e curare le relazioni internazionali. Per condurre a buon fine dei negoziati è fondamentale che la controparte o il pubblico non vengano a conoscenza delle relative strategie e intenzioni. 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 (si veda anche l'art. 7 cpv. 1 lett. d LTras e il n. 2.2.2.1.4 del messaggio LTras);
- lett. d: la comunicazione non autorizzata o la falsificazione di determinate informazioni, nonché la perturbazione del funzionamento di 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 significato (si veda anche l'art. 7 cpv. 1 lett. f LTras e il n. 2.2.2.1.6 del messaggio LTras);
- lett. e: qui 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 infatti moltissime informazioni che devono proteggere in virtù delle più disparate disposizioni legali (p. es. LPD, LOGA, LParl, LBN, LAPub, LFC, LATer ecc.) o che ricevono da terzi soltanto a condizione di garantire una protezione adeguata. Anche se i segreti professionali, d'affari o di fabbricazione o la tutela della confidenzialità e integrità di dati personali non rappresentano interessi diretti della Confederazione, qualora dovesse emergere che le autorità federali non rispettano i loro impegni per proteggere queste informazioni, la loro affidabilità potrebbe tuttavia 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. (Si veda anche l'art. 7 cpv. 1 lett. e, g e h LTras e i n. 2.2.2.1.5 e 2.2.2.1.7-8 del messaggio LTras).

Art. 2

L'articolo 2 include il campo d'applicazione istituzionale e amministrativo.

Il capoverso 1 stabilisce quali autorità vengono assoggettate all'applicazione della legge nel loro ambito di competenza. Quali autorità assoggettate, vengono menzionati l'Assemblea federale, il Consiglio federale, i tribunali della Confederazione (Tribunale federale, Tribunale penale federale, Tribunale amministrativo federale, Tribunale federale dei brevetti), 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. Tutte queste istituzioni, nella loro attività quali autorità, non sono assoggettate ad alcuna facoltà diretta di emanare istruzioni di un'altra autorità. In conseguenza del flusso di informazioni tra le 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, si veda il numero 1.2.2.2.

Rimane inteso che, in singole normative, la legge deve tenere conto della posizione costituzionale e delle particolarità delle varie autorità o istituzioni. Contiene perciò, ad esempio, deroghe all'obbligo del controllo di sicurezza relativo alle persone (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 o organizzazioni, questi vengono specificati di conseguenza (si vedano p. es. gli art. 19, 33 cpv. 4, 35, 36 e 84 cpv. 1). Al livello della legge non può però venire stabilita l'intera organizzazione esecutiva delle varie autorità e le competenze dei loro organi o servizi. Ciò deve avvenire mediante la relativa disposizione d'esecuzione delle singole autorità.

Il capoverso 2 considera che le autorità menzionate nel capoverso 1 devono occuparsi soltanto limitatamente 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, 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, dell'Amministrazione federale, ivi comprese le unità amministrative decentrate, nonché dell'esercito.

- la lettera d prevede un sostanziale assoggettamento alla legge per organizzazioni di diritto pubblico e privato che adempiono compiti amministrativi della Confederazione ai sensi dell'articolo 2 capoverso 4 LOGA e che, nel farlo, sono soggette alla vigilanza della Confederazione (si veda in proposito l'art. 8 cpv. 4 e 5 LOGA). Sono, in particolare, organizzazioni che per legge sono autorizzate a emanare decisioni nei confronti di privati. In questo contesto, presupposto per un assoggettamento è che queste organizzazioni esercitino attività sensibili sotto il profilo della sicurezza nell'ambito dell'adempimento dei propri compiti amministrativi (si veda il cpv. 3). L'assoggettamento vale solamente per questi compiti amministrativi. Non è attuabile, nell'ambito del presente atto normativo, determinare in maniera esaustiva e duratura le singole organizzazioni assoggettate. Spetta perciò al Consiglio federale stabilire a livello di ordinanza chi è assoggettato e in quale misura (si veda l'art. 87 cpv. 4);
- lettera e: per adempiere i rispettivi compiti, Confederazione e Cantoni dipendono da una strettissima collaborazione. Si scambiano reciprocamente moltissime informazioni, tra le quali rientrano anche informazioni classificate della Confederazione. Le infrastrutture e i sistemi TIC della Confederazione e dei Cantoni vengono inoltre sempre più collegati fra loro. Aumenta così il rischio che gli attacchi e le minacce nell'ambito di competenza di un'autorità si propaghino agli ambiti di competenza di altri partecipanti. I Cantoni sono direttamente competenti per la sicurezza delle proprie informazioni. Se però adempiono compiti della Confederazione sotto la vigilanza diretta della Confederazione, in linea di massima si applicano anche a loro le direttive della Confederazione. La legge prevede un assoggettamento dei Cantoni secondo criteri basati sui rischi: vanno assoggettati per adempiere compiti soltanto se nel farlo esercitano attività sensibili sotto il profilo della sicurezza per incarico della Confederazione e sotto la sua vigilanza diretta (si veda il cpv. 3).

  La legge non include le autorità e i servizi cantonali che, di loro competenza, attuano il diritto federale. La LSIn non disciplina, in maniera specifica, il collegamento tra reti cantonali e reti federali. In simili casi le autorità della Confederazione e dei Cantoni devono concordare misure di sicurezza appropriate alla situazione che garantiscano materialmente il livello di protezione richiesto dalla legge per le autorità federali. In merito all'esecuzione da parte dei Cantoni, si veda l'articolo 89.

Il capoverso 3 definisce la nozione di *«attività sensibile sotto il profilo della sicurezza»*, centrale per l'applicazione di questa legge. L'esercizio di un'attività sensibile sotto il profilo della sicurezza, infatti, non è solamente il presupposto per l'applicazione della legge a organizzazioni di diritto pubblico e privato che adempiono compiti amministrativi e ai Cantoni, bensì anche per l'esecuzione di controlli di sicurezza relativi alle persone (CSP) o di procedure di sicurezza relative alle aziende (PSA) presso terzi ai quali vanno affidati compiti della Confederazione. L'attività sensibile sotto il profilo della sicurezza viene definita nel contesto della sicurezza delle informazioni. Come nell'attuale LMSI, il suo contenuto materiale pone in primo piano la gestione delle informazioni. Nella sua definizione si è badato al parallelismo con le normative sulla protezione delle informazioni classificate e sulla sicurezza nell'impiego di mezzi TIC.

- Lettera a: adducendo il livello di classificazione «CONFIDENZIALE» come punto di partenza per definire l'attività sensibile sotto il profilo della sicurezza, si 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 nella gestione di informazioni classificate è inoltre non il semplice *«accesso»* a queste informazioni, bensì il loro «*trattamento*» effettivo e autorizzato. In altre parole, ad esempio, il personale addetto alla pulizia 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 talvolta possa accedere fattivamente a informazioni classificate perché i collaboratori non sempre rispettano le prescrizioni di sicurezza.

  È menzionata anche la gestione del materiale classificato. Si tratta di vari materiali e oggetti la cui esistenza o natura deve essere protetta in quanto tale dalla conoscenza da parte di persone non autorizzate o le cui caratteristiche possono rivelare informazioni classificate: il materiale *è* o contiene dunque l'informazione. Ne sono interessati principalmente gli oggetti d'armamento, i sistemi d'arma o i sistemi di comunicazione integrati. Sovente uno Stato terzo che ha autorizzato la fornitura alla Svizzera prescrive una classificazione di simili materiali e oggetti. Fino a oggi la Svizzera conosce corrispondenti classifica-

zioni soltanto in ambito militare; in ambito civile (p. es. polizia e Corpo delle guardie di confine) mancava finora una corrispondente base, che ora viene creata implicitamente con questa disposizione;

- lettera b: qui vengono considerate le attività connesse a particolari diritti di accesso a mezzi TIC 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 TIC 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). La lettera b include soprattutto determinati amministratori o responsabili delle applicazioni;
- lettera c: come sensibile sotto il profilo della sicurezza viene infine designato l'accesso alle zone di sicurezza disciplinate nell'articolo 31, poiché in queste zone, a causa delle informazioni e dei mezzi TIC che vi si trovano, il potenziale di danno in caso di spionaggio o di sabotaggio è molto alto.

Il capoverso 3 contiene ulteriori deroghe al vigente disciplinamento secondo l'articolo 19 capoverso 1 LMSI. In virtù della presente legge, ad esempio, l'accesso periodico a dati personali degni di particolare protezione, la cui rivelazione potrebbe pregiudicare pesantemente i diritti personali degli interessati, non rappresenta più un'attività sensibile sotto il profilo della sicurezza. Neanche la gestione di segreti d'affari e di fabbricazione va considerata come sensibile sotto il profilo della sicurezza nel senso della LSIn. Rimane da osservare che una parte delle esigenze relative ai dati personali e ai segreti d'affari e di fabbricazione viene coperta attraverso le norme nell'ambito dei mezzi TIC. Un altro importante cambiamento rispetto all'attuale disciplinamento consiste nel fatto che l'elemento della periodicità nell'esercizio delle attività indicate non è parte integrante della sensibilità sotto il profilo della sicurezza di tale attività. Il trattamento, per un'unica volta, di informazioni classificate «CONFIDENZIALE» è dunque già considerato per la LSIn come sensibile sotto il profilo della sicurezza. Questo cambiamento è necessario in relazione al controllo di sicurezza di terzi destinati a eseguire compiti della Confederazione. Poiché queste categorie di persone non eserciteranno le proprie attività costantemente nell'ambito controllato dalle autorità o organizzazioni assoggettate, a *esse* devono applicarsi presupposti differenziati per l'assoggettamento al CSP.

In merito al rapporto con i controlli di sicurezza relativi alle persone, si veda il numero 1.2.4.

Art. 3

Capoverso 1: con una riserva per le disposizioni della LTras viene stabilito chiaramente che il campo d'applicazione della legge sulla trasparenza non viene limitato in alcun modo dal disciplinamento della sicurezza delle informazioni. Le informazioni che sono state classificate in virtù della LSIn non rientrano nella riserva di cui all'articolo 4 LTras (disposizioni speciali che dichiarano segrete determinate informazioni). Quindi le disposizioni della LTras sull'accesso ai documenti ufficiali trovano applicazione anche alle informazioni che sono state classificate in virtù della LSIn.

La valutazione di documenti nella procedura in virtù della LTras avviene indipendentemente dalle disposizioni della LSIn. Per le domande di accesso ai 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 di informazioni può essere tuttavia considerata come indizio del carattere «non pubblico» del corrispondente documento. La decisione sulla classificazione presuppone infatti una valutazione della necessità di protezione dell'informazione riguardo a un pregiudizio per gli interessi pubblici di cui all'articolo 1 capoverso 2 LSIn che, di per sé, dovrebbe corrispondere materialmente a una valutazione quanto alla limitazione, al differimento e alla negazione di cui all'articolo 7 capoverso 1 LTras. Dal profilo del contenuto, le disposizioni riguardanti la classificazione sono impostate in maniera tale che non dovrebbero contraddire il catalogo delle eccezioni di cui all'articolo 7 LTras.

Per il resto, occorre segnalare che, in linea di massima, il campo d'applicazione della LSIn deve essere più ampio rispetto a quello della LTras, in quanto la LSIn è applicabile a tutte le autorità federali. Si concentra inoltre non soltanto sulla protezione della confidenzialità, bensì protegge anche la disponibilità, l'integrità e la verificabilità di informazioni.

Il capoverso 2 disciplina il rapporto del nuovo atto normativo con le numerose leggi federali che fissano requisiti per la protezione della confidenzialità, della disponibilità, dell'integrità o della verificabilità di informazioni o per la disponibilità e l'integrità di mezzi TIC (si veda l'art. 4 cpv. 2 lett. a-d). Le disposizioni della LSIn devono trovare un'applicazione integrativa per simili leggi. Ciò 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,.

L'esempio della LPD consente di spiegare questo principio. La LPD contiene i requisiti posti al trattamento conforme al diritto, nonché alla protezione di dati personali. Rimane inteso che i dati personali nel settore di compiti delle autorità federali devono e possono continuare a venire trattati secondo le norme della legge sulla protezione dei dati. Poiché, tuttavia, la stessa LPD contiene prescrizioni poco dettagliate riguardanti misure di protezione organizzative, in materia di personale, tecniche e fisiche, le pertinenti prescrizioni della presente legge vanno applicate quale diritto completivo al trattamento di dati personali. Purché, infine, ad esempio per la salvaguardia della sicurezza pubblica, anche dati personali debbano essere valutati come essenziali, essi vanno trattati ed eventualmente classificati secondo le corrispondenti prescrizioni della presente legge.

Capoverso 3: nella Strategia nazionale per la protezione della Svizzera contro i rischi informatici, il Consiglio federale è rimasto fedele al principio del disciplinamento decentralizzato delle infrastrutture critiche. Sempre che vi sia una necessità di agire a livello di legge formale in determinati settori, la corrispondente legislazione specifica deve essere adeguata (si vedano i n. 1.1.2.2 e 1.2.6). Con la LSIn la Confederazione dispone però di strumenti particolari nell'ambito della sicurezza delle informazioni dei quali determinati regolatori e gestori di infrastrutture critiche vorrebbero servirsi, in particolare il CSP. Suscitano interesse in parte anche le disposizioni riguardanti la classificazione o la sicurezza nell'impiego di TIC. Determinate infrastrutture critiche 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 (si vedano gli art. 5 e 24 LENu). Anche nell'ambito della sorveglianza dello spazio aereo (Skyguide), determinati impiegati vengono sottoposti preliminarmente a un CSP. Ora anche taluni impiegati della società nazionale di rete che gestisce la rete di trasporto per l'elettricità a livello svizzero (Swissgrid) andranno sottoposti al CSP. Si mantiene perciò il principio che la legislazione speciale è determinante per un assoggettamento alla LSIn (o a parti di essa).

In merito alla corrispondente modifica della legislazione speciale, si vedano anche i numeri 2.9 e 2.10.

2.1.2 Misure generali per la sicurezza delle informazioni

Art. 4

L'articolo 4 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 gli obiettivi di protezione dettagliati.

Il capoverso 1 stabilisce che le autorità e le organizzazioni assoggettate devono valutare la necessità di protezione delle informazioni per le quali sono competenti. 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 necessità di protezione specifica assai sovente viene implicitamente prevista da altre leggi (si vedano anche l'art. 1 cpv. 2 lett. e l'art. 3 cpv. 2).

Capoverso 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, nello specifico la tutela della confidenzialità, integrità, disponibilità e verificabilità delle informazioni. Spesso vengono menzionati ulteriori criteri di protezione che però, in linea di principio, vengono coperti dai criteri indicati nel capoverso 2 o tutt'al più da una combinazione degli stessi, ad esempio l'autenticità (nella presente legge inclusa sotto «integrità»), l'imputabilità o l'incontestabilità (nella presente legge derivanti dai criteri della «integrità» e della «tracciabilità»).

- Lettera a: il principio della confidenzialità viene concretato nel senso che le informazioni sono 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 assai grande. Se le informazioni vanno rese accessibili al pubblico, la cerchia è illimitata;
- lettera b: la disponibilità delle informazioni non va intesa in senso assoluto, ma, per garantire la capacità di decisione e d'azione delle autorità e organizzazioni, è necessario 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 sempre e senza interruzioni per l'adempimento di compiti essenziali. Ciò vale in particolare nel caso in cui queste informazioni vengano trattate elettronicamente;
- lettera c: la salvaguardia dell'integrità (inalterabilità ed esattezza) delle informazioni è un importante compito parziale della protezione di informazioni che, nell'ottica dell'affidabilità delle autorità, è ri-

levante anche per informazioni destinate a essere pubblicate. È decisiva anche per il corretto funzionamento dei mezzi TIC.

- lettera d: 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'esercizio delle funzioni di controllo e di vigilanza e il modo di procedere in caso di abusi.

Le autorità e le organizzazioni assoggettate devono dunque procedere a una valutazione della necessità di protezione di informazioni e stabiliscono, per quale aspetto e in che misura le informazioni devono essere protette (requisiti di sicurezza). La protezione della confidenzialità è, ad esempio, necessaria solamente se tale confidenzialità deve essere garantita per una ragione giuridica (p. es. LPD, segreti d'affari o di fabbricazione di terzi o art. 14 LSIn). Occorre però anche osservare che determinate informazioni possono avere requisiti più elevati rispetto alla 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 TIC che supportano processi lavorativi critici. La necessità di protezione risulta dunque anche dall'importanza dell'adempimento dei compiti legali nei quali o per sostenere i quali vengono utilizzate le informazioni.

Capoverso 3: per una sicurezza integrale delle informazioni, la protezione della disponibilità e dell'integrità dei mezzi TIC rappresenta un'importante complemento dei quattro criteri menzionati. Sebbene questo requisito, in linea di massima, risulti già dal capoverso 2 lettere b e c, il requisito di una protezione adeguata dall'utilizzazione abusiva e dai disturbi viene ancora menzionato esplicitamente perché il supporto delle TIC ai processi lavorativi assume una rilevanza sempre maggiore. Il loro buon funzionamento rappresenta oggi addirittura un presupposto indispensabile per l'adempimento efficace dei compiti delle autorità federali.

Capoverso 4: la sicurezza delle informazioni deve essere attuata in base ai rischi e in maniera adeguata ed economica. Una valutazione possibilmente obiettiva dei rischi deve essere determinante per l'applicazione di misure di sicurezza (si vedano gli art. 6 e 7). 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 la linea gerarchica deve procedere a una ponderazione degli interessi tra i costi legati alla sicurezza e i benefici derivanti da essa.

In questo contesto viene anche menzionato il principio della praticità. Le persone che trattano informazioni o gestiscono mezzi TIC, spesso devono rispettare determinate norme di comportamento affinché sia garantita la sicurezza delle informazioni (p. es. si deve chiudere a chiave la porta dell'ufficio o crittare una mail). Se però le misure di sicurezza rendono troppo difficile ai collaboratori adempiere i propri compiti, per esperienza è grande la probabilità che non vengano rispettate oppure vengano addirittura eluse di proposito.

Art. 5

La sicurezza è affare dei capi. L'articolo 5 definisce il contenuto della massima responsabilità direttiva nell'ambito della sicurezza delle informazioni ed è diretto perciò soltanto alle autorità assoggettate (art. 2 cpv. 1), che, sole, assumono questa responsabilità.

Nel capoverso 1 le autorità assoggettate vengono invitate a organizzare la sicurezza delle informazioni nel loro ambito di competenza.

- Lettera a: la sicurezza delle informazioni deve essere organizzata, attuata e verificata secondo lo stato della dottrina e della tecnica. Varie norme tecniche non vincolanti formulano cosiddette migliori prassi (*best practices)* in relazione alla gestione della sicurezza delle informazioni (p. es. norme DIN ISO/IEC 27001 e 27002). Particolarmente importante riguardo a queste norme è che, da un lato, sono state sperimentate nella pratica e, dall'altro, sono strutturate secondo il necessario approccio integrale. Stabiliscono inoltre requisiti per l'applicazione di misure di sicurezza che possono essere adeguati ai bisogni delle rispettive autorità, organizzazioni o di parti di esse.

  Autorità più piccole (p. es. Tribunale federale dei brevetti, Tribunale militare di cassazione e autorità di vigilanza sul Ministero pubblico della Confederazione) non potranno ovviamente realizzare da sole una siffatta organizzazione. La legge consente però, ad esempio, ai tribunali della Confederazione di decidere di costituire un'unica organizzazione comune che nel contempo tuteli l'autonomia dei vari tribunali;

- lettera b: la realizzazione della sicurezza delle informazioni concerne molti ambiti specialistici, ad esempio le finanze (ripercussioni finanziarie dell'organizzazione e delle misure), i servizi del personale (compiti del personale), i settori diritto e *compliance* (basi giuridiche della sicurezza delle informazioni), l'informatica (influssi della sicurezza delle informazioni sull'impiego delle TIC nonché applicazione dei

requisiti in sistemi TIC) e il settore «gestione dei rischi e controlling» (sicurezza delle informazioni come parte della gestione dei rischi). Un'efficace sicurezza delle informazioni richiede perciò che gli ambiti specialistici menzionati condividano gli obiettivi della sicurezza delle informazioni e partecipino al processo decisionale, come pure che le misure vengano coordinate trasversalmente tra tali ambiti.

Capoverso 2: per la sicurezza in generale è importante che i compiti e le competenze vengano disciplinati in modo chiaro e inequivocabile. Ciò vale in particolare per la sicurezza delle informazioni, poiché molti ambiti specialistici fisseranno requisiti per il trattamento sicuro di informazioni o assumeranno responsabilità parziali per l'applicazione della presente legge. Competenze poco chiare possono fare sì che rischi sostanziali non vengano identificati, che nessuno si senta responsabile per l'applicazione di talune misure atte a ridurre i rischi o che nessuno assuma consapevolmente i rischi.

Nel capoverso 3 le autorità assoggettate vengono invitate a stabilire, per il loro ambito di competenza, determinati principi intesi a rendere note le loro intenzioni riguardo alla sicurezza delle informazioni.

- Lettera a: gli obiettivi delle autorità assoggettate stabiliscono il livello di sicurezza che deve essere raggiunto (stato AUSPICATO della sicurezza delle informazioni). Questi obiettivi presuppongono un'analisi costi-benefici (di quanta sicurezza vuole beneficiare l'autorità e quanto è disposta a pagarla) e devono essere determinanti per concedere le necessarie risorse. Esempio: i segreti d'affari di terzi che vengono trattati dalle autorità o organizzazioni della Confederazione devono venire protetti dalla conoscenza da parte di persone non autorizzate. Se si vogliono proteggere queste informazioni dai servizi informazioni più attivi e più ricchi di risorse del mondo, allora le misure da adottare sono notevolmente più dispendiose di quelle che si adotteranno se l'autorità accetta il rischio relativamente elevato che tali servizi informazioni esteri si procureranno queste informazioni. Le previste verifiche dell'efficacia (si veda l'art. 24 cpv. 2) si rifanno a questi obiettivi.
- Lettera b: qui si intende disciplinare in particolare come le organizzazioni assoggettate devono gestire i rischi, quali rischi possono correre senza problemi 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 sostenuti a livello operativo (dipartimento, ufficio o addirittura unità subordinata), determinati rischi possono avere un'impronta strategica. Ciò è in particolare il caso per i rischi connessi con informazioni classificate «SEGRETO» (art. 14 cpv. 3) o con mezzi TIC del livello di sicurezza «protezione molto elevata» (art. 21 cpv. 3). I rischi strategici vanno comunicati all'autorità interessata prima che si verifichi un evento.
- Lettera c: in ogni organizzazione ci sono di continuo persone che non prendono sul serio la sicurezza delle informazioni e gestiscono informazioni o mezzi TIC in maniera contraria alle prescrizioni o senza la debita cura. Molto spesso simili infrazioni vengono scusate *a priori* e, di conseguenza, non vengono analizzate. Queste infrazioni possono tuttavia avere, quale conseguenza, considerevoli ripercussioni. Non andrebbero dunque considerate semplicemente come reati minori. Le autorità assoggettate devono perciò imporre in maniera coerente l'applicazione delle prescrizioni, definendo e spiegando le conseguenze in caso di inosservanza.

Capoverso 4: le autorità assoggettate devono provvedere a un'informazione periodica e conforme al rispettivo livello dei quadri e del personale in relazione agli affari inerenti alla sicurezza delle informazioni. Si tratta, ad esempio, di comunicare cambiamenti nel disciplinamento dell'organizzazione e delle competenze oppure di informare i quadri e gli specialisti sulle origini e sulle conseguenze di incidenti. Una comunicazione periodica deve avvenire perché in questo modo i quadri e il personale percepiscono che la direzione riconosce l'importanza della sicurezza delle informazioni e possono reagire ai cambiamenti. Tale comunicazione consente loro, nel proprio ambito di competenza, di trarre gli insegnamenti dagli incidenti. I quadri e il personale andrebbero anche formati di conseguenza.

Art. 6

L'articolo 6 obbliga le autorità e le organizzazioni a esercitare una gestione dei rischi nell'ambito della sicurezza delle informazioni (sulla gestione dei rischi, si veda il n. 1.2.3.2).

Il capoverso 1 stabilisce che le autorità e le organizzazioni assoggettate devono identificare, analizzare, valutare e verificare i rischi, e precisamente sia nel proprio ambito di competenza, sia nell'ambito della collaborazione con terzi. L'ideale sarebbe che tutte le autorità e le organizzazioni assoggettate utilizzino metodi uniformi. Il Consiglio federale definirà in proposito requisiti e misure standard (si veda l'art. 88). Ciò sapendo che i criteri per l'accettazione dei rischi, determinanti per la valutazione di questi ultimi, vengono stabiliti dalle rispettive autorità assoggettate in base alle proprie necessità in materia di sicurezza delle informazioni (si veda anche l'art. 5 cpv. 3 lett. a e b).

La valutazione dei rischi presuppone profonde conoscenze dei compiti legali e dei corrispondenti processi lavorativi critici, la valutazione periodica delle minacce e dei pericoli per i valori da proteggere, l'analisi dei punti deboli, nonché la stima della probabilità che si verifichi un evento e della portata potenziale dei danni che possono risultare da taluni rischi. Il processo di gestione dei rischi nell'ambito della sicurezza delle informazioni deve venire svolto in maniera continua. Ciò vale in particolare per il settore informatico, poiché ogni giorno vengono sviluppati programmi dannosi. Di conseguenza, le applicazioni e i software di sicurezza devono venire aggiornati costantemente.

Secondo il capoverso 2 devono essere adottate le misure necessarie per evitare o ridurre i rischi. Ovviamente i rischi possono anche essere accettati o sostenuti (si veda il cpv. 3). Non dovrebbero però venire ignorati. 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 o si vieta ad esempio di trattare informazioni classificate «SEGRETO» con mezzi TIC in rete). Le misure da adottare appartengono alle seguenti categorie che in parte si sovrappongono:

- *misure organizzative:* ad esempio, emanazione di basi giuridiche, definizione della politica e dell'organizzazione di sicurezza, attribuzione di chiare responsabilità e competenze, classificazione delle informazioni, separazione delle funzioni sensibili sotto il profilo della sicurezza, normative e controlli di accesso per persone, controlli generali, normative di accesso ai sistemi, realizzazione di piani di sicurezza delle informazioni per mezzi TIC, organizzazione del trattamento di incidenti.
- *misure in materia di personale:* ad esempio, formazione e sensibilizzazione, obbligo contrattuale di rispettare la sicurezza delle informazioni, esecuzione di CSP, colloqui personali periodici con persone chiave per promuovere la percezione consapevole di determinati pericoli, definizione e applicazione di sanzioni.
- *misure tecniche:* ad esempio, crittaggio di informazioni, ridondanza di servizi importanti, protezione dai programmi dannosi, forte autenticazione, limitazione all'accesso a reti.
- *misure edili*: ad esempio, recinzione di perimetri sensibili sotto il profilo della sicurezza, utilizzazione di sistemi di chiusura di sicurezza, allestimento di zone e locali di sicurezza, impiego di impianti di sorveglianza.

Il capoverso 3 stabilisce che vanno chiaramente dimostrati i rischi che permangono dopo l'attuazione delle previste misure di sicurezza (cosiddetti rischi residui) o i rischi che non vanno ridotti. 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 dimostrabile e di conseguenza anche essere sostenuti.

Il capoverso 4 rileva che la gestione dei rischi nell'ambito della sicurezza delle informazioni deve essere imperativamente integrata a tutti i livelli nel processo generale di gestione dei rischi della Confederazione. Anche se la gestione dei rischi richiesta nel presente caso è specifica e perciò deve essere gestita ed esercitata da specialisti, la sicurezza delle informazioni rimane un obiettivo che riguarda la gestione di rischi d'esercizio abituali. Le autorità assoggettate devono perciò disciplinare la collaborazione dell'organizzazione specialistica della gestione generale dei rischi con l'organizzazione specialistica della sicurezza delle informazioni.

Art. 7

Il capoverso 1 richiede che nel definire i loro requisiti e le loro misure di sicurezza le autorità e le organizzazioni si orientino ai requisiti e alle misure standard del Consiglio federale di cui all'articolo 88. Per le autorità e le organizzazioni che non sono subordinate al Consiglio federale non sussiste alcun obbligo di seguire questi standard. Poiché un obiettivo importante di questa legge consiste nel raggiungere standard di sicurezza il più possibile uniformi per tutte le autorità, il Consiglio federale viene incaricato di definire requisiti e misure standardizzati secondo lo stato della dottrina e della tecnica. L'economicità impone che non tutte le autorità o organizzazioni debbano «reinventare la ruota» se sono state sviluppate o trovate da un'altra autorità o organizzazione buone soluzioni sperimentate nella pratica.

Capoverso 2: le misure di sicurezza devono orientarsi allo stato della dottrina e della tecnica. La sicurezza delle informazioni è un settore di compiti relativamente recente che evolve periodicamente. Anche se i principi organizzativi hanno raggiunto una certa stabilità e maturità perché sono conformi ai principi organizzativi generali nell'ambito della gestione dei rischi, periodicamente vengono sviluppate misure organizzative migliori che sono più efficaci o più economiche. «*Orientarsi allo stato della dottrina*» significa dunque nel contesto del presente capoverso che le autorità e le organizzazioni assoggettate devono applicare soluzioni e approcci organizzativi collaudati (*best practices).*

Nuovi sviluppi avvengono assai rapidamente nell'ambito della sicurezza tecnica delle informazioni, in particolare nei mezzi TIC, ma anche nella tecnologia dei sensori (p. es. rivelatori di fuoco, calore o movimento) o nella tecnica di chiusura (p. es. sistemi di chiusura per porte). È molto importante che le misure di sicurezza non si basino su tecnologie obsolete, bensì si mostrino efficaci contro le minacce attuali.

Art. 8

Sono considerati terzi secondo la presente legge tutte le autorità, organizzazioni e persone di diritto pubblico o privato che non sono un'autorità o un'organizzazione assoggettata di cui all'articolo 2 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. Le autorità e le organizzazioni che conferiscono i mandati devono provvedere affinché nel conferimento e nell'esecuzione dei mandati vengano rispettate le misure previste dalla legge.

Di regola, questa collaborazione con terzi e le misure di sicurezza da rispettare vengono disciplinate contrattualmente. In linea di massima, terzi dovrebbero ottenere l'accesso a informazioni o a mezzi TIC della Confederazione solamente se hanno attuato le misure necessarie. La LSIn richiede dalle autorità e dalle organizzazioni assoggettate anche che verifichino l'applicazione delle misure. 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 (si veda l'art. 32 segg.) o richiedere l'esecuzione di una PSA (si veda l'art. 56 segg.).

Art. 9

Incidenti nell'ambito della sicurezza delle informazioni si verificheranno anche in futuro. È perciò necessario applicare un approccio uniforme ed effettivo per la gestione di simili incidenti. Le autorità e le organizzazioni assoggettate devono dapprima adottare le misure necessarie per identificare precocemente incidenti riguardanti la sicurezza delle informazioni (p. es. controlli periodici, sensori, impianti d'allarme, sorveglianza della rete, valutazione periodica di *log-file* ecc.). Esse devono definire una procedura in base alla quale agire se vengono identificati eventi 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 valutate. Si intende così migliorare costantemente l'identificazione e il trattamento di incidenti.

Art. 10

Nell'ambito della sicurezza delle informazioni, le autorità devono garantire una cosiddetta gestione della continuità operativa («Business Continuity Management», BCM). BCM significa che vengono adottati tutti i provvedimenti necessari affinché le autorità possano adempiere i loro compiti cruciali entro i termini stabiliti persino in situazioni straordinarie (si veda anche l'art. 6 cpv. 3 LOGA). A motivo della crescente dipendenza dall'impiego delle TIC per adempiere il mandato, i rischi e le pianificazioni preventive nell'ambito della sicurezza delle informazioni vanno inserite obbligatoriamente nel BCM generale delle autorità. La legge richiede l'allestimento di simili pianificazioni preventive solamente per i compiti irrinunciabili delle autorità assoggettate, e non per quelli delle organizzazioni assoggettate. Per l'Amministrazione federale ciò significa che il Consiglio federale deve provvedere affinché, *dal suo punto di vista strategico*, vengano identificati quelli che sono i compiti più critici dell'Amministrazione federale e dell'esercito. Sebbene la legge non li impegni in tal senso, i dipartimenti e le unità amministrative sono comunque liberi di allestire le pianificazioni preventive per i loro compiti critici non considerati dal Consiglio federale.

Art. 11

In merito all'ente di controllo e all'ente di auditing, si veda il numero 1.2.3.3.

Il capoverso 1 richiede dalle autorità e dalle organizzazioni assoggettate che verifichino periodicamente il rispetto delle prescrizioni. In linea di principio, questo controllo spetta ai superiori gerarchici. In conformità con l'articolo 84 capoverso 2 lettera c, anche gli incaricati della sicurezza delle informazioni effettueranno controlli e audit per incarico della propria autorità.

Il capoverso 2 si rivolge soltanto alle autorità assoggettate. Una verifica indipendente periodica è necessaria poiché deve principalmente focalizzarsi sull'efficacia dell'organizzazione della sicurezza delle informazioni. Questa organizzazione include naturalmente i compiti di quelle persone che sono competenti per i controlli ordinari. La decisione, sia sulla periodicità della verifica dell'efficacia, sia sul servizio che deve effettuare la verifica, spetta all'autorità interessata. Le autorità possono, ad esempio, incaricare il proprio servizio di revisione interno oppure una ditta o un servizio esterni. Esse possono anche incaricare il servizio specializzato

della Confederazione per la sicurezza delle informazioni (si veda l'art. 86 cpv. 1 lett. c). Il Consiglio federale può inoltre chiedere al CDF di eseguire simili verifiche.

Art. 12

Il capoverso 1 stabilisce che la classificazione di informazioni è obbligatoria purché siano soddisfatti i criteri per la classificazione di cui all'articolo 14. Oggi ogni autorità assoggettata è, in linea di massima, libera di definire il proprio sistema di classificazione (eventualmente), i propri motivi di classificazione, nonché le proprie prescrizioni in materia di trattamento. Alcuni incidenti negli ultimi anni hanno mostrato che questo trattamento variabile delle informazioni classificate può comportare una maggiore mancanza di fiducia. È necessario un disciplinamento uniforme dei livelli e dei motivi di classificazione.

Con il capoverso 2 si intende enunciare nella legge che, in considerazione del principio di trasparenza e anche dell'onere connesso con la classificazione, la classificazione di informazioni deve, in linea di principio, costituire un'eccezione.

Il capoverso 3 rileva che la classificazione va, per quanto possibile, limitata nel tempo. Spesso, con il passare del tempo, le informazioni non sono più degne di protezione o quest'ultima 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 o comporterebbe problemi dopo l'archiviazione delle informazioni. 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 in anticipo una classificazione temporanea, mediante l'obbligo di verificare periodicamente la necessità delle classificazioni, contenuto nel capoverso 4, si garantisce che le informazioni non rimangano classificate inutilmente.

Art. 13

Capoverso 1: le autorità assoggettate devono stabilire chi è competente per la classificazione. Nell'Amministrazione federale oggi questa competenza viene 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. La normativa del Consiglio federale non deve però essere vincolante per le altre autorità federali, le quali così possono anche decidere che la classificazione, ad esempio, può essere fatta dalla direzione dell'autorità, da un organo competente centrale o soltanto della linea gerarchica. La nozione di «servizio incaricato della classificazione» è importante in particolare per decidere in merito alla cerchia dei destinatari abilitati, per declassificare, archiviare e distruggere informazioni classificate, ma anche per eventuali misure di protezione provvisorie che devono essere adottate se vengono minacciate informazioni classificate (si veda l'art. 18).

Nel capoverso 2 viene disciplinato il carattere vincolante della classificazione. 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. A una modifica o a una soppressione della classificazione può, in linea di massima, procedere solamente il servizio che ha stabilito la classificazione. Rimane inteso che anche qui sono previsti la via di servizio, la vigilanza gerarchica e le relative 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.

Art. 14

In merito agli obiettivi del disciplinamento della classificazione, si veda il numero 1.2.3.4.

L'articolo 14 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 per la classificazione 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: la protezione degli interessi pubblici ai sensi della lettera e non rappresenta un vero e proprio motivo 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 massima, 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 vale per informazioni che vengono trattate presso i tribunali o i ministeri pubblici nell'ambito dei loro procedimenti ordinari. La maggioranza 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 o devono invece venire

classificate. Se, ad esempio, vengono trattati in un sistema d'informazione dati personali degni di particolare protezione, allora deve venire classificato il corrispondente concetto 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* gli interessi in questione: 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 fattispecie 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 questo potenziale pregiudizio per gli interessi protetti. Indispensabile è quindi 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. Pur se la protezione della libera formazione dell'opinione e della volontà delle autorità e delle organizzazioni assoggettate viene considerata 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.

La proposta indicata qui con tre livelli di classificazione corrisponde formalmente alle norme dell'OPrI vigenti attualmente. Come menzionato all'inizio, vengono però aumentati i valori limite per la classificazione nei rispettivi livelli (sulla relazione con il principio di trasparenza si veda l'art. 3 cpv. 1).

Capoverso 1: una classificazione «AD USO INTERNO» viene richiesta se una comunicazione dell'informazione ha quale conseguenza un pregiudizio per gli interessi pubblici di cui all'articolo 1 capoverso 2 lettere a-d. Quale criterio per distinguere tra «non classificato» e «classificato» occorre quindi, anche nel caso di un pregiudizio «semplice» agli interessi in questione, che vi siano indizi qualificati in grado di giustificare la classificazione «AD USO INTERNO». Il danno potenziale che può derivare da una conoscenza da parte di persone non autorizzate, non può essere semplicemente trascurabile: il pregiudizio per gli interessi di cui all'articolo 1 capoverso 2 lettere a-d deve piuttosto essere sensibile.

Quando si tratta di *informazioni rilevanti per la sicurezza* ai sensi dell'articolo 1 capoverso 2 lettera b, il valore soglia per la classificazione «AD USO INTERNO» viene per lo più raggiunto relativamente in fretta. «AD USO INTERNO» viene anche utilizzata il più sovente per siffatti casi. Così, singole documentazioni di sicurezza su mezzi TIC o semplici piani d'intervento di forze di sicurezza possono, di regola, venire classificate «AD USO INTERNO». Ma, ad esempio, è anche ipotizzabile che il fatto di conoscere uno scadenzario per l'applicazione di una misura concreta potrebbe procurare un vantaggio ingiustificato a determinate persone. Anche se così non verrebbe impedita la misura in quanto tale, verrebbe per lo meno pregiudicata la sua attuazione conforme alla legge e quindi la capacità di decisione e d'azione dell'autorità federale interessata. In questo caso sarebbe giustificata una classificazione «AD USO INTERNO» dello scadenzario limitata nel tempo.

In linea di principio, classificazioni globali «AD USO INTERNO» sono contrarie alle prescrizioni. La prassi (ipotetica) di un'unità organizzativa dell'Amministrazione federale, in virtù della quale tutti gli appunti di colloqui e verbali di sedute verrebbero classificati fin da principio «AD USO INTERNO», ignorando l'effettiva necessità di protezione delle informazioni, contraddirebbe sia lo spirito della LTras sia la norma del capoverso 1. Sarebbe invece, ad esempio, giustificata la classificazione di verbali di sedute *con contenuto operativo* dal settore di fedpol. Tuttavia, di regola, le informazioni dai lavori di commissioni parlamentari *possono* venire classificate «AD USO INTERNO». In questo modo può essere fatta chiarezza in merito a quali informazioni dal lavoro parlamentare, per la protezione della libera formazione dell'opinione e della volontà del Parlamento, sono destinate soltanto a una cerchia di persone limitata.

Capoverso 2: per la classificazione «CONFIDENZIALE» è richiesto che gli interessi di cui all'articolo 1 capoverso 2 lettere a-d possano essere «*gravemente pregiudicati*» nel caso di una conoscenza non autorizzata. In confronto all'attuale norma, in virtù della quale è richiesto semplicemente un «danno» non qualificato (art. 6 OPrI), la nuova normativa proposta rappresenta un aumento dei requisiti per la classificazione.

Anche la concretizzazione dettagliata della nozione di «*grave pregiudizio*» deve ancora avvenire tenendo conto della politica in materia di gestione dei rischi. Con l'espressione scelta è tuttavia richiesto un danno chiaro, ad esempio:

- la libera formazione dell'opinione e della volontà delle autorità assoggettate viene 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 viene reso considerevolmente più difficile su un lungo periodo;
- determinate risorse dell'esercito o degli organi di sicurezza della Confederazione non sono temporaneamente operative;
- la posizione della Svizzera nell'ambito di negoziati internazionali viene resa considerevolmente più difficile;
- la sicurezza di persone o gruppi di persone viene minacciata;
- alla Confederazione ne deriva un considerevole danno finanziario.

Capoverso 3: per la classificazione «SEGRETO» (massimo livello di classificazione) è richiesto che gli interessi di cui all'articolo 1 capoverso 2 lettere a-d possano essere «*gravemente pregiudicati*» nel caso di una conoscenza non autorizzata. Come per i livelli di classificazione «AD USO INTERNO» e «CONFIDENZIALE», anche per questo livello di classificazione deve essere ancora concretizzata la nozione chiave di «*grave pregiudizio*». Con la formulazione scelta è tuttavia richiesto un danno 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 resa seriamente più difficile su un lungo periodo;
- l'adempimento di compiti irrinunciabili di un'organizzazione assoggettata viene temporaneamente impedito o reso seriamente più difficile su un lungo periodo;
- risorse essenziali dell'esercito o degli organi di sicurezza della Confederazione non sono operative;
- la vita e l'integrità di gruppi della popolazione vengono minacciate;
- la fornitura di prestazioni di servizi da parte di infrastrutture critiche viene interrotta;
- le funzioni di un impianto nucleare particolarmente sensibili sotto il profilo della sicurezza vengono sabotate;
- la Confederazione subisce un grave danno finanziario.

Art. 15

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 ad avere 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 incarico 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 (si veda l'art. 32 segg.) può inoltre costituire un ulteriore presupposto per il trattamento.

Capoverso 2: la maggioranza dei Paesi e delle organizzazioni internazionali con i quali la Svizzera ha concluso un accordo per lo scambio di informazioni classificate richiede che le loro informazioni classificate vengano 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 possono

dunque, in linea di massima, essere rese accessibili a persone di altra nazionalità. È fatta salva un'autorizzazione preliminare dell'autore delle informazioni classificate.

Art. 16

Capoverso 1: le informazioni classificate devono venire trattate in modo tale da venire protette dalla conoscenza da parte di persone non autorizzate. Questa protezione deve essere garantita per l'intero periodo durante il quale le informazioni in questione sono considerate degne di essere protette. Le informazioni classificate non vengono archiviate fintanto che, secondo le disposizioni della LSIn, sono ancora degne di essere protette.

Conformemente al capoverso 2, le informazioni classificate devono contenere un'indicazione relativa al servizio incaricato della classificazione. Questa indicazione è importante in particolare per declassificare, archiviare e distruggere informazioni classificate, ma anche per eventuali misure di protezione provvisorie che devono essere adottate se tali informazioni classificate sono minacciate (si veda l'art. 18).

Capoverso 3: sempre che la Svizzera abbia concluso un accordo per lo scambio di informazioni classificate con un determinato Paese o una determinata organizzazione internazionale, il trattamento delle informazioni che rientrano nel campo d'applicazione di tale accordo viene disciplinato secondo le particolari prescrizioni previste nell'accordo stesso. In mancanza di quest'ultimo, il trattamento di informazioni classificate provenienti dall'estero si fonda sulle prescrizioni della LSIn e sulle sue disposizioni d'esecuzione.

Art. 17

L'articolo 17 capoverso 1 contiene una riserva del diritto procedurale dell'Assemblea federale e di quello dei tribunali e dei ministeri pubblici. Per la comunicazione di 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 fino a che punto simili informazioni possono essere rese accessibili ai partecipanti alla procedura per consultazione, fino a che punto possono essere rese note nell'ambito di procedure pubbliche o fino a che punto i testimoni possono rifiutare di deporre adducendo obblighi legali di mantenere il segreto (si vedano p. es. gli art. 47, 150, 153 e 154 LParl, gli art. 56 cpv. 2 e 59 cpv. 2 LTF, gli art. 16 cpv. 2, 18 cpv. 2, 27 e 28 PA, l'art. 40 cpv. 3 LTAF o gli art. 70, 170, 173 cpv. 2 e 194 cpv. 2 CPP, nonché gli art. 45, 48 cpv. 2, 77 PPM; si veda anche l'art. 58 dell'ordinanza del 24 ottobre 1979 concernente la giustizia penale militare [RS 322.2]).

Tuttavia, conformemente al capoverso 2, prima di decidere in merito alla comunicazione di informazioni classificate si può dare al servizio incaricato della classificazione l'opportunità di esprimersi quanto ai motivi di classificazione e consultarlo in merito alle eventuali ripercussioni di una comunicazione. L'organo o il tribunale competenti decideranno poi come procedere ulteriormente alla luce delle circostanze.

Art. 18

Gli obblighi qui formulati corrispondono dal profilo materiale ai vigenti articoli 15 e 16 OPrI. Purché il servizio incaricato della classificazione non risulti evidente dall'informazione, la comunicazione va fatta all'autorità di vigilanza competente che, avvalendosi del suo potere di apprezzamento, deve stabilire come procedere ulteriormente.

Art. 19

Il capoverso 1 richiede previamente dalle autorità assoggettate (ma non dalle organizzazioni) che stabiliscano una procedura per l'attuazione e il miglioramento continui della sicurezza delle informazioni nell'impiego di mezzi TIC. La procedura deve definire compiti, competenze e responsabilità inerenti alla sicurezza di quei servizi che pianificano e decidono l'impiego di mezzi TIC nonché li sviluppano, esercitano, amministrano, modificano, mantengono, verificano e infine li mettono fuori servizio. La procedura include in particolare i disciplinamenti materiali degli articoli 20-26.

Tutte le autorità federali utilizzano già oggi una simile procedura. Ma queste procedure devono essere sistematizzate e, dove necessario, completate. Le più importanti fasi procedurali devono venire uniformate. Spesso, inoltre, l'esecuzione della procedura non viene verificata o viene verificata soltanto parzialmente. Soltanto assai di rado le misure attuate vengono verificate quanto alla loro efficacia.

Conformemente al capoverso 2 la competenza per l'esecuzione della procedura di sicurezza spetta a quell'autorità o a quell'organizzazione che conferisce il mandato dell'impiego di mezzi TIC (beneficiario di prestazioni). Il beneficiario di prestazioni è infatti responsabile dei processi lavorativi e dell'attuazione dei requisiti di sicurezza. Deve perciò comunicare chiaramente le proprie esigenze aziendali e di sicurezza a quel servizio che gestisce i mezzi TIC (fornitore di prestazioni).

Nel capoverso 3 viene stabilito il principio che la procedura di sicurezza (o almeno le relative fasi procedurali) deve essere ripetuta in caso di mutamento dei rischi. La sicurezza delle informazioni è una condizione che cambia in modo continuo e dinamico. Le autorità assoggettate devono perciò fissare la verifica periodica o in base ai rischi delle condizioni di sicurezza e la ripetizione della procedura.

Art. 20

L'analisi delle necessità di protezione di cui al capoverso 1 rappresenta la prima fase della procedura di sicurezza. Un servizio che esegue lo sviluppo, l'acquisizione o la modifica di un mezzo TIC o conferisce un mandato in tal senso, vuole impiegare questo mezzo TIC per determinati scopi e per una durata stabilita. Questa prima fase in relazione all'attuazione della sicurezza delle informazioni consiste, nella definizione della finalità d'impiego del mezzo TIC, nel determinare i processi lavorativi che vanno supportati con il mezzo TIC 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 di cui all'articolo 4 capoverso 1 e valutare le potenziali ripercussioni di disturbi o di un'utilizzazione abusiva del mezzo TIC da impiegare sugli interessi di cui all'articolo 1 capoverso 2. Nella valutazione della necessità di protezione occorre anche considerare che i mezzi TIC per lo più vengono messi in rete e gestiti in un determinato ambiente tecnico e/o logico (cosiddetta architettura). L'identificazione precoce delle interconnessioni e dipendenze aiuta anche ad attuare le misure di sicurezza là dove sono più efficaci.

Oggigiorno, in parte non si procede ad alcuna valutazione della necessità di protezione oppure essa viene avviata solamente quando il mezzo TIC è già in funzione. L'attuazione a posteriori di misure di sicurezza è però, di regola, molto più difficile da realizzare e genera costi nettamente maggiori.

Dall'analisi delle necessità di protezione risultano i requisiti posti alla protezione della confidenzialità, disponibilità, integrità e verificabilità delle informazioni, nonché alla disponibilità e all'integrità del mezzo TIC. L'analisi delle necessità di protezione è anche determinante per i livelli di sicurezza dei mezzi TIC di cui all'articolo 21.

Nel capoverso 2 viene disciplinato il caso di un'autorità o di un'organizzazione che vuole impiegare una nuova tecnologia (hardware o software), dunque non solamente un nuovo mezzo TIC. L'autorità o l'organizzazione interessata deve valutare i rischi connessi con l'impiego di questa nuova tecnologia prima di impiegarla. Si richiede poi che l'autorità o l'organizzazione comunichi la sua valutazione dei rischi al servizio specializzato della Confederazione per la sicurezza delle informazioni. Informando il servizio specializzato si intende garantire che le nuove tecnologie possibilmente vengano valutate soltanto una volta e che tutte le autorità e le organizzazioni assoggettate ne possano trarre un adeguato vantaggio. Le valutazioni dei rischi eseguite devono servire anche a esaminare la conformità delle nuove tecnologie con le basi, anche strategiche, esistenti.

Conformemente all'articolo 86 capoverso 1 lettera d, le autorità assoggettate hanno la possibilità di incaricare il servizio specializzato della Confederazione di eseguire questa valutazione dei rischi.

Art. 21

L'articolo 21 sistematizza e uniforma i livelli di sicurezza dei mezzi TIC per tutte le autorità e le organizzazioni assoggettate. 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 con tre livelli si rifà allo standard del *Bundesamt für Sicherheit in der Informationstechnik* (BSI) tedesco.

I livelli di sicurezza sono in primo luogo una misura per identificare la criticità di un determinato mezzo TIC in relazione agli interessi pubblici di cui all'articolo 1 capoverso 2. L'assegnazione a un livello di sicurezza stabilisce anche quali requisiti di sicurezza si applicano e come devono essere definite le misure di protezione (si vedano gli art. 22-24). Per ogni livello di sicurezza, il Consiglio federale deve fissare requisiti e misure di sicurezza standardizzati quanto a protezione della confidenzialità, integrità, disponibilità e verificabilità (si veda l'art. 88). La standardizzazione dei requisiti e delle misure di sicurezza è obbligatoriamente necessaria per uno scambio di informazioni tra autorità efficiente e sicuro. Essa presenta un importante vantaggio: ai servizi di sviluppo e agli organi di acquisizione di mezzi TIC vengono indicati sin dall'inizio chiari requisiti di sicurezza da adempiere che li aiuteranno nell'implementare la sicurezza nei mezzi TIC. I costi della sicurezza diventano più trasparenti e più semplici da calcolare e pianificare (i costi legati alla sicurezza sono costi progettuali).

Capoverso 1: il livello di sicurezza «protezione di base» si applica a tutti i mezzi TIC che non presentano requisiti di protezione delle informazioni particolarmente elevati (si veda anche l'art. 22). 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, vengono trattate con mezzi così classificati.

Capoverso 2: ai mezzi TIC del livello di sicurezza «protezione elevata» si applicano, oltre ai requisiti della protezione di base, requisiti e misure di sicurezza particolari, ad esempio il requisito dell'allestimento di un concetto in materia di sicurezza delle informazioni, nonché l'esecuzione di un CSP per le persone che devono provvedere all'esercizio, all'amministrazione, alla manutenzione o alla verifica di simili mezzi.

- Lettera a: i mezzi TIC rientrano in questo livello di sicurezza se le informazioni che vanno trattate con essi presentano requisiti elevati quanto a confidenzialità, disponibilità, integrità o verificabilità. I rispettivi requisiti vengono valutati riguardo a un pregiudizio potenzialmente considerevole per gli interessi di cui all'articolo 1 capoverso 2 che può essere causato dalla violazione di uno dei quattro criteri di protezione menzionati. Per le informazioni classificate «CONFIDENZIALE» il pregiudizio potenziale è già contenuto nella definizione del livello di classificazione (*considerevole* pregiudizio). I mezzi TIC con i quali vanno trattate le informazioni classificate «CONFIDENZIALE» rientrano quindi nel livello «protezione elevata». Ciò vale anche per i mezzi TIC che vanno utilizzati per il trattamento di dati personali degni di particolare protezione o di segreti professionali o di fabbricazione, sempre che il danno potenziale in caso di violazione della confidenzialità di queste informazioni sia considerevole.
- Lettera b: se con un mezzo TIC vengono supportati processi lavorativi il cui venire meno può comportare un considerevole pregiudizio per la capacità d'azione di un'autorità, allora il mezzo TIC va parimenti assegnato a questo livello di sicurezza. Ma la lettera b è di fatto già contenuta nella lettera a, poiché le TIC servono esclusivamente al trattamento di informazioni e non sono fini a se stesse. I disturbi e l'utilizzazione abusiva della funzionalità del mezzo TIC stesso vengono però ripresi nella legge come motivo di classificazione perché questa norma è assai più comprensibile per molti non specialisti.

Capoverso 3: i mezzi TIC rientrano nel livello «protezione molto elevata» se le informazioni che vanno trattate con essi presentano requisiti molto elevati quanto a confidenzialità, disponibilità, integrità o verificabilità. Questa disposizione si sviluppa in modo identico al capoverso 2, ma il danno potenziale deve essere *grave*. Qui si tratta ad esempio di mezzi TIC con i quali vengono trattate informazioni classificate «SEGRETO», o di quelli il cui venire meno può arrecare gravi danni agli interessi di cui all'articolo 1 capoverso 2.

Art. 22

Capoverso 1: la prassi ha mostrato che con un adeguato numero di determinati e predefiniti requisiti e misure i rischi per una maggioranza dei mezzi TIC possono essere ridotti a un'entità accettabile. La totalità di tutti questi requisiti e misure forma la protezione di base. Il vantaggio di una protezione di base definita e standardizzata consiste nel fatto che, per i mezzi TIC di questo livello, le autorità e le organizzazioni non devono effettuare valutazioni dei rischi dettagliate e dispendiose. Le autorità assoggettate devono stabilire quale livello di sicurezza minimo vogliono richiedere per tutti i loro mezzi TIC. Fissare una protezione di base non è una faccenda tecnica che va decisa da esperti, bensì un compito direttivo che presuppone la ponderazione di obiettivi in materia di sicurezza e costi. Secondo l'intensità della protezione di base, le misure organizzative, in materia di personale, tecniche e fisiche da attuare possono infatti risultare più o meno costose.

Il capoverso 2 stabilisce il principio che, indipendentemente dal livello di sicurezza assegnato loro, tutti i mezzi TIC devono adempiere i requisiti della protezione di base. Essa viene quindi anche definita come fondamenta sulle quali devono svilupparsi mezzi TIC dei livelli di sicurezza «protezione elevata» e «protezione molto elevata». Le misure della protezione di base devono quindi essere configurate anche in maniera relativamente flessibile e modulare. Se determinate misure non sono attuabili per un particolare mezzo TIC, vanno applicate altre misure che consentono una protezione equivalente.

Art. 23

Capoverso 1: per i mezzi TIC dei livelli di sicurezza «protezione elevata» e «protezione molto elevata» non bastano i requisiti e le misure della protezione di base. Per simili mezzi viene dapprima richiesta l'esecuzione di un'analisi dei rischi riferita 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, un mezzo TIC viene classificato nel 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. Dopo l'analisi dei rischi, deve essere allestito un concetto in materia di sicurezza delle informazioni. La responsabilità in merito è del beneficiario delle prestazioni, ma è necessaria una stretta collaborazione con il fornitore di prestazioni. L'applicazione delle misure tecniche si situa infatti, in linea di principio, nell'ambito di competenza di quel servizio che provvederà all'esercizio del mezzo TIC e per questo dispone del know-how tecnico.

Il capoverso 2 stabilisce le competenze per la verifica e l'approvazione del concetto in materia di sicurezza delle informazioni. Per assicurare che il concetto in materia di sicurezza delle informazioni venga verificato da personale comprovatamente competente, la legge richiede che sia l'incaricato della sicurezza delle informazioni (art. 84) a procedere a queste verifiche. Si tratta di esaminare se il concetto adempie i requisiti formali, giuridici e aziendali, così che descriva l'effettivo stato della sicurezza delle informazioni e mostri nel dettaglio i rischi residui da sostenere. L'ideale sarebbe che l'incaricato della sicurezza delle informazioni accompagni l'allestimento del concetto in materia di sicurezza delle informazioni per riconoscere precocemente eventuali problemi e risolverli in modo mirato. In seguito il concetto in materia di sicurezza delle informazioni deve essere approvato dall'autorità o dall'organizzazione stessa. Questa approvazione ha luogo già nella fase di pianificazione o in quella concettuale, dunque ancora prima che il progetto TIC si trovi nella fase di realizzazione. In questo modo si intende garantire che la direzione assuma precocemente la propria responsabilità riguardo alla sicurezza delle informazioni. Essa non deve trovarsi nella situazione di dover decidere praticamente alla vigilia dell'entrata in servizio del mezzo TIC (si veda l'art. 25), quando sono già stati impiegati notevoli mezzi finanziari.

Capoverso 3: il concetto in materia di sicurezza delle informazioni non è un documento che deve essere allestito semplicemente una volta (in occasione della pianificazione dell'impiego di un mezzo TIC) e poi rimane in forma invariata. Le misure pianificate spesso non coincidono con quelle effettivamente attuate. Perciò, il concetto in materia di sicurezza delle informazioni deve essere costantemente aggiornato per descrivere l'attuale stato della sicurezza. Anche nel caso di mutamenti dei rischi deve essere adeguato di conseguenza.

Art. 24

Il capoverso 1 richiede, per tutti i mezzi TIC che ottengono il nullaosta per la messa in funzione in conformità con i criteri di sicurezza, una prova che la procedura di sicurezza è stata eseguita conformemente al diritto e che sono state attuate le misure della protezione di base o eventualmente del concetto in materia di sicurezza delle informazioni. Le autorità assoggettate devono stabilire chi deve eseguire questa verifica.

Capoverso 2: per i mezzi TIC del livello di sicurezza «protezione molto elevata» si richiede in più che venga verificata l'efficacia delle misure attuate. In occasione di tale verifica dell'efficacia vengono eseguiti attacchi reali contro il mezzo TIC, così da identificare e correggere prima della messa in funzione eventuali falle nella sicurezza e punti deboli che qualcuno potrebbe sfruttare a proprio vantaggio (p. es. mediante test di penetrazione, *penetration test*). La verifica dell'efficacia viene richiesta solamente per i mezzi TIC del livello «protezione molto elevata», perché è connessa a un onere finanziario non indifferente (dallo 0,5 al 2 per cento del totale dei costi di investimento).

Art. 25

Capoverso 1: la direzione dell'autorità o dell'organizzazione beneficiaria delle prestazioni assume la responsabilità della sicurezza delle informazioni. Si richiede perciò che la stessa direzione dell'autorità o dell'organizzazione rilasci il nullaosta per la messa in funzione dei propri mezzi TIC in conformità con i criteri di sicurezza.

Capoverso 2: il nullaosta di sicurezza significa che l'autorità o l'organizzazione conosce i rischi residui identificati ed è 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.

Art. 26

Per una gestione efficace dei rischi è necessario mantenere una visione d'insieme su tutti i mezzi TIC impiegati. Le autorità e le organizzazioni assoggettate devono perciò registrare in un inventario o in un portafoglio i mezzi TIC che impiegano. Tutti i mezzi TIC devono potere essere attribuiti a una persona o a un servizio competente.

L'inventario deve fra l'altro contenere i livelli di sicurezza dei mezzi TIC, il nome della persona o la denominazione del servizio competenti, le documentazioni di sicurezza, nonché tutte le dovute informazioni sul sistema che sono necessarie per ripristinare l'esercizio nel caso di un disturbo o di una interruzione del funzionamento dei mezzi TIC.

Art. 27

Autorità, organizzazioni o terzi che gestiscono mezzi TIC su mandato delle autorità e delle organizzazioni assoggettate, sono responsabili di garantire la sicurezza delle informazioni nell'esercizio di tali mezzi. I fornitori di prestazioni interni rientrano tutti nel campo d'applicazione della presente legge e devono perciò applicare anche gli articoli 19-26 alle proprie attività. I fornitori di prestazioni esterni, per contro sono considerati terzi ai sensi dell'articolo 8 e devono essere obbligati contrattualmente a osservare le misure della pre-

sente legge. Le autorità e le organizzazioni assoggettate che danno mandato di gestire i mezzi TIC devono convenire con il fornitore di prestazioni i loro requisiti inerenti ai mezzi.

Nell'esercizio, quanto alla sicurezza delle informazioni, il fornitore di prestazioni deve assicurare le seguenti capacità e attività:

- gestione della rete, ad esempio: ruoli e responsabilità; design della rete; audit di sicurezza;
- gestione del traffico, ad esempio: configurazione di dispositivi di rete; normative per la gestione degli accessi, crittaggio e autenticazione; *firewall*; accessi esterni; accessi attraverso tecnologie *wireless*;
- esercizio della rete, ad esempio: descrizioni dettagliate delle prestazioni e osservanza degli accordi sui livelli di servizio *SLA*; monitoraggio (incl. sorveglianza della rete); *release-*, *change-*, *life-cycle-management*; *incident-* e *security-management; capacity-* e *ressource-management; desaster-* e *recovery-management*;
- rapporto di audit al beneficiario delle prestazioni.

Art. 28

Le persone che devono gestire informazioni o mezzi TIC della Confederazione, devono soddisfare determinati requisiti. Spetta al datore di lavoro o al mandante provvedere affinché i lavoratori o i mandatari adempiano questi requisiti.

- Lettera a: nella scelta delle persone da assumere o da incaricare, i criteri devono corrispondere a quelli per le informazioni degne di protezione o alla criticità dei mezzi TIC. 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;
- lettera b: 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 formati e sensibilizzati periodicamente. Occorre prestare particolare attenzione all'istruzione dei superiori;
- lettera c: sempre che gli impiegati o i mandatari debbano gestire informazioni che presentano requisiti elevati quanto alla protezione dalla confidenzialità, devono essere tenuti a mantenere il segreto. In virtù dell'articolo 22 LPers, gli impiegati della Confederazione che sono sottoposti alla LPers devono mantenere il segreto d'ufficio. Per i terzi che eseguono mandati per la Confederazione, l'obbligo di mantenere il segreto deve essere stabilito per scritto nel contratto ed essere connesso a chiare conseguenze in caso di inosservanza.

Art. 29

Chi lavora o esegue un mandato per un'autorità federale necessita eventualmente, per adempiere i compiti, di un accesso a determinate informazioni, mezzi TIC o locali. Il capoverso 1 enuncia un principio centrale della sicurezza delle informazioni. 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.

Il capoverso 2 richiede l'amministrazione permanente di queste autorizzazioni. 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 subito bloccate o revocate. Entrambe le misure devono contribuire a ridurre il rischio di un reato dall'interno.

Il capoverso 3 richiede un processo adeguato per verificare periodicamente le autorizzazioni.

Art. 30

Con le misure di protezione fisiche si tratta di ridurre i rischi dovuti a minacce fisiche. Fanno tra l'altro parte di questi rischi atti umani quali lo spionaggio, il furto, il vandalismo o il sabotaggio, ma anche i danni causati da elementi naturali, quali quelli dovuti al calore, al fuoco, all'acqua, alla polvere, alle vibrazioni ecc. Per la valutazione delle misure di protezione fisica, della cosiddetta protezione delle opere, è competente fedpol in collaborazione con l'UFCL. Per parti del DDPS e l'esercito, è competente la PIO in collaborazione con armasuisse o l'UFCL.

Il capoverso 1 stabilisce il principio che le autorità e le organizzazioni assoggettate devono garantire la protezione fisica delle loro informazioni e dei loro mezzi TIC nei loro locali. Occorre in particolare impedire l'accesso non autorizzato a informazioni o mezzi TIC, ad esempio mediante controlli dell'entrata, videocamere, sistemi di chiusura, locali e contenitori di sicurezza, apparecchi di distruzione di documenti e di supporti di dati, protezione visiva ecc. Contro i danni causati da elementi naturali vengono ad esempio impiegati impianti di rivelazione e di segnalazione di incendi e impianti di spegnimento automatici.

Il capoverso 2 disciplina il caso di informazioni o mezzi TIC che sono accessibili pubblicamente. Si tratta, da un lato, di informazioni e mezzi TIC che vengono portati via dal loro posto abituale (ufficio) e che in seguito, al di fuori del perimetro di sicurezza abituale, devono essere protetti adeguatamente. Ma si tratta anche di informazioni e installazioni, cavi e linee di distribuzione che non stanno 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. 31

Nella LSIn, la nozione di «zona di sicurezza» viene utilizzata per locali e settori nei quali sovente vengono trattate informazioni classificate del livello «CONFIDENZIALE» o «SEGRETO» o gestiti mezzi TIC del livello di sicurezza «protezione elevata» o «protezione molto elevata» e che a tale scopo vengono particolarmente protetti. L'esclusione di questi locali o settori quale zona di sicurezza rappresenta una misura fisica della sicurezza delle informazioni che già oggi viene parzialmente adottata presso la Confederazione, in particolare per proteggere i locali dei server o determinati locali di condotta. Una zona di sicurezza deve essere predefinita, identificabile ed essere protetta di conseguenza. Le disposizioni d'esecuzione del Consiglio federale definiranno probabilmente due generi di zone di sicurezza, secondo la criticità delle informazioni o dei mezzi TIC. Le misure nelle zone di sicurezza dei rispettivi livelli dovranno essere impostate in funzione dei rischi. Il Consiglio federale e i servizi federali competenti per la protezione delle opere (fedpol, UFCL, PIO e armasuisse), stabiliranno misure standard per le zone di sicurezza in collaborazione con il servizio specializzato della Confederazione per la sicurezza delle informazioni (si veda l'art. 88).

Nel capoverso 1 vengono dapprima stabiliti i presupposti per designare una zona di sicurezza in virtù della LSIn: nel settore da designare devono sovente venire trattate informazioni classificate «CONFIDENZIALE» o «SEGRETO» o gestiti mezzi TIC del livello di sicurezza «protezione elevata» o «protezione molto elevata». Contrariamente alla legislazione di altri Paesi o di organizzazioni internazionali (si veda anche cpv. 5), per le autorità e le organizzazioni assoggettate in virtù della LSIn non sussiste però alcun obbligo di designare simili settori quali zone di sicurezza. In merito al loro effettivo allestimento decide la valutazione dei rischi.

Il capoverso 2 stabilisce che solamente le persone identificate e autorizzate possono ottenere l'accesso a una zona di sicurezza. L'accesso deve dunque essere necessario per adempiere un determinato compito. Ciò presuppone corrispondenti controlli d'accesso e la verbalizzazione degli accessi.

Il capoverso 3 disciplina i particolari poteri dell'autorità o dell'organizzazione che allestisce una zona di sicurezza:

- lettera a: per il controllo dell'accesso l'autorità o l'organizzazione può utilizzare metodi di identificazione biometrici (p. es. impronta digitale o scansione dell'iride). Questi metodi di identificazione sono nettamente più affidabili dell'identificazione mediante un normale documento. Già oggi vengono impiegati in taluni ambiti;
- lettera b: può essere limitata la possibilità di prendere con sé taluni oggetti in una zona di sicurezza. Di regola, prendere con sé apparecchi per registrazioni audiovisive (incl. *smartphone* o *notebook* con pertinenti funzioni) è consentito soltanto con un'autorizzazione particolare;
- lettera c: 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 venire essere mediante apparecchi di registrazione video;
- lettera d: all'entrata o all'uscita, l'autorità o l'organizzazione può far eseguire controlli di borse e persone. In questo modo si intende impedire che persone portino con sé senza autorizzazione apparecchi nella zona di sicurezza (si veda la lettera b) o sottraggano informazioni (p. es. con una chiave USB);
- lettera e: per applicare prescrizioni in materia di sicurezza delle informazioni, devono essere possibili controlli di uffici anche in una zona di sicurezza. Nei controlli di uffici viene fra l'altro verificato il rispetto della cosiddetta *«Clean Desk Policy»* (non devono esserci sulla scrivania o in altro luogo informazioni degne di protezione, 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.

Conformemente al capoverso 4, in determinate zone di sicurezza l'autorità o l'organizzazione deve avere la possibilità, se necessario, di esercitare un impianto di telecomunicazione che provoca interferenze di cui all'articolo 34 capoverso 1ter della legge del 30 aprile 1997 sulle telecomunicazioni (LTC; RS 784.10). L'effettiva necessità e le condizioni per l'esercizio di un simile impianto vengono valutate in virtù della LTC.

Nel capoverso 5 vengono fatte salve le prescrizioni per zone di sicurezza conformemente ai trattati internazionali (art. 90) e le corrispondenti prescrizioni sulla protezione di impianti militari. In entrambi i casi, l'allestimento di una zona di sicurezza o di una zona di protezione non costituisce un'opzione, bensì un obbligo (si veda, p. es., ISA CH-EU).

2.1.3 Controlli di sicurezza relativo alle persone

Art. 32

Il controllo di sicurezza relativo alle persone (CSP) è una misura preventiva per la protezione contro gli autori di reati dall'interno. È intesa a identificare il rischio di un pregiudizio per gli interessi di cui all'articolo 1 capoverso 2 che è connesso con l'esercizio di un'attività sensibile sotto il profilo della sicurezza da parte di una determinata persona. Si tratta dunque di stimare la probabilità che una determinata persona da sottoporre al controllo pregiudicherà intenzionalmente o per negligenza gli interessi di cui all'articolo 1 capoverso 2. A tale scopo vengono rilevati dati rilevanti sulla condotta di vita di questa persona. Basandosi su questi dati, specialisti formati a tale scopo (*Risk Profiler*) procedono a una valutazione del rischio per la sicurezza. Rimane inteso che una simile valutazione non può essere mai assolutamente affidabile.

Dopo avere preso atto della valutazione del rischio da parte del servizio specializzato CSP competente, è unicamente l'autorità o l'organizzazione assoggettata a decidere se vuole sostenere un eventuale rischio elevato, se vuole ridurlo mediante determinate condizioni o se vuole evitarlo non assumendo o licenziando la persona in questione.

Per la comprensione della normativa proposta sono fondamentali due punti:

- la valutazione del rischio per la sicurezza da parte del servizio specializzato CSP competente rappresenta una raccomandazione. Per la decisione in merito a un'eventuale assunzione o un eventuale incarico è competente unicamente il servizio che assume o che conferisce mandati. Di conseguenza, il rischio non viene mai sostenuto dal servizio specializzato CSP competente per la valutazione del rischio per la sicurezza. Ciò vale sia nel caso di una dichiarazione di rischio (sussiste un rischio per la sicurezza) sia nel caso di una dichiarazione di sicurezza (non sussiste alcun rischio per la sicurezza). Anche se alla persona sottoposta al controllo è stata rilasciata una dichiarazione di sicurezza, i superiori non vengono esonerati dall'obbligo di identificare eventuali rischi elevati connessi con tale persona e, se del caso, farvi fronte;
- il CSP deve venire impiegato in funzione dei rischi. La presente legge stabilisce chiari presupposti per l'esecuzione del controllo. Ciò non significa che quelle funzioni, che finora sono state sottoposte al controllo in via supplementare, sarebbero meno importanti o non sarebbero esposte a un rischio elevato. Per queste funzioni e per tutte le altre funzioni che non vengono sottoposte al controllo, la responsabilità della valutazione del rischio per la sicurezza viene però unicamente e solamente assunta dalla linea gerarchica. Con la proposta introduzione di un nuovo articolo 20*a* LPers, in futuro i datori di lavoro di cui all'articolo 3 LPers disporranno a tal fine di mezzi idonei (estratti del casellario giudiziale e del registro esecuzioni e fallimenti).

Art. 33

L'articolo 33 disciplina, in combinato disposto con l'articolo 34 capoverso 1, l'assoggettamento dei membri delle autorità e delle organizzazioni assoggettate. Le autorità assoggettate (dunque non le organizzazioni di cui all'articolo 2 cpv. 2) devono emanare per il loro ambito di competenza un elenco di quelle funzioni per l'adempimento dei cui compiti *è necessario* esercitare un'attività sensibile sotto il profilo della sicurezza e che quindi vanno sottoposte al controllo. Per i presupposti materiali per iscrivere una funzione nell'elenco delle funzioni non viene però semplicemente ripreso l'attuale sistema. Come menzionato al numero 1.2.4, pur prescindendo dal criterio della *periodicità*, in particolare nel trattamento di informazioni classificate, decisiva per l'assoggettamento degli impiegati federali al controllo di sicurezza relativo alle persone è però la questione se il titolare di una determinata funzione per l' adempimento dei propri compiti *deve* 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 solamente 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 relativo alle costruzioni e agli impianti militari. Per adempiere i propri compiti deve trattare informazioni classificate e talvolta avere l'accesso a tali impianti. La sua funzione deve venire inserita nell'elenco delle funzioni;
- un collaboratore dell'Amministrazione federale delle finanze deve, eccezionalmente, valutare le ripercussioni di una proposta, classificata «CONFIDENZIALE», del DFGP al Consiglio federale. Per simili affari sono normalmente competenti altri collaboratori che però sono assenti per ferie o malattia. In linea di massima, questo compito non fa parte della sua funzione, che di conseguenza non può essere menzionato nell'elenco;
- il personale di pulizia di un'autorità ha talvolta, senza volerlo, accesso a informazioni classificate quando, nell'ambito dell'adempimento ordinario dei suoi compiti, 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 venire inserito 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, nell'elenco degli obblighi di una funzione, soltanto il 5 per cento del grado d'occupazione è previsto per l'adempimento di compiti sensibili sotto il profilo della sicurezza, questa funzione va inserita nell'elenco delle funzioni. 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 visione d'insieme dei processi lavorativi 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 sostanziale misura 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 (o gli elenchi degli obblighi) delle rispettive funzioni devono contenere un'esatta definizione dei compiti per il cui adempimento è necessario 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 organizzative e personali per limitare al minimo necessario la cerchia delle persone che devono esercitare attività sensibili sotto il profilo della sicurezza.

L'espressione «*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 quindi, in linea di principio, mantenere l'attuale sistema, in virtù del quale il Consiglio federale designa queste funzioni nell'allegato all'OCSP (si veda il n. 1.2.4). In virtù dei disciplinamenti delle competenze in conformità con la LOGA, potrà però continuare ad autorizzare i dipartimenti e la Cancelleria federale a emanare i propri elenchi dettagliati.

Art. 34

Capoverso 1: l'articolo 34 stabilisce chi deve essere sottoposto al controllo.

- Lettera a: nel caso degli impiegati delle autorità e delle organizzazioni assoggettate, vengono sottoposte al controllo solamente quelle persone la cui funzione è contenuta negli elenchi delle funzioni di cui all'articolo 33. L'elenco delle funzioni è dunque vincolante. Le eccezioni sono disciplinate nei capoversi 3 e 4.
- Lettera b: per terzi, il controllo viene eseguito se nell'ambito di un mandato, partecipano all'esercizio di un'attività sensibile sotto il profilo della sicurezza.
- Lettera c: il presupposto per l'esecuzione del CSP nel contesto internazionale viene disciplinato da pertinenti trattati internazionali. In linea di massima, si applica la norma del capoverso 2.

Capoverso 2: il principio del capoverso 1 lettera b si applica anche alle persone che, su mandato di un'autorità estera o internazionale, devono esercitare un'attività sensibile sotto il profilo della sicurezza.

Il capoverso 3 disciplina il caso di una funzione che soddisfa i criteri di cui all'articolo 33, ma ancora non è stata inserita nel relativo elenco. In questo caso il controllo può essere eseguito, sempre che l'autorità assoggettata lo consenta. L'elenco dovrà poi essere adeguato di conseguenza.

Capoverso 4: nel caso di membri di autorità che vengono eletti dal Popolo o di magistrati eletti dall'Assemblea federale, non può essere eseguito preliminarmente un controllo di sicurezza relativo alle persone, anche se queste persone spesso esercitano le attività più sensibili sotto il profilo della sicurezza.

Art. 35

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 da sottoporre al controllo 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.

L'avamprogetto prevede ora (si veda il n. 1.2.4) i due livelli di controllo seguenti:

- lettera a: 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 TIC del livello di sicurezza «protezione elevata»; e (c) accesso alle zone di sicurezza nei quali vengono esercitate attività di cui ad (a) e a (b). Per l'accesso a zone di protezione 2 di un impianto militare è parimenti necessario un CSP di questo livello.
- Lettera b: 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 TIC del livello di sicurezza «protezione molto elevata»; e (c) all'accesso alle zone di sicurezza nelle quali vengono esercitate attività di cui ad (a) e a (b). Per l'accesso a zone di protezione 3 di un impianto militare è parimenti necessario un CSP di questo livello.

Spetta alle autorità assoggettate stabilire i livelli di controllo per le funzioni e i mandati corrispondenti.

Art. 36

I servizi specializzati CSP non possono in alcun caso avviare ed eseguire un CSP di propria iniziativa; necessitano sempre di un pertinente mandato. Da un lato, non può essere di competenza delle massime autorità avviare direttamente tutte le procedure di controllo, dall'altro, neppure ogni servizio dovrebbe poter conferire simili mandati di propria iniziativa. L'articolo 36 prevede perciò che ciascuna autorità assoggettata designi per il proprio ambito di competenza quei servizi che sono autorizzati ad avviare le procedure di controllo e a conferire il relativo mandato ai servizi specializzati CSP. Si tratta di una competenza formale. In questo contesto occorre segnalare che il servizio che chiede l'avvio del controllo sovente non coincide con il servizio che dopo il controllo, in applicazione dell'articolo 44, decide in merito all'attribuzione del compito sensibile sotto il profilo della sicurezza (servizio competente per l'attribuzione).

Purché lo reputi opportuno, il Consiglio federale può anche autorizzare determinati terzi ad avviare CSP. Ciò concerne in particolare le aziende che sovente esercitano per la Confederazione attività sensibili sotto il profilo della sicurezza e sono in possesso di una dichiarazione di sicurezza aziendale di cui all'articolo 68. Può anche essere il caso dei Cantoni o delle organizzazioni di cui all'articolo 2 capoverso 2 lettera e.

Art. 37

L'esecuzione del CSP richiede, in linea di principio, il consenso della persona interessata (cpv. 1). Secondo il capoverso 2, unicamente nell'ambito dell'esercito o della protezione civile possono venire 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.

Art. 38

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 (di per sé opportuna) normativa vigente, in pratica non può tuttavia avvenire senza un sostanziale aumento delle risorse di personale dei servizi specializzati. Perciò, nel capoverso 1 viene attenuata la norma per gli impiegati delle autorità e delle organizzazioni assoggettate: si richiede ancora che soltanto per questo gruppo di persone il CSP venga avviato prima dell'attribuzione della funzione. I datori di lavoro continuano ovviamente a essere liberi di attendere la dichiarazione del ser-

vizio specializzato CSP prima di assumere la persona interessata. 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 (art. 43 cpv. 1 lett. b), di una dichiarazione di rischio (art. 43 cpv. 1 lett. c) o di una dichiarazione di constatazione (art. 43 cpv. 1 lett. d) può costituire un motivo 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 esecuzioni e fallimenti (art. 20a LPers).

Il capoverso 2 corrisponde al diritto vigente (art. 19 cpv. 3 LMSI) ed è una conseguenza dell'inchiesta della Commissione della gestione del Consiglio nazionale sulle circostanze che all'epoca hanno portato alla nomina del comandante di corpo Roland Nef a capo dell'esercito. La normativa indicata è stata decisa con modifica della LMSI del 23 dicembre 2011 ed è entrata in vigore il 1° luglio 2012.

Il capoverso 3 disciplina il momento del CSP per terzi destinati a eseguire per un'autorità o un'organizzazione assoggettata un mandato sensibile sotto il profilo della sicurezza. In questo caso, deve continuare a essere applicata l'attuale normativa: il CSP deve essere concluso prima che alla persona possa essere affidato l'esercizio di un'attività sensibile sotto il profilo della sicurezza. Il motivo della disparità 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 massima, 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.

Conformemente al capoverso 4, il momento del CSP per le persone che devono essere controllate in virtù di un accordo internazionale si rifà alle prescrizioni di tale accordo. Anche se non è disciplinato esplicitamente nell'accordo, in questi casi si richiede sempre che venga rilasciata una dichiarazione di sicurezza prima di esercitare un'attività sensibile sotto il profilo della sicurezza.

Art. 39

Questa disposizione disciplina l'acquisizione dei dati per entrambi i livelli di controllo. L'acquisizione dei dati si orienta per lo più alla legislazione e alla prassi attuali. A motivo della riduzione da tre a soltanto due livelli di controllo, l'acquisizione dei dati all'interno dei livelli di controllo è stata riorganizzata in modo che il controllo di base viene rafforzato in particolare grazie alla possibilità di consultare i registri degli uffici di esecuzione e fallimento.

Per quanto riguarda l'acquisizione dei dati, per entrambi i livelli di controllo si tratta di una prescrizione potestativa. 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 da tre a due livelli non deve fare sì che i costi del CSP aumentino in misura considerevole. Il Consiglio federale, che emanerà le disposizioni d'esecuzione relative ai CSP, potrà anche stabilirvi quali dati e quando *devono* essere acquisiti.

Capoverso 1: per il controllo di base possono venire consultate le seguenti fonti:

- lettere a-d: il casellario giudiziale, nonché le raccolte di dati del Servizio delle attività informative 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 online al registro nazionale di polizia (si veda il n. 2.10). Ora i dati degli organi di polizia cantonali connessi si schiuderanno loro in maniera semplice ed efficiente. Ovviamente, eventuali risultati vanno ponderati nell'ottica della prevista attività della persona da sottoporre al controllo e posti nel giusto contesto;
- lettera e: le informazioni dai registri delle autorità di esecuzione e fallimento sono necessari per poter valutare la situazione finanziaria delle persone da sottoporre al controllo nell'ottica di un eventuale rischio per la sicurezza come, ad esempio, la corruttibilità;
- la lettera f prevede ora che possono essere addotti anche le documentazioni e i risultati di precedenti controlli di sicurezza;
- lettera g: qui è stabilito esplicitamente che i servizi specializzati CSP possono ricorrere anche a dati da fonti accessibili pubblicamente (p. es. da Internet, con motori di ricerca come Google). Un'esigenza in tal senso risulta, da un lato, dalla prevista funzione e da eventuali indicazioni inerenti al singolo caso. Le informazioni dai *social network* che non sono rivolte alla collettività, bensì sono destinate solamente a cerchie di persone chiuse, non possono tuttavia essere acquisite.

Capoverso 2: oltre alle fonti di cui al capoverso 1, nel CSP ampliato possono venire consultate le seguenti fonti:

- lettera a: dati dai registri fiscali federali e cantonali possono fornire informazioni supplementari sulla situazione economica delle persone da sottoporre al controllo, ad esempio nel caso di evidenti discrepanze tra tenore di vita e dati fiscali;
- lettera b: i dati dai registri dei controlli degli abitanti non sempre vengono acquisiti perché spesso hanno soltanto un valore aggiunto limitato. Esse possono però, in funzione della situazione, fornire importanti indicazioni per la valutazione della situazione personale degli interessati;
- lettera c: nel controllo ampliato viene esaminata nel dettaglio la situazione finanziaria della persona sottoposta al controllo. Perciò, possono essere acquisiti sistematicamente dati presso istituti finanziari e banche con i quali la persona interessata intrattiene relazioni d'affari;
- lettera d: l'audizione personale serve ad affrontare argomenti che non risultano o risultano solamente in modo poco chiaro dalle consultazioni dei registri.

Il capoverso 3 disciplina l'acquisizione dei dati all'estero. I dati che secondo i capoversi 1 e 2 possono essere acquisiti in Svizzera, se necessario possono essere acquisiti anche all'estero.

Il capoverso 4 chiede che per la valutazione del rischio per la sicurezza, i servizi specializzati CSP devono potersi basare su una quantità sufficiente di dati relativi a un periodo di tempo adeguato. Se questi requisiti non sono soddisfatti, non si può valutare se esiste un rischio per la sicurezza. Se necessario, la persona interessata viene sentita anche secondo il capoverso 5. Ciò può, ad esempio, essere il caso 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 è possibile acquisire dati affidabili. L'espressione «*periodo di tempo adeguato*» è stata consapevolmente formulata in modo aperto. L'attuale normativa dell'articolo 19 capoverso 3 OCSP, in virtù della quale i servizi specializzati CSP devono disporre almeno di dati concernenti i cinque anni precedenti l'avvio del controllo di base e i dieci anni precedenti l'avvio del controllo ampliato, è stata in parte giudicata sproporzionata e troppo assoluta. Sono perciò ipotizzabili due approcci di soluzione: o, nell'ambito delle sue disposizioni d'esecuzione sui CSP, il Consiglio federale precisa l'espressione «*quantità sufficiente di dati relativi a un periodo di tempo adeguato*», oppure l'interpretazione di questa espressione rimane a discrezione dei servizi specializzati CSP.

Il capoverso 5 prevede che i servizi specializzati CSP possono sentire personalmente la persona da sottoporre al controllo indipendentemente dal livello di controllo se nell'ambito dell'acquisizione dei dati vengono scoperte circostanze rilevanti in materia di sicurezza. Una simile audizione può avere luogo anche se ai sensi del capoverso 4 il servizio specializzato CSP non ha potuto acquisire una quantità sufficiente di dati relativi a un periodo di tempo adeguato. Questa audizione personale non va confusa con l'audizione di cui al capoverso 2 lettera d. Quest'ultima può essere eseguita senza indizi di un rischio per la sicurezza e non è limitata quanto alla sua portata. Per il chiarimento di particolari circostanze rilevanti 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.

Capoverso 6: succede che i dati necessari per la valutazione del rischio 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 sposata. Il capoverso 6 prevede perciò che anche questi dati personali devono poter essere trattati, sempre che siano indivisibilmente connessi con i dati sulla persona sottoposta al controllo e indispensabili per la valutazione del rischio. L'onere connesso ogni volta con l'ottenimento del consenso della persona terza al trattamento dei dati sarebbe sproporzionatamente elevato per i servizi specializzati CSP. Per ragioni di trasparenza, i servizi specializzati CSP devono dunque informare questi terzi sul trattamento dei dati. Se l'informazione non è possibile o lo è solamente con un onere sproporzionato, si applica l'articolo 18a capoverso 4 lett. b LPD.

Art. 40

Il concorso di autorità alla procedura deve continuare a essere fornito gratuitamente (cpv. 1). I terzi, ad esempio banche o istituti di credito, ai quali si ricorre affinché collaborino, devono essere indennizzati se l'onere così 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. 41

Capoverso 1: una procedura di controllo già avviata viene abbandonata se la persona da sottoporre al controllo nel corso della procedura revoca il suo consenso o rifiuta di collaborare, oppure se per un altro motivo

essa non entra più in considerazione per la funzione cui mirava o il mandato in questione (p. es. insolvenza della ditta per la quale la persona da sottoporre al controllo avrebbe dovuto operare).

Il capoverso 2 prevede che sia la persona da sottoporre al controllo sia il servizio che ha avviato la procedura vengano informati dell'abbandono della procedura. La persona interessata è di conseguenza considerata «non controllata» e non può esercitare la pertinente attività sensibile sotto il profilo della sicurezza o non può assumere la relativa funzione.

Il capoverso 3 stabilisce che dopo l'abbandono della procedura di controllo i dati e i documenti già acquisiti dal servizio specializzato CSP siano distrutti. Vengono distrutti i dati acquisiti, ma non la dichiarazione di abbandono e il verbale di distruzione. Né l'una né l'altro possono però contenere dati che potrebbero essere svantaggiosi per la persona interessata. Le disposizioni d'esecuzione del Consiglio federale disciplineranno la durata di conservazione della dichiarazione di abbandono e del verbale di distruzione.

Art. 42

In passato è stato da più parti criticato il fatto che la normativa vigente della LMSI non menziona esplicitamente che cosa va considerato come rischio per la sicurezza. 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.

Capoverso 1: 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 «*notevole o grave pregiudizio 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 le vanno assegnati, 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 deve quindi venire presunto nel senso della presente legge 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 appropriato e che così pregiudicherà almeno considerevolmente gli interessi di cui all'articolo 1 capoverso 2.

Il capoverso 2 statuisce chiaramente che i servizi specializzati CSP si focalizzano in primo luogo sulla probabilità che si verifichi l'evento. Nella valutazione di una simile probabilità si tratterà inevitabilmente sempre di una previsione associata a incertezze. La base per questa previsione è costituita dalla totalità di tutte le circostanze, ad esempio la personalità della persona interessata, la sua vita anteriore e le sue condizioni di vita, sempre che 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 Tribunale federale.

Anche se le definizioni mirano, in linea di massima, 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 essere certi 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 tra gli indizi e i nessi dimostrano la mancanza di affidabilità di una persona, la sua presunta ricattabilità o la sua pregiudicata capacità di valutare e di decidere, non può essere specificato al livello della legge, bensì deve, in ultima analisi, essere accertato e illustrato in ogni singola valutazione.

Il capoverso 3 chiarisce che può esserci un rischio per la sicurezza anche senza una colpa della persona interessata. Il CSP è una misura preventiva per proteggere interessi pubblici preponderanti da reati dall'interno, commessi intenzionalmente o per negligenza, fondata 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 che nel 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. Si stabilisce altresì che 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 pure congetture, in particolare se riguardano l'orientamento politico della persona da sottoporre al controllo.

Il capoverso 4 deve infine assicurare l'autonomia dei servizi specializzati CSP per la valutazione del rischio per la sicurezza. Il CSP non può essere utilizzato abusivamente per intrighi politici.

Art. 43

Il capoverso 1 disciplina le varie dichiarazioni dei servizi specializzati CSP nelle quali viene registrato il risultato della valutazione:

- lettera a: se il servizio specializzato CSP giunge alla conclusione che la persona sottoposta al controllo non presenta rischi per quanto riguarda l'attività sensibile sotto il profilo della sicurezza, rilascia una dichiarazione di sicurezza;
- lettera b: se il servizio specializzato CSP accerta che nell'esercizio dell'attività sensibile sotto il profilo della sicurezza da una persona sottoposta al controllo derivano taluni rischi per la sicurezza e che questi però possono essere ridotti imponendo determinate condizioni, rilascia una dichiarazione di sicurezza con riserva e raccomanda al servizio competente per l'attribuzione pertinenti condizioni;
- lettera c: se giunge alla conclusione che l'esercizio dell'attività sensibile sotto il profilo della sicurezza da parte la persona sottoposta al controllo costituisce un rischio, il servizio specializzato CSP rilascia una dichiarazione di rischio;
- lettera d: se a motivo dell'insufficienza dei dati acquisti di cui all'articolo 39 capoverso 4 una persona non può essere valutata secondo le norme, il servizio specializzato CSP rilascia una dichiarazione di constatazione.

Capoverso 3: sebbene, di per sé, il diritto formale di essere sentiti non si applichi senza problemi nel caso di un atto materiale (si veda l'art. 51 cpv. 3), il capoverso 3 è inteso a garantire che la persona interessata possa tutelare adeguatamente i propri interessi già a questo stadio della procedura. La disposizione prevede perciò che prima del rilascio delle dichiarazioni di cui alle lettere b-d, alla persona sottoposta al controllo debba essere data l'opportunità di esprimersi al riguardo. Di fatto, ciò significa che, in presenza di una bozza di dichiarazione di cui alle lettere b-d, la persona interessata va informata in modo adeguato sul contenuto e le va concesso un termine adeguato per esprimersi al riguardo.

Art. 44

Conformemente al capoverso 1, la dichiarazione deve essere comunicata per scritto alla persona controllata e al servizio competente per l'attribuzione dell'attività sensibile sotto il profilo della sicurezza. Anche se la dichiarazione non costituisce una decisione ai sensi dell'articolo 5 PA (si veda l'art. 51 cpv. 3), la persona interessata deve avere la possibilità di prendere atto dei risultati della valutazione ed eventualmente chiedere che venga emanata una decisione. Questo capoverso corrisponde sostanzialmente al diritto vigente (art. 21 cpv. 2-4 LMSI).

Il capoverso 2 stabilisce che, nel caso delle persone che vanno nominate dal Consiglio federale, la comunicazione della valutazione deve essere fatta al dipartimento proponente.

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'articolo 20*b* LPers). In questo caso il servizio specializzato CSP deve potere informare il rispettivo servizio competente per l'attribuzione in merito al risultato del controllo principale. Il disciplinamento dell'esame dell'affidabilità di cui all'articolo 20*b* LPers, nonché di cui all'articolo 14 LM, esige che le due procedure vengano riunite se, in virtù della presente legge, una persona deve parimenti essere sottoposta a un CSP.

Il capoverso 4 consente ai servizi specializzati CSP, in caso di militari potenzialmente violenti, di informare in merito al risultato della loro valutazione il servizio competente in virtù dell'articolo 113 LM per la cessione o il ritiro dell'arma militare personale. Se, nell'ambito di un controllo, il servizio specializzato CSP constata che la persona interessata, che è soggetta all'obbligo di prestare servizio militare, presenta un elevato potenziale di violenza, deve informare le autorità militari affinché queste possano decidere in merito al ritiro dell'arma militare.

Art. 45

L'articolo 45 prevede che, nel caso di una fondata riserva riguardo alla sicurezza e di urgenza, nell'ottica della prevenzione dai pericoli i servizi specializzati CSP possono informare in merito alle loro constatazioni i competenti servizi di cui all'articolo 44 già prima che la procedura sia conclusa. In seguito a ciò, il servizio competente può adottare misure di sicurezza preventive, il che corrisponde al vigente articolo 20 OCSP.

Art. 46

Il capoverso 1 stabilisce che il servizio competente per l'attribuzione dell'attività o funzione sensibile sotto il profilo della sicurezza (servizio competente per l'attribuzione) non è vincolato alla dichiarazione del servizio specializzato CSP. Ciò corrisponde all'attuale articolo 21 capoverso 4 LMSI. Non spetta ai servizi specializzati CSP adottare o limitare la responsabilità della linea gerarchica per decisioni in materia di personale, bensì unicamente informare l'autorità che decide in merito al rischio connesso con l'attribuzione di un'attività sensibile sotto il profilo della sicurezza a una determinata persona.

Capoverso 2: prima della sua decisione, il servizio competente per l'attribuzione deve però prendere conoscenza della dichiarazione del servizio specializzato CSP, poiché soltanto allora può decidere tenendo conto degli eventuali rischi.

Il capoverso 3 autorizza il servizio competente per l'attribuzione, in particolare sulla base delle raccomandazioni del servizio specializzato CSP, a imporre condizioni per l'esercizio dell'attività sensibile sotto il profilo della sicurezza. Queste condizioni rappresentano misure atte a ridurre i rischi che per lo più riguardano il diritto in materia di personale. Il servizio competente per l'attribuzione può, ad esempio, esigere che la persona interessata renda nota periodicamente la sua situazione finanziaria o si sottoponga a un test antidroga ecc. Importante in questo contesto è la precisazione che queste condizioni devono orientarsi esclusivamente all'esercizio dell'attività sensibile sotto il profilo della sicurezza e non possono riferirsi all'esercizio di altri compiti. Se, ad esempio, il servizio competente per l'attribuzione decide che la persona interessata non può esercitare l'attività sensibile sotto il profilo della sicurezza, ma sarà impiegata per altri compiti non rilevanti sotto il profilo della sicurezza, allora non si può più stabilire alcuna condizione. Per lo più, le condizioni più idonee vengono raccomandate dal servizio specializzato CSP. Il servizio competente per l'attribuzione non è però vincolato a queste condizioni e può stabilire autonomamente le condizioni. Se tuttavia il servizio competente si scosta dalle condizioni raccomandate, allora deve informare per scritto il servizio specializzato CSP (si veda l'art. 47 lett. b).

Art. 47

Questo articolo statuisce un obbligo di comunicazione del servizio competente per l'attribuzione. Se prende una decisione, che si discosta dalla valutazione del servizio specializzato CSP, deve darne comunicazione a quest'ultimo. La comunicazione può avere luogo mediante un'annotazione nel sistema d'informazione per i CSP di cui agli articoli 52-54. Si tratta, per il servizio specializzato CSP, di mantenere la visione d'insieme sulla prassi dei servizi competenti per l'attribuzione e di trarne i necessari insegnamenti.

Art. 48

Se alla persona da sottoporre al controllo è già stata rilasciata una dichiarazione ancora valida ed equivalente, per motivi di economia procedurale non deve, per quanto possibile, essere eseguita una nuova procedura di controllo. L'articolo 48 prevede perciò che in questo caso vi si può rinunciare. Di regola, 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 assolutamente possibile che per il trattamento di informazioni classificate «SEGRETO» sussista un rischio per la sicurezza, che però 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. 49

Le autorità di sicurezza estere accordano esclusivamente a persone che sono state sottoposte al CSP l'accesso a informazioni classificate, a materiale classificato o a zone di protezione e zone di sicurezza. L'autorità svizzera competente può rilasciare l'attestazione di sicurezza relativa alle persone necessaria in siffatti casi esclusivamente alle persone che hanno ricevuto una dichiarazione di sicurezza.

Art. 50

Il capoverso 1 disciplina l'ordinaria ripetizione del CSP. Nella legge si rinuncia a prescrivere intervalli fissi per la ripetizione. Essa fissa unicamente principi generali per la ripetizione del controllo. Il motivo è che in futuro la ripetizione dovrà avvenire sempre più in conformità con l'effettiva esigenza di sicurezza. Il Consiglio federale dovrebbe disciplinare in dettaglio le ripetizioni nelle sue disposizioni d'esecuzione. Ovviamente potrà però anche lasciare tale competenza alle autorità e alle organizzazioni assoggettate e non prescrivere nulla.

Il capoverso 2 conferisce sia al servizio che chiede l'avvio della procedura sia al servizio competente per l'attribuzione la possibilità di predisporre una ripetizione del CSP al di fuori dei cicli di ripetizione legali. Il motivo di una simile ripetizione anticipata è l'insorgere di nuovi rischi inerenti alla persona interessata, ad esempio l'apertura di un procedimento penale contro di essa che presenta un rapporto con l'attività sensibile sotto il profilo della sicurezza. Questa norma corrisponde alla disposizione d'esecuzione vigente (si veda l'art. 18 cpv. 2 OCSP).

Nell'ambito della sua competenza a emanare diritto completivo sulla procedura dei CSP (si veda l'art. 55), il Consiglio federale dovrà anche decidere se vuole introdurre ulteriori ripetizioni anticipate del controllo. Un *controllo successivo* potrebbe, ad esempio nel caso di dichiarazioni di sicurezza con riserva, essere utile per esaminare l'efficacia delle condizioni imposte.

Art. 51

I capoversi 1 e 2 disciplinano la possibilità della persona controllata di consultare i documenti del controllo e di esigere la rettifica dei dati errati. Nonostante l'adeguamento della formulazione, la normativa corrisponde al diritto vigente (si veda l'art. 21 cpv. 2 LMSI).

Capoverso 3: secondo il diritto vigente, le dichiarazioni dei servizi specializzati CSP vengono emanate sotto forma di decisione (si veda l'art. 20 cpv. 3 LMSI e l'art. 22 OCSP). Tuttavia, qualificare come decisioni le dichiarazioni è giuridicamente sbagliato, poiché esse hanno solamente carattere di raccomandazione (si veda l'art. 21 cpv. 4 LMSI, nonché l'art. 46 cpv. 1 LSIn). I diritti delle persone controllate vengono toccati soltanto se i servizi competenti per l'attribuzione in seguito non attribuiscono la funzione o l'incarico. Le dichiarazioni corrispondono giuridicamente piuttosto al risultato di un *assessment* che le autorità e le organizzazioni sovente fanno eseguire prima di assumere persone chiave. Anche la valutazione da parte degli addetti agli *assessment* non viene comunicata sotto forma di decisione impugnabile perché il datore di lavoro può decidere liberamente. Le dichiarazioni dei servizi specializzati CSP rappresentano atti materiali ai sensi dell'articolo 25*a* PA. Per la presente situazione ciò significa che, entro 30 giorni dal ricevimento della dichiarazione, la persona interessata può richiedere una decisione impugnabile al servizio specializzato CSP. L'ulteriore iter procedurale si fonda sulla PA. La normativa prevista ridurrà l'onere per il CSP delle persone soggette all'obbligo di leva nell'ambito del reclutamento militare. I servizi specializzati CSP potranno semplicemente comunicare i risultati della valutazione alle persone soggette all'obbligo di leva e soltanto in caso di contestazione delle stesse, emanare una decisione completa.

Art. 52

L'articolo 52 corrisponde sostanzialmente al diritto vigente (si vedano gli art. 144-149 LSIM).

Il capoverso 1 stabilisce che i servizi specializzati CSP devono impiegare un sistema d'informazione per l'esecuzione e la gestione dei CSP.

Capoverso 2: ciascun servizio specializzato CSP è responsabile del trattamento dei dati conforme al diritto.

Capoverso 3: tra questi dati possono anche esserci dati personali degni di particolare protezione e profili della personalità (art. 3 lett. c e d LPD).

Il capoverso 4 enumera i dati che vengono trattati nel sistema d'informazione.

Capoverso 5: i dati che vengono trattati al di fuori del sistema d'informazione devono esservi menzionati. Si tratta in particolare di documenti cartacei e di registrazioni audio nell'ambito delle audizioni.

Art. 53

L'articolo 53 corrisponde sostanzialmente al diritto vigente (si vedano gli art. 144-149 LSIM).

Capoverso 1: procedura di richiamo

- lettera a: i servizi specializzati CSP hanno accesso a tutti i dati per i quali sono competenti;
- lettera b: i servizi che chiedono l'avvio del controllo ottengono soltanto l'accesso a quei dati che essi stessi hanno acquisito in occasione dell'avvio, nonché al risultato del CSP;
- la lettera c stabilisce a quali dati hanno accesso i servizi competenti per l'attribuzione;
- la lettera d disciplina a quali dati hanno accesso gli incaricati della sicurezza delle informazioni per l'adempimento dei loro compiti di controllo;
- lettera e: le organizzazioni della Confederazione e dei Cantoni presso i quali sono acquisiti dati hanno accesso soltanto a dati sull'identità delle persone da sottoporre al controllo o controllate. Esse necessitano di questi dati per sapere su quale persona devono eseguire ricerche supplementari e fornire dati.

Capoverso 2: interfacce

- la lettera a disciplina a quali dati ha accesso il servizio specializzato per la sicurezza aziendale;
- lettera b: affinché (come finora) lo Stato maggiore dell'esercito possa trattare efficacemente le richieste di visite all'estero con accesso a informazioni classificate, i dati di cui all'articolo 52 capoverso 4 lettere a e d devono venire trasferiti attraverso un'interfaccia nel sistema d'informazione per le richieste di visita;
- la lettera c numeri 1-3 disciplina a quali dati lo Stato maggiore di condotta dell'esercito ha accesso per il controllo dell'accesso alle zone di sicurezza, per l'adempimento dei suoi compiti legali in relazione al Sistema di gestione del personale dell'esercito e per l'esecuzione del reclutamento delle persone soggette all'obbligo di leva e del personale previsto per il promovimento della pace.

Capoverso 3: ulteriori organizzazioni della Confederazione (in particolare fornitori di prestazioni TIC) necessitano dei risultati del CSP per controllare l'accesso a zone di sicurezza.

Capoverso 4: i servizi specializzati CSP comunicano alle autorità e alle organizzazioni assoggettate elenchi e statistiche solamente se esse ne hanno bisogno per l'adempimento dei loro compiti di controllo secondo la presente legge. Siffatti elenchi vengono dunque consegnati soltanto in caso di corrispondente necessità. La comunicazione di simili elenchi avviene al di fuori del sistema d'informazione di cui all'articolo 52.

Art. 54

L'articolo 54 corrisponde sostanzialmente al diritto vigente (si vedano gli art. 144-149 LSIM, nonché l'OCSP).

Il capoverso 1 costituisce il fondamento giuridico per la registrazione audio delle audizioni.

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.

Il capoverso 3 disciplina la distruzione di dati di una persona già controllata che non ha dato seguito alla sua assunzione (si veda anche l'art. 41).

Capoverso 5: i dati che vengono trattati al di fuori del sistema d'informazione (si veda l'art. 52 cpv. 5), devono essere conservati e distrutti conformemente ai capoversi 2 e 3. Quando si distruggono questi dati vanno nel contempo cancellate le menzioni nel sistema.

Capoverso 6: se dei documenti vanno archiviati secondo le prescrizioni in materia di archiviazione, non possono essere distrutti.

Art. 55

Nell'articolo 55 vengono indicati quei settori nei quali il Consiglio federale deve emanare normative completive o 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.

- Lettere a-b: riguardo all'organizzazione va osservato che oggi vi sono due servizi specializzati CSP. Uno è aggregato alla Cancelleria federale e controlla all'attenzione del Consiglio federale i quadri superiori e gli impiegati dell'altro servizio specializzato CSP. Attualmente esegue perciò esclusivamente CSP ampliati con audizione. L'altro servizio specializzato CSP, nel DDPS, è aggregato alla Protezione delle informazioni e delle opere, in seno allo Stato maggiore dell'esercito, ed esegue la stragrande maggioranza dei controlli. La lettera b lascia la possibilità di più servizi specializzati, consentendo però al Consiglio federale di scegliere se mantenere questa organizzazione.
- Lettere c-d: in applicazione dell'articolo 16 capoverso 2 LPD, il Consiglio federale deve emanare normative completive sulla protezione dei dati nell'ambito del CSP. Ne sono interessati in particolare l'organizzazione delle competenze e delle responsabilità per la protezione dei dati (incl. la sicurezza dei dati) in relazione con il sistema d'informazione di cui all'articolo 52, nonché il controllo indipendente periodico della legalità del trattamento dei dati.

2.1.4 Procedura di sicurezza relativa alle aziende

Art. 56

In merito allo scopo della PSA, si veda il numero 1.2.5.

Art. 57

Capoverso 1: quale *«azienda»* ai sensi della legge non si considera necessariamente l'intera impresa. Ne sono interessati piuttosto solamente 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 di cui all'articolo 56 a un'impresa che vi si candida. La PSA costituisce, in linea di principio, una questione nazionale. Perciò, le aziende con sede all'estero che vogliono candidarsi per un mandato sensibile sotto il profilo della sicurezza della Svizzera, devono farsi controllare da parte dello Stato nel quale si trova la loro sede. Le competenze e le modalità di controllo sono parte integrante dei pertinenti trattati internazionali di cui all'articolo 90. In siffatti casi viene richiesta alle autorità di sicurezza estere mediante una cosiddetta «*Facility Security Clearance Information Sheet*» la prova di una dichiarazione di sicurezza aziendale (DSA) del mandatario o, qualora l'azienda in questione non fosse stata ancora controllata, l'avvio della procedura di controllo.
- Il capoverso 1 lettera b considera 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 certificazione ivi connessa rappresentano un'attività ufficiale che non può essere attribuita all'economia privata perché le autorità estere esigono, senza eccezioni, un «sigillo di sicurezza» ufficiale dello Stato in cui ha sede l'azienda.

Il capoverso 2 rileva che, in ogni caso, una PSA può essere eseguita soltanto con il consenso dell'azienda interessata. In pratica, il necessario consenso dell'azienda per l'esecuzione della PSA non rappresenta tuttavia mai un problema perché le aziende hanno un interesse finanziario al conferimento del mandato.

Capoverso 3: nel caso d'applicazione del capoverso 1 lettera b, la Confederazione non ha alcun interesse proprio diretto all'esecuzione della procedura. Il Consiglio federale disciplinerà la questione dei costi a livello di ordinanza.

Art. 58

Capoverso 1: la PSA viene eseguita solamente 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. Secondo la lettera d, ciò può anche avvenire 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 prescrive che, dopo l'abbandono della procedura, vanno distrutti tutti i dati e i documenti connessi con essa.

Art. 59

Il capoverso 1 stabilisce in primo luogo che le PSA vengano eseguite da un *«servizio specializzato per la sicurezza aziendale»* (servizio specializzato SA). In seno alla Confederazione (come finora) un unico servizio deve dunque occuparsi di questa procedura. Il servizio specializzato SA si attiva soltanto su *domanda* (e non su mandato) di un'autorità o di un'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.

Capoverso 2: nel loro ambito di competenza, le autorità assoggettate devono stabilire chi presenta la domanda di avvio della procedura. 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.

Il capoverso 3 disciplina la competenza nel caso di un mandato sensibile sotto il profilo della sicurezza di un'autorità estera o internazionale. Di regola, la procedura viene avviata mediante una domanda da parte dell'autorità di sicurezza estera (*Facility Security Clearance Information Sheet, FSCIS*) alle autorità di sicurezza e una conferma dell'azienda interessata. Alla domanda si risponde secondo una procedura standardizzata i cui dettagli vanno disciplinati mediante ordinanza.

Art. 60

Capoverso 1: una volta giunta la domanda di esecuzione della PSA, il servizio specializzato SA esamina dapprima se vi sono i presupposti per l'avvio della procedura (p. es. presenza di un mandato sensibile sotto il profilo della sicurezza) e se del caso avvia la PSA.

Capoverso 2: se, nel caso concreto, i rischi per la sicurezza delle informazioni possono essere ridotti al minimo mediante altre misure, il servizio specializzato SA, per motivi di economia amministrativa, può rinunciare all'esecuzione della PSA. Se, ad esempio, il mandato viene svolto sotto la vigilanza del servizio che conferisce il mandato nei suoi locali e al mandatario (azienda) non viene consegnata alcuna documentazione, bastano ad esempio, eventualmente, i corrispondenti CSP. Se il servizio specializzato SA rinuncia a eseguire

la 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. 61

Dopo l'avvio della procedura, il servizio specializzato SA si mette in contatto con il servizio che conferisce il mandato (mandante) e discute i dettagli del mandato. D'intesa con il mandante, definisce i requisiti in materia di sicurezza delle informazioni per l'adempimento del mandato. Sempre che l'esercizio di un'attività sensibile sotto il profilo della sicurezza sia necessario già nell'ambito della procedura di aggiudicazione, anche per questa fase vengono stabiliti i requisiti. In particolare, ciò si verifica periodicamente se per l'allestimento di un'offerta durante la procedura di aggiudicazione è necessario conoscere informazioni classificate.

Art. 62

La nozione di *«idoneità»* va intesa nel senso della sistematica del diritto in materia di appalti pubblici. Anche se la garanzia della sicurezza delle informazioni non rappresenta un esplicito criterio di idoneità di cui all'articolo 9 LAPub, il presente avamprogetto lo introduce però per l'esecuzione di mandati sensibili sotto il profilo della sicurezza.

Capoverso 1: il mandante deve comunicare al servizio specializzato SA tutte le aziende che entrano in considerazione per l'aggiudicazione del mandato.

Capoverso 2: il servizio specializzato SA valuta quindi se tali aziende sono idonee per l'esecuzione del mandato sensibile sotto il profilo della sicurezza oppure se con il conferimento del mandato a una determinata azienda o a determinate aziende si crea un rischio per la sicurezza di cui all'articolo 64. Se sussiste un rischio per la sicurezza in relazione a un offerente/fornitore, questi non è quindi idoneo sotto il profilo della sicurezza delle informazioni.

Capoverso 3: 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 (si veda anche l'art. 42 cpv. 4 per il CSP).

Art. 63

L'articolo 63 costituisce la base legale formale per l'acquisizione dei dati in vista della valutazione dell'idoneità delle aziende sotto il profilo della sicurezza di cui all'articolo 62 capoverso 2.

Il capoverso 1 elenca quali dati può rilevare il servizio specializzato SA per la valutazione dell'idoneità. Le modalità per simili domande e le informazioni che vengono fornite di conseguenza vanno disciplinate a livello di ordinanza.

- Secondo la lettera a, sostanzialmente i dati necessari vengono acquisiti presso l'azienda stessa con il suo consenso (si veda anche l'art. 57);
- la lettera b costituisce la base legale formale per ulteriori informazioni che il servizio specializzato SA richiede al Servizio delle attività informative della Confederazione;
- la lettera c consente al servizio specializzato SA, se necessario, di acquisire dati sulla ditta dal registro di commercio o da Internet. Simili ricerche possono fornire importanti indicazioni sull'affidabilità della ditta (si veda l'art. 39 cpv. 1 lett. g per il CSP).

Capoverso 2: il servizio specializzato SA, ad esempio, sfrutterà questa possibilità se ditte estere si candideranno presso le autorità federali per un mandato sensibile sotto il profilo della sicurezza.

Art. 64

Questa disposizione è simmetrica all'articolo 42 (valutazione del rischio per la sicurezza nella CSP). I meccanismi di valutazione del rischio sono, in linea di massima, identici.

Secondo il capoverso 1 sussiste 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.

Il capoverso 2 elenca in seguito i tre più importanti motivi per un'elevata probabilità che il mandato venga eseguito in maniera contraria alle prescrizioni o non appropriata.

- Lettera a: ciò può, ad esempio, essere il caso se i dati acquisiti mostrano che l'azienda ha commesso reati che sono rilevanti per la sicurezza delle informazioni;
- lettera b: con questa disposizione si intende impedire il trasferimento di informazioni sensibili sotto il profilo della sicurezza alle aziende che per i loro rapporti di proprietà, le loro strutture organizzati-

ve o le loro relazioni d'affari, vengono ad esempio dirette da servizi informazioni esteri o da organizzazioni di stampo criminale;

- lettera c: se l'azienda è costituita da una singola persona sussiste (ditta individuale) o se per l'adempimento del mandato sono indispensabili determinate persone (p. es. perché queste persone sono esperti 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 può avere quale conseguenza per queste persone che l'azienda nella sua totalità debba essere valutata come un rischio per la sicurezza.

Il capoverso 3 rileva che il rischio menzionato deve essere motivato dalle circostanze effettive dell'azienda interessata. 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.

Art. 65

Capoverso 1: 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. 76 cpv. 3). Il mandante può continuare la procedura di aggiudicazione o le sue trattative con tutte le aziende nelle quali non è riconoscibile alcun rischio per la sicurezza. Esso non è autorizzato a presentare ricorso e perciò viene solamente informato sulla valutazione.

Capoverso 2: se il servizio specializzato SA riconosce rischi per la sicurezza in relazione a un'azienda o più aziende, il mandante non può invece né aggiudicare il mandato a quell'azienda (o a quelle aziende), né stipulare il contratto con una simile azienda (o con simili aziende). Esso esclude dalla procedura di aggiudicazione l'azienda o le aziende in questione in quanto non idonee sotto il profilo della sicurezza. Il mandante è dunque vincolato alla valutazione del servizio specializzato SA. Il motivo consiste nel fatto che un'impresa o un'azienda alla quale viene rilasciata una dichiarazione di sicurezza aziendale, riceve un «sigillo di sicurezza» statale. La salvaguardia dell'integrità di questo sigillo può essere assicurata soltanto se la decisione sull'idoneità viene presa da specialisti.

Art. 66

Capoverso 1: appena il mandante ha aggiudicato il mandato, informa il servizio specializzato SA, che avvia le ulteriori fasi della procedura.

Capoverso 2: affinché sia garantita la necessaria sicurezza delle informazioni nell'azienda che deve esercitare l'attività sensibile sotto il profilo della sicurezza, occorre adottare pertinenti misure organizzative, in materia di personale, tecniche e fisiche. In un concetto in materia di sicurezza viene perciò stabilito come devono essere applicati i requisiti posti alla sicurezza delle informazioni già definiti dal servizio specializzato SA con il mandante dopo l'avvio della procedura (si veda l'art. 61).

Capoverso 3: di regola, le aziende hanno già adottato misure di sicurezza nei più svariati ambiti che devono soltanto essere ancora verificate e, ove necessario, completate dal servizio specializzato SA. Tutte le misure necessarie, quelle già adottate e quelle necessarie in aggiunta, vengono sancite nel concetto di cui al capoverso 2. Il servizio specializzato acquisisce i dati necessari direttamente presso l'azienda.

Art. 67

Capoverso 1: per i collaboratori che devono esercitare un'attività sensibile sotto il profilo della sicurezza viene eseguito un CSP. Queste persone vengono controllate in virtù dell'articolo 34 capoverso 1 lettera b ed eventualmente lettera c o dell'articolo 34 capoverso 2. Il livello di controllo si fonda sull'articolo 35.

Capoverso 2: il servizio specializzato SA decide successivamente al CSP, in modo vincolante, se alla persona sottoposta al controllo può essere affidata l'attività sensibile sotto il profilo della sicurezza.

Art. 68

Capoverso 1: appena l'azienda ha adottato le necessarie misure di sicurezza e ha così comprovatamente attuato il concetto in materia di sicurezza, il servizio specializzato SA le rilascia una dichiarazione di sicurezza aziendale (DSA). La DSA è una decisione secondo l'articolo 5 PA.

Capoverso 2: se il concetto in materia di sicurezza non viene attuato dall'azienda, il che finora in pratica è successo soltanto assai di rado, non vengono soddisfatti i requisiti relativi alla sicurezza delle informazioni. Perciò, in siffatti casi, il servizio specializzato SA rifiuta di rilasciare la DSA e dispone l'abbandono della procedura. Prima di poter disporre il rifiuto di rilasciare la DSA, il servizio specializzato SA deve accordare un termine suppletorio all'azienda affinché possa ottemperare ai suoi obblighi.

Capoverso 3: diversamente dalla dichiarazione di sicurezza nell'ambito del CSP, il rilascio o il mancato rilascio della DSA costituisce una decisione perché espleta effetti giuridici diretti per i partecipanti (si veda l'art. 69 segg.). Se non è d'accordo con la decisione del servizio specializzato SA, l'azienda può presentare ricorso contro questa decisione dinanzi al Tribunale amministrativo federale (art. 76 cpv. 1). La decisione viene comunicata anche al mandante, perché non può più affidare un'attività sensibile sotto il profilo della sicurezza all'azienda alla quale è stata rifiutata la DSA (art. 69). A quel momento il mandante ha probabilmente investito già molto denaro nel progetto e in questo caso, contrariamente all'articolo 65 capoverso 1, anch'esso ha dunque diritto di presentare ricorso.

Capoverso 4: 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 di cui all'articolo 62 segg.. Grazie a essa sarà possibile tenere conto delle modifiche fondamentali nell'azienda che influiscono sulla sicurezza delle informazioni.

Art. 69

Il mandante è vincolato alla decisione del servizio specializzato SA. Esso non può più affidare un'attività sensibile sotto il profilo della sicurezza all'azienda alla quale è stata rifiutata la DSA (si veda l'art. 68 cpv. 3). 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 38 capoverso 3 nell'ambito del CSP.

Art. 70

Capoverso 1: 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 concetto in materia di sicurezza.

Secondo il capoverso 2, 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 nuovi collaboratori ai quali deve essere affidato l'esercizio di attività sensibili sotto il profilo della sicurezza affinché nei loro confronti venga eseguito un CSP. L'azienda deve poi annunciare senza indugio al servizio specializzato SA se si è verificato un incidente rilevante sotto il profilo della sicurezza.

Art. 71

Il capoverso 1 autorizza il servizio specializzato SA a controllare nell'azienda il rispetto delle misure di sicurezza, previste nel concetto in materia di sicurezza e rilevanti per il mandato. Può verificare gli ambiti dell'azienda nei quali viene eseguito un mandato sensibile sotto il profilo della sicurezza. Può anche consultare documenti dell'azienda rilevanti per il mandato. Per sua stessa natura, l'ispezione può anche avvenire senza preavviso. Può essere eseguita solamente in compagnia o alla presenza di una persona appartenente all'azienda, di regola l'incaricato della sicurezza.

Capoverso 2: in presenza di indizi concreti di una minaccia per la sicurezza delle informazioni, il servizio specializzato SA può adottare le necessarie misure di protezione. Il servizio specializzato SA 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 vale anche per i casi nei quali, dopo il fallimento di un'azienda, i documenti o i mezzi TIC ancora esistenti devono essere separati rapidamente dalla massa fallimentare.

Art. 72

Capoverso 1: nell'aggiudicazione di altri mandati sensibili sotto il profilo della sicurezza, le aziende titolari di una DSA sono considerate idonee ai sensi dell'articolo 62. La loro idoneità non viene valutata di nuovo. Si applica una procedura semplificata, che il Consiglio federale disciplinerà a livello di ordinanza.

Secondo il capoverso 2, in siffatti casi occorre tuttavia esaminare se il concetto in materia di sicurezza in vigore deve essere adeguato. Ciò potrebbe ad esempio essere il caso se finora l'azienda in questione ha dovuto trattare «soltanto» informazioni classificate «CONFIDENZIALE», ma in futuro dovrà trattare anche informazioni classificate «SEGRETO».

Art. 73

Le aziende con sede in Svizzera che vogliono candidarsi per un mandato estero sensibile sotto il profilo della sicurezza, devono presentare alle autorità di quel Paese una dichiarazione di sicurezza delle autorità svizzere (si vedano l'art. 57 cpv. 1 lett. b e l'art. 68 cpv. 1). Il servizio specializzato SA rilascia perciò alle aziende con una DSA, su loro richiesta, una corrispondente attestazione.

Art. 74

Capoverso 1: la DSA viene revocata se l'azienda non adempie i propri obblighi di cui all'articolo 70 o se, nell'ambito di una ripetizione della procedura, una nuova valutazione di cui all'articolo 62 fa emergere un rischio per la sicurezza.

Secondo il capoverso 2, la revoca deve avvenire sotto forma di una decisione contro la quale, in virtù dell'articolo 76 capoverso 3, si può presentare ricorso dinanzi al Tribunale amministrativo federale. Il diritto di ricorso spetta anche al mandante poiché una revoca può essere svantaggiosa anche per esso. Può, ad esempio, avere un considerevole interesse finanziario che la DSA non venga revocata.

Art. 75

La PSA viene ripetuta se alla scadenza della durata di validità della DSA un mandato sensibile sotto il profilo della sicurezza è ancora pendente e viene elaborato dall'azienda. Durante la procedura di ripetizione l'adempimento del mandato non viene interrotto. Se il mandato è quasi adempiuto e 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 sono emersi nuovi rischi per la sicurezza, la procedura va parimenti ripetuta.

Art. 76

Il capoverso 1 accorda agli organi dell'azienda vari diritti (consultare i documenti, esigere la rettifica dei dati errati, esigere la soppressione di dati obsoleti, far apporre una menzione di contestazione) analogamente all'articolo 51 capoverso 1 per i CSP.

Secondo il capoverso 2, contro le decisioni del servizio specializzato SA è ammesso il ricorso al Tribunale amministrativo federale. Con questa norma si stabilisce che, nel presente caso, non si applica la disposizione d'eccezione dell'articolo 32 capoverso 1 lettera a della legge sul Tribunale amministrativo federale (la 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).

Art. 77

Capoverso 1: il servizio specializzato SA impiega un sistema d'informazione per eseguire e gestire la PSA. Tale sistema esiste da anni e, di recente, è stato completamente ripensato. Per ragioni di sistematica, l'attuale base giuridica per il sistema (art. 150 segg. LSIM) va spostata nella presente legge.

Capoverso 2: poiché il sistema può contenere dati personali degni di particolare protezione e profili della personalità, necessita di una base legale formale (art. 17 cpv. 2 LPD), costituita dagli articoli 77-80.

Il capoverso 3 elenca esaustivamente tutti i dati memorizzati nel sistema d'informazione.

Il capoverso 4 disciplina la responsabilità per il trattamento conforme al diritto dei dati nel sistema e per la sicurezza del sistema stesso.

Art. 78

L'articolo 78 fornisce la base necessaria per rendere accessibili a determinati servizi taluni dati del sistema d'informazione.

- Lettera a: i mandanti hanno accesso ai dati che li riguardano e all'elenco con tutte le aziende titolari di una DSA. Ciò consente loro di vedere rapidamente se un'azienda è già titolare di una DSA;
- lettera b: nel suo diritto esecutivo il Consiglio federale può autorizzare determinate aziende ad avviare autonomamente CSP per il proprio 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 inoltre consultare la decisione in merito al controllo e il livello di sicurezza (livello di controllo) dei collaboratori della loro azienda.

Art. 79

Il disciplinamento della conservazione e della distruzione dei dati corrisponde, *mutatis mutandis*, a quello proposto per il CSP (si veda l'art. 54).

Art. 80

Il Consiglio federale deve emanare le necessarie disposizioni completive alla PSA.

2.1.5 Sicurezza delle informazioni nelle infrastrutture critiche (IC)

In merito alla Strategia nazionale per la protezione della Svizzera contro i rischi informatici, si vedano i numeri 1.1.2.2 e 1.2.6.

Gli articoli 81-83 disciplinano i compiti della Confederazione per sostenere i gestori di infrastrutture critiche nel campo della sicurezza delle informazioni. Per partecipare al partenariato pubblico-privato nell'ambito di MELANI e ricevere le prestazioni di servizio della Confederazione non è necessario alcun assoggettamento alla legge, in virtù di una legislazione speciale, ai sensi dell'articolo 3 capoverso 3. La collaborazione avviene su base volontaria.

Art. 81

Conformemente al capoverso 1, il sostegno da parte della Confederazione concerne in particolare l'individuazione precoce e la valutazione di minacce e pericoli per informazioni e sistemi d'informazione degni di protezione, la corrispondente valutazione dei rischi, l'individuazione di incidenti, il ripristino della sicurezza delle informazioni a seguito di incidenti e l'analisi di incidenti. Per i gestori di infrastrutture critiche si tratta di importanti prestazioni di servizio della Confederazione.

Conformemente al capoverso 2, la Confederazione, da un lato, gestisce un servizio nazionale di allarme precoce 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 (*Governmental Computer Emergency Response Team*, GovCERT) che può procedere ad analisi tecniche, ad esempio su software nocivi ed emanare raccomandazioni per misure tecniche concrete volte a sventare pericoli o individuare incidenti. Per acquisire conoscenze, i servizi ai quali vengono assegnati compiti di cui al capoverso 2 possono anche simulare sistemi vulnerabili (*honeypot*) nelle reti.

Conformemente al capoverso 3, 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. Sovente minacce e pericoli riguardano non soltanto un singolo obiettivo, bensì varie organizzazioni operanti in un determinato settore o addirittura tutti i gestori di infrastrutture critiche di vari settori. Tuttavia, il ricorso alle prestazioni di servizio di cui all'articolo 81 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.

Art. 82

Le informazioni riguardo ai pericoli e agli indicatori per incidenti nell'ambito della sicurezza tecnica delle informazioni contengono periodicamente indicazioni su elementi d'indirizzo nel settore delle telecomunicazioni (p. es. indirizzi IP, indirizzi e-mail, nomi di dominio). Questi elementi d'indirizzo sono accomunati dal fatto che (per lo meno in teoria) si riferiscono, rispettivamente, a determinate o determinabili persone e ad apparecchi o collegamenti di telecomunicazione che a loro volta possono essere attribuiti a una determinata o determinabile persona. Di conseguenza, gli elementi d'indirizzo vanno potenzialmente considerati dati personali e, in conformità con gli articoli 4 capoverso 3 e 17 capoverso 1 LPD, necessitano di una base legale per il loro trattamento.

Il capoverso 1 prevede di conseguenza che i servizi competenti secondo l'articolo 81 possano trattare dati personali. Tuttavia, in particolare nel caso di elementi d'indirizzo registrati all'estero, l'identificazione periodica della persona interessata, che comunque non è affatto necessaria per sventare pericoli, non è possibile o lo è soltanto con una spesa notevole. Poiché dunque, di norma, non ha luogo alcuna identificazione, il trattamento di dati non può né essere reso noto alle persone interessate, né esse possono venire informate in merito al trattamento. Il presente articolo va quindi visto come *lex specialis* rispetto all'articolo 4 capoverso 4 LPD. Se invece sussiste il sospetto che un elemento d'indirizzo (svizzero) o che un apparecchio che utilizza questo elemento d'indirizzo venga utilizzato abusivamente da persone non autorizzate e che così ne risulta un pericolo, l'utente conforme al diritto può eventualmente essere identificato e venire informato in merito all'abuso. L'identificazione non deve tuttavia avvenire per forza da parte delle autorità competenti: ad esempio, nel caso di indirizzi IP dinamici, il fornitore di servizi di telecomunicazione può venire informato affin-

ché 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.

Nel capoverso 2 viene accordata la competenza per il trattamento dei dati per dati personali connessi con procedimenti e sanzioni di carattere amministrativo o penale. Conformemente all'articolo 3 lettera c numero 4 LPD, simili dati personali sono considerati dati personali degni di particolare protezione e, in virtù dell'articolo 17 capoverso 2 LPD, gli organi federali necessitano di una base legale formale per poterli trattare. Lo scambio di informazioni su infrastrutture criminali e abusi di elementi d'indirizzo può essere necessario per sventare pericoli o individuare incidenti. Anche se non viene comunicato il fatto che è stata avviata una procedura 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 si intende impedire che questo scambio non possa più avere luogo appena viene avviata un'inchiesta penale o una sanzione amministrativa riguardo a un elemento d'indirizzo.

Il capoverso 3 concede a gestori di mezzi TIC e fornitori di servizi TIC la possibilità di comunicare volontariamente ai servizi competenti di cui all'articolo 81 informazioni connesse con pericoli e incidenti nell'ambito della sicurezza tecnica delle informazioni. In virtù di questa disposizione, per sventare pericoli e di conseguenza per impedire danni essi possono dare indicazioni in merito alle prestazioni di servizi, alle trasmissioni e ad altre operazioni effettuate. Essa consente loro anche il trattamento conforme al diritto di corrispondenti dati personali. Poiché, mediante una simile comunicazione di dati, in un eventuale procedimento può essere pregiudicata la tutela di diritti di difesa, i dati così acquisiti non sono utilizzabili a fini giudiziari. Ai procedimenti giudiziari continuano ad applicarsi le rispettive norme per l'assunzione delle prove.

Art. 83

Il Consiglio federale deve disciplinare a livello di ordinanza la ripartizione dei compiti e la collaborazione tra i servizi che assumono i compiti di cui all'articolo 81. Essi devono presentarsi compatti nei confronti dei gestori di infrastrutture critiche. Viceversa, il Consiglio federale è libero di organizzare come vuole al loro interno questi servizi, affinché possano assumere i compiti della Confederazione nel modo più efficiente possibile. Nella futura legge federale sulle attività informative sono previste competenze di quest'ultimo nel campo della protezione delle infrastrutture critiche. Il Consiglio federale deve potere stabilire nel dettaglio la ripartizione dei compiti e la collaborazione pertinenti. In ragione delle particolarità che comporta il trattamento di informazioni di *intelligence*, il Consiglio federale deve disciplinare nello specifico il loro scambio tra servizi federali e la loro comunicazione ai gestori di infrastrutture critiche. I servizi competenti non vanno necessariamente collocati nel medesimo dipartimento. Per creare trasparenza e garantire certezza del diritto, il Consiglio federale disciplina il trattamento di dati e lo scambio di dati tra questi servizi nonché la sicurezza dei dati da considerare in proposito.

2.1.6 Organizzazione ed esecuzione

Art. 84

In merito al ruolo degli incaricati della sicurezza delle informazioni, si veda il numero 1.3.2.1.

Capoverso 1: in ragione della necessità preponderante di una direzione integrale dell'attuazione della presente legge, la legge interviene nell'autonomia organizzativa delle autorità. Chiede che, per il proprio ambito di competenza, le autorità assoggettate nonché i dipartimenti e la Cancelleria federale provvedano a designare un incaricato della sicurezza delle informazioni (a livello internazionale: *Chief Information Security Officer, CISO*) e un'adeguata supplenza. 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 i propri incaricati 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 (p. es. Tribunale federale dei brevetti e Tribunale militare di cassazione). La legge ammette dunque che, ad esempio, i tribunali della Confederazione possano designare un organo e un relativo sostituto unici 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 della sicurezza delle informazioni. Nell'ambito dell'adempimento del suo obbligo

organizzativo, il Consiglio federale deve decidere a livello di ordinanza come deve essere organizzata e diretta la sicurezza dell'informazione 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 per le decisioni nell'ambito della sicurezza tecnica delle informazioni devono continuare a rimanere presso la linea gerarchica, dunque presso le autorità competenti e i servizi subordinati. Gli incaricati della sicurezza delle informazioni devono però assistere e sostenere la linea gerarchica nelle questioni tecniche;
- la lettera b stabilisce che, per incarico della propria autorità o organizzazione, gli incaricati della sicurezza delle informazioni devono dirigere la sicurezza delle informazioni e la corrispondente gestione dei rischi sotto il profilo tecnico;
- 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 accertata necessità di agire, debbano presentare una richiesta in tal senso;
- la lettera d rileva che gli incaricati della sicurezza delle informazioni possono annunciare incidenti accertati rilevanti sotto il profilo della sicurezza sia al servizio specializzato della Confederazione per la sicurezza delle informazioni (art. 86) e alla Conferenza degli incaricati della sicurezza delle informazioni (art. 85), sia ai servizi che assumono i compiti riguardanti la sicurezza delle informazioni presso le infrastrutture critiche. Si rinuncia quindi a un *obbligo* generale di annuncio per tutte le autorità. Anche se la comunicazione di simili incidenti è assai raccomandabile, l'autonomia delle autorità non va però toccata.

Capoverso 3: gli incaricati della sicurezza delle informazioni devono essere indipendenti nella loro posizione e nell'assunzione dei loro compiti e non possono essere esposti ad alcun conflitto di interessi materiale. Nella pratica, la mancanza di una separazione delle funzioni porta di continuo a problemi nell'esecuzione delle direttive di sicurezza. Così oggi, ad esempio, la maggioranza degli incaricati della sicurezza delle TIC è ancora subordinata alle direzioni delle TIC. Spesso i responsabili delle TIC 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 TIC, 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 possibilmente obiettiva dei rischi per la sicurezza.

L'esatta collocazione della funzione è affidata alle autorità o ai dipartimenti e alla CaF. Basandosi su esperienze pratiche, la dottrina 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 lavorativi e valutare le esigenze aziendali. Sarebbe inoltre auspicabile, collocare gli incaricati della sicurezza delle informazioni in modo che possano assicurare uno stretto coordinamento con gli attuali gestori dei rischi, consulenti alla protezione dei dati, incaricati della sicurezza (protezione delle opere) ed eventualmente consulenti in materia di trasparenza.

Art. 85

In merito alla Conferenza, si veda il numero 1.3.2.2.

Il capoverso 1 stabilisce chi è membro permanente in questa Conferenza. In particolare devono essere rappresentati i dipartimenti e la Cancelleria federale.

Il capoverso 2 definisce i compiti della Conferenza, che servono tutti a coordinare efficacemente l'esecuzione. Il servizio specializzato della Confederazione per la sicurezza delle informazioni (si veda l'art. 86), da istituire *ex novo*, dovrà servire a consultare e coinvolgere la Conferenza su tutte le questioni importanti relative alla sicurezza delle informazioni. Particolarmente importante è la consulenza al servizio specializzato da parte della Conferenza nelle questioni riguardanti la strategia in materia di sicurezza delle informazioni. La Conferenza deve anche servire a riconoscere tendenze o rischi e a pianificare a lungo termine misure appropriate. Solamente così sarà possibile trovare soluzioni efficaci e creare il necessario consenso. Appare importante anche che il coordinamento con l'IFPDT venga sancito esplicitamente quale mandato (lett. d). Per i suoi accertamenti e la formazione di una propria opinione, la Conferenza può ricorrere anche a rappresentanti dei Cantoni e a esperti indipendenti.

Il capoverso 3 stabilisce che la Conferenza deve definire la propria organizzazione e i propri processi lavorativi e decidere inoltre sulla propria direzione.

Art. 86

In merito al servizio specializzato della Confederazione per la sicurezza delle informazioni, si veda il n. 1.3.2.3.

Il capoverso 1 contiene un catalogo dei compiti e delle competenze, concernenti tutte le autorità, del futuro servizio specializzato:

- la lettera a obbliga il servizio specializzato a fornire consulenza alle autorità assoggettate e ai loro incaricati della sicurezza delle informazioni. Esse possono anche chiedere l'assistenza tecnica del servizio specializzato, in particolare nell'elaborazione di incidenti nell'ambito della sicurezza delle informazioni;
- secondo la lettera b, il servizio specializzato deve potere raccomandare misure di protezione preventive in caso di minacce dirette alla sicurezza delle informazioni;
- lettera c: le autorità assoggettate o i servizi da esse autorizzati possono incaricare il servizio specializzato di eseguire presso di loro determinati controlli e *audit* nell'ambito della sicurezza delle informazioni. Il servizio specializzato non può eseguire spontaneamente simili verifiche. In particolare per *audit* di sicurezza tecnici sono necessarie elevate conoscenze specialistiche che non tutte le autorità assoggettate dovrebbero procurarsi per sé: approntare un *pool* di esperti è più economico;
- lettera d: in virtù dell'articolo 20, le autorità e le organizzazioni assoggettate che vogliono impiegare nuove tecnologie sono tenute a eseguire una valutazione dei rischi. Per le tecnologie particolarmente importanti o che possono avere un ampio campo d'applicazione, devono potere chiedere al servizio specializzato di eseguire questa analisi dei rischi;
- la lettera e, su richiesta delle autorità e delle organizzazioni assoggettate, autorizza l'organo specializzato a esaminare, per quanto riguarda aspetti rilevanti sotto il profilo della sicurezza, l'idoneità di determinati processi, mezzi, installazioni, oggetti e prestazioni di servizio. Nell'ambito della sicurezza delle informazioni a livello tecnico, i fornitori di prestazioni TIC sono, ad esempio, interessati a sapere se le soluzioni tecniche che sviluppano soddisfano i requisiti fissati dalla Confederazione. Se ciò è il caso, allora possono impiegarli molto più semplicemente per altri progetti o mezzi TIC. Lo stesso vale anche, ad esempio, per casseforti o per prestazioni di servizio. 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 per il contesto internazionale: il servizio specializzato deve assumere il ruolo (oggi mancante), usuale a livello internazionale, della *National Accreditation Authority* (si veda il n. 4.2);
- lettera f: se vengono avviati importanti progetti che coinvolgono più autorità e hanno un sostanziale rapporto con la sicurezza delle informazioni, su richiesta delle autorità assoggettate il servizio specializzato deve assumere all'interno dei progetti la direzione e il coordinamento delle questioni inerenti alla sicurezza delle informazioni;
- lettera g: poiché le corrispondenti conoscenze specialistiche vanno raggruppate per la Confederazione nel previsto servizio specializzato, quest'ultimo deve essere 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 (si veda il n. 4.2.). Altre autorità o organizzazioni potranno però continuare a intrattenere contatti specialistici in questo settore;
- lettera h: il servizio specializzato dovrà allestire annualmente un rapporto per il Consiglio federale.

In conformità con il capoverso 3, nel suo diritto esecutivo il Consiglio federale deve disciplinare l'organizzazione del servizio specializzato. Per questo dovrà stabilire quali compiti deve esercitare il servizio specializzato stesso e quali adempiere in collaborazione con altri servizi federali. In questo contesto, il Consiglio federale dovrà ovviamente decidere anche sulla questione della loro collocazione.

Art. 87

Capoverso 1: l'autonomia delle autorità assoggettate non sarà messa in discussione. Esse non saranno assoggettate alle disposizioni d'esecuzione del Consiglio federale. Per contro, dovranno emanare per il proprio ambito le disposizioni necessarie per l'esecuzione della presente legge. Il capoverso stabilisce anche che il Consiglio federale può delegare alla Cancelleria federale l'emanazione di disposizioni esecutive in relazione con la gestione degli affari del Consiglio federale (si veda anche art. 15 cpv. 2 LOGA).

Capoverso 2: con questa normativa e l'articolo 70 LParl, l'Assemblea federale ha tutte le disposizioni necessarie affinché essa e i Servizi del Parlamento possano applicare direttamente la LSIn e le sue disposizioni d'esecuzione.

Nel capoverso 3 viene stabilito un cosiddetto «*opting out*»: le disposizioni d'esecuzione del Consiglio federale di cui al capoverso 1 si applicano, per analogia, a tutte le autorità assoggettate, sempre che non emanino

proprie disposizioni d'esecuzione. Rimane inteso che il Consiglio federale consulta le altre autorità prima di emanare le proprie disposizioni d'esecuzione. Che il Consiglio federale sia competente, in maniera autonoma, per l'emanazione delle disposizioni d'esecuzione necessarie al controllo di sicurezza relativo alle persone e alla procedura di sicurezza relativa alle aziende risulta dal fatto che i relativi servizi competenti sono parte dell'Amministrazione federale, la cui organizzazione è affare del Consiglio federale.

Capoverso 4: prima che le organizzazioni di diritto pubblico o privato di cui all'articolo 2 capoverso 2 lettera e possano essere assoggettate alla legge, si deve valutare se esercitano attività della Confederazione sensibili sotto il profilo della sicurezza. Il Consiglio federale deve procedere a tale valutazione per queste organizzazioni e in seguito fissare a livello di ordinanza il campo d'applicazione dettagliato. Ciò può avvenire nelle disposizioni d'esecuzione della legislazione speciale o nelle disposizioni d'esecuzione della presente legge. Se necessario, il Consiglio federale può fare applicare da queste organizzazioni soltanto parti della legge (p. es. disposizioni sulla classificazione, sull'impiego delle TIC o sui controlli di sicurezza relativi alle persone).

Art. 88

Capoverso 1: per raggiungere il necessario livello di sicurezza uniforme, il Consiglio federale deve stabilire, secondo lo stato della dottrina e della tecnica, requisiti e misure standard. Non si tratta di requisiti e misure organizzative fondamentali bensì, in primo luogo, di requisiti di minore importanza, ad esempio:

- standard per rilevare le necessità di protezione di informazioni in relazione ai quattro criteri dell'articolo 4 capoverso 2;
- metodo standard per valutare il rischio di cui all'articolo 6 capoverso 1;
- standard per le misure organizzative, in materia di personale, tecniche ed edili di cui all'articolo 6 capoverso 2;
- requisiti standard per determinati processi e mezzi volti a proteggere informazioni classificate di cui agli articoli 12-18;
- requisiti e misure standard per la protezione di base, per l'allestimento di piani di sicurezza delle informazioni e per la sicurezza di mezzi TIC dei livelli di sicurezza «protezione elevata» e «protezione molto elevata» di cui agli articoli 19-27; ecc.

Capoverso 2: se necessario, il Consiglio federale delegherà a servizi subordinati l'elaborazione e l'adozione degli standard. Ciò concerne in primo luogo il servizio specializzato della Confederazione per la sicurezza delle informazioni, ma anche, ad esempio, fedpol nell'ambito della protezione delle opere. I fornitori di prestazioni TIC della Confederazione dovrebbero, parimenti, potere elaborare standard di sicurezza tecnici ed eventualmente, ai fini della standardizzazione, farli verificare dal servizio specializzato quanto alla loro idoneità per la Confederazione (si veda l'art. 86 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 necessariamente andrebbero 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.

Capoverso 3: gli standard non sono vincolanti per le altre autorità assoggettate.

Art. 89

Capoverso 1: in casi nei quali i Cantoni o le loro autorità e i loro servizi rispettivi rientrano nel campo d'applicazione della legge (si veda l'art. 2 cpv. 2 lett. f), devono adottare le necessarie misure di sicurezza secondo la presente legge. I servizi federali non ricevono così però alcuna facoltà diretta di emanare istruzioni bensì, in linea di principio, sono i Cantoni stessi responsabili dell'esecuzione nel loro ambito di competenza.

Capoverso 2: il Consiglio federale deve disciplinare nel suo diritto esecutivo la verifica dell'applicazione delle misure e l'esecuzione di controlli di sicurezza relativi alle persone per gli impiegati cantonali. In particolare dovrà disciplinare come, eventualmente, le autorità federali controllano l'applicazione delle prescrizioni da parte dei Cantoni. Rimane inteso che, nel farlo, terrà conto dello statuto istituzionale dei Cantoni e in particolare della loro autonomia organizzativa.

Nel capoverso 3 i Cantoni vengono obbligati, per simili casi, a designare ciascuno un servizio quale interlocutore delle autorità e delle organizzazioni assoggettate competenti. In questo modo si intende garantire che lo scambio di informazioni abbia luogo sistematicamente e che l'applicazione delle misure secondo la presente legge avvenga in modo coordinato.

Art. 90

I trattati internazionali nel campo della sicurezza delle informazioni contengono previamente normative tecniche sul riconoscimento reciproco di prescrizioni e procedure nazionali (p. es. la procedura del controllo di sicurezza relativo alle persone e la procedura di sicurezza relativa alle aziende), elenchi di concordanza sull'applicazione di classificazioni 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 eventualmente con le autorità federali riceventi una più o meno rigida protezione delle sue informazioni. Di conseguenza, nelle disposizioni di esecuzione e organizzative che attribuiscono le rispettive competenze di concludere trattati, vanno sancite le necessarie riserve. Per motivi di economia amministrativa, il Consiglio federale va autorizzato a concludere direttamente simili trattati in materia di sicurezza delle informazioni.

L'interconnessione e la collaborazione crescenti sul piano internazionale sono necessarie per ridurre al minimo i rischi legati alla sicurezza delle informazioni. L'applicazione della SNPC richiede perciò che, per quanto riguarda le esperienze, i lavori di ricerca e sviluppo, le informazioni riferite a incidenti, le attività di formazione e le esercitazioni, vengano rafforzati gli scambi (si veda anche il n. 1.1.2.2). Il Consiglio federale va perciò autorizzato anche a concludere trattati internazionali per lo scambio di informazioni su pericoli, carenze e incidenti, in particolare per quanto riguarda le infrastrutture critiche. Si tratta soprattutto di questioni organizzative e tecniche secondarie (p. es. collaborazione con altri GovCERT; si veda l'art. 81).

Art. 91

Ogni legge deve essere periodicamente verificata quanto alla sua effettiva applicazione, nonché all'adeguatezza, all'efficacia e all'economicità. Secondo il capoverso 1, il Consiglio federale deve essere competente a tale scopo. L'Assemblea federale deve determinare la commissione incaricata di trattare i rapporti del Consiglio federale (cpv. 2).

Art. 92

In virtù della nuova normativa devono essere adeguate altre leggi federali.

Art. 93

Per motivi di economia procedurale, le dichiarazioni di sicurezza relative alle persone e le dichiarazioni di sicurezza aziendali secondo il diritto anteriore devono mantenere la loro validità fino alla loro scadenza. Il Consiglio federale stabilirà i termini transitori per l'adeguamento delle prescrizioni sul trattamento di informazioni classificate e sulla tutela della sicurezza delle informazioni nell'impiego di TIC.

2.2 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.

2.3 Legge sull'archiviazione

Art. 6 cpv. 2

L'archiviazione di documenti della Confederazione è disciplinata in maniera uniforme dalla LAr. Sono considerati documenti in particolare «tutte le informazioni registrate, indipendentemente dal loro supporto, che sono state raccolte o prodotte nell'adempimento di compiti pubblici della Confederazione» (art. 3 cpv. 1 LAr). I servizi della Confederazione devono offrire all'Archivio federale per la loro archiviazione tutti i documenti «dei quali non hanno più bisogno in modo permanente» (art. 6 LAr). Le informazioni classificate sono anch'esse soggette alla legislazione in materia di archiviazione. In questo ambito la loro protezione è garantita da termini di protezione secondo gli articoli 9 segg. LAr.

Il nuovo capoverso 2 dell'articolo 6 LAr disciplina il rapporto tra la LAr e la LSIn. La disposizione serve alla chiara delimitazione dei campi di applicazione delle due leggi in questione. La LAr disciplina l'archiviazione, motivo per cui questo aspetto non è disciplinato nella LSIn bensì nella LAr stessa. Secondo l'articolo 6 capoverso 2 LAr, le informazioni classificate non sono offerte per l'archiviazione, sino a quando

secondo le disposizioni della LSIn, sono ancora degne di protezione. Non appena possono essere declassificate in applicazione delle disposizioni della legislazione sulla sicurezza delle informazioni, devono essere offerte per l'archiviazione. La classificazione e la declassificazione sono rette dalle disposizioni della LSIn. La maggior parte delle informazioni classificate sono degne di essere protette per un periodo limitato e devono poter essere archiviate secondo le norme usuali della LAr. È ovvio che la classificazione non può essere utilizzata per sottrarsi all'obbligo di archiviazione.

2.4 Legge sul personale federale

Art. 20a

L'innalzamento del valore 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. *Nonostante la legge* esiste comunque il rischio che nella prassi il valore soglia per i CSP venga abbassato o 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 deve essere avanzata solo nella misura in cui sia necessario per la tutela degli interessi del datore di lavoro. Al riguardo il Consiglio federale emanerà le disposizioni d'esecuzione.

Art. 20b

La LSIn limita la sua regolamentazione riguardante il CSP ad attività sensibili sotto il profilo della sicurezza che riguardano la gestione di informazioni e mezzi TIC classificati nonché l'accesso a determinate zone di sicurezza. Queste attività dovrebbero interessare la maggioranza dei CSP necessari. Rimangono però altre attività nel settore di compiti delle autorità federali, che non riguardano direttamente la gestione di informazioni o mezzi TIC ma il cui esercizio potrebbe pregiudicare considerevolmente gli interessi della Confederazione. Per il personale della Confederazione (ad eccezione dell'esercito e dalla Banca nazionale) queste regolamentazioni rientrano nella LPers. Con l'introduzione di una nuova disposizione sulla verifica dell'affidabilità nell'articolo 20*b* LPers, si intende coprire un fabbisogno di verifica identificato.

- Secondo la lettera a, il Consiglio federale può far verificare l'affidabilità di candidati e impiegati destinati a rappresentare regolarmente la Svizzera all'estero e che in tale contesto potrebbero pregiudicare considerevolmente l'immagine della Confederazione. Si tratta soprattutto 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).
- Secondo la lettera b, il Consiglio federale può anche far verificare l'affidabilità di candidati e impiegati destinati a esercitare competenze decisionali o compiti di vigilanza in affari finanziari o fiscali essenziali e che in tale contesto potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione (ad es. impiegati con competenze decisionali nell'aggiudicazione di mandati importanti o persone che svolgono compiti particolarmente sensibili in relazione alle finanze pubbliche).

Capoverso 2: nelle sue norme d'esecuzione concernenti la LPers, il Consiglio federale definirà i gruppi di persone che devono essere sottoposti alla verifica dell'affidabilità. Questa verifica è ordinata solo se la necessità è dimostrata. Tale disposizione non deve servire a raggirare la limitazione dei motivi di verifica secondo la LSIn.

Capoverso 3: dato che le questioni da chiarire sono di principio analoghe a quelle della sicurezza delle informazioni, non è ragionevole introdurre una procedura particolare per la verifica dell'affidabilità. Per l'esecuzione della 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 e delle normative sulle conseguenze della valutazione.

Capoverso 4: se la persona da controllare in base a questa disposizione deve essere contemporaneamente sottoposta a un CSP secondo la LSIn, le due procedure saranno riunite per ragioni di economia procedurale.

2.5 Codice penale

Art. 365 cpv. 2 lett. d

L'adeguamento di questo articolo è puramente formale. Dato che i CPS non sono 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 dal casellario giudiziale devono essere adeguati in modo corrispondente. Quale scopo dell'acquisizione di dati viene ora elencata anche la valutazione del rischio per la sicurezza nel quadro delle verifiche dell'affidabilità secondo la legislazione speciale. Per contro, l'esame del potenziale di violenza è già disciplinato nelle lettere n e p.

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

Vedi il commento all'articolo 365 capoverso 2 lettera d.

2.6 Legge federale sui sistemi d'informazione di polizia della Confederazione

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

L'adeguamento di questi due articoli è puramente formale. Dato che i CSP saranno disciplinati non più nella LMSI, bensì nella LSIn, le disposizioni concernenti i servizi che beneficiano dell'autorizzazione di accesso e lo scopo dell'acquisizione di dati dal sistema di ricerca informatizzato di polizia e dal registro nazionale di polizia devono essere modificate in modo corrispondente. Inoltre, sono ora menzionati tra gli scopi dell'acquisizione di dati anche la valutazione del rischio per la sicurezza nel quadro di una verifica dell'affidabilità secondo la legislazione speciale nonché la valutazione del potenziale di violenza nel quadro dei relativi controlli.

2.7 Legge militare

Art. 14

L'avamprogetto della LSIn limita la sua regolamentazione prevista per i CSP a determinate attività sensibili sotto il profilo della sicurezza (cfr. sopra ad art. 20b LPers). Anche nell'esercito vi sono tuttavia altre attività che potrebbero notevolmente pregiudicare l'immagine della Confederazione e delle sue istituzioni oppure importanti interessi finanziari della Confederazione.

Il capoverso 1 prevede pertanto, in sintonia con il proposto articolo 20b LPers, che nel quadro delle sue disposizioni d'esecuzione relative alla LM il Consiglio federale possa sottoporre a una verifica dell'affidabilità due settori di compiti:

- secondo la lettera a, il Consiglio federale può sottoporre a verifica i militari destinati a rappresentare regolarmente la Svizzera all'estero e che in tale contesto potrebbero considerevolmente pregiudicare l'immagine della Confederazione. Si tratta in particolare di militari che rappresentano la Svizzera in occasione di impieghi all'estero o che adempiono compiti nel settore della diplomazia militare.
- Secondo la lettera b, il Consiglio federale può inoltre sottoporre a verifica i militari destinati a esercitare competenze decisionali o compiti di vigilanza in affari finanziari essenziali e che in tale contesto potrebbero pregiudicare considerevolmente gli interessi finanziari della Confederazione.

Capoverso 2: nella sua normativa d'esecuzione concernente la LM, il Consiglio federale deve definire i gruppi di persone che devono essere sottoposti alla verifica dell'affidabilità. Questa verifica è ordinata solo se la necessità è dimostrata, in modo da evitare un aggiramento della limitazione dei motivi di controllo secondo la LSIn.

Capoverso 3: come per la regolamentazione proposta in sede di LPers, dato che le questioni da chiarire sono di principio analoghe a quelle della sicurezza delle informazioni, non è ragionevole introdurre una procedura particolare. Per l'esecuzione della verifica sarà pertanto ripresa la regolamentazione della LSIn. La procedura sarà ripresa in particolare per quanto riguarda l'applicazione dei principi dell'acquisizione dei dati e delle normative sulle conseguenze della valutazione.

Capoverso 4: se la persona da controllare in base a questa disposizione deve essere contemporaneamente sottoposta a un CSP secondo la LSIn, le due procedure saranno riunite per ragioni di economia procedurale.

Art. 113 cpv. 5

A causa della limitazione del CPS secondo la LSIn alle attività sensibili sotto il profilo della sicurezza che riguardano la gestione di informazioni e mezzi TIC classificati si rende necessario fondare su una base legale

speciale l'esame del potenziale di violenza dei militari destinati a essere equipaggiati con un'arma. Per quanto riguarda la procedura, il disciplinamento previsto dalla LSIn sarà applicato per analogia. Se sono state avviate due procedure, saranno riunite per ragioni di economia procedurale.

Art. 150 cpv. 4 abrogazione

La competenza di concludere trattati internazionali destinati a garantire la tutela del segreto militare è ora contemplata dall'articolo 90 LSIn. Inoltre, spesso non si distingue più tra tutela del segreto militare e civile, ma viene conclusa una convenzione per entrambi gli ambiti, ossia per la tutela del segreto in generale. Per garantire l'omogeneità del diritto, l'articolo 150 capoverso 4 della legge militare deve pertanto essere abrogato.

2.8 Legge federale sui sistemi d'informazione militari

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

Attualmente i sistemi d'informazione per il CSP e la procedura di sicurezza relativa alle aziende sono disciplinati nella LSIM. Entrambi i sistemi d'informazione saranno in futuro disciplinati direttamente nella LSIn (art. 52-54 per il CSP e art. 77-79 per la procedura di sicurezza relativa alle aziende). Pertanto entrambe le corrispondenti sezioni della LSIM devono essere abrogate.

2.9 Legge federale sull'energia nucleare

Art. 5 cpv. 3

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.

Art. 24

Il disciplinamento vigente secondo l'articolo 24 LENu prevede già controlli dell'affidabilità per le persone impiegate in funzioni essenziali della sicurezza nucleare interna ed esterna. Queste persone sono sottoposte a un CSP sulla base dell'OCSPN. Dato che la verifica è eseguita applicando, per analogia, le disposizioni della LSIn concernenti il CSP, nella nuova versione, il tenore dell'articolo 24 LENu è adeguato alla nuova terminologia in materia di verifiche dell'affidabilità.

2.10 Legge sull'approvvigionamento elettrico

Art. 26a

La società nazionale di rete (Swissgrid), che gestisce la rete di trasporto per l'intero territorio svizzero, chiede da anni che determinati gruppi di persone siano soggetti ai CSP. Alla luce della criticità della rete di trasporto e della necessaria protezione contro il sabotaggio, occorre introdurre nella LAEI una nuova disposizione concernente l'esecuzione di verifiche dell'affidabilità per gruppi di persone particolari.

Il capoverso 1 stabilisce il principio della verifica dell'affidabilità di impiegati della società nazionale di rete che adempiono compiti essenziali per la sicurezza della rete di trasporto a livello nazionale e il suo esercizio affidabile ed efficiente.

Secondo il capoverso 2, il Consiglio federale stabilisce i gruppi di persone che devono essere soggetti alla verifica. Al riguardo deve limitarsi alle funzioni che possono provocare un danno considerevole in caso di azioni di sabotaggio o di sabotaggio per negligenza.

Capoverso 3: la procedura di verifica si fonda sulle disposizioni della LSIn concernenti il CSP.

Il capoverso 4 si rifà all'analoga regolamentazione secondo l'articolo 24 LENu. La direzione di Swissgrid nonché i regolatori (UFE e ElCom) in qualità di servizi competenti per l'attribuzione della funzione, devono avere accesso ai dati della verifica.

2.11 Legge sulla banca nazionale

Art. 16, rubrica e cpv. 5

In virtù dei suoi compiti di politica monetaria (vedi anche art. 1 cpv. 2 lett. d), la Banca nazionale va considerata come un'autorità assoggettata alla LSIn secondo l'articolo 2 capoverso 1 LSIn. Con l'adeguamento dell'articolo 16 LBN si rimanda espressamente al fatto che la LSIn si applica anche alla Banca nazionale. La rubrica dell'articolo è modificata in modo corrispondente.

3 Ripercussioni

3.1 Ripercussioni per la Confederazione

Le informazioni vengono protette in quanto una violazione della loro confidenzialità, disponibilità, integrità o tracciabilità (cfr. art. 4) può compromettere i diritti di terzi (ad es. dati personali, segreti d'affari o di fabbricazione), pregiudicare interessi pubblici essenziali (ad es. la capacità d'azione delle autorità federali, la sicurezza nazionale, le relazioni internazionali o l'approvvigionamento del Paese) o arrecare danni alle organizzazioni interessate (ad es. perdita di produttività o disfunzioni nell'esercizio). 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. I suoi costi devono pertanto essere ponderati con la corrispondente riduzione dei rischi.

Secondo le stime attuali, la legge comporterà un miglioramento notevole e durevole della sicurezza delle informazioni in seno alla Confederazione. In prima linea disciplina la gestione della sicurezza delle informazioni e aumentandone l'efficienza. Sovente una gestione efficiente migliora in particolare la sicurezza in modo più efficace, economico e durevole che non gli 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 – a medio termine può addirittura generare risparmi. L'avamprogetto prevede anche diverse misure organizzative che, rispetto ad oggi, oltre a migliorare la protezione delle informazioni, dovrebbero comportare determinati risparmi in termini di costi, nella misura in cui vengono attuate coerentemente. L'innalzamento dei valori soglia per la classificazione, ad esempio, dovrebbe ridurre il numero di informazioni classificate e quindi il relativo dispendio (cfr. n. 1.2.3.4). Per quanto riguarda i controlli di sicurezza relativi alle persone (CSP), il valore soglia per l'esecuzione di un simile CSP sarà innalzato e, nel contempo, il numero di attività per il cui esercizio è necessario (e ammesso) un CSP verrà ridotto. Pertanto, in futuro i CSP dovrebbero diminuire (cfr. n. 1.2.4). Inoltre, ad esempio, la proposta standardizzazione dei requisiti e delle misure di sicurezza (cfr. art. 88), il miglioramento dello scambio di informazioni tra autorità federali e il sostegno alle autorità federali da parte del servizio specializzato della Confederazione per la sicurezza delle informazioni (cfr. art. 84-86) contribuiranno a fare in modo che non si debba «reinventare la ruota» per ogni progetto. Infine, la nuova regolamentazione agevolerà la cooperazione internazionale nel settore della sicurezza (cfr. n. 4.2).

Il necessario miglioramento della sicurezza delle informazioni a livello di Confederazione provocherà costi, che tuttavia potranno essere stimati oggettivamente solo dopo l'esecuzione della procedura di consultazione. A tale scopo sono necessarie in particolare varianti a livello di organizzazione e risorse in relazione agli incaricati della sicurezza delle informazioni e al servizio specializzato della Confederazione per la sicurezza delle informazioni nonché dati più precisi sul numero dei mezzi TIC esistenti che in futuro rientreranno nel livello di sicurezza «protezione molto elevata». Nel suo messaggio, il Consiglio federale presenterà in modo trasparente le ripercussioni finanziarie e in materia personale del disegno di legge.

I costi imputabili direttamente alla legge devono essere chiaramente delimitati dai costi delle misure che le singole autorità federali possono decidere liberamente nell'ambito dell'attuazione. La legge disciplina in particolare solo la gestione della sicurezza delle informazioni e non definisce né un livello di sicurezza da raggiungere né – salvo alcune eccezioni (cfr. più sotto) – misure dettagliate. Essa non è pertanto attuabile direttamente, in quanto le autorità federali devono emanare disposizioni proprie per il rispettivo ambito di competenza e dispongono al riguardo – ad eccezione del settore organizzativo – di un margine di manovra pressoché illimitato (cfr. art. 87 cpv. 1). In questo contesto devono definire il livello di sicurezza che intendono raggiungere (cfr. art. 5 cpv. 3 lett. a) e, su questa base, decidere, a livello di ordinanza, di istruzioni o addirittura di progetto, i requisiti e le misure dal punto di vista organizzativo, del personale, tecnico ed edile necessari al raggiungimento di questo livello. Quanto più il livello di sicurezza da raggiungere è elevato, tanto più i costi delle misure di sicurezza saranno alti. La legge in sé non ha influsso su questi costi. Pertanto, nella valutazione delle ripercussioni finanziarie e in materia di personale della legge non possono nemmeno essere quantificati.

Già oggi tutte le autorità federali sono tenute ad adottare misure per garantire la sicurezza delle informazioni. Determinante per la valutazione dei costi sono quindi le disposizioni della legge che definiscono nuovi compiti o modificano compiti e processi esistenti. Qui di seguito sono descritti i cinque fattori di costo più importanti dell'avamprogetto di legge:

1. *organizzazione, gestione, attuazione e controllo della sicurezza delle informazioni (art. 5 cpv. 1 lett. a)*: la nuova organizzazione richiesta dalla legge comporterà un impegno organizzativo da non sottovalutare e richiederà risorse finanziarie. In particolare nella fase di allestimento e di introduzione si dovranno acquisire le conoscenze tecniche che attualmente in parte mancano alle autorità federali. Per la gestione e l'esercizio di una simile organizzazione interna saranno competenti gli incaricati della sicurezza delle informazioni. Per ogni autorità nonché per i dipartimenti e la CaF la legge prevede almeno due incaricati della sicurezza delle informazioni. L'adempimento di questi compiti dovrà essere garantito principalmente con le risorse di personale disponibili. Il fabbisogno effettivo di personale risulterà tuttavia variabile e dipenderà dalle dimensioni dell'autorità o organizzazione (effettivo di personale), dal rispettivo settore di compiti nonché dal numero e dalla criticità dei mezzi TIC da esse impiegati;
2. *verifiche e audit migliorati (art. 11 cpv. 2 nonché ad es. art. 24 cpv. 2)*: per l'esecuzione dei controlli, un compito dirigenziale ordinario, è di principio competente la linea gerarchica. Gli incaricati della sicurezza delle informazioni eseguiranno anch'essi verifiche e audit su mandato della propria autorità o organizzazione. La legge prevede tuttavia due nuovi tipi di verifiche che comporteranno ripercussioni finanziarie e personali, ossia una verifica dell'efficacia indipendente e periodica delle misure adottate (art. 11 cpv. 2) nonché una verifica tecnica dell'efficacia dei mezzi TIC più critici (art. 24 cpv. 2). I costi che ne risultano dipenderanno dalla frequenza di questi controlli. Grossomodo si possono ipotizzare i seguenti dati:
   - *audit esterni (art. 11 cpv. 2)*: secondo le indicazioni del CDF, per una piccola verifica trasversale sono necessari, in base all'esperienza, circa 100 giorni/persona, mentre per un'ampia verifica trasversale si contano circa 300 giorni/persona;
   - *verifiche tecniche dell'efficacia (art. 24 cpv. 2)*: nella Confederazione sono impiegati approssimativamente da 50 a 70 sistemi TIC che in futuro saranno attribuiti al livello di sicurezza «protezione molto elevata» e che quindi dovranno essere sottoposti a una verifica dell'efficacia. In base all'esperienza, i costi per gli audit (spese per il personale) ammontano di regola dallo 0,5 per cento al 2 per cento delle spese totali per investimenti destinati al sistema TIC sottoposto all'audit;
3. *controlli di sicurezza relativi alle persone (CSP; art. 32-55)*: uno degli obiettivi della legge è armonizzare e snellire i CSP. Con le modifiche proposte, in futuro dovranno essere eseguiti meno CSP e quindi i relativi costi dovrebbero diminuire a medio termine;
4. *procedura di sicurezza relativa alle aziende (art. 56-80):* oggi per l'esecuzione della procedura di sicurezza relativa alle aziende nel quadro di mandati militari classificati, il DDPS impiega due posti a tempo pieno. L'estensione al settore civile e alle altre autorità federali proposta dal Consiglio federale comporterà un aumento del numero delle aziende interessate e quindi un maggior fabbisogno di personale. Le aziende che si candidano per mandati di autorità estere per la cui esecuzione è necessaria un'attestazione di sicurezza relativa alle aziende devono sopportare i costi per la procedura di sicurezza da eseguire (art. 57 cpv. 3);
5. *servizio specializzato della Confederazione per la sicurezza delle informazioni (art. 86)*: la creazione di questo nuovo servizio comporterà costi di riorganizzazione che dipenderanno dall'attribuzione amministrativa del servizio specializzato nonché dall'entità della fusione di organi esistenti. Nonostante il servizio specializzato debba adempiere i suoi compiti principalmente con le risorse di personale esistenti dell'Amministrazione federale, sarà necessario personale supplementare. Il servizio specializzato non opererà solo per l'Amministrazione federale, ma anche per le altre autorità federali. Inoltre dovrà svolgere nuovi compiti, in particolare:
   - esecuzione di verifiche e audit (art. 86 cpv. 1 lett. c): vedi più sopra il numero *2. Verifiche e audit migliorati;*
   - verifica dell'idoneità dal punto di vista della sicurezza di determinati processi, mezzi e prestazioni (art. 86 cpv. 1 lett. e). Questo nuovo compito è necessario per la standardizzazione auspicata e per la collaborazione internazionale;
   - direzione e coordinazione dell'ambito della sicurezza delle informazioni in occasione di progetti importanti che coinvolgono più autorità (art. 86 cpv. 1 lett. f). Con questo nuovo compito si intende, da un lato, garantire che le competenze nell'ambito di questi progetti vengano chiaramente disciplinate e, dall'altro lato, anche che esperti riconosciuti accompagnino il progetto sotto il profilo della sicurezza;

- elaborazione o definizione di requisiti di sicurezza standardizzati secondo lo stato della dottrina e della tecnica (art. 88 cpv. 1 e 2). Questa misura è necessaria per un'esecuzione possibilmente unitaria. Essa può tuttavia comportare anche risparmi (cfr. sopra).

Il Consiglio federale disciplinerà l'organizzazione del servizio specializzato a livello di ordinanza (art. 86 cpv. 3). Al riguardo deciderà anche quali organi esistenti verranno riuniti nonché come e con quali mezzi il servizio specializzato adempirà i suoi compiti.

3.2 Ripercussioni sui Cantoni e i Comuni

I Cantoni sono interessati solo nella misura in cui, su mandato diretto e sotto la vigilanza della Confederazione, esercitano attività sensibili sotto il profilo della sicurezza (cfr. art. 2 cpv. 2 lett. f nonché art. 89). In simili casi devono adottare le misure di sicurezza necessarie richieste dalla legge e sono inoltre tenuti a designare un servizio che funga da interlocutore per le autorità federali competenti. Il Consiglio federale disciplinerà a livello di ordinanza lo svolgimento dei controlli di sicurezza relativi alle persone nel caso degli impiegati cantonali nonché il controllo dell'attuazione delle misure da parte dei Cantoni. Al riguardo terrà conto dell'autonomia cantonale.

Le ripercussioni sui Cantoni saranno dunque esigue.

3.3 Ripercussioni sull'economia

I terzi sono interessati dalla legge solo indirettamente, vale a dire se sono destinati a gestire informazioni o mezzi TIC della Confederazione nel quadro di un contratto. In seguito all'introduzione di una procedura unitaria di sicurezza relativa alle aziende, le aziende che si candidano per mandati civili della Confederazione che comportano attività sensibili sotto il profilo della sicurezza saranno soggette a tale procedura. L'assoggettamento è connesso a un onere amministrativo supplementare minimo, tuttavia la concorrenzialità delle imprese svizzere viene 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 di sicurezza relativa alle aziende (cfr. art. 56-80).

Inoltre l'economia beneficerà di una migliore protezione dei segreti d'affari o di fabbricazione affidati alle autorità federali.

3.4 Ripercussioni sulla società

La società è interessata sotto due aspetti. In primo luogo è rafforzata la sua fiducia nel trattamento sicuro di informazioni da parte delle autorità federali. Essa ha la certezza che la Confederazione considera importanti le informazioni che riguardano la società (in particolare i dati personali nonché i segreti d'affari e di fabbricazione) e le protegge di conseguenza. In secondo luogo, sono resi noti i principi della classificazione di informazioni. Ciò è particolarmente importante in relazione al principio della trasparenza, la cui efficacia non può essere assolutamente pregiudicata dalla legge.

3.5 Rapporto con le strategie nazionali del Consiglio federale

3.5.1 Strategia per una società dell'informazione in Svizzera

Il presente avamprogetto è menzionato nel Catalogo dei progetti società dell'informazione 2011-2015 (stato: giugno 2013) sotto l'ambito d'intervento «Sicurezza e fiducia». La legge creerà una chiara base per la concretizzazione dei requisiti in materia di sicurezza nei progetti gestiti dalla Confederazione. Riguardo alla strategia: cfr. numero 1.2.1.1.

3.5.2 Strategia nazionale per la protezione della Svizzera contro i rischi informatici

Per quanto riguarda la Strategia nazionale per la protezione della Svizzera contro i rischi informatici: cfr. il numero 1.1.2.2; per quanto riguarda il rapporto tra tale strategia e l'avamprogetto: cfr. il numero 1.2.6; per il sostegno degli esercenti di infrastrutture critiche nel settore della sicurezza delle informazioni, cfr. gli articoli 81-83.

3.5.3 Strategia nazionale per la protezione delle infrastrutture critiche (strategia PIC)

La strategia PIC del 27 giugno 2012 (FF 2012 6875) si prefigge di rafforzare la resilienza (capacità di resistenza) della Svizzera in relazione alle 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 in vista di interruzioni gravi. In questo senso vengono elaborate pianificazioni volte a limitare i

danni e a sostenere in modo sussidiario i gestori di infrastrutture critiche in caso di interruzioni gravi. Il Consiglio federale intende sostenere i gestori di infrastrutture critiche nei loro sforzi di protezione. Al riguardo si deve raggiungere la maggior resilienza possibile dal profilo della sicurezza delle informazioni.

Diverse misure della strategia PIC si focalizzano direttamente su esigenze riguardanti una migliore sicurezza delle informazioni. La misura 7, ad esempio, prevede di creare una base legale che permetta di sottoporre determinate categorie di personale dei gestori di infrastrutture critiche a controlli di sicurezza. L'esecuzione di controlli di sicurezza deve essere in linea di massima prevista ai sensi della strategia nazionale per la protezione della Svizzera contro i rischi informatici (cfr. n. 1.1.2.2 nonché art. 3 cpv. 3). L'avamprogetto crea pure nella LAEI (cfr. art. 26a LAEI) una base legale per l'esecuzione di verifiche dell'affidabilità di determinati impiegati di Swissgrid. La LSIn sostiene quindi anche l'attuazione della strategia PIC.

4 Aspetti giuridici

4.1 Costituzionalità

Secondo l'articolo 42 Cost. per le sue regolamentazioni il legislatore federale necessita di una base costituzionale (esplicita o implicita). Per la prevista legislazione nell'ambito della sicurezza delle informazioni esistono sufficienti basi costituzionali. Sotto il profilo formale, nel caso della normativa da emanare 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 inerente alla ripartizione delle competenze tra Confederazione e Cantoni della Cost., 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 (cfr. l'ingresso della LParl). Inoltre, nella legislazione vigente in materia di organizzazione si rinvia anche all'articolo 173 capoverso 2 Cost. che attribuisce all'Assemblea federale tutte le questioni che rientrano nella competenza della Confederazione e non sono attribuite ad altre autorità (cfr. l'ingresso (con la nota a piè di pagina 1) della LOGA, l'ingresso della LTras nonché della LSIC).

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 […] (cfr. l'ingresso della LMSI)».

Non rientrano tra gli obiettivi menzionati in precedenza le disposizioni sul controllo di sicurezza relativo alle aziende, sempre che sia previsto 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.

4.2 Compatibilità con gli impegni internazionali della Svizzera

La Svizzera ha firmato con diversi Stati e organizzazioni internazionali accordi sulla protezione delle informazioni o accordi in materia di sicurezza (cosiddetti *Security Agreements o Security Arrangements*; cfr. RS 0.514). Con questi accordi internazionali, la Svizzera si è impegnata a rispettare determinati standard in materia di protezione di informazioni classificate. Oltre che con l'UE, la Svizzera ha concluso, nel 1997, anche un accordo in materia di protezione delle informazioni con la NATO nel quadro del «Partenariato per la pace» nonché, nel 2004, con l'Agenzia spaziale europea (ESA). Da un lato, questi accordi contengono disposizioni materiali quali ad esempio i meccanismi di protezione unitari in occasione del trattamento di informazioni classificate o il riconoscimento reciproco di certificati di sicurezza. Dall'altro, contengono anche norme organizzative e strutturali. Menzionano ad esempio di volta in volta l'organo competente per la concretizzazione delle misure di sicurezza (la cosiddetta *National Security Authority NSA* o *Designated Security Authority DSA*). In particolare in ambito COMSEC sono richieste autorità nazionali (cosiddette *National Accreditation Authority NAA* o *Security Accreditation Authority SAA*) che definiscono standard unitari nel settore TIC. Il servizio specializzato della Confederazione per la sicurezza (art. 86) assumerà questi compiti e le responsabilità nel contesto internazionale.

4.3 Forma dell’atto

Già nella sua decisione del 12 maggio 2011 relativa all'elaborazione delle basi legali formali in materia di protezione delle informazioni, 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 essenziali 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 spiegare anche effetti su tutte le autorità. Dall'altro lato, si tratta di disposizioni che, in particolare nell'ambito dei controlli di sicurezza, comportano considerevoli ingerenze in ambiti protetti dalla Costituzione.

4.4 Delega di competenze normative

Le autorità assoggettate alla LSIn dovranno emanare prescrizioni d'esecuzione in particolare per disciplinare i compiti, le competenze e le misure organizzative nei rispettivi ambiti di competenza. Non si tratta sostanzialmente di disposti ordinativi surrogatori della legge nel senso dei principi di delega riconosciuti, bensì di prescrizioni d'esecuzione (autonome) vere e proprie i cui principi materiali sono stabiliti nella legge e che non concedono ai privati alcun diritto immediato né impongono loro degli obblighi. La stessa Costituzione attribuisce di principio le competenze per l’emanazione di tali prescrizioni d’esecuzione alle autorità assoggettate alla LSIn. Pertanto nell’avamprogetto di legge esse non vengono indicate in maniera dettagliata. Espresse norme di delega sono tuttavia contenute nella legge laddove:

- è fatto obbligo alle autorità interessate di emanare disposizioni esecutive o disposti ordinativi surrogatori della legge (ad es. art. 5 cpv. 1, art. 19 cpv. 1, art. 22 cpv. 1 ecc.);
- autorizza il Consiglio federale a concludere autonomamente trattati internazionali (art. 90).