Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Segreteria generale del DDPS
Affari giuridici DDPS

16 ottobre 2014

Avamprogetto di legge federale sulla sicurezza delle informazioni (LSIn)

Rapporto sui risultati della procedura di consultazione

Avamprogetto di legge federale sulla sicurezza delle informazioni (LSIn): rapporto sui risultati della procedura di consultazione

Indice

1 Situazione iniziale

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.

In collaborazione con i dipartimenti, con la Cancelleria federale e con altre autorità federali, il DDPS ha elaborato l'avamprogetto di una nuova legge federale sulla sicurezza delle informazioni. Questa legge, il cui obiettivo è riunire in un unico atto normativo gli elementi fondamentali della sicurezza delle informazioni, disciplina in particolare la gestione dei rischi, la classificazione delle informazioni e i principi della sicurezza nell'impiego delle tecnologie dell'informazione e della comunicazione. Il principio di trasparenza dell'amministrazione rimane in vigore senza limitazioni, motivo per cui la LSIn prevede esplicitamente che è fatta salva la legge sulla trasparenza. L'avamprogetto mira inoltre a ridisciplinare i controlli di sicurezza relativi alle persone e a creare una procedura di sicurezza relativa alle aziende unitaria, come pure a regolamentare l'appoggio alle infrastrutture critiche nel quadro della gestione dei rischi in materia di sicurezza delle informazioni. Un ulteriore obiettivo è infine quello di fornire una base legale per la conclusione, da parte del Consiglio federale, di trattati internazionali nel campo della sicurezza delle informazioni.

Vista la crescente interconnessione dei sistemi e considerato l'aumento dello scambio di informazioni per via elettronica, la legge si applicherà non soltanto all'Amministrazione federale e all'esercito, ma anche al Parlamento, ai tribunali della Confederazione, al Ministero pubblico della Confederazione e alla sua autorità di vigilanza nonché alla Banca nazionale. I Cantoni, i privati e le imprese saranno assoggettati alla legge solo nella misura in cui, per incarico della Confederazione, esercitano attività sensibili sotto il profilo della sicurezza.

Il 26 marzo 2014 il Consiglio federale ha incaricato il DDPS di svolgere presso i Cantoni, i partiti politici, le associazioni mantello nazionali dei Comuni, delle Città e delle regioni di montagna, le associazioni mantello nazionali dell'economia e altre cerchie interessate una procedura di consultazione relativa all'avamprogetto di legge sulla sicurezza delle informazioni. La procedura di consultazione si è conclusa il 4 luglio 2014.

2 Partecipanti alla consultazione

Sono state invitate a partecipare alla consultazione 62 organizzazioni:

- tutti i 26 Cantoni e la Conferenza dei Governi cantonali;
- tutti i 13 partiti politici rappresentati nell'Assemblea federale;
- 3 associazioni mantello nazionali dei Comuni, delle Città e delle regioni di montagna;
- 9 associazioni mantello nazionali dell'economia;
- 10 altre organizzazioni interessate.

L'apertura della procedura di consultazione è stata inoltre pubblicata nel Foglio federale dell'8 aprile 2014.

Hanno espresso un parere:

- tutti i 26 Cantoni;
- 4 partiti politici rappresentati nell'Assemblea federale;
- 1 associazione mantello nazionale dei Comuni, delle Città e delle regioni di montagna;
- 4 associazioni mantello nazionali dell'economia;
- 9 altre organizzazioni interessate;
- 11 partecipanti non invitati individualmente.

In totale sono pervenuti 55 pareri.

Qui di seguito sono riportati i nomi dei partecipanti alla consultazione che hanno espresso il proprio parere per scritto. Tra parentesi sono indicate le abbreviazioni utilizzate nel testo.

2.1 Cantoni

Hanno espresso un parere:

- il Cantone di Zurigo (ZH);
- il Cantone di Berna (BE);
- il Cantone di Lucerna (LU);
- il Cantone di Uri (UR);
- il Cantone di Svitto (SZ);
- il Cantone di Obvaldo (OW);
- il Cantone di Nidvaldo (NW);
- il Cantone di Glarona (GL);
- il Cantone di Zugo (ZG);
- il Cantone di Friburgo (FR);
- il Cantone di Soletta (SO);
- il Cantone di Basilea Città (BS);
- il Cantone di Basilea Campagna (BL);
- il Cantone di Sciaffusa (SH);
- il Cantone di Appenzello Interno (AI);
- il Cantone di Appenzello Esterno (AR);
- il Cantone di San Gallo (SG);
- il Cantone dei Grigioni (GR);
- il Cantone di Argovia (AG);
- il Cantone di Turgovia (TG);
- il Cantone Ticino (TI);
- il Cantone di Vaud (VD);
- il Cantone del Vallese (VS);
- il Cantone di Neuchâtel (NE);
- il Cantone di Ginevra (GE);
- il Cantone del Giura (JU).

2.2 Partiti politici rappresentati nell'Assemblea federale

Hanno espresso un parere:

- il Partito popolare democratico (PPD);
- il PLR.I Liberali (PLR);
- l'Unione democratica di centro (UDC);
- il Partito socialista svizzero (PS).

2.3 Associazioni mantello nazionali dei Comuni, delle Città e delle regioni di montagna

L'Unione delle città svizzere (UCS) ha espressamente rinunciato a esprimere un parere per mancanza di capacità disponibili, pur riconoscendo l'indiscussa importanza del progetto legislativo, ma rimanda al parere della Conferenza svizzera sull'informatica.

2.4 Associazioni mantello nazionali dell'economia

Hanno espresso un parere:

- economiesuisse;

- l'Unione svizzera delle arti e mestieri (USAM).

L'Unione svizzera degli imprenditori (USI) ha espressamente rinunciato a esprimere un parere poiché ritiene che il progetto legislativo non riguardi direttamente l'economia come datore di lavoro. A causa delle limitate risorse disponibili, la Società svizzera degli impiegati di commercio (SSIC) ha espressamente rinunciato a esprimere un parere in merito a un progetto che, a suo avviso, non contiene punti concernenti specificamente gli impiegati di commercio.

2.5 Altre organizzazioni interessate

Hanno espresso un parere:

- l'Autorità di vigilanza sul Ministero pubblico della Confederazione (AV-MPC);
- il Ministero pubblico della Confederazione (MPC);
- privatim, gli incaricati svizzeri della protezione dei dati (privatim);
- la Conferenza svizzera sull'informatica (CSI);
- la Banca nazionale svizzera (BNS);
- il Tribunale federale svizzero (TF);
- swico, l'associazione economica per la Svizzera digitale (swico).

Hanno espressamente rinunciato a esprimere un parere:

- il Tribunale federale dei brevetti (TFB);
- il Tribunale amministrativo federale svizzero (TAF).

2.6 Partecipanti non invitati individualmente

Hanno espresso un parere:

- l'Associazione svizzera per la sicurezza dei sistemi d'informazione (Clusis);
- il Centre Patronal, Equipes Patronales (CP);
- il Centre Patronal, Chambre vaudoise des arts et métiers (CVAM);
- la Federazione delle imprese romande (FER);
- insecor GmbH (insecor);
- IT-Riskmanagement GmbH (it-rm);
- Lehmann Beat (LB);
- il Servizio delle attività informative della Confederazione (SIC);
- il Consiglio dei politecnici federali (Consiglio dei PF);
- la Conferenza dei Rettori delle Università Svizzere (crus.ch);
- la Federazione dei medici svizzeri (FMH).

3 Valutazione generale

Le tabelle riportate qui di seguito forniscono una panoramica della valutazione generale dell'avamprogetto di legge da parte dei partecipanti alla consultazione:

Panoramica sommaria dei risultati

Chi	Sì	Sì, ma	No, ma	No	Nessun commento	Totale
Cantoni	7	18	1			*26*
Partiti	1	2		1		*4*
Associazioni mantello dei Comuni, delle Città e delle regioni di montagna					1	*1*
Associazioni mantello dell'economia		1	1		2	*4*
Altre organizzazioni interessate	1	6			2	*9*
Partecipanti non invitati individualmente	2	8	1			*11*
Totale	**11**	**35**	**3**	**1**	**5**	**55**

Legenda

Sì:	approvazione senza riserve
Sì, ma:	approvazione di principio con proposte di modifica
No, ma:	rigetto di principio con proposte di modifica
No:	rigetto totale
Nessun commento:	espressa rinuncia a un parere

Panoramica sommaria dei pareri e dei rispettivi autori

Giudizio complessivo	Numero	Partecipanti
Sì: approvazione senza riserve	**11**	7 Cantoni (SZ, OW, BL, SH, AR, VS, JU) 1 partito politico rappresentato nell'Assemblea federale (PLR) 1 altra organizzazione interessata (TF) 2 partecipanti non invitati individualmente (CP, CVAM)
Sì, ma: approvazione di principio con proposte di modifica	**35**	18 Cantoni (ZH, LU, UR, NW, GL, ZG, FR, SO, BS, AI, SG, GR, AG, TG, TI, VD, NE, GE) 2 partiti politici rappresentati nell'Assemblea federale (PPD, PS) 1 associazione mantello nazionale dell'economia (economiesuisse) 6 altre organizzazioni interessate (AV-MPC, MPC, privatim, CSI, BNS, swico) 8 partecipanti non invitati individualmente (Clusis, FER, insecor, it-rm, SIC, Consiglio dei PF, crus.ch, FMH)
No, ma: rigetto di principio con proposte di modifica	**3**	1 Cantone (BE) 1 associazione mantello nazionale dell'economia (USAM) 1 partecipante non invitato individualmente (LB)
No: rigetto totale	**1**	1 partito politico rappresentato nell'Assemblea federale (UDC)
Nessun commento: espressa rinuncia a un parere	**5**	1 associazione mantello nazionale dei Comuni, delle Città e delle regioni di montagna (UCS) 2 associazioni mantello nazionali dell'economia (USI, SSIC) 2 altre organizzazioni interessate (TFB, TAF)
Totale	**55**	

Contenuti principali dei pareri

- La stragrande maggioranza dei partecipanti alla consultazione accoglie favorevolmente la creazione di una legge sulla sicurezza delle informazioni.
- Molti Cantoni chiedono precisazioni in merito alle modalità di applicazione della legge ai Cantoni stessi e alla collaborazione tra questi ultimi e la Confederazione.
- Alcuni Cantoni auspicano di non dover creare parallelamente organizzazioni proprie, ma di poter usufruire di quelle della Confederazione.
- Alcuni Cantoni chiedono di essere coinvolti nell'elaborazione delle disposizioni esecutive.
- Da più parti vengono criticati il carattere troppo generico e l'insufficiente chiarezza dei termini utilizzati nella legge, che lascerebbero un notevole margine discrezionale alle autorità. Si chiede pertanto di fare in modo che almeno le disposizioni esecutive siano chiare e circoscritte.
- In singoli casi si richiama l'attenzione sulla necessità di chiarire ulteriormente le interfacce tra sicurezza delle informazioni, protezione dei dati e principio di trasparenza dell'amministrazione.

3.1 Cantoni

ZH accoglie favorevolmente l'emanazione di prescrizioni unitarie per la gestione sicura delle informazioni da parte delle autorità federali e di altre organizzazioni. Nel complesso, considera l'avamprogetto riuscito e ben ponderato a livello concettuale, ma ritiene che le sue ripercussioni sui Cantoni siano ancora incerte e vadano chiarite al più tardi al momento dell'attuazione della legge e dell'emanazione delle relative disposizioni esecutive.

BE può approvare l'avamprogetto soltanto a condizione che le autorità cantonali e comunali, nella misura in cui applicano la LSIn (direttamente in qualità di autorità assoggettate o nel quadro della ripresa di prescrizioni della LSIn nel diritto cantonale), possano assegnare incarichi anche ai servizi specializzati centrali della Confederazione previsti da tale legge, in modo da non essere obbligate a crearne di nuovi, e che vengano fissati periodi transitori adeguati.

In linea di principio, LU condivide lo scopo e l'impostazione dell'avamprogetto di legge. È infatti dell'avviso che, con il suo orientamento a una sicurezza integrale delle informazioni, esso tenga adeguatamente conto della trasformazione sociale e tecnica in atto nella gestione delle informazioni. Nel capitolo 3 (Controllo di sicurezza relativo alle persone) constata tuttavia un certo eccesso di regolamentazione che determinerebbe un onere troppo elevato per i Cantoni. LU fa inoltre notare la mancanza di chiarezza per quanto concerne i costi a carico dei Cantoni e ritiene che l'esecuzione debba essere impostata in modo tale da non generare consistenti oneri amministrativi per i Cantoni stessi.

In linea di principio, UR accoglie favorevolmente l'avamprogetto della LSIn e la certezza del diritto che esso intende garantire nell'ambito della sicurezza delle informazioni. Per quanto concerne i costi nel quadro della gestione dei rischi e le necessarie misure di sicurezza e di protezione, ritiene indispensabile procedere con il dovuto senso della misura. A suo avviso è inoltre necessario tenere conto della gestione di dati e sistemi classificati e delle relative conseguenze per i Cantoni mediante indicazioni integrative giuridicamente vincolanti. UR riconosce l'importanza dei controlli di sicurezza relativi alle persone.

SZ è favorevole alla creazione di una base legale formale unitaria per la gestione della sicurezza delle informazioni nell'ambito di competenza della Confederazione e appoggia pertanto la LSIn. SZ presuppone che i Cantoni, nella misura in cui dovessero essere interessati, vengano invitati a esprimere un parere anche nel quadro della procedura di consultazione sulle disposizioni esecutive.

OW accoglie favorevolmente l'orientamento del presente avamprogetto, che mira a disciplinare in maniera completa la sicurezza delle informazioni con un livello di approfondimento adeguato ai singoli ambiti. A suo avviso, considerata la quota piuttosto esigua di compiti fe-

derali sulla totalità dei compiti che i Cantoni sono tenuti ad adempiere, gli oneri supplementari per questi ultimi dovrebbero essere abbastanza contenuti.

Per NW la presente legge sulla sicurezza delle informazioni rappresenta in primo luogo una buona e completa attuazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS, dall'inglese Information Security Management System) conformemente allo Standard ISO 2700x. I Cantoni sono interessati dall'avamprogetto solo nella misura in cui, su mandato diretto e sotto la vigilanza della Confederazione, esercitano attività sensibili sotto il profilo della sicurezza. Secondo NW, potrebbe essere difficile definire criteri unitari che tengano conto delle diverse realtà cantonali. Qualora la LSIn dovesse entrare in vigore nella versione posta in consultazione, le relative ordinanze d'esecuzione potrebbero generare per NW un onere operativo notevole. NW presuppone che i Cantoni vengano invitati a partecipare anche alla procedura di consultazione sulle disposizioni esecutive concernenti la LSIn.

Secondo GL, la legge sulla sicurezza delle informazioni garantisce chiarezza alle autorità federali. A suo avviso, anche per i Cantoni sarebbe utile una sintesi dei compiti più importanti nonché delle principali competenze e responsabilità. GL ritiene inoltre che alcune nozioni debbano essere ulteriormente concretizzate. In particolare, per GL non è chiaro in quale forma specifica i singoli Cantoni saranno interessati da eventuali condizioni e dalla necessità di misure di formazione.

ZG condivide il desiderio della Confederazione di migliorare la sicurezza delle informazioni e di tenere conto in tal modo delle esigenze di una società dell'informazione interconnessa. Accoglie inoltre con favore il ruolo di precursore assunto dalla Confederazione nella legislazione in materia di sicurezza delle informazioni. Per ZG l'obiettivo deve essere il raggiungimento di un livello di sicurezza e di una dottrina specifica il più possibile unitari e, in linea di principio, a suo avviso il presente avamprogetto di legge appare adatto a tale scopo. ZG mette tuttavia in discussione l'utilità della clausola di esenzione proposta (il cosiddetto «*opting out*»), secondo cui ogni autorità esegue autonomamente l'atto normativo nel proprio ambito di competenza ed emana le relative disposizioni a livello di ordinanza, e ritiene che, se si vuole garantire la sicurezza delle informazioni presso tutte le autorità coinvolte, la legge non debba limitarsi a fissare semplici standard minimi. A tale proposito, ZG sottolinea la necessità e l'importanza di definire standard e norme trasversali. Per questo, a suo avviso, sarebbe anche opportuno, in linea di principio, coinvolgere i Cantoni. ZG è tuttavia del parere che nell'avamprogetto di legge e nel rapporto esplicativo non siano state sufficientemente ponderate le ripercussioni sui Cantoni.

FR condivide la volontà del Consiglio federale di uniformare gli standard applicabili in materia di sicurezza delle informazioni a livello federale. Sottolinea tuttavia come lo stesso Consiglio federale debba ancora fissare le norme volte a disciplinare la verifica dell'applicazione delle misure basate sulla LSIn e l'esecuzione di controlli di sicurezza relativi alle persone per gli organi cantonali. FR vorrebbe inoltre avere la possibilità di esprimersi in merito alle disposizioni esecutive che saranno elaborate dal Consiglio federale.

SO accoglie favorevolmente il disciplinamento, da parte della Confederazione, dei principi della sicurezza delle informazioni un un'unica legge. Ritiene infatti che la responsabilità della gestione sicura delle informazioni possa essere assunta soltanto se si dispone di strumenti moderni per la protezione di queste ultime e se si colmano le lacune presenti nel diritto vigente. Per SO è anche importante che, a livello di legge, vengano definite regole chiare per il controllo di sicurezza relativo alle persone, in quanto le misure in quest'ambito comportano una forte ingerenza nei diritti della personalità degli interessati. SO formula inoltre proposte di modifica in merito ad alcuni punti.

In linea di principio, BS accoglie favorevolmente il disciplinamento previsto, pur formulando proposte di modifica o osservazioni integrative in merito ad alcuni aspetti.

BL approva l'avamprogetto di legge. A suo avviso, la necessità di intervenire nel campo della sicurezza delle informazioni è generalmente riconosciuta e le misure legislative previste contribuiscono a migliorare tale sicurezza. Per questo le appoggia. BL ritiene tuttavia che l'assoggettamento alla nuova legge non debba generare costi per i Cantoni, visto che tali costi non sono documentati nel rapporto esplicativo.

SH si dichiara d'accordo con l'avamprogetto.

AI è d'accordo con la nuova legge fatte salve tre condizioni: che la Confederazione garantisca un indennizzo totale ai Cantoni per le spese sostenute, che i Cantoni possano accedere gratuitamente ai servizi specializzati della Confederazione e che abbiano la possibilità di esprimersi in merito alle ordinanze del Consiglio federale.

AR accoglie favorevolmente l'avamprogetto, anche se i Cantoni/singoli uffici cantonali sono a suo avviso interessati soltanto in modo marginale dalle disposizioni della legge federale. Per questo ritiene che, date le circostanze, si possa rinunciare a esprimere un parere dettagliato.

SG limita il proprio parere al capitolo concernente i controlli di sicurezza relativi alle persone, in quanto soltanto queste disposizioni interessano direttamente il Cantone. SG non ha obiezioni di principio nei confronti delle nuove disposizioni.

Di principio, GR accoglie favorevolmente la creazione di una legge federale sulla sicurezza delle informazioni, ma ritiene che non siano ancora sufficientemente chiare le interfacce tra Confederazione e Cantoni. A suo avviso è inoltre necessario accordare ai Cantoni la possibilità di assegnare incarichi ai servizi specializzati centrali della Confederazione che dovranno essere istituiti secondo la LSIn. GR è infine del parere che, tenendo conto del ciclo di vita dei sistemi TIC, per l'attuazione della legge si debbano prevedere adeguati periodi transitori che abbiano almeno una durata compresa tra i cinque e i dieci anni.

In linea di principio, AG accoglie favorevolmente l'emanazione della LSIn, ma chiede che le questioni ancora aperte concernenti il controllo di sicurezza relativo alle persone per gli impiegati cantonali, la procedura di vigilanza da parte della Confederazione e le interfacce tra il diritto in materia di sicurezza delle informazioni e la vigilanza cantonale sulla protezione dei dati vengano chiarite nel quadro della procedura legislativa e spiegate nel pertinente messaggio.

TG ritiene che una buona legge sulla sicurezza delle informazioni possa rivelarsi molto importante dal punto di vista del diritto in materia di protezione dei dati. È tuttavia dell'avviso che, se formulata in modo troppo rigoroso, una simile legge possa anche comportare diversi rischi per i diritti della personalità degli interessati.

TI condivide lo scopo e l'impostazione della revisione legislativa, che, a suo avviso, ha quale scopo principale di consolidare e coordinare quanto già esiste e permetterà di valutare correttamente con il dovuto anticipo le future minacce, legate alla continua diffusione di sistemi TIC, alla delocalizzazione dei dati e alla loro sempre maggiore interconnessione. A suo avviso, pertanto, basi legali di rango legislativo chiare e di alta densità normativa si giustificano in modo particolare in questo settore, in cui vengono in parte operate ingerenze gravi nei diritti fondamentali che tutelano la libertà personale, la personalità e la sfera privata dei cittadini.

VD non ha obiezioni di principio nei confronti dell'avamprogetto considerato, volto a uniformare le basi legali che disciplinano la gestione e l'organizzazione della sicurezza delle informazioni in seno alla Confederazione in un contesto caratterizzato da rischi sempre maggiori e diversificati e tenendo conto delle esigenze legali in materia di protezione dei dati. VD ha preso atto dell'analisi secondo cui le conseguenze per i Cantoni sarebbero esigue poiché questi ultimi sono interessati dalla legge soltanto nella misura in cui, per incarico della Confederazione e sotto la sua vigilanza, esercitano attività sensibili sotto il profilo della sicurezza, ma non può escludere che l'impatto in termini di risorse umane e finanziarie possa essere più consistente del previsto. Per questo ritiene necessario che tale punto venga debitamente analizzato al momento dell'elaborazione delle disposizioni esecutive. VD auspica in particolare che, in questo contesto, i servizi informazioni e di polizia cantonali, attualmente incaricati di svolgere i controlli di sicurezza relativi alle persone e autorizzati ad accedere ai dati necessari a tal fine, mantengano anche in futuro detta competenza nonché i relativi strumenti.

VS accoglie favorevolmente il presente avamprogetto di legge volto a creare basi legali uniformi per la gestione e l'organizzazione della sicurezza delle informazioni in seno alla Confederazione. Comprende anche che il Consiglio federale debba disciplinare, nelle sue disposizioni esecutive, la verifica dell'applicazione delle misure nonché i controlli di sicurezza relativi al personale cantonale e, a tale proposito, auspica che i servizi competenti del Cantone del

Vallese siano coinvolti in questi lavori sin dall'inizio allo scopo di potervi partecipare attivamente.

NE condivide la volontà del Consiglio federale di creare un quadro normativo trasversale per la propria politica di gestione della sicurezza delle informazioni. Secondo NE la legge proposta va nella giusta direzione e risponde sicuramente già alle preoccupazioni del Consiglio federale senza imporre particolari oneri ai Cantoni. Tuttavia, a suo avviso, la sicurezza delle informazioni deve anche essere esaminata congiuntamente ai partner cantonali e comunali, come nel caso di tutti i problemi legati alla sicurezza. NE auspica pertanto l'integrazione in questa nuova legge di un organo di coordinamento tra la Confederazione e i Cantoni al fine di garantire una politica comune per la sicurezza delle nostre infrastrutture di comunicazione e soprattutto per la lotta contro la cyber-criminalità.

In linea generale, GE accoglie favorevolmente l'iniziativa volta a ridurre i rischi nella gestione e nell'organizzazione della sicurezza delle informazioni in seno alla Confederazione. Ritiene che questa legge sia completa e che tenga conto di tutti i parametri necessari. È pertanto favorevole al presente avamprogetto di legge, che a suo avviso non dovrebbe influire in maniera significativa sull'amministrazione cantonale.

JU accoglie con favore il presente avamprogetto di legge, consapevole della necessità di adeguare il quadro legale di fronte agli sviluppi delle tecnologie digitali e dei rischi associati a queste ultime. Ritiene che, nel suo complesso, il testo contenga gli elementi essenziali per una politica di sicurezza in grado di consentire alla Svizzera di limitare considerevolmente i rischi connessi al settore digitale e non ha nulla da segnalare né riguardo alla forma né riguardo alla sostanza. Per JU queste basi legali pongono l'accento sulla gestione dei rischi come strumento per migliorare la sicurezza e vanno chiaramente nella direzione di un incremento globale del livello di sicurezza richiesto su scala nazionale. JU condivide pienamente l'avamprogetto.

3.2 Partiti politici rappresentati nell'Assemblea federale

In linea di principio, il PPD accoglie favorevolmente la creazione di una legge federale sulla sicurezza delle informazioni. È infatti dell'avviso che, nella nostra società interconnessa, la protezione delle informazioni assuma un'importanza sempre maggiore, anche perché l'evoluzione verso una società dell'informazione non porta soltanto opportunità, ma anche rischi. Per tali motivi il PPD si pronuncia a favore di una base legale unitaria per la gestione e l'organizzazione della sicurezza delle informazioni da parte delle autorità assoggettate. Chiede tuttavia che il Consiglio federale, nel proprio messaggio, illustri le interfacce con i sistemi già esistenti nonché tra istituzioni e privati al di fuori dell'Amministrazione federale.

Il PLR condivide il principio di fondo della presente legge, che mira a migliorare la sicurezza del nostro Paese. È a favore del principio generale alla base dell'avamprogetto, che si pone come obiettivo il miglioramento della sicurezza delle informazioni in linea con il crescente utilizzo delle TIC (tecnologie dell'informazione e della comunicazione), da cui le autorità della Confederazione dipendono in misura sempre maggiore, e constata come, di conseguenza, la gestione dei rischi legati all'impiego delle TIC in tutti i settori della Confederazione sia diventata una necessità intrinseca allo sviluppo della società dell'informazione. Il PLR ritiene che la presente legge sia effettivamente necessaria non solo per colmare le lacune tecniche del nostro sistema di protezione delle informazioni, ma anche per ovviare alle carenze di carattere organizzativo. Per questo si pronuncia a favore del raggruppamento delle misure in materia di protezione delle informazioni in un unico atto normativo omogeneo concernente tutte le autorità federali e le organizzazioni ad esse subordinate. Per il PLR è importante che si trovi un equilibrio tra il livello di sicurezza e le spese necessarie per realizzarlo, al fine di evitare un'esplosione dei costi.

Secondo l'UDC, l'avamprogetto deve essere respinto. A suo avviso, infatti, una legge federale sulla sicurezza delle informazioni non genera alcun valore aggiunto determinante, ma provoca piuttosto un aumento della burocrazia e contribuisce soltanto in misura limitata a un'applicazione uniforme delle disposizioni. L'UDC evidenzia inoltre come, nel quadro dell'indipendenza e dell'autonomia organizzativa delle singole autorità federali,

l'avamprogetto lasci a queste ultime un notevole margine di manovra a livello di esecuzione. In quest'ottica ritiene pertanto che sia più vantaggioso mantenere il sistema attuale e apportare eventualmente miglioramenti mirati nel quadro delle strutture esistenti.

Il PS condivide lo scopo e l'impostazione dell'avamprogetto di legge. È infatti del parere che, con il suo orientamento a una sicurezza integrale delle informazioni, il presente avamprogetto di legge federale sulla sicurezza delle informazioni (LSIn) tenga adeguatamente conto della trasformazione sociale e tecnica in atto nella gestione delle informazioni. Il PS considera la nuova LSIn, nel suo complesso, una buona base per un'organizzazione moderna, professionale e globale della protezione delle informazioni e ritiene che il raggiungimento o meno dell'obiettivo finale possa dipendere essenzialmente dalle risorse finanziarie e di personale a disposizione. Per il PS è fondamentale che la LSIn non entri in conflitto con il principio di trasparenza, con la protezione dei dati, con i requisiti per un buon servizio pubblico e con altri principi equivalenti. Il PS si aspetta che, come richiesto dall'articolo 12, le classificazioni rimangano effettivamente limitate «al minimo indispensabile» e che anche i livelli di sicurezza dei mezzi TIC siano applicati in maniera tale da consentire al personale (statale) di continuare a svolgere i propri compiti con semplicità e razionalità. Il PS chiede inoltre di rafforzare la protezione dei dati in diversi punti della legge e di garantire il rispetto dell'obbligo di archiviazione.

3.3 Associazioni mantello nazionali dei Comuni, delle Città e delle regioni di montagna

L'Unione delle città svizzere (UCS) rinuncia espressamente a esprimere un parere, ma rimanda al parere della Conferenza svizzera sull'informatica.

3.4 Associazioni mantello nazionali dell'economia

Economiesuisse accoglie favorevolmente l'obiettivo, perseguito con il presente avamprogetto di legge, di adeguare la gestione delle informazioni da parte delle autorità federali alle esigenze della moderna e interconnessa società dell'informazione. Esprime pertanto un parere nel complesso positivo in merito alla legge proposta, finalizzata alla creazione di una base legale formale unitaria per la protezione delle informazioni e la sicurezza nell'impiego di mezzi TIC. Economiesuisse sottolinea come, per le imprese, sia importante che venga garantita la confidenzialità nell'ambito del trattamento di informazioni sensibili da parte delle autorità federali, ma fa anche notare l'esistenza, nell'avamprogetto, di numerose nozioni indefinite e di portata troppo ampia. Chiede pertanto che, nell'ordinanza ancora da emanare, il margine di discrezionalità venga limitato con definizioni più precise e criteri di valutazione chiari.

L'USAM respinge il presente avamprogetto poiché a suo avviso la legge ha un titolo fuorviante e la qualità del materiale esplicativo è carente. Qualora si procedesse a un netto miglioramento del rapporto esplicativo e a una precisazione della denominazione della legge, approverebbe nella sostanza l'avamprogetto. Al contempo, nel proprio parere l'USAM rimanda, allegandola, a un parere della Chambre vaudoise des arts et métiers (Fédération patronale vaudoise, FPV) che approva espressamente l'avamprogetto di legge.

L'USI e la SSIC hanno rinunciato espressamente a esprimere un parere in quanto, a loro avviso, l'avamprogetto non le concerne.

3.5 Altre organizzazioni interessate

L'AV-MPC prende atto del fatto che l'autorità di vigilanza, indicata all'articolo 2 capoverso 1 lettera d come autorità assoggettata, può emanare disposizioni esecutive proprie secondo l'articolo 87 capoverso 1. Vengono così a cadere alcune delle riserve che l'autorità aveva formulato in occasione della consultazione degli uffici del 2 aprile 2013. L'AV-MPC ritiene tuttavia che, in riferimento alla stessa autorità di vigilanza e al Ministero pubblico della Confederazione, non sia ancora chiaro presso quale autorità possa essere impugnata una decisione del servizio incaricato del controllo e se, per le persone che attualmente non sono sot-

toposte al controllo di sicurezza relativo alle persone ma che dovrebbero esserlo in virtù delle nuove disposizioni, sia necessario effettuare un simile controllo a posteriori.

Per quanto concerne la gestione e la protezione delle informazioni derivanti da procedimenti penali, il MPC ritiene di dover applicare in primo luogo le direttive del Codice di procedura penale (CPP), che disciplina esaustivamente in particolare l'accesso a informazioni ottenute nell'ambito di questo tipo di procedimenti. Le direttive contemplate dalla LSIn vengono prese in considerazione dal MPC già nel quadro dell'attuazione del progetto «Sicurezza integrale». Per il resto, il MPC rimanda al suo parere del 12 aprile 2013 (Classificazione di atti e informazioni derivanti da procedimenti penali, livelli di sicurezza dei mezzi TIC).

In linea di principio, privatim può accogliere favorevolmente la creazione di una legge federale sulla sicurezza delle informazioni sulla base di due riflessioni: la sicurezza delle informazioni assumerebbe finalmente quel ruolo che avrebbe già dovuto ricoprire da tempo sia nelle attività amministrative quotidiane che nella società e lo svolgimento dei controlli di sicurezza relativi alle persone (CSP) verrebbe disciplinato in una base legale formale necessaria a tal fine. Ritiene tuttavia che, dal punto di vista del diritto della protezione dei dati e dell'informazione, l'avamprogetto e il rapporto esplicativo sollevino diverse questioni che occorre necessariamente discutere e chiarire apportando i miglioramenti del caso.

La CSI accoglie favorevolmente qualsiasi miglioramento della sicurezza delle informazioni nonché qualsiasi forma di collaborazione in tale ambito tra i diversi livelli dello Stato federale, ossia Confederazione, Cantoni e Comuni. A causa delle scarse risorse a disposizione dell'Ufficio tecnico della CSI, quest'ultima si limita a esprimere un parere sui temi di rilevanza cantonale. La CSI può approvare l'avamprogetto soltanto a condizione che, nella misura in cui applicano la LSIn, le autorità cantonali e comunali possano assegnare incarichi anche ai servizi specializzati centrali della Confederazione previsti da tale legge, segnatamente ai servizi specializzati per i controlli di sicurezza relativi alle persone (CSP) o al servizio specializzato per la sicurezza aziendale (SA), in modo da non essere obbligate a crearne di nuovi, e che vengano fissati periodi transitori adeguati. In caso contrario, ritiene che i Cantoni debbano essere esclusi dal campo d'applicazione della LSIn. La CSI si aspetta uno stretto coinvolgimento dei Cantoni, nonché delle relative autorità specializzate, nell'elaborazione delle disposizioni esecutive della Confederazione, in particolare nella misura in cui tali disposizioni riguardano anche i Cantoni.

In linea di principio, la BNS accoglie favorevolmente l'impostazione dell'avamprogetto di legge, che mira alla protezione degli interessi nazionali e, in particolare, degli interessi in materia di politica economica, finanziaria e monetaria della Svizzera. Ritiene inoltre che, con questo avamprogetto, venga raccolta la sfida di creare una base comune per la sicurezza delle informazioni sia per le autorità che per le organizzazioni. La BNS considera tuttavia impegnativo l'assoggettamento delle autorità di cui all'articolo 2 capoverso 1 dell'avamprogetto di legge, in quanto, nell'ambito della loro attività, tali autorità non sono in linea di principio direttamente sottoposte a un'altra autorità con la facoltà di impartire istruzioni. Per questo, a suo avviso, l'avamprogetto non rispetta pienamente il principio secondo cui l'autonomia costituzionale delle autorità indicate non va intaccata. Per la BNS è importante che le disposizioni dell'avamprogetto di legge siano compatibili con l'indipendenza della Banca nazionale garantita dalla Costituzione federale (art. 99 cpv. 2 Cost.).

Il TF fa notare che alcuni articoli rivestono un'importanza fondamentale per il TF stesso e ritiene che non debbano essere modificati a suo discapito. Per il resto, il TF rinuncia a esprimere un parere.

Dopo aver esaminato i documenti, il TFB rinuncia a esprimere un parere.

Il TAF rinuncia espressamente a esprimere un parere, sottolineando come tale atteggiamento debba essere considerato un'astensione e non un'approvazione dell'avamprogetto.

Swico accoglie favorevolmente l'adeguamento, previsto nel presente avamprogetto di legge, delle basi legali alla moderna e interconnessa società dell'informazione. Ritiene tuttavia che, per quanto concerne la terminologia utilizzata, l'avamprogetto di legge contenga nozioni perlopiù indefinite e dalla portata troppo ampia, il che determina a suo avviso anche un eccessi-

vo margine di discrezionalità. Per questo swico chiede disposizioni concrete e definizioni chiare nella relativa ordinanza d'esecuzione.

3.6 Partecipanti non invitati individualmente

Clusis si esprime su alcuni articoli specifici senza fornire esplicitamente un giudizio complessivo sull'avamprogetto.

Il CP e la CVAM ritengono di poter approvare l'avamprogetto di legge federale sulla sicurezza delle informazioni (LSIn). A loro avviso, questa legge organizzativa permetterà tutt'al più alla Confederazione di creare basi legali chiare e omogenee in materia, anche se, a livello pratico, dovrebbe aumentare solo di poco il livello di sicurezza. Il CP e la CVAM sono inoltre del parere che la procedura relativa alle aziende sia in grado di migliorare la competitività di queste ultime in un settore sensibile.

La FER formula osservazioni soltanto su quattro articoli e una sezione, senza fornire esplicitamente un giudizio complessivo sull'avamprogetto.

Insecor accoglie molto favorevolmente la regolamentazione unitaria della sicurezza delle informazioni e il relativo disciplinamento a livello di legge. A suo avviso, la nuova LSIn colma una lacuna urgente nel panorama legislativo in materia di sicurezza delle informazioni e delle tecnologie dell'informazione e della comunicazione, il che non solo si rivelerà particolarmente importante per l'Amministrazione federale o per le autorità cantonali, ma potrà fornire anche preziosi punti di riferimento all'economia privata. In linea di principio, insecor approva l'avamprogetto di legge, formulando tuttavia riflessioni e suggerimenti al riguardo.

It-rm accoglie molto favorevolmente il fatto che venga presentato al Parlamento un disegno di legge che disciplina la protezione delle informazioni in seno all'Amministrazione federale e alle autorità ad essa vicine. A suo avviso, tuttavia, l'avamprogetto di legge attribuisce un'eccessiva importanza alla confidenzialità delle informazioni (ad es. per quanto concerne la classificazione di cui all'art. 14), relegando a un ruolo subalterno la protezione di informazioni di altro genere, ossia non confidenziali. It-rm ritiene che, per garantire il funzionamento di una società e di un'amministrazione moderne e dotate di mezzi TIC, come pure per tutelare gli interessi di politica economica e finanziaria di uno Stato, sia indispensabile garantire una particolare protezione non solo delle informazioni confidenziali, ma anche di quelle informazioni su cui tutti i cittadini e tutti i funzionari dovrebbero poter fare affidamento, ad esempio quelle provenienti da un registro o da un archivio.

LB ha l'impressione che l'approccio globale previsto dalla LSIn per garantire la sicurezza delle informazioni nell'ambito di tutte le applicazioni in seno alle autorità assoggettate della Confederazione e dei Cantoni nonché in seno alle organizzazioni private incaricate di svolgere compiti dell'Amministrazione non sia conforme allo scopo della stessa LSIn. A suo avviso, si dovrebbe mirare a limitare la LSIn alle applicazioni decisive per la tutela degli interessi del nostro Paese, della sua società e della sua economia, trovando un'adeguata soluzione al riguardo. Da questo punto di vista, con i suoi 94 articoli distribuiti su 31 pagine, la LSIn appare a LB un mostro legislativo che, per quanto è dato sapere, non ha eguali in nessuna legislazione estera, contiene un cospicuo numero di nozioni giuridiche indefinite e lascia aperte molte questioni, dando così luogo a un'attuazione particolarmente onerosa in settori che non dovrebbero essere decisivi per l'interesse generale del Paese. Secondo LB occorrerebbe pertanto mirare a incentrare il campo d'applicazione della LSIn sulle minacce esistenziali che interessano i settori chiave di cui all'articolo 1 capoverso 2 LSIn per la gestione di informazioni vitali e dei mezzi TIC impiegati in quest'ambito, al fine di ottimizzare il rapporto tra costi e benefici in materia di sicurezza delle informazioni. LB è inoltre del parere che si debba riflettere sulla possibilità di eliminare dalla LSIn un consistente numero di prescrizioni dettagliate, tra le quali figurano molte ovvietà in materia di sicurezza delle informazioni, in quanto si tratta a suo avviso di prescrizioni che dovrebbero in realtà essere contemplate a livello di ordinanza oppure di raccomandazioni, istruzioni o liste di controllo.

Il SIC fa riferimento ad alcuni articoli di cui, a suo avviso, sarebbe necessario adeguare il contenuto. Per il resto, non si esprime sull'avamprogetto.

In linea di principio, il Consiglio dei PF accoglie favorevolmente il presente avamprogetto e in particolare l'unificazione delle direttive per l'intero ambito federale. Sottolinea tuttavia la particolare posizione assunta dalla ricerca, anche all'interno dell'ambito federale stesso, per via della sua dipendenza da uno scambio il più possibile aperto e da una cooperazione impeccabile a livello nazionale e internazionale. Per il Consiglio dei PF sarebbe pertanto opportuno trattare nel modo più ampio possibile questi aspetti nell'ordinanza concernente la LSIn, prevedendo eventualmente specifiche deroghe per il settore della ricerca. In caso contrario, il Consiglio dei PF ritiene che potrebbe essere a rischio la piazza scientifica svizzera nella sua forma attuale. In sintesi, secondo il Consiglio dei PF l'avamprogetto di legge appare ancora troppo poco coerente e non sufficientemente ponderato, oltre a presentare numerose incertezze a livello giuridico e a lasciare un eccessivo margine d'interpretazione.

La CRUS (crus.ch) è consapevole dell'importanza della sicurezza delle informazioni. L'avamprogetto di legge sulla sicurezza delle informazioni si applica tuttavia esclusivamente alle autorità esplicitamente menzionate all'articolo 2, mentre le università dovrebbero essere interessate soltanto nella misura in cui ricevono mandati da una di queste autorità. Le misure relative alla sicurezza delle informazioni derivanti da tali mandati dipenderanno quindi dalle disposizioni delle autorità che li conferiscono. Per la CRUS è importante che le autorità in questione provvedano a coprire i costi generati dall'applicazione di queste disposizioni da parte delle università. Ritiene inoltre opportuno fare in modo che le suddette misure non impediscano la pubblicazione di risultati scientifici ottenuti nel quadro di mandati di ricerca.

La FMH accoglie favorevolmente l'impostazione dell'avamprogetto di legge, che mira a creare basi legali unitarie per tutte le autorità federali nel campo della «sicurezza delle informazioni» intesa come «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». Dal suo punto di vista è tuttavia importante, nell'ambito dell'ampia accezione della sicurezza delle informazioni descritta nel rapporto esplicativo, proteggere in particolare i dati personali.

4 Pareri in merito alla parte generale del rapporto esplicativo

Qui di seguito vengono riportati i pareri concernenti i singoli temi della parte generale del rapporto esplicativo. Sono indicati soltanto i temi della parte generale in merito ai quali è stato esplicitamente o implicitamente espresso un parere.

4.1 Rischi della società dell'informazione

Il PS condivide l'analisi delle opportunità e dei rischi della società dell'informazione contenuta nella parte generale del rapporto esplicativo, in particolare il messaggio secondo cui la lotta contro i rischi non deve comportare una riduzione delle opportunità offerte dalla società dell'informazione. Per il PS non sarebbe accettabile un ingresso della Svizzera nella corsa agli armamenti digitali in atto tra alcune grandi potenze. È infatti del parere che occorra piuttosto adottare misure volte a creare fiducia attraverso la massima trasparenza possibile e la cooperazione internazionale. Il PS condivide pertanto quanto affermato nel rapporto esplicativo concernente la LSIn, ovvero che i rischi non sono da ricercare soltanto in ambito cyber, ma dovrebbero essere oggetto di un'analisi più ampia. Nel contempo, tuttavia, il PS ritiene che finora il Consiglio federale abbia svolto un buon lavoro nel quadro dell'analisi e della formulazione di una «Strategia nazionale per una società dell'informazione in Svizzera 2011–2015», di una «Strategia nazionale per la protezione della Svizzera contro i cyberrischi» (SNPC) e di una «Strategia nazionale per la protezione delle infrastrutture critiche» (Strategia PIC), sebbene a suo avviso sussistano notevoli lacune nell'attuazione di tali strategie.

4.2 Organizzazione attuale della sicurezza della sicurezza delle informazioni nell'Amministrazione federale

SO fa notare che al numero 1.3.1.2 del rapporto esplicativo (pag. 29), viene descritta l'organizzazione della protezione dei dati senza spiegare le competenze degli incaricati can-

tonali della protezione dei dati. A tale proposito, SO sottolinea come questi ultimi siano responsabili della vigilanza in materia di protezione dei dati sulle autorità cantonali, anche nei casi in cui dette autorità eseguono compiti federali. A suo avviso sarebbe pertanto necessario chiarire che non sono previsti cambiamenti per quanto concerne la responsabilità della vigilanza in materia di protezione dei dati e che le autorità cantonali che esercitano attività sensibili sotto il profilo della sicurezza per incarico della Confederazione rimangono sottoposte alla vigilanza degli incaricati cantonali della protezione dei dati.

Al numero 1.3.1.2 del rapporto esplicativo, privatim chiede di chiarire che la vigilanza in materia di protezione dei dati sulle autorità cantonali che esercitano attività sensibili sotto il profilo della sicurezza per incarico della Confederazione rimane di competenza degli incaricati cantonali della protezione dei dati e che, nel quadro dell'esecuzione di compiti federali, gli organi pubblici cantonali non diventano organi federali e rimangono pertanto assoggettati alla legge cantonale sulla protezione (delle informazioni e) dei dati nonché alla vigilanza cantonale in materia di protezione dei dati.

5 Pareri sull'avamprogetto di legge e sul commento ai singoli articoli nel rapporto esplicativo

Qui di seguito vengono riportati i pareri concernenti specificatamente singoli articoli dell'avamprogetto di legge o il relativo commento nel rapporto esplicativo. Sono indicati soltanto gli articoli in merito ai quali è stato esplicitamente o implicitamente espresso un parere.

5.1 Legge federale sulla sicurezza delle informazioni

In generale

NW fa notare che nella legge federale è fondamentale la nozione di sicurezza delle informazioni, cosa che ancora non avviene nella legislazione cantonale. A suo avviso potrebbe quindi essere difficile definire criteri unitari che tengano conto delle diverse realtà cantonali. A titolo di esempio, NW cita, da un lato, la definizione di «attività sensibili sotto il profilo della sicurezza» di cui all'articolo 2 capoverso 3 LSIn e, dall'altro, la classificazione dei dati e delle informazioni (ad es. «segreto», «confidenziale» o «ad uso interno»).

SO osserva che né l'avamprogetto della LSIn né il rapporto esplicativo trattano la questione del ciclo di vita dei documenti e delle informazioni. A suo avviso sarebbe tuttavia importante disciplinare le modalità di applicazione delle singole disposizioni della LSIn alla creazione, all'utilizzo, alla memorizzazione, all'archiviazione e allo smaltimento di documenti e informazioni.

L'USAM fa notare la scarsa qualità del materiale esplicativo. Ritiene che frasi come «Le informazioni sono il mezzo di scambio della società dell'informazione» (pag. 3) o «Da alcuni decenni, il mondo sta vivendo un profondo mutamento sociale» (pag. 9) siano soltanto parole vuote che non spiegano nulla. È del parere che tali frasi, inserite nel materiale esplicativo in modo sconnesso e senza una previa ponderazione, rimarrebbero comunque oggettivamente false anche se fossero considerate affermazioni fondamentali. Secondo l'USAM, inoltre, le carenze a livello qualitativo si notano anche nei modelli concettuali utilizzati. A tale proposito, cita come esempio particolarmente calzante l'affermazione semplicistica riportata a pagina 80: «In primo luogo è rafforzata la sua fiducia [fiducia della società] nel trattamento sicuro di informazioni da parte delle autorità federali», sottolineando il sorprendente causalismo spicciolo contenuto nella frase in questione. Per l'USAM è anche palesemente inverosimile che questa affermazione sia stata sottoposta a una verifica empirica, tanto che, a suo avviso, risulta inspiegabile come una frase del genere possa essere stata formulata e addirittura pubblicata.

Secondo swico, il presente avamprogetto di legge contiene diverse nozioni e disposizioni indefinite che si prestano a interpretazioni troppo ampie (ad es. attività sensibili sotto il profilo della sicurezza, settori sensibili sotto il profilo della sicurezza ecc.). Swico chiede di introdurre nella relativa ordinanza, che deve ancora essere emanata, una chiara limitazione del

margine di discrezionalità nonché definizioni e criteri chiari per prevenire il rischio di disparità di trattamento e di distorsioni della concorrenza.

Insecor osserva che alcuni contenuti fondamentali, tra cui ad esempio una serie di nozioni, sono contemplati soltanto nel rapporto esplicativo e non nell'avamprogetto di legge. Ritiene pertanto necessario verificare in maniera approfondita quali contenuti del rapporto esplicativo dovrebbero essere ripresi nel testo di legge, per garantirne una migliore comprensione, e quali invece no.

Titolo

L'USAM fa notare che il titolo della legge crea confusione. A suo avviso, dall'articolo relativo allo scopo e dal rapporto esplicativo si evince chiaramente che la LSIn è destinata alle autorità e a organizzazioni analoghe e che, in particolare, tale legge non costituisce una normativa sull'informazione e sulla sicurezza delle informazioni rivolta all'intera società. Questo aspetto dovrebbe essere chiarito anche nel titolo, ad esempio integrandolo come segue: «Legge federale sulla sicurezza delle informazioni in seno alle autorità federali e a organizzazioni analoghe».

Capitolo 1: Disposizioni generali

In generale

Per favorire una comprensione uniforme, BS propone di definire, nella parte introduttiva dell'atto normativo, la nozione di sicurezza delle informazioni e i suoi tre ambiti, ossia la protezione delle informazioni, la protezione dei dati e la sicurezza informatica.

Secondo privatim, né la LSIn né il rapporto esplicativo trattano la questione del ciclo di vita dei documenti e delle informazioni da proteggere. Quali sono le modalità di applicazione delle classificazioni alle varie fasi del ciclo di vita dei documenti e delle informazioni, dalla creazione all'utilizzo fino alla memorizzazione e allo smaltimento? Per privatim è assolutamente necessario tornare su questo argomento e, anche senza disciplinarlo nella legge stessa, trattarlo almeno nel messaggio.

Insecor suggerisce di intitolare come segue gli articoli iniziali della LSIn (per la motivazione si vedano anche le osservazioni esposte più avanti in merito agli art. 2 e 3 LSIn) e di definire già nella presente legge le nozioni principali relative alla sicurezza delle informazioni e alla classificazione: articolo 1 Scopo (o «Oggetto»), articolo 2 Campo d'applicazione, articolo 3 Definizioni. Secondo insecor, infatti, la mancanza di definizioni legali nell'ambito della sicurezza delle informazioni genera spesso notevoli incertezze e conseguenti discussioni. A suo avviso, in caso di basi legali concernenti temi piuttosto complessi è particolarmente importante garantire la necessaria chiarezza già a livello di legge federale.

Il Consiglio dei PF deplora la completa cancellazione del precedente articolo 5 LSIn, che era contemplato nella versione del 2013 della legge e conteneva le definizioni. Ritiene infatti che, in seguito all'eliminazione delle definizioni delle nozioni rilevanti all'interno della LSIn, non sia più possibile comprendere con assoluta chiarezza tutto ciò che si debba intendere, ad esempio, per «mezzi TIC». Il Consiglio dei PF propone di riprendere l'elenco delle definizioni delle suddette nozioni nella sede più opportuna, ossia nella LSIn stessa oppure nella relativa ordinanza. Secondo il Consiglio dei PF, l'inserimento nell'ordinanza è preferibile poiché in questo modo sarebbe più semplice integrare e correggere le varie definizioni.

Articolo 1 Scopo

Considerata la prevista clausola di esenzione, ossia il cosiddetto «opting out» (art. 87 cpv. 3 LSIn), secondo cui ogni autorità assoggettata può emanare proprie disposizioni a livello di ordinanza e, pertanto, le misure e i requisiti standard fissati dal Consiglio federale hanno soltanto carattere di raccomandazione, ZH ritiene che vi sia il rischio che le varie nozioni, alcune delle quali particolarmente generiche, possano essere oggetto di interpretazioni difformi e vengano disciplinate in modo diverso dalle varie autorità nelle rispettive disposizioni esecutive. ZH è pertanto dell'avviso che la legge, di per sé molto dettagliata,

debba essere ulteriormente precisata almeno per quanto concerne gli interessi pubblici da tutelare definiti all'articolo 1 capoverso 2 LSIn e i livelli di classificazione previsti.

TI ritiene che l'elenco degli scopi della normativa sia troppo limitativo, nella misura in cui si riferisce espressamente solo alla tutela degli interessi pubblici (in particolare della Confederazione) mentre richiama quelli di privati solo indirettamente. A suo avviso, l'esigenza di tutelare i diritti della personalità e la sfera privata (e quindi i dati personali), come pure i segreti professionali, di fabbricazione e d'affari, che certifica in fin dei conti la fiducia nei confronti dei servizi che trattano questi tipi di informazioni in virtù del diritto speciale, non dovrebbe essere confinata solo implicitamente nel disposto (lett. e). TI ritiene che questi elementi vadano espressamente indicati, anche solo a titolo esemplificativo, adeguando la pertinente lettera della norma e che, parimenti e in questa misura, andrebbe inserito nel periodo introduttivo del capoverso 2 il richiamo anche alla tutela degli interessi privati (e non solo pubblici).

Il PS condivide lo scopo della LSIn, descritto all'articolo 1 capoverso 1, di garantire la gestione sicura di informazioni nonché l'impiego sicuro di tecnologie dell'informazione e della comunicazione. Può inoltre ritenersi d'accordo con la rinuncia a una definizione legale di ciò che si debba intendere per «informazione», in quanto, a suo avviso, va da sé che tale termine include implicitamente anche i dati (elettronici) di ogni genere. Il PS considera comprensibile anche il tentativo, al capoverso 2, di designare gli «interessi pubblici» da tutelare, ma è del parere che le definizioni scelte siano talmente astratte da lasciare un margine d'interpretazione estremamente ampio. Ciò, secondo il PS, comporta il rischio di interpretazioni eccessive, che a suo avviso è reso ancora più elevato dal fatto che l'articolo 1 capoverso 2 lettere a-d viene citato anche più avanti nel testo di legge come base per determinare i livelli di classificazione (art. 14 LSIn) e i livelli di sicurezza dei mezzi TIC (art. 21 LSIn). Il PS valuta positivamente la presenza, nel rapporto esplicativo, di definizioni restrittive degli «interessi pubblici» da tutelare, ma sottolinea come tale restrizione non si evinca dal testo dell'articolo 1 capoverso 2 lettera d LSIn. Suggerisce pertanto di utilizzare, nell'articolo relativo allo scopo, nozioni e formulazioni più precise, ovvero inequivocabili.
Privatim deplora il fatto che il proposto articolo 1 LSIn si riferisca soltanto alla tutela degli interessi propri della Confederazione e comprenda solo indirettamente la tutela degli interessi della popolazione. A suo avviso, la tutela dei diritti della personalità garantiti dalla Costituzione (art. 10 cpv. 2 e art. 13 cpv. 2 Cost.) o di segreti professionali, d'affari e di fabbricazione è inclusa nello scopo della legge soltanto nella misura in cui eventuali lacune a livello di sicurezza delle informazioni possono comportare una perdita di fiducia nei confronti della Confederazione (cfr. rapporto esplicativo, commento all'art. 1 cpv. 2 lett. d LSIn). Secondo privatim, la sicurezza delle informazioni deve servire a tutelare anche gli interessi delle persone direttamente interessate dal trattamento di dati da parte delle autorità. Pertanto, privatim propone di adeguare come segue l'articolo 1 capoverso 2 dell'avamprogetto della LSIn:

> [2] Mira in tal modo a tutelare gli interessi pubblici e privati seguenti:
>
> a) la capacità di decisione e d'azione delle autorità federali;
> b) la sicurezza interna ed esterna della Svizzera;
> c) gli interessi in materia di politica estera della Svizzera;
> d) gli interessi in materia di politica economica, finanziaria e monetaria della Svizzera;
> e) i diritti fondamentali delle persone interessate garantiti dalla Costituzione;
> f) i segreti professionali, d'affari e di fabbricazione;
> g) l'adempimento di ulteriori obblighi legali e contrattuali delle autorità federali per la protezione di informazioni.

Vista l'importanza attribuita dalla Svizzera alla protezione dei dati e al rispetto della sfera privata, FER ritiene opportuno indicare o aggiungere un ulteriore punto al capoverso 2 di questo articolo, ossia: «la classificazione delle informazioni concernenti gli individui e/o i profili della personalità eventualmente allestiti/raccolti nel quadro della protezione degli interessi sopra descritti». Questo per precisare che le informazioni in possesso della Confederazione sono trattate come informazioni classificate nella categoria «protezione molto elevata», sia che si tratti di dati ottenuti tramite raccolta (nel quadro del controllo relativo alle persone) o di

informazioni destinate a qualsiasi altra procedura che abbia come oggetto specifico degli individui o la loro personalità.

Per LB si farebbe chiarezza se la lettera e venisse integrata come segue: «… per la protezione di informazioni e di dati». A suo avviso occorrerebbe inoltre verificare se non sia il caso di includere le infrastrutture critiche, indispensabili per il funzionamento della società, dell'economia e dello Stato, nell'elenco di cui all'articolo 1 capoverso 2 LSIn in quanto importante interesse degno di particolare protezione.

Il Consiglio dei PF chiede di integrare l'articolo 1 capoverso 2 lettera d come segue: «… della Svizzera, delle sue autorità e organizzazioni nonché di terzi interessati». Considerando l'intera LSIn, il Consiglio dei PF è infatti dell'avviso che non si tratti soltanto di interessi nazionali, ma anche e soprattutto di interessi specifici delle autorità e delle organizzazioni interessate, le cui attività comprendono anche i rispettivi segreti professionali, d'affari e di fabbricazione nonché gli interessi degni di protezione di terzi. Ciò consentirebbe in particolare di tutelare, con i livelli di classificazione AD USO INTERNO, CONFIDENZIALE e SEGRETO, anche gli interessi economici del Consiglio dei PF senza pregiudicare la compatibilità con il principio di trasparenza.

Il Consiglio dei PF fa inoltre notare l'utilizzo, all'articolo 1 capoverso 2 lettera e, della nozione di autorità federali. A suo avviso, tale nozione crea confusione poiché non figura in nessun'altra parte del testo, visto che in seguito si parla esclusivamente di autorità assoggettate e di organizzazioni assoggettate. Per il Consiglio dei PF non è pertanto chiaro se per autorità federali si intendano soltanto le autorità assoggettate definite all'articolo 2 oppure anche le organizzazioni assoggettate. Secondo l'Empa sarebbe inoltre scandaloso se soltanto le autorità, ma non le organizzazioni, potessero beneficiare di una simile protezione delle informazioni.

La FMH chiede di menzionare esplicitamente all'articolo 1 capoverso 2 lettera e i dati personali dei cittadini. Ritiene infatti che la protezione dei cittadini debba essere indicata chiaramente nel testo di legge, poiché, in caso di abuso in materia di dati personali, potrebbero essere gravemente violati i diritti della personalità delle persone di cui vengono trattati i dati. Certi dati personali sono ricercati tanto quanto le informazioni tecnologiche dell'industria. Il loro valore finanziario non dovrebbe essere sottovalutato.

Articolo 2 Autorità e organizzazioni assoggettate

Nonostante alcuni dubbi, in linea di principio ZH ritiene di per sé ragionevole il fatto che, secondo l'articolo 2 capoverso 2 lettera f LSIn, le autorità e i servizi cantonali che, per incarico della Confederazione e sotto la sua vigilanza, esercitano attività sensibili sotto il profilo della sicurezza rientrino nel campo d'applicazione della LSIn. A suo avviso, soltanto in questo modo è possibile garantire la sicurezza generale delle informazioni nell'intera sfera di responsabilità della Confederazione. Secondo ZH, infatti, è vero che la normativa rappresenta un'ingerenza nell'autonomia organizzativa dei Cantoni, ma applicare due o più regimi di sicurezza diversi all'interno di un'amministrazione non sarebbe una soluzione praticabile.

ZG chiede di modificare l'articolo 2 capoverso 2 lettera f come segue: «^{2} Si applica alle organizzazioni seguenti (organizzazioni assoggettate): f. alle autorità e ai servizi cantonali che, ~~per incarico della Confederazione e sotto la sua vigilanza~~ in collaborazione con la Confederazione, esercitano attività sensibili sotto il profilo della sicurezza». A suo avviso, infatti, la sicurezza delle informazioni non riguarda i Cantoni soltanto in veste di autorità che eseguono compiti federali, come invece lascia intendere l'avamprogetto. A tale proposito, ZG fa notare che i Cantoni non operano nell'ambito della sicurezza come organi di esecuzione classici «per incarico della Confederazione e sotto la sua vigilanza», ma, nel campo della sicurezza interna, esercitano poteri sovrani. Ricorda inoltre che gli organi federali fanno parte della Rete integrata Svizzera per la sicurezza e, occasionalmente, ricevono addirittura mandati dai Cantoni, i quali però non rientrano nel campo d'applicazione dell'avamprogetto se non agiscono «per incarico della Confederazione». Questo per ZG non ha alcun senso, in quanto anche nell'ambito della sicurezza interna si producono e si scambiano informazioni e dati sensibili e classificati che meritano una particolare protezione.

Secondo BS, né dal testo di legge proposto (art. 2 cpv. 2 lett. f LSIn) né dal rapporto esplicativo si evince con chiarezza quali siano le attività delle autorità cantonali che rientrano nel campo d'applicazione dell'atto normativo. BS suggerisce pertanto di integrare l'articolo 87 LSIn con una disposizione nella quale si stabilisca che il Consiglio federale deve fissare per via di ordinanza le attività di cui all'articolo 2 capoverso 2 lettera f. Inoltre, affinché sia possibile stimare le ripercussioni sul Cantone, una versione attuale dell'elenco di tali attività dovrebbe a suo avviso essere contenuta già nel messaggio, il quale dovrebbe anche chiarire che cosa si debba intendere per «sotto la vigilanza».

Secondo GE sarà opportuno indicare con esattezza le autorità e i servizi cantonali previsti all'articolo 2 capoverso 2 lettera f e precisare in particolare che cosa si intende con «per incarico della Confederazione e sotto la sua vigilanza, esercitano attività sensibili». Queste informazioni consentono di misurare con precisione le eventuali conseguenze tecniche e finanziarie sulle infrastrutture.

Il PS ritiene che il campo d'applicazione della LSIn, contemplato all'articolo 2, sia decisamente ampio. È tuttavia dell'avviso che tale ampiezza sia giustificata da validi motivi, visto che la LSIn riguarda un settore caratterizzato da un livello di interconnessione talmente elevato che una procedura legislativa più settoriale o federalista mostrerebbe ben presto i propri limiti.

In linea di principio, privatim trova ragionevole che, secondo l'articolo 2 capoverso 2 lettera f LSIn, le autorità e i servizi cantonali che, per incarico della Confederazione e sotto la sua vigilanza, esercitano attività sensibili sotto il profilo della sicurezza rientrino nel campo d'applicazione della LSIn. A suo avviso, soltanto in questo modo è possibile garantire la sicurezza generale delle informazioni nell'intera sfera di responsabilità della Confederazione. Secondo privatim, tuttavia, questo comporta la necessità pratica, per i Cantoni, di adeguare alla LSIn le proprie regole in materia di sicurezza delle informazioni, in quanto l'applicazione di due o più regimi di sicurezza diversi all'interno di un'amministrazione non sarebbe una soluzione praticabile. Tutto ciò rende inoltre indispensabile un intervento a livello cantonale (ed eventualmente comunale), poiché la LSIn prevede misure (segnatamente il controllo di sicurezza relativo alle persone e la procedura di sicurezza relativa alle aziende) che, in gran parte, probabilmente non sono ancora disciplinate dai Cantoni (ed eventualmente dai Comuni) oppure lo sono soltanto in misura minima. Per questo i Cantoni dovrebbero poter usufruire delle prestazioni dei servizi specializzati della Confederazione. Nella misura in cui i servizi cantonali sono direttamente assoggettati alla LSIn, le prestazioni (ad es. esecuzione del CSP) dovrebbero essere finanziate dalla Confederazione. Per tale ragione privatim chiede di integrare l'articolo 89 LSIn con una disposizione che contempli la possibilità, per le autorità e i servizi cantonali, di usufruire delle prestazioni dei servizi specializzati della Confederazione previsti dalla LSIn. Se i servizi che usufruiscono di dette prestazioni sono diversi da quelli previsti all'articolo 1 capoverso 2 lettera f LSIn (cioè se il Cantone introduce un CSP per ulteriori collaboratori cantonali), la Confederazione deve riscuotere emolumenti sufficienti a coprire i costi. Qualora questa richiesta non venisse accolta, privatim ritiene che la soluzione contemplata nella legge federale sulla protezione dei dati sia da preferire a quella proposta nell'articolo 2 capoverso 2 lettera f LSIn (responsabilità individuale dei Cantoni nella misura in cui vengono rispettati gli standard minimi previsti, art. 37 cpv. 1 LPD).

La CSI chiede di stralciare la lettera f se la sua richiesta relativa all'articolo 89 non dovesse essere accolta (cfr. più avanti le osservazioni della CSI sull'art. 89).

Insecor suggerisce di intitolare l'articolo «Campo d'applicazione». Ritiene inoltre che definire i servizi federali assoggettati in un unico articolo insieme alle «attività sensibili sotto il profilo della sicurezza» crei più confusione che chiarezza. Raccomanda pertanto di suddividere adeguatamente questi due diversi temi (cfr. le osservazioni sulle «Definizioni»). Per insecor urge definire con maggiore precisione il campo d'applicazione materiale nel rapporto esplicativo (cap. 1.2.2.1) e nel testo di legge, sottolineandovi l'importanza di una considerazione globale dei pericoli (sicurezza integrale). Pur constatando la difficoltà di separare nettamente il tema della «sicurezza IT» da quello della «cyber-sicurezza», insecor è dell'avviso che, laddove opportuno, sia necessario operare tale distinzione.

Secondo it-rm, per motivi di sicurezza non è sufficiente assoggettare alla legge soltanto le autorità cantonali che, per incarico della Confederazione e sotto la sua vigilanza, esercitano attività sensibili sotto il profilo della sicurezza. A suo avviso, alla legge dovrebbero essere assoggettate piuttosto tutte le autorità cantonali che, nell'adempimento della loro funzione, hanno la facoltà di consultare informazioni della Confederazione sensibili sotto il profilo della sicurezza, inviano alla Confederazione questo tipo di informazioni o sono chiamate a trattarle. In caso contrario, i vari servizi cantonali potrebbero adottare misure di sicurezza più o meno efficaci, con conseguenti divergenze nel livello di protezione delle informazioni. It-rm fa inoltre notare che, nonostante la nozione di incarico dia l'impressione di un rapporto di subordinazione, può anche accadere che tra Confederazione e Cantoni vengano trasferite informazioni sensibili necessarie per lo svolgimento di attività che rientrano nella sovranità dei Cantoni. Per it-rm sarebbe altresì necessario precisare che la presente legge si applica anche alle organizzazioni e alle istituzioni che gestiscono infrastrutture critiche (art. 81 segg.). It-rm ritiene infine che l'elenco di cui al capoverso 3 non sia esaustivo e debba pertanto essere integrato con un «segnatamente» o un «tra l'altro».

Per le attività sensibili sotto il profilo della sicurezza, saranno assoggettate alla LSIn anche «organizzazioni di diritto privato». Secondo l'articolo 87 capoverso 4 LSIn, il Consiglio federale stabilisce per via di ordinanza a quali organizzazioni di diritto privato sarà applicabile totalmente o parzialmente la presente legge. LB raccomanda di coinvolgere nell'emanazione di tale ordinanza gli ambienti economici interessati, comprese le associazioni di categoria attive nel settore dell'informatica come ICT Switzerland e i relativi membri nonché le organizzazioni specializzate nella sicurezza delle informazioni quali ISSS, Clusis, swissecurity.org e le organizzazioni che ne fanno parte.

Articolo 3 Rapporto con la legislazione speciale

Nonostante all'articolo 3 capoverso 1 LSIn sia fatta salva l'applicazione della LTras, ZH si chiede se una classificazione a priori in virtù dell'articolo 14 LSIn lascerebbe intatti il margine di discrezionalità e la libertà di decisione di un'autorità competente secondo l'articolo 10 capoverso 1 LTras. Ne dubita. Per questo ritiene auspicabile un coordinamento a livello legislativo.

TI condivide il principio secondo cui le disposizioni della legge federale sul principio di trasparenza dell'amministrazione (LTras) relative all'accesso ai documenti ufficiali trovino applicazione sia alle informazioni non classificate sia a quelle classificate in base alla LSIn (ad uso interno, confidenziale, segreto). A suo avviso, sarà poi il risultato dell'usuale ponderazione degli interessi in base alla LTras (art. 7) a giustificare eventuali limitazioni del diritto di accesso alle informazioni. Quanto al rapporto della LSIn con altre leggi federali, TI fa notare come il capoverso 2 indichi correttamente che la LSIn va considerata come diritto completivo con particolare riferimento alla protezione dei dati personali. Ciò significa che i dati personali nel settore dei compiti delle autorità federali continueranno, giustamente, a essere trattati secondo la LPD e, per quanto riguarda le misure di protezione (organizzative, tecniche, fisiche e in materia di personale), verranno integrate dalle pertinenti e puntuali disposizioni della LSIn. Ciò significa al contempo che dati personali essenziali per la salvaguardia della sicurezza pubblica potranno essere classificati secondo le prescrizioni della LSIn senza che questo intacchi, o quanto meno relativizzi, il carattere generale e trasversale della LPD.

Per il PS è fondamentale che la nuova LSIn non comporti un aumento delle classificazioni rispetto al passato. In caso contrario, a suo avviso il rischio che venga limitato il principio di trasparenza è notevole, in quanto, come dimostra la prassi relativa alla LTras, una volta che i documenti sono stati classificati, è molto più raro che vengano resi accessibili in virtù di tale principio. Nonostante all'articolo 3 capoverso 1 LSIn sia fatta espressamente salva la legge sulla trasparenza (LTras, RS 152.3), il PS ritiene che non vengano realmente chiarite le interazioni tra la LSIn e il principio di trasparenza sancito dalla LTras. Si aspetta pertanto che, a livello contenutistico, le disposizioni concernenti la classificazione non esulino in alcun modo dall'elenco delle eccezioni di cui all'articolo 7 LTras e che, almeno, non siano in contraddizione con il relativo contenuto. A suo avviso occorre garantire che, in futuro, la LSIn non generi un ulteriore aumento delle controversie tra i fruitori della LTras e l'Amministrazione.

Per il PS, il principio di trasparenza è strettamente legato alla nozione degli Open Government Data (OGD), che sono parte integrante della strategia di e-government Svizzera. Il PS fa notare che, in seguito alla ratifica della Convenzione di Aarhus, la Svizzera applica il principio di trasparenza per quanto concerne i dati ambientali. A suo avviso, inoltre, anche il progetto pilota «Single Point of Orientation» dell'Archivio federale svizzero mostra come sia possibile fornire in modo pratico ai cittadini una panoramica dei documenti dell'Amministrazione federale. Il PS si aspetta che la nuova LSIn non ostacoli né i progetti né, in generale, la strategia OGD confermata dal Consiglio federale nel suo rapporto del 13 settembre 2013. Ritiene pertanto che si debba esaminare l'eventuale necessità di formulare nella LSIn un'esplicita riserva in tal senso.

Clusis deplora l'assenza di riferimenti alla legge federale sulla protezione dei dati. Il capoverso 2, che recita: «Se le informazioni devono essere protette in virtù di altre leggi federali, le disposizioni della presente legge si applicano a titolo completivo», dovrebbe essere integrato come segue: «Si applicano inoltre le disposizioni della LPD».

Secondo insecor non è comprensibile per quale motivo al capoverso 2 si faccia riferimento esclusivamente alle «informazioni». A suo avviso sarebbe corretto scrivere: «Se le informazioni e le tecnologie dell'informazione e della comunicazione devono essere protette in virtù di altre leggi federali…».

Per LB, l'importante nozione di «infrastrutture critiche» e il rimando generale alla «legislazione speciale» applicabile devono essere definiti in maniera più concreta e precisa, dato che la legge deve essere applicabile anche alle organizzazioni di diritto privato che gestiscono infrastrutture critiche.

Il disegno di legge federale sule attività informative prevede all'articolo 66 una deroga al principio di trasparenza per i documenti riguardanti l'acquisizione di informazioni secondo tale legge. Il SIC presuppone che questo principio non venga toccato dall'articolo 3 LSIn. Inoltre, non comprende pienamente il motivo per cui, ad esempio, i documenti classificati SEGRETO, la cui conoscenza da parte di persone non autorizzate può pregiudicare gravemente gli interessi pubblici di cui all'articolo 1 capoverso 2 LSIn, debbano rimanere assoggettati al principio di trasparenza.

Capitolo 2: Misure generali per la sicurezza delle informazioni

In generale

LB raccomanda di verificare in tutta la LSIn se un determinato requisito, una determinata prescrizione o un determinato disciplinamento concerne unicamente le «autorità assoggettate» o anche le «organizzazioni assoggettate» (di diritto privato), quando quest'ultime sono assoggettate al campo d'applicazione della LSIn secondo l'articolo 2 capoverso 2 lettera e LSIn.

La FMH mette in discussione la distinzione tra la classificazione delle informazioni e la classificazione dei livelli di sicurezza dei mezzi TIC nonché il loro diverso campo d'applicazione: dopotutto lo scopo della protezione dei sistemi è quello di proteggere le informazioni che contengono.

Articolo 4 Sicurezza delle informazioni

Secondo TG manca il principio della proporzionalità. La disposizione deve quindi essere completata affinché una misura sia ammessa soltanto finché ha raggiunto il suo scopo o è evidente che ciò non potrà avvenire. Tale misura non deve inoltre comportare alcun svantaggio in manifesta sproporzione con il risultato auspicato. Sebbene successivamente (art. 12 dell'avamprogetto della LSIn) venga menzionata la limitazione al minimo indispensabile per quanto riguarda la classificazione delle informazioni, essa deve essere presente in tutte le disposizioni concernenti la sicurezza delle informazioni; tale principio deve quindi essere integrato chiaramente nelle disposizioni generali. TG ritiene che nel quadro della sicurezza delle informazioni occorra inoltre garantire la corretta origine dei documenti, ovvero che sia possibile riconoscere che la fonte è quella indicata. Nell'articolo 4 dell'avamprogetto LSIn

viene tuttavia menzionata unicamente la «tracciabilità»; è quindi necessario includere anche il concetto di «autenticità». In questo modo è possibile garantire anche l'autenticità delle informazioni, ciò che rappresenta un aspetto importante della sicurezza delle informazioni.

Il PS svizzero ritiene che nell'articolo 4 manchi il principio di proporzionalità. Il PS propone quindi la seguente aggiunta: «^{3bis} Assicurano la proporzionalità delle misure di protezione adottate, le quali sono ammesse soltanto finché hanno raggiunto il loro scopo o è evidente che ciò non potrà avvenire. Tali misure non devono inoltre comportare alcun svantaggio in manifesta sproporzione con il risultato auspicato».

FER propone di concentrarsi sulla classificazione delle informazioni e non su una competenza valutata nell'ottica di un eventuale pregiudizio per gli interessi di cui all'articolo 1 capoverso 2. L'obiettivo consiste nel definire una strategia preventiva e non di reagire, o addirittura reagire in modo esagerato, in caso di eventi che richiedono, a posteriori, l'adeguamento delle procedure esistenti.

Insecor constata che nel testo tedesco al capoverso 3 appare all'improvviso l'abbreviazione «mezzi TIC» per il termine «tecnologie dell'informazione e della comunicazione». Poiché tale espressione viene menzionata più volte in articoli precedenti, la relativa abbreviazione dovrebbe apparire già all'inizio dell'avamprogetto di legge, ovvero nell'articolo 1 capoverso 1.

Per it-rm al capoverso 2 deve essere aggiunta una nuova lettera «e. siano attendibili». L'attendibilità presuppone anche la correttezza del contenuto, ovvero l'acquisizione e il trattamento corretto e completo delle informazioni. L'attendibilità delle informazioni è un fattore centrale. Il cittadino deve poter fare affidamento sulla correttezza delle informazioni contenute nei registri (protezione della buona fede). Se le informazioni contenute nei registri dovessero rivelarsi errate ne risulterebbe un gran numero di contestazioni o addirittura procedure litigiose. Per it-rm occorre inoltre aggiungere una nuova lettera «f. siano autentiche o anonime». I dati e le informazioni sono autentiche quando sono riconducibili a una persona o a un apparecchio. In caso contrario risulterebbe un problema di sicurezza poiché non è possibile sapere chi ha avuto accesso alle informazioni e le ha inviate. Per accertare la legittimità di una richiesta online di dati e informazioni confidenziali, in primo luogo è necessaria una conferma dell'attendibilità concreta della responsabilità della richiesta. Ciò richiede il controllo dell'autenticità della richiesta. L'anonimato ha lo scopo opposto dell'autenticità, ovvero l'impossibilità di attribuire le informazioni. Il segreto di voto presuppone la protezione dell'anonimato. Ciò che deve essere protetto nel quadro del segreto di voto è l'impossibilità di attribuire il voto a una persona naturale.

Articolo 5 Massima responsabilità direttiva

Per insecor non è chiaro perché nel capoverso 1 la massima responsabilità direttiva sia attribuita unicamente alle «autorità assoggettate» e non anche alle «organizzazioni assoggettate» (ovvero, ad esempio, all'«Amministrazione federale»). In considerazione delle responsabilità già menzionate nella LOGA (RS 172.010) non è possibile che l'amministrazione federale non consideri la sicurezza come «affare dei capi» (cfr. Rapporto esplicativo, commento all'articolo 5, p. 41). Per quanto concerne il capoverso 4, il personale non dovrebbe unicamente essere «informato» regolarmente e conformemente al rispettivo livello, ma anche «formato e obbligato». Una semplice informazione in merito alla sicurezza delle informazioni non è mai stata efficace.

It-rm ritiene che la verifica delle tecnologie dell'informazione secondo lo stato della dottrina e della tecnica stabilita nel capoverso 1 lettera a non sia applicabile nell'ambito delle tecnologie dell'informazione poiché sarebbe un'operazione interminabile. L'it-rm è dell'avviso che l'organo di coordinamento per l'elaborazione e l'aggiornamento di uno standard minimo debba assumersi la responsabilità della verifica. Le autorità dovrebbero quindi basare la propria verifica su tali direttive. In caso contrario ci sarebbe il pericolo che l'entità della verifica venga definita individualmente dalle autorità, ciò che comprometterebbe l'omogeneità delle misure di sicurezza e della loro applicazione. It-rm propone di includere un rimando all'articolo 88 LSIn e in tale sede completare il trattamento della questione della verifica e autorizzare

l'organo di coordinamento a emanare le prescrizioni riguardanti le misure di verifica da eseguire per il relativo fabbisogno di protezione.

LB propone che l'articolo 5, come già accade per l'articolo 6, oltre alle autorità assoggettate includa anche le organizzazioni assoggettate. Poiché proprio nell'ambito dell'economia privata è auspicabile poter fare riferimento a un principio generale secondo cui la tutela della sicurezza delle informazioni è di competenza dell'organo direttivo supremo.

Sulla base del commento all'articolo 6, per il Consiglio dei PF non è chiaro se l'articolo 5 si applichi effettivamente anche alle unità decentrali della Confederazione. Tanto più che, per quanto riguarda la gestione dei rischi, nel settore dei PF verrebbero applicate disposizioni proprie.

Articolo 6 Gestione dei rischi

TG e PS chiedono di eliminare l'aggettivo «identificati» dall'ultima frase del secondo capoverso. Come indicato nell'avamprogetto, anche TG ritiene che i rischi debbano essere identificati, analizzati, valutati e verificati conformemente alla gestione dei rischi. Il capoverso 2 dell'articolo 6 è tuttavia eccessivamente aggrovigliato nella relativa sistematica terminologica. Non devono essere evitati unicamente i rischi «identificati», ma tutti i rischi. PS è dell'avviso che le autorità e le organizzazioni responsabili debbano, in generale, evitare o ridurre a un livello sostenibile i rischi – sia quelli identificati che quelli non ancora identificati.

Secondo it-rm, l'espressione «livello sostenibile» manca di concretezza e in fase di attuazione lascia ampio spazio a interpretazioni individuali. Tale indeterminatezza in un contesto tecnico suscita incertezze giuridiche. Inoltre, può comportare discordanze nel dispositivo di sicurezza. It-rm propone di integrare il seguente complemento: «L'organo di coordinamento stabilisce standard minimi per i rispettivi livelli di classificazione, i quali definiscono l'entità dei danni ritenuta tollerabile in caso di violazione o elusione della sicurezza delle informazioni».

Articolo 7 Requisiti e misure di sicurezza

TG ritiene che si possa stralciare il capoverso 2 poiché, per quanto riguarda la definizione dei requisiti e delle misure standard, l'articolo 88 dell'avamprogetto della LSIn (Sezione 2: Esecuzione) contiene già un riferimento allo stato della dottrina e della tecnica. Tale disposizione esecutiva nell'ultima parte dell'avamprogetto stabilisce quindi già che anche le misure di sicurezza menzionate nell'articolo 7 devono soddisfare lo stato (riconosciuto) della dottrina e della tecnica.

Secondo insecor è insolito il riferimento a un articolo di legge che si trova solo alla fine della presente legge. Insecor propone di includere già all'inizio della LSIn un'indicazione in merito ai «requisiti e alle misure standard» e in tale sede fare riferimento all'articolo 88.

Poiché secondo il rapporto esplicativo per le autorità e le organizzazioni che non sono subordinate al Consiglio federale non sussiste alcun obbligo di ottemperare agli standard di cui all'articolo 88, il Consiglio dei PF propone di precisare in tal senso l'articolo 7 capoverso 1.

Articolo 8 Collaborazione con terzi

Per privatim manca il principio secondo cui la responsabilità della tutela della sicurezza delle informazioni rimane delle autorità o organizzazioni che per l'adempimento dei loro compiti decidono di collaborare con terzi. Per dare maggiore rilievo a tale principio, l'articolo 8 LSIn deve essere completato con un passaggio concernente la responsabilità dell'autorità o dell'organizzazione committente.

Secondo it-rm, in linea di principio un contratto non giustifica l'accesso da parte di terzi esterni a segreti d'ufficio. Con la clausola inserita in questo articolo è tuttavia reso possibile per legge l'accesso di terzi a dati sensibili dal punto vista penale. Nel rapporto esplicativo occorrerebbe fare un riferimento esplicito a questo aspetto affinché il Parlamento ne sia consapevole. Se le autorità non sono titolari del segreto, ma unicamente depositarie del segreto, sarebbe preoccupante se collaborassero con terzi. Onde individuare per tempo un eventuale conflitto d'interessi, è quindi preferibile informare il titolare del segreto. Ai fini della certezza del diritto e della trasparenza nei confronti dei terzi interessati, it-rm ritiene che deve essere

regolata anche la questione della responsabilità nel caso in cui detti terzi arrechino un danno a una persona privata. Inoltre l'articolo 8 dovrebbe essere completato affinché l'organo di coordinamento emani prescrizioni esecutive in merito alla procedura di scelta di terzi e ai criteri che devono essere soddisfatti in ogni singolo caso.

Per il Consiglio dei PF questo articolo deve chiarire quali tipi di collaborazioni sono contemplati. L'applicazione dell'articolo 8 capoverso 2 al settore dei PF è sproporzionata e comporterebbe costi supplementari. Tale disposizione complicherebbe notevolmente la procedura d'acquisto, in particolare per quanto riguarda lo svolgimento operativo della valutazione delle offerte (tempi più lunghi). Una disposizione di così ampia portata, secondo cui nelle convenzioni e nei contratti con terzi si deve tenere conto dei requisiti e delle misure stabiliti dalla LSIn, non è applicabile nella pratica: l'ampiezza dei requisiti e delle misure della LSIn non consente una visione d'insieme della loro portata ed efficacia; né un'autorità né un'organizzazione sarebbero quindi in grado di includere nei loro contratti le pertinenti clausole in adempimento alle disposizioni dell'articolo 8. L'Empa ritiene inoltre che un intervento così marcato non sia compatibile con l'autonomia di un istituto di diritto pubblico; simili direttive non sono nemmeno conciliabili con i principi della libertà contrattuale e della libertà d'insegnamento e di ricerca. Il Consiglio dei PF propone la seguente nuova formulazione: «Nel quadro di contratti di collaborazione con terzi, le autorità e le organizzazioni assoggettate devono fare sommariamente riferimento alla validità e al rispetto delle disposizioni della Legge federale sulla sicurezza delle informazioni (LSIn)».

Articolo 9 Procedura in caso di violazione della sicurezza delle informazioni

Per TG manca una disposizione secondo cui nel caso dell'individuazione di violazioni devono essere adottate le relative contromisure. Nell'articolo viene unicamente indicato che nel caso di violazioni della sicurezza delle informazioni devono essere minimizzate le ripercussioni. L'articolo deve essere completato in tal senso affinché risulti sensato nel suo insieme.

La FER si domanda il perché dell'assenza di una definizione esplicita delle eventuali conseguenze giudiziarie e/o penali in caso di violazione della sicurezza delle informazioni.

Articolo 10 Pianificazioni preventive

LB propone che l'articolo 10 includa, oltre alle «autorità assoggettate», anche le «organizzazioni assoggettate» poiché proprio nell'ambito dell'economia privata sarebbe auspicabile poter fare riferimento a un principio relativo ai contenuti, in base al quale per tutelare la sicurezza delle informazioni devono essere allestite pianificazioni preventive e svolte le relative esercitazioni.

Articolo 11 Controlli

Per TG è importante che la confidenzialità dell'organo indipendente venga stabilita per legge, in particolare poiché nel corso delle sue verifiche otterrà inevitabilmente l'accesso a documenti molto confidenziali.

VD ritiene che i commenti sono poco precisi per quanto riguarda le modalità e i costi dei controlli nei casi in cui la legge si applica alle le autorità cantonali. Tutto sommato, un organo come il Controllo cantonale delle finanze è legalmente e professionalmente idoneo a svolgere le verifiche indicate al capoverso 2.

Il PS propone la seguente integrazione: «[3] Gli esiti delle verifiche secondo il capoverso 1 e 2 vengono comunicati periodicamente alle Commissioni della gestione delle Camere federali». Ai sensi dell'articolo 11 le autorità assoggettate sono tenute a verificare periodicamente il rispetto delle disposizioni della LSIn. Queste sono informazioni che interessano anche l'alta vigilanza parlamentare.

Articoli 12–18 Classificazione delle informazioni

A causa della mancanza di definizioni legali in questa sezione, insecor si domanda se le disposizioni menzionate riguardino anche il «materiale classificato». Ciò è alquanto insoddisfacente e sono assolutamente necessarie precisazioni.

Articoli 12–14 Classificazioni

Il PPD è favorevole alla creazione di una regolamentazione uniforme per i livelli di classificazione e i motivi di classificazione per tutte le autorità assoggettate.

Il MPC è contrario all'obbligo di classificazione per atti di procedimenti penali. Già a suo tempo nell'OPrI non era stato stabilito l'obbligo di classificazione per tali atti. Il trattamento di questi dati e il loro accesso sono retti esclusivamente dal CPP. L'obbligo di classificazione secondo la LSIn non è solo inutile (vale il segreto istruttorio di diritto processuale penale), ma non è nemmeno applicabile in procedimenti penali onerosi e complessi come quelli del MPC. Una classificazione secondo la LSIn comporterebbe livelli di classificazione diversi per atti dello stesso procedimento penale, i quali di conseguenza dovrebbero essere trattati diversamente. La conseguente separazione di singoli atti non impedirebbe unicamente la gestione degli atti secondo la legislazione e la giurisprudenza, ma sarebbe anche contraria ai principi dell'unità e della completezza degli atti procedurali. Per evitare ciò, tutti gli atti – secondo quanto è stato praticato sinora nel quadro del CCP in vigore, garantendo il segreto istruttorio – devono avere un unico livello di classificazione, ovvero quello delle informazioni più sensibili presenti negli atti. Tutto questo non sarebbe tuttavia nell'ottica del presente avamprogetto, tanto più che secondo il rapporto esplicativo, nell'interesse di un onere esecutivo sostenibile la quantità delle informazioni classificate deve essere limitata al minimo indispensabile e che quindi non a tutto il gruppo di atti deve essere assegnato il medesimo livello di classificazione. Inoltre per il MPC ne risulterebbero problemi irrisolvibili nel quadro degli scambi con le autorità cantonali di perseguimento penale. In linea di principio le autorità cantonali non sono difatti soggette alla LSIn.

Articolo 12 Principi della classificazione

Secondo it-rm occorre specificare che l'organo di coordinamento deve elaborare delle istruzioni su come classificare le informazioni sensibili.

Secondo il SIC a livello delle disposizioni esecutive relative al capoverso 4 occorre elaborare prescrizioni semplificate per il SIC (analogamente alle vigenti regole sulle operazioni semplificate con informazioni classificate nel settore dei servizi di informazione e della polizia del 18 gennaio 2008).

Articolo 13 Competenze

TG ritiene che nel caso di una delega della competenza di classificazione a un altro servizio o persona anche l'autorità assoggettata (nell'articolo unicamente: il servizio incaricato della classificazione e l'organo superiore) debba avere la possibilità di modificare la classificazione.

Il PS ritiene che, a seconda della situazione, anche l'autorità assoggettata debba avere la possibilità di modificare o sopprimere le classificazioni e non solo il servizio incaricato della classificazione e il suo organo superiore.

Per il SIC, a livello delle disposizioni esecutive relative al capoverso 2 occorre elaborare prescrizioni semplificate per il SIC (analogamente alle vigenti regole sulle operazioni semplificate con informazioni classificate nel settore dei servizi di informazione e della polizia del 18 gennaio 2008).

Articolo 14 Livelli di classificazione

UR accoglie favorevolmente la definizione di tre soli livelli classificazione. La gestione di dati e sistemi classificati e le conseguenze che ne risultano per i Cantoni non sono tuttavia esplicitate in dettaglio nell'avamprogetto. Di ciò bisogna tenere conto mediante disposizioni legali complementari.

TG non comprende perché per tutti i livelli di classificazione vi sia un rinvio unicamente alle lettere a–d dell'articolo 1 dell'avamprogetto della LSIn e non anche alla lettera e. Evidentemente in un secondo momento è stata effettuata una modifica dell'articolo 1 dell'avamprogetto, di cui erroneamente non è si è tenuto conto in questo articolo.

Privatim ritiene che, per ragioni di completezza, almeno il messaggio debba fare riferimento al significato di una non classificazione: tali informazioni sono comunque soggette al segreto d'ufficio? Che ne è dell'accesso secondo il principio di trasparenza?

Per Clusis i tre livelli di classificazione «AD USO INTERNO», «CONFIDENZIALE» e «SEGRETO» sono comprensibili. Ma come mai non esiste il livello «PUBBLICO»? È impossibile che non vi siano dei documenti pubblici, tanto più che è fatta salva la legge sulla trasparenza.

It-rm ritiene che lo schema di classificazione proposto sia troppo poco differenziato per poter proteggere lo svolgimento regolare delle procedure delle autorità federali, secondo quanto inteso da questa legge. Oltre alla divulgazione di informazioni confidenziali, vi sono ulteriori perturbazioni nell'ambito del trattamento di informazioni in grado di infliggere gravi danni allo Stato e all'amministrazione. It-rm propone di modificare i livelli di classificazione come segue: «AD USO INTERNO», «DEGNO DI PROTEZIONE O PROTEZIONE ELEVATA» e «DEGNO DI PROTEZIONE STRAORDINARIA O PROTEZIONE MOLTO ELEVATA». Per garantire il funzionamento di una società e di un'amministrazione provviste di mezzi TIC moderni e per salvaguardare gli interessi economici e di politica finanziaria di uno Stato, non basta proteggere in modo particolare le informazioni confidenziali, ma è necessario proteggere anche le informazioni su cui possono fare affidamento tutti i cittadini e funzionari come, ad esempio, le informazioni contenute in registri o archivi.

LB sottolinea che i criteri per determinare il livello di classificazione delle informazioni sono formulati in modo molto generico e offrono un ampio margine di apprezzamento all'organo incaricato della classificazione. Al riguardo, la legge si potrebbe eventualmente completare con il principio secondo cui le informazioni che fanno riferimento a informazioni classificate o ne contengono devono perlomeno avere il medesimo livello di classificazione. Ciò rappresenterebbe un'indicazione utile per il comportamento delle organizzazioni private nella gestione (ricezione, trattamento, scambio ecc.) di informazioni classificate provenienti dalle autorità assoggettate.

Il Consiglio dei PF sottolinea che gli istituti del settore dei PF, così come tutte le organizzazioni, hanno anch'essi dati interni confidenziali protetti da misure organizzative o, nel caso di sistemi, da un'apposita gestione delle autorizzazioni. Negli ambiti fondamentali «ricerca», «insegnamento» e «consulenza», la maggior parte delle informazioni sono in linea di principio pubbliche. Esistono tuttavia un numero esiguo di progetti non pubblicamente accessibili che sono convenuti contrattualmente con i finanziatori.

La FMH non comprende per quale motivo i dati personali dei cittadini vengono esclusi esplicitamente dalla classificazione (articolo 14). Ciò è in contraddizione con il rapporto esplicativo che giustamente afferma: «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». A causa dell'incremento dello scambio elettronico di informazioni, FMH ritiene che anche i dati personali siano sempre più minacciati. In particolare, mediante la raccolta di informazioni su di una persona è ormai sempre più facile identificarla.

La FMH propone di rettificare come segue i capoversi 1–3 dell'articolo 14: «gli interessi di cui all'articolo 1 capoverso 2 lettere a–e». Le informazioni concernenti i cittadini – ad esempio dati riguardanti la salute – dovrebbero anch'essi ottenere la protezione di una classificazione secondo l'articolo 14. Tale classificazione non può limitarsi «alla capacità di decisione e

d'azione delle autorità federali, alla sicurezza interna ed esterna della Svizzera, agli interessi in materia di politica estera della Svizzera e agli interessi in materia di politica economica, finanziaria e monetaria della Svizzera».

Articolo 15 Accesso a informazioni classificate

La FMH ritiene che nel quadro dell'esecuzione dell'articolo 15 occorra assicurarsi che venga effettivamente dimostrata l'impossibilità di adempiere al compito legale senza le corrispondenti informazioni.

Articolo 17 Comunicazione di informazioni classificate in procedure particolari

Ai sensi di una procedura giudiziaria equa, TG propone di rinunciare al capoverso 2 dell'articolo 17 dell'avamprogetto della LSIn poiché potrebbe dare l'impressione che i tribunali abbiano la facoltà di basarsi su prove segrete, ciò che non può assolutamente accadere. Nell'articolo 17 dell'avamprogetto della LSIn viene menzionato che la comunicazione di informazioni ai tribunali e ai ministeri pubblici si fonda sul rispettivo diritto procedurale applicabile. In questo modo si vuole assicurare che l'accertamento della verità nel quadro della procedura giudiziaria non venga reso più difficoltoso dalla classificazione. All'articolo 2 del presente articolo si aggiunge tuttavia che il tribunale competente può consultare il servizio incaricato della classificazione. Ciò lascia supporre che la classificazione potrebbe limitare le procedure giudiziarie. Affinché tuttavia i tribunali possano continuare ad adempiere i propri compiti, nelle procedure giudiziarie non vi deve essere alcuna classificazione. La classificazione concerne dati segreti. È assolutamente necessario evitare qualsiasi tipo di *tribunale segreto* poiché si spalancherebbero le porte all'arbitrio dello Stato.

Il TF sottolinea che questo articolo è fondamentale per il TF e che non va modificato a suo sfavore.

Articolo 18 Misure di protezione provvisorie

Il Consiglio dei PF propone di stralciare le organizzazioni assoggettate dall'articolo 18 o di escludere esplicitamente le unità decentrali dell'Amministrazione federale e il settore dei PF poiché secondo l'articolo 13 unicamente le autorità assoggettate designano un servizio competente per la classificazione.

Articolo 19 – 27 Sicurezza in occasione dell'impiego di mezzi TIC

La «procedura di sicurezza» menzionata nell'articolo 19 LSIn riguarda evidentemente le misure descritte negli articoli 20 – 23 LSIn. A tal proposito LB sottolinea che per le autorità cantonali e comunali assoggettate, le quali sono sottoposte alla LSIn secondo l'articolo 2 capoverso 2 lettera f e che nell'ambito della loro attività impiegano ampiamente mezzi TIC, l'adempimento dei requisiti dell'articolo 19 e seguenti LSIn può comportare oneri considerevoli che ricadrebbero sui contribuenti. Almeno nell'ambito della «protezione di base» sarebbe necessario prevedere un sistema di misure applicabili in modo semplice, rapido ed economico. Ciò corrisponde alla concezione attuale in materia di sicurezza informatica: in primo luogo un'elevata protezione delle informazioni chiave per continuare l'attività, in secondo luogo una protezione dei dati e dei processi impiegati nel lavoro quotidiano limitata a quanto necessario affinché non possano essere facilmente modificati, cancellati, abusati o dissimulati.

Articolo 19 Procedura di sicurezza

Per TG manca il principio della proporzionalità, motivo per il quale quest'ultimo deve essere assolutamente incluso nell'articolo 4 dell'avamprogetto della LSIn (come già menzionato in precedenza).

Per VD la nozione di procedura di sicurezza deve essere più esplicita.

Secondo insecor in questo articolo non è chiaro che cosa si intende con «procedura di sicurezza» e per quale motivo concerne unicamente le «autorità» e non le «organizzazioni». È quindi necessario specificare che la procedura di sicurezza comprende gli articoli seguenti (art. 20–26).

Secondo it-rm ognuno ha opinioni diverse su quale sia la protezione adeguata per i differenti livelli di sicurezza o di classificazione. Per questo motivo è necessario che un servizio specializzato centrale, ovvero l'organo di coordinamento, sia autorizzato a definire quali misure di sicurezza minime debbano essere applicate al corrispondente fabbisogno di protezione o classificazione delle informazioni. Sulla base di ciò le autorità devono stabilire una procedura secondo il capoverso 1.

Secondo i commenti all'articolo 19 capoverso 1 unicamente le autorità assoggettate devono esplicitamente stabilire una procedura di sicurezza per i mezzi TIC; le organizzazioni assoggettate ne sono quindi escluse. Tuttavia, le disposizioni degli articoli 19–27 fanno ripetutamente riferimento a quest'ultime. Per il Consiglio dei PF non è quindi chiaro quali siano gli obblighi concreti di queste organizzazioni.

Articolo 20 Analisi delle necessità di protezione e valutazione dei rischi

Secondo privatim l'articolo 20 LSIn deve essere completato affinché l'analisi delle necessità di protezione e la valutazione dei rischi non si debbano eseguire unicamente per l'impiego di nuove tecnologie, ma anche per l'impiego di nuovi sistemi IT. Mediante nuovi sistemi IT si generano nuovi rischi e vulnerabilità, tuttavia è anche possibile eliminare le carenze delle soluzioni esistenti e istituzionalizzare nuove misure e meccanismi di controllo.

Secondo l'articolo 20 capoverso 2 in caso di impiego di nuove tecnologie non solo le organizzazioni, ma anche le autorità, sono tenute a comunicare la valutazione dei rischi al servizio specializzato della Confederazione per la sicurezza delle informazioni. La BNS appoggia apertamente lo scambio, su base volontaria, degli esiti dalle valutazioni dei rischi. Tuttavia non è favorevole all'obbligo di comunicazione definito all'articolo 20 capoverso 2 poiché a causa della tecnologia impiegata (per es. software) si potrebbe risalire, ad esempio, a determinate attività per la concretizzazione di misure di politica monetaria. In tali ambiti, l'obbligo di comunicazione non produrrebbe il beneficio auspicato dallo scambio di informazioni poiché nessun'altra autorità o organizzazione assoggettata è attiva nel medesimo ambito aziendale della BNS. La formulazione dell'articolo 20 capoverso 2 come disposizione potestativa terrebbe conto della richiesta della BNS.

Per LB l'impiego di «nuove tecnologie» (il termine necessita di una precisazione: una generazione di mezzi TIC presente sul mercato, ma finora mai impiegata presso l'autorità assoggettata, può essere definita «nuova»?) nell'ambito dei mezzi TIC, caratterizzati da uno sviluppo tecnologico molto rapido, avviene (quasi) quotidianamente. Per le organizzazioni private l'obbligo di comunicare la valutazione dei rischi al servizio specializzato della Confederazione per la sicurezza delle informazioni è una questione delicata poiché ciò potrebbe causare la divulgazione di segreti d'affari. In linea di principio, per tutte le informazioni non liberamente accessibili al pubblico e provenienti da organizzazioni private che sarebbero comunicate alle autorità assoggettate o al servizio specializzato della Confederazione ai fini della sicurezza delle informazioni, deve essere garantito esplicitamente il segreto d'affari. LB propone di completare in tal senso la LSIn.

Articolo 21 Livelli di sicurezza dei mezzi TIC

Secondo it-rm il capoverso 2 lettera a deve essere completato con i criteri di sicurezza dell'attendibilità, dell'autenticità e dell'anonimato (cfr. anche l'osservazione all'art. 4 cpv. 2).

Per il Consiglio dei PF la classificazione dei mezzi TIC con i quali vengono trattati dati personali degni di particolare protezione continua a non essere chiara. Le pertinenti considerazioni a pagina 46 e 50 del rapporto esplicativo sono difficilmente comprensibili e non forniscono indicazioni chiare. In particolare è singolare l'affermazione a pagina 46 del rapporto esplicativo secondo cui, quando in un sistema d'informazione vengono trattati dati personali degni di particolare protezione, il corrispondente concetto in materia di sicurezza delle informazioni deve essere classificato. Concretamente, deve essere protetto il concetto, ma non i dati stessi: non avrebbe senso!

Il Consiglio dei PF reputa che tale disposizione sia formulata in modo estremamente vago (che cosa significa precisamente «protezione di base»?) e che comporti incertezze il cui chiarimento non dovrebbe essere lasciato alle disposizioni esecutive. Alcuni istituti del setto-

re dei PF sono arrivati alla conclusione di non avere in sostanza informazioni classificabili come «AD USO INTERNO», «CONFIDENZIALE» o «SEGRETO» ai sensi di questa legge e che verosimilmente tale situazione non cambierà in futuro. Il rapporto esplicativo conforta tale conclusione. Di conseguenza non gestiscono nemmeno «mezzi TIC del livello di sicurezza "protezione elevata" o "protezione molto elevata"».

Articolo 22 Requisiti di sicurezza del livello di sicurezza «protezione di base»

Per insecor non è chiaro chi stabilisce i requisiti minimi. Il capoverso 1 è in contraddizione con il mandato legale dell'ODIC che ha il compito di definire i requisiti minimi per i mezzi TIC dell'Amministrazione federale (cfr. per es. art. 17 cpv. 1 lett. d OIAF). D'altra parte secondo il capoverso 2 «tali requisiti minimi devono essere soddisfatti da tutti i mezzi TIC». Chi controlla che vengano rispettati? In virtù di quali basi e requisiti? Sono necessarie precisazioni in tal senso.

It-rm chiede di completare il capoverso 1 con una frase del seguente tenore: «Al riguardo, devono essere rispettati gli standard minimi definiti dall'organo di coordinamento». Tale organo deve stabilire anche standard minimi per le corrispondenti esigenze di protezione.

Per quanto riguarda le infrastrutture TIC, LB propone, indipendentemente dai dubbi riguardanti l'ingerenza nella sovranità dei Cantoni (art. 3 Cost.) e dal principio della sussidiarietà (art. 5*a* e art. 43*a* Cost.), di assegnare al servizio specializzato della Confederazione la competenza di definire in modo unitario i requisiti per i tre livelli di sicurezza dei mezzi TIC per tutto il territorio svizzero; tale servizio dovrà emanare standard, istruzioni, raccomandazioni, liste di controllo o requisiti minimi. L'articolo 88 LSIn ne rappresenterebbe la base legale.

Articolo 23 Concetto in materia di sicurezza delle informazioni

SO ritiene che i contenuti minimi del concetto in materia di sicurezza delle informazioni debbano essere concretizzati nella legge o perlomeno nell'ordinanza.

Per privatim nel testo di legge non è chiaro che cosa sia concretamente un concetto in materia di sicurezza delle informazioni, quali siano i suoi contenuti (minimi) e quali effetti si vogliano ottenere. È quindi necessario valutare se nella legge, nell'ordinanza o nel messaggio relativo alla LSIn sia necessario concretizzare il contenuto di un concetto in materia di sicurezza delle informazioni — in caso contrario non sarebbe possibile garantire l'uniformità a livello federale per quanto riguarda la sicurezza delle informazioni e l'articolo 23 LSIn non avrebbe alcun effetto pratico.

Clusis si domanda per quale motivo l'analisi dei rischi e l'allestimento di un concetto in materia di sicurezza delle informazioni riguardino unicamente i mezzi TIC dei livelli di sicurezza «protezione elevata» e «protezione molto elevata». L'analisi dei rischi dovrebbe precedere le misure di sicurezza che si adottano in base ai livelli di sicurezza.

Poiché in precedenza non è stata formulata alcuna definizione, per insecor non è chiaro che cosa si intende per «concetto in materia di sicurezza delle informazioni». Nel concetto deve essere presa in considerazione unicamente la «sicurezza delle informazioni»? Che cosa significa esattamente? La protezione dei dati non rientra più in tale obbligo secondo quanto previsto nel metodo di gestione di progetti HERMES per sistemi d'informazione e nei concetti SIPD? Come bisogna affrontare a livello cantonale e comunale queste direttive e come applicare le relative misure (cfr. art. 89)? È necessario chiarire in modo approfondito questi aspetti.

Il Consiglio dei PF sottolinea che alcune istituzioni dispongono già di un concetto in materia di sicurezza delle informazioni.

Articolo 24 Verifiche della conformità e dell'efficacia

Privatim propone di integrare nell'articolo 24 LSIn «Verifiche della conformità e dell'efficacia» anche le conseguenze. È necessario disciplinare, o perlomeno esplicitare nel messaggio, se oltre all'efficacia deve essere verificata anche l'efficienza delle misure decise e adottate (cfr. art. 4 cpv. 4 LSIn). Bisognerebbe inoltre disciplinare che cosa accadrebbe nel caso in cui i risultati delle verifiche venissero ignorati.

LB ritiene che i requisiti per la sicurezza di mezzi TIC debbano poter essere soddisfatti anche mediante l'impiego di prodotti certificati. Per prodotti certificati nel quadro di una determinata procedura e secondo gli standard di sicurezza riconosciuti a livello internazionale (per es. «Common Criteria») non dovrebbe essere necessaria un'ulteriore verifica della conformità e dell'efficacia. In considerazione del continuo alternarsi dei mezzi impiegati e del numero sempre maggiore di apparecchi terminali privati usati a fini commerciali, l'obbligo d'inventario dei mezzi TIC potrebbe comportare un importante onere organizzativo e amministrativo.

Articolo 25 Nullaosta di sicurezza

Per TG non è comprensibile per quale motivo con il nullaosta di sicurezza l'autorità può accettare i rischi residui. Per evitare un uso sconsiderato dei nullaosta è necessario rinunciare al secondo capoverso. Se all'articolo 23 dell'avamprogetto della LSIn viene stabilito che il concetto in materia di sicurezza delle informazioni deve essere costantemente aggiornato, due articoli dopo non si può affermare che con il nullaosta di sicurezza non occorre più preoccuparsi dei rischi esistenti, ma semplicemente accettarli. La disposizione secondo cui si accettano i rischi residui deve essere eliminata; se si potesse semplicemente fare affidamento sul nullaosta di sicurezza e non pensare più agli ulteriori rischi, le tecnologie dell'informazione e della comunicazione verrebbero utilizzate in modo superficiale e sconsiderato.

Articolo 27 Sicurezza nell'esercizio

VD reputa utile precisare che la sicurezza prevede quattro criteri: «confidenzialità», «integrità», «disponibilità» e «tracciabilità».

La FER ritiene che le nozioni di conservazione e backup, per quanto riguarda l'accesso da parte dei tecnici, siano sottointese. Tuttavia, considerando i furti avvenuti sarebbe opportuno affrontare questi due punti.

Articolo 28–29 Misure in materia di personale

Per quale motivo manca una distinzione tra le misure preventive e correttive? La sezione 4 con gli articoli 28 e 29 potrebbe essere denominata «Misure preventive in materia di personale».

Secondo il Consiglio dei PF questo articolo è eccessivo per quanto riguarda i mandatari che devono gestire informazioni o mezzi TIC dei PF o della Confederazione. Nella prassi ciò significherebbe che nel quadro dell'assegnazione di mandati a terzi (imprese) i PF dovrebbero assicurare la formazione e il perfezionamento adeguati dei mandatari nell'ambito della sicurezza delle informazioni. L'applicazione di tale disciplinamento nella pratica avrebbe ripercussioni finanziarie.

Articolo 29 Rilascio restrittivo di autorizzazioni

TG accoglie favorevolmente il fatto che in questo articolo non vi siano diverse categorie di controlli di sicurezza generali, ma che vengano rilasciate soltanto le autorizzazioni necessarie per l'adempimento di compiti. Tutt'al più sarebbe opportuno definire chiaramente, analogamente a quanto previsto dall'articolo 50 dell'avamprogetto della LSIn per il controllo di sicurezza relativo alle persone, un periodo di tempo entro il quale ripetere il controllo di sicurezza. Il capoverso 2 stabilisce che le autorizzazioni possono essere revocate anche solo se sussistono «indizi» di un pericolo per la sicurezza delle informazioni. Per la persona interessata ciò potrebbe rappresentare una misura alquanto severa; nel caso concreto, un analisi più attenta potrebbe escludere in un secondo momento l'esistenza di una minaccia effettiva, nonostante la presenza di indizi. Se una persona interessata si unisce in matrimonio con una persona proveniente da una zona di crisi, ciò potrebbe rappresentare in un primo momento un indizio di pericolo. In seguito si dovrebbe tuttavia poter dimostrare che, nonostante la presenza di indizi, è escluso il pericolo concreto. In base al principio giuridico «audiatur et altera pars», ovvero il diritto di essere sentiti, nel quadro di misure in materia di personale la persona interessata a cui è stata revocata provvisoriamente l'autorizzazione deve poter esporre in un'ampia procedura che nonostante i presunti indizi non vi sia alcun pericolo.

Il PPD è favorevole al rilascio restrittivo di autorizzazioni per la gestione di informazioni e mezzi TIC e alla verifica periodica della loro validità.

Clusis è favorevole al contenuto di questo articolo, ma si chiede come mai la revoca dell'autorizzazione non sia definita espressamente come automatica. Se ciò è sottointeso, sarebbe meglio esplicitarlo.

Articolo 31 Zone di sicurezza

Sulla base di considerazioni in materia di protezione dei dati, SO ritiene che per i metodi di verifica biometrici sia necessario definire chiaramente (nella legge o perlomeno nel rapporto esplicativo) che non è consentito salvare i dati grezzi.

Secondo TG l'impiego di metodi di verifica biometrici dovrebbe essere disciplinato più dettagliatamente. In particolare, è necessario definire quanto a lungo possono essere conservati i relativi profili. L'autorizzazione a eseguire controlli di borse e persone potrebbe ledere di fatto segreti d'ufficio e professionali. Tale disposizione rappresenta inoltre un grande pericolo per la sicurezza poiché durante il controllo degli effetti di detentori di segreti dei massimi livelli è inevitabile che personale di controllo non qualificato per il corrispondente livello di sicurezza venga a conoscenza di segreti che non gli competono. Il permesso di eseguire controlli di borse e persone, a cui in futuro potrebbe aggiungersi anche il controllo (e il pericolo di manipolazione) di computer portatili, deve quindi essere disciplinato con maggiore precisione affinché lo scopo della legge non diventi obsoleto. Anche il controllo senza preavviso di locali del personale deve essere disciplinato con maggiore precisione, tanto più che potrebbe interessare anche locali abitativi privati, ciò che nel caso di un'autorizzazione di controllo generale sarebbe in conflitto con il rispetto della vita privata e famigliare sancito dall'articolo 8 della CEDU.

TI considera l'indicazione di cui al capoverso 3 lettera a riduttiva siccome tiene conto della tecnica in uso attualmente. Ritiene pertanto opportuno modificare la formulazione in modo da poter tenere conto di eventuali sviluppi di tecnologie future; ciò avrebbe il pregio di non dover necessariamente por mano a una modifica legislativa.

In considerazione del principio di proporzionalità, VD ritiene che sia necessario precisare quali necessità le autorità assoggettate possono indicare per ottenere l'autorizzazione di esercitare i tipi di impianti secondo il capoverso 4.

Per SP l'impiego di metodi di verifica biometrici ai sensi del capoverso 3 lettera a deve essere disciplinato più dettagliatamente. È necessario definire quanto a lungo i relativi profili possono essere conservati. L'autorizzazione a eseguire controlli di borse e persone ai sensi del capoverso 3 lettera d potrebbe violare di fatto segreti d'ufficio e professionali. Il permesso di eseguire controlli di borse e persone deve quindi essere disciplinato più in dettaglio affinché lo scopo della legge non diventi obsoleto. Anche il controllo senza preavviso di locali del personale ai sensi del capoverso 3 lettera e dovrebbe essere disciplinato con maggiore precisione, tanto più che potrebbe interessare anche locali abitativi privati, ciò che nel caso di un'autorizzazione di controllo generale sarebbe in conflitto con il rispetto della vita privata e famigliare sancita dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

Privatim chiede che almeno nel messaggio l'articolo 31 capoverso 3 lettera a LSIn sia completato in modo che per i metodi di verifica biometrici possano essere registrati unicamente i valori hash dei corrispondenti dati e non i dati grezzi.

Clusis è favorevole a questo articolo che costituisce una base legale sufficiente per il trattamento dei dati personali, segnatamente di quelli sensibili.

Capitolo 3: Controlli di sicurezza relativi alle persone

In generale

Per quanto riguarda il capitolo concernente i controlli di sicurezza relativi alle persone, LU constata una certa sovraregolamentazione che spinge i Cantoni a introdurre diverse nuove

e, soprattutto, costose procedure. LU propone pertanto una rielaborazione generale del capitolo allo scopo di ridurre l'onere amministrativo dei Cantoni.

UR riconosce l'importanza dei controlli di sicurezza relativi alle persone, poiché vi è la possibilità che insorga una delle minacce più sensibili e intense per la sicurezza quando persone che hanno accesso a informazioni con una classificazione di livello elevato commettono atti di tradimento o sabotaggio. 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.

Per SG la riduzione dei livelli di controllo non ha ripercussioni sulla collaborazione della polizia cantonale nella procedura in materia di controlli di sicurezza relativi alle persone. La collaborazione della polizia cantonale è disciplinata dall'articolo 39 LSIn e non si differenzia molto dalle disposizioni della vigente legge federale sulle misure per la salvaguardia della sicurezza interna (RS *120*). Poiché le disposizioni attualmente in vigore si sono rivelate efficaci, SG non ha obbiezioni di fondo contro le nuove disposizioni concernenti i controlli di sicurezza relativi alle persone.

Il PS propone di riprendere nella LSIn l'articolo 20 capoverso 1 LMSI in una forma modificata: «Art. 32bis Contenuto del controllo di sicurezza: Il controllo consiste nel raccogliere i dati rilevanti in materia di sicurezza concernenti il modo di vita della persona interessata, segnatamente le relazioni personali strette e quelle familiari, la situazione finanziaria, i rapporti con l'estero e le attività illegali atte a minacciare la sicurezza interna ed esterna. Non sono raccolti dati sull'esercizio del diritto costituzionale alla libertà d'opinione e d'informazione.» Poiché si tratta di dati estremamente sensibili dal punto di vista della protezione dei dati e della personalità, per il PS in tale ambito è necessaria un'adeguata densità normativa. Inoltre, come finora, è esplicitamente escluso che si allestiscano schede sulle attività politiche.

Per il CP e la CVAM, il capitolo 3 della LSIn (art. 32 a 55) che disciplina le condizioni e le modalità del controllo di sicurezza relativo alle persone costituisce un progresso notevole in materia di garanzia dei diritti individuali e di certezza del diritto per le persone fisiche nel settore sensibile della sicurezza delle informazioni in cui l'interesse pubblico ha un ruolo importante, se non preponderante.

Privatim accoglie favorevolmente il chiaro disciplinamento dei controlli di sicurezza relativi alle persone (CSP) e dei sistemi d'informazione. Nondimeno, per quanto riguarda due punti privatim rileva un'urgente necessità di chiarimenti (cfr. osservazioni concernenti gli articoli 47 e 53).

Insecor approva un disciplinamento chiaro e uniforme dei controlli di sicurezza relativi alle persone.

LB osserva che nel settore dei controlli di sicurezza relativi alle persone si dovrebbero rispettare le esigenze della protezione della personalità e dei dati, poiché il controllo di sicurezza relativo alle persone costituisce un'ingerenza nel diritto fondamentale alla protezione della sfera privata (art. 13 Cost.) delle persone interessate.

Per il Consiglio dei PF non è chiaro se le disposizioni del capitolo 3 si applicherebbero unicamente alle autorità assoggettate (in base a un'interpretazione letterale si potrebbe intendere così) e che, di conseguenza, le organizzazioni assoggettate non sarebbero in alcun caso sottoposte a tale capitolo. Secondo l'articolo 34 capoverso 1 lettera b, nel quadro di un mandato sensibile sotto il profilo della sicurezza può succedere che gli impiegati di un'azienda alla quale si intende affidare un mandato siano sottoposti a un CSP, ma che ciò non sia il caso per i collaboratori dell'istituzione del settore dei PF che conferiscono il mandato. Poiché secondo l'articolo 38 capoverso 3 e l'articolo 46 capoverso 2 prima dell'assegnazione di un mandato occorre attendere il risultato del CSP, per l'istituzione interessata del settore dei PF ciò può comportare importanti ritardi nell'assegnazione del mandato. Pertanto, occorre fissare una durata massima (breve) per un CSP al fine di evitare ritardi sproporzionati nell'assegnazione dei mandati.

Articolo 33 Elenco delle funzioni con attività sensibili sotto il profilo della sicurezza

Il TF rammenta che per esso questo articolo è essenziale e che, di conseguenza, non deve in nessun caso essere modificato a suo scapito.

Articolo 34 Persone da sottoporre al controllo

Se già a livello di diritto federale il Consiglio federale e il cancelliere della Confederazione sono esclusi dall'assoggettamento al controllo di sicurezza relativo alle persone, per TG non ha alcun senso nei Cantoni esonerare dal controllo unicamente i membri dei governi cantonali. La disposizione ignora che nei Cantoni i cancellieri dello Stato sono pure considerati dei magistrati e come tali dovrebbero ugualmente essere esonerati dal controllo. In caso contrario, gli affari dei governi cantonali non potrebbero essere espletati.

Il TF rammenta che per esso questo articolo è essenziale e che, di conseguenza, non deve in nessun caso essere modificato a suo scapito.

Articolo 33 in combinato disposto con l'articolo 34

Il Consiglio dei PF rileva che, mentre l'articolo 34 capoverso 1 lettera b coinvolge in un controllo di sicurezza relativo alle persone anche persone che eseguono un'attività per un'autorità o un'organizzazione assoggettata, l'articolo 33 prevede a sua volta che solo le autorità assoggettate hanno l'obbligo di allestire un elenco delle funzioni per l'adempimento dei cui compiti è necessario l'esercizio di un'attività sensibile sotto il profilo della sicurezza. Ciò può portare alla situazione particolare in cui, nel caso di un mandato sensibile sotto il profilo della sicurezza, gli impiegati dell'azienda a cui si intende assegnarlo siano sottoposti al CSP, ma non i collaboratori del PF che lo conferiscono. Pertanto, occorre rivedere nuovamente l'articolo 33. Verosimilmente l'ordinanza sui controlli di sicurezza relativi alle persone (RS *120.4*) si limita a menzionare questo elenco delle funzioni con attività sensibili sotto il profilo della sicurezza e l'elenco richiesto dall'articolo 33 dovrebbe essere probabilmente identico a quello menzionato nell'OCSP. Se l'elenco delle funzioni con attività sensibili sotto il profilo della sicurezza è identico a quello nell'OCSP, il Consiglio dei PF propone che ciò venga chiaramente stabilito nella LSIn e che l'OCSP faccia parimenti riferimento all'articolo 33 LSIn.

Articolo 35 Livelli di controllo

Secondo il SIC l'audizione personale standardizzata di persone che hanno accesso a informazioni classificate SEGRETO da parte di personale debitamente formato è, senza eccezioni, parte integrante di ogni CSP. Il rapporto esplicativo concernente la LSIn osserva giustamente che una delle minacce più sensibili e intense per la sicurezza insorge quando sono commessi atti di tradimento o sabotaggio (cfr. rapporto pag. 21). Di regola simili minacce non sono ravvisabili consultando unicamente registri, ma presuppongono un confronto approfondito con la persona sottoposta al controllo. La rinuncia a questa misura è in contraddizione con l'osservazione appena citata e significa una limitazione considerevole della possibilità di individuare tempestivamente i rischi per la sicurezza. Il SIC chiede pertanto lo svolgimento di audizioni personali quale misura standard in occasione di controlli di cui all'articolo 35 lettera b.

Articolo 37 Consenso

BE propone di completare l'articolo 37 con un nuovo capoverso 3 del seguente tenore: «[3] I Cantoni possono prevedere per legge, anche per altre funzioni, la possibilità di eseguire controlli di sicurezza relativi alle persone senza il consenso delle persone da sottoporre al controllo». I Cantoni devono avere la possibilità di eseguire un controllo di sicurezza relativo alle persone senza il consenso della persona da sottoporre al controllo anche in altri settori sensibili delle amministrazioni cantonali e comunali (per es. per l'accesso a infrastrutture importanti o a dati classificati), quali la polizia.

TI non mette in discussione il principio della norma che condivide. Si domanda unicamente quali potrebbero essere le conseguenze nel caso di un diniego del consenso della persona da sottoporre al controllo.

Per Clusis è escluso che il controllo di sicurezza possa essere eseguito senza il consenso della persona interessata. Occorrerebbe piuttosto precisare che l'impiego di una persona nell'ambito di mandati sensibili implica l'esecuzione preliminare del controllo di sicurezza. Pertanto, sarebbe più opportuna una formulazione quale: «un controllo di sicurezza può essere eseguito prima dell'assegnazione di un mandato sensibile. Gli interessati ne sono preliminarmente informati».

LB osserva che secondo i principi della protezione della personalità e dei dati (art. 4 cpv. 5 LPD) il consenso presuppone la debita informazione preliminare della persona interessata sul controllo di sicurezza relativo alle persone e sui dati raccolti in tale ambito conformemente all'articolo 39 LSIn. Poiché i dati raccolti includono anche dati degni di particolare protezione ai sensi dell'articolo 3 lettera c LPD, il consenso dovrebbe essere espresso in modo esplicito.

Articolo 38 Momento del controllo di sicurezza relativo alle persone

Per il Consiglio dei PF nell'avamprogetto posto in consultazione manca un disciplinamento che stabilisca chiaramente quali sono le procedure da seguire o le disposizioni da applicare se un controllo di sicurezza relativo alle persone (CSP) non è stato eseguito preliminarmente o se non è stato svolto prima dell'attribuzione di una funzione. Nel settore della ricerca in particolare, a persone coinvolte in progetti di ricerca potrebbero essere affidati, soltanto in un secondo momento o a breve termine – e dunque senza previa possibilità di controllo – dei compiti i cui aspetti rilevanti sotto il profilo della sicurezza non sono ravvisabili a prima vista né sono preliminarmente riconoscibili come tali dai partner di progetto. La mancanza di un disciplinamento chiaro per lo svolgimento di un CSP a posteriori e in particolare le relative conseguenze condurranno inevitabilmente, nella pratica, a un conflitto duraturo tra le pretese in materia di diritto del personale della persona interessata e le intenzioni della LSIn in materia di politica di sicurezza. Il Consiglio dei PF propone che in questi casi il CSP avvenga a posteriori con il consenso della persona interessata. Se la persona rifiuta il suo consenso a un CSP, l'autorità assoggettata competente deve avere il diritto di sollevare tale persona da una funzione o di vietarle di svolgere un'attività per la quale è previsto un CSP, senza conseguenze finanziarie, di diritto del personale o d'altro genere.

Articolo 39 Acquisizione dei dati

Per VD i servizi di polizia e i servizi informazioni cantonali dovranno, come finora, essere incaricati dell'esecuzione dei controlli di sicurezza relativi alle persone; dovranno essere altresì autorizzati ad accedere a tutti i dati di cui all'articolo 39.

NE constata che, in qualità di autorità fiscale, può essere chiamato a trasmettere informazioni che sottostanno al segreto fiscale nel quadro di un controllo di sicurezza relativo alle persone (CSP). Secondo l'articolo 176 capoverso 2 della «Loi sur les contributions directes» (LCdir) è possibile comunicare informazioni se ciò è espressamente previsto da una base legale federale o cantonale. Al riguardo, l'articolo 39 capoverso 2 lettera a della nuova legge costituisce una base legale sufficiente. I relativi dati potranno essere richiesti esclusivamente nel quadro di un CSP ampliato. Si tratta in tal modo d'identificare e di valutare il rischio che gli interessi di cui all'articolo 1 capoverso 2 della legge siano minacciati da una persona nell'esercizio di un'attività sensibile.

Il PS suggerisce di mantenere la limitazione contenuta finora nella LMSI secondo cui è possibile interrogare terze persone unicamente con il consenso della persona interessata. Il PS rifiuta l'elusione totale del segreto bancario proposta dall'articolo 39 capoverso 2 lettera c LSIn. Il segreto bancario va revocato in forma adeguata nei confronti delle autorità fiscali. In tal modo gli organi addetti al controllo di sicurezza relativo alle persone potranno consultare presso le autorità fiscali tutti i dati rilevanti sulla situazione finanziaria della persona interessata e non dovranno rivolgersi a privati (banche ecc.).

Clusis accoglie favorevolmente questo articolo che costituisce una base legale sufficiente per il trattamento dei dati personali, in particolare di quelli sensibili.

Il SIC chiede che a livello di disposizioni d'esecuzione si stabilisca che lo scambio di informazioni debba svolgersi per il tramite del SIC quando il servizio estero è parte di un'organizzazione di intelligence.

Articolo 40 Assunzione dei costi

AI chiede di inserire nell'articolo 40 la riserva secondo cui la Confederazione assume integralmente i costi dei controlli di sicurezza relativi alle persone eseguiti su suo mandato. Le spese dei Cantoni connesse ad attività svolte su incarico della Confederazione dovrebbero essere completamente indennizzate. Ciò dovrebbe essere stabilito nella legge in maniera esplicita e inequivocabile.

Per TG occorre menzionare, in materia di assunzione dei costi, il principio secondo cui i costi di un controllo di sicurezza non dovrebbero essere addebitati alla persona privata da sottoporre al controllo, poiché esisterebbe il rischio che, in considerazione della situazione finanziaria delle persone eventualmente interessate, si procederebbe piuttosto raramente a controlli di sicurezza.

TI fa notare che, per il controllo di sicurezza di base, i servizi specializzati per i controlli di sicurezza relativi alle persone competenti per la valutazione del rischio per la sicurezza possono acquisire dati sulla persona sottoposta al controllo facendo anche capo a registri (cfr. lett. d ed e). Per la polizia, in modo particolare, che dispone di varie banche dati contenenti numerose informazioni (per es. «il giornale cantonale»), risulta indispensabile poter disporre di una definizione precisa di questo termine per evitare di utilizzare dati non pertinenti allo scopo.

Articolo 41 Abbandono della procedura

TG nota l'assenza di un disciplinamento che stabilisca che cosa accade ai dati acquisiti una volta concluso il controllo di sicurezza. La durata di conservazione di tali dati non è, per esempio, disciplinata. Ciò dovrebbe essere disciplinato a livello di legge. Il diritto a una cancellazione completa di dati obsoleti dovrebbe essere parimenti menzionato affinché le persone che in passato non hanno soddisfatto i criteri abbiano, in un secondo tempo, la possibilità di essere sottoposte a una nuova valutazione.

Articolo 42 Rischio per la sicurezza

Il PPD si pronuncia a favore di una definizione che specifichi cosa va considerato come rischio per la sicurezza.

Per LB non è ancora del tutto chiaro come valutare il rischio per la sicurezza, se la persona da sottoporre al controllo nega il suo consenso per un primo controllo o per una sua ripetizione secondo l'articolo 50 LSIn oppure revoca il suo consenso o non collabora al controllo (art. 41 cpv. 1 LSIn). In tal caso la persona è considerata «non controllata» (art. 41 cpv. 2 secondo periodo LSIn): la persona interessata non potrà quindi essere assolutamente impiegata per un'attività sensibile sotto il profilo della sicurezza secondo l'articolo 33 LSIn oppure dovrà essere rimossa da tale attività in caso di rifiuto della ripetizione del controllo? La decisione sull'impiego della persona interessata per un'attività sensibile sotto il profilo della sicurezza incombe quindi, secondo gli articoli 46 e 47 LSIn, manifestamente al servizio competente per l'attribuzione.

Articolo 43 Risultato della valutazione

TI ritiene insoddisfacente l'articolo 43 capoverso 1 lettera d, poiché neppure il commento nel rapporto esplicativo permette di comprendere se a seguito di una simile dichiarazione, trascorso un determinato periodo, il risultato della valutazione viene riesaminato.

Articolo 44 Comunicazione della valutazione

ZG propone di sostituire la «disposizione potestativa» dell'articolo 44 capoverso 4 con una «disposizione cogente». Nel caso di persone potenzialmente violente, i servizi competenti per la cessione o il ritiro dell'arma militare personale devono essere obbligatoriamente informati. L'annuncio di tali persone non dovrebbe essere lasciato all'apprezzamento del servizio che esegue il controllo. I relativi rischi sarebbero troppo elevati.

SG rileva che l'articolo 14 della legge militare (RS *510.10*) al quale si fa riferimento a pagina 60 del rapporto esplicativo nell'ambito delle osservazioni concernenti l'articolo 44 capoverso 3 LSIn, non esiste più essendo stato abrogato con effetto dal 1° gennaio 2004.

Articolo 47 Obbligo di comunicazione

Le dichiarazioni dei servizi specializzati CSP hanno carattere di raccomandazione (art. 46 LSIn). Ciononostante, il servizio competente per l'attribuzione della funzione deve comunicare al servizio specializzato CSP se attribuisce o no a una persona l'esercizio di attività sensibili sotto il profilo della sicurezza e se, in occasione dell'attribuzione dell'attività, deroga alle eventuali condizioni raccomandate dal servizio specializzato CSP. Secondo il commento relativo all'articolo 47 LSIn, la ragione di quest'obbligo di comunicazione consisterebbe nel mantenere la visione d'insieme sulla prassi dei servizi competenti per l'attribuzione e di trarne i necessari insegnamenti. Per BS tale argomentazione non è convincente: perché i servizi specializzati CSP dovrebbero effettuare la loro valutazione in base a criteri oggettivi o adeguare la loro prassi, se constatano che i servizi competenti per l'attribuzione non osservano o osservano solo parzialmente le loro raccomandazioni? Vi è il rischio che i servizi specializzati CSP non facciano più i loro controlli con la necessaria obiettività. È addirittura immaginabile che ciò conduca il servizio specializzato CSP a orientarsi ai desideri e alle esigenze del servizio competente per l'attribuzione. Ciò comporterebbe, a sua volta, nuovi rischi per la sicurezza.

Per privatim non è chiaro per quale ragione i servizi specializzati CSP che devono effettuare la loro valutazione in base a criteri oggettivi, dovrebbero poi adeguare la loro prassi, se constatano che i servizi competenti per l'attribuzione non seguono o seguono solo parzialmente le loro raccomandazioni. Ciò non condurrà, in ultima analisi, a far sì che i servizi specializzati CSP si pieghino ai desideri e alle esigenze dei servizi competenti per l'attribuzione e non eseguano più con la necessaria obiettività il loro compito fondamentale, ossia la valutazione di un eventuale rischio per la sicurezza? Non si dovrebbe piuttosto fornire mezzi maggiormente vincolanti ai servizi specializzati CSP, affinché possano agire in modo efficace di fronte a eventuali rischi per la sicurezza e non unicamente formulando raccomandazioni? Tali questioni dovrebbero essere chiarite nel commento agli articoli 46 e seguenti.

La Banca nazionale critica l'obbligo di comunicazione, sancito dall'articolo 47, nel caso in cui il servizio competente per l'assegnazione dell'attività sensibile sotto il profilo della sicurezza ignori una dichiarazione di rischio o di constatazione dell'organo di controllo o deroghi alle condizioni raccomandate e lo respinge quale ingerenza inammissibile nell'autonomia delle autorità sul piano dell'esecuzione. Tale obbligo di comunicazione è altresì in contraddizione con l'articolo 46, secondo cui le dichiarazioni dell'organo di controllo hanno (unicamente) carattere di raccomandazione e la decisione sull'attribuzione di attività sensibili sotto il profilo della sicurezza incombe esclusivamente al servizio competente per l'attribuzione.

Articolo 50 Ripetizione

TI considera che i tempi indicati per la ripetizione di un controllo di sicurezza siano troppo ampi e propone di eseguire i controlli di base entro 5 anni e quelli ampliati entro i 3 anni.

Articolo 51 Tutela giurisdizionale

Per TG il disciplinamento secondo cui la persona controllata potrebbe richiedere la decisione di un servizio specializzato CSP entro 30 giorni dal ricevimento della dichiarazione è contrario alla disposizione precedente secondo cui è possibile consultare i documenti del controllo soltanto per 10 giorni. Chi interpone ricorso dovrebbe avere la possibilità di prendere visione degli atti durante l'intero periodo che intercorre fino al termine d'impugnazione. Di conseguenza, il termine di 10 giorni di cui al capoverso 1 va prolungato a 30 giorni. Non avrebbe senso, per esempio, che un avvocato, al quale una persona intende ricorrere dopo due settimane, interponga ricorso senza avere la possibilità di prendere visione degli atti, poiché il relativo termine di 10 giorni è già scaduto.

Con riferimento all'autorità di vigilanza e al Ministero pubblico della Confederazione, per l'AV-MPC il testo di legge non specifica presso quale autorità sarebbe possibile impugnare una decisione dell'organo di controllo.

Il TAF assicura che non ha nulla da obiettare contro la nuova concezione della tutela giurisdizionale ai sensi dell'articolo 51 capoverso 3 LSIn.

Articolo 52 Sistema d'informazione per i controlli di sicurezza relativi alle persone

Clusis accoglie favorevolmente questo articolo che costituisce una base legale sufficiente per il trattamento dei dati personali, in particolare di quelli sensibili.

Per LB nella formulazione dell'articolo 52 capoverso 1 non è del tutto chiaro se il «sistema d'informazione» da impiegare si basa su una struttura unitaria predefinita dalla Confederazione – ciò che faciliterebbe il relativo accesso ai servizi autorizzati di cui all'articolo 53 LSIn – o se la LSIn lascia ai servizi specializzati CSP l'installazione e la gestione di un sistema d'informazione secondo criteri propri.

Per motivi inerenti alla protezione dei dati, LB nutre notevoli dubbi nei confronti della registrazione del numero d'assicurato AVS nel sistema d'informazione, poiché secondo l'articolo 52 capoverso 3 lettera a LSIn il sistema contiene già dati sull'identità delle persone registrate e che, conformemente all'articolo 36 capoverso 4 lettera c LPD e all'articolo 50*e* LAVS, la registrazione del numero d'assicurato AVS al di fuori del settore delle assicurazioni sociali sottostà a condizioni e restrizioni severe, nella misura in cui facilita il raggruppamento di informazioni concernenti le persone interessate e il cosiddetto «profiling». Dal punto di vista di LB non esiste alcun interesse legittimo per cui il numero d'assicurato AVS sia registrato nel sistema d'informazione per i controlli di sicurezza relativi alle persone: l'obiettivo di agevolare l'accesso alla persona registrata secondo l'articolo 53 LSIn non è un motivo che giustifica questo impiego discutibile dal punto di vista della protezione dei dati del numero d'assicurato AVS al di fuori del settore delle assicurazioni sociali. LB raccomanda altresì che, per analogia con l'articolo 77 capoverso 4 LSIn, l'articolo 52 capoverso 2 LSIn sia completato con l'indicazione della «responsabilità del servizio specializzato CSP ai fini della sicurezza del sistema d'informazione», poiché, rispetto ai dati concernenti i risultati contenuti nel sistema d'informazione per l'esecuzione della procedura di sicurezza relativa alle aziende, per i dati personali memorizzati nel sistema d'informazione del servizio specializzato CSP sussistono esigenze più elevate in materia di sicurezza.

Articolo 53 Comunicazione dei dati

Per TG la disposizione dell'articolo 53 capoverso 2 lettera c numero 1 dell'avamprogetto della LSIn, secondo cui lo Stato maggiore di condotta dell'esercito dovrebbe disporre di un'interfaccia con il sistema d'informazione per il controllo dell'accesso alle zone di sicurezza, va troppo lontano. Secondo l'articolo 3 dell'ordinanza concernente la protezione delle opere militari (RS *510.518.1*) nel caso della zona protetta 1 si tratta di impianti che, in parte, sono persino liberamente accessibili. Pertanto, lo Stato maggiore di condotta dell'esercito dovrebbe ricevere l'autorizzazione di accedere ai dati del controllo di sicurezza relativo alle persone unicamente a partire dalla zona protetta 2. Questo punto va, di conseguenza, adeguato. Si pone parimenti la domanda in che misura lo Stato maggiore di condotta dell'esercito debba disporre, per il reclutamento delle persone soggette all'obbligo di leva, di un corrispondente accesso ai dati del controllo di sicurezza relativo alle persone, tanto più che nel caso delle persone soggette all'obbligo di leva si tratta per lo più di giovani che raramente hanno già assolto, in precedenza, un controllo di sicurezza relativo alle persone.

Per privatim dal rapporto esplicativo non si evince per quale motivo è fondamentale per l'autorità di controllo accedere a dati personali «sensibili» per adempire il suo compito: il controllo dell'esecuzione dei CSP non può altresì avvenire sulla base di dati anonimizzati? Non vi sarebbe eventualmente la possibilità di ricorrere a dati «sensibili» solo in casi eccezionali e, di regola, svolgere l'attività di controllo mediante record di dati senza ulteriori riferimenti personali? Questo punto va chiarito.

Clusis accoglie favorevolmente questo articolo che costituisce una base legale sufficiente per il trattamento dei dati personali, in particolare di quelli sensibili. La comunicazione elettronica di dati deve avvenire in modo sicuro. Anche ciò va precisato.

Articolo 54 Conservazione e distruzione dei dati

Per SG l'attuale sistema d'informazione per i controlli di sicurezza relativi alle persone ha dato buone prove. Nondimeno, per quanto concerne i termini di cancellazione occorre tener conto che in virtù dell'articolo 54 capoverso 2 LSIn i termini stabiliti inizialmente sono di fatto prolungati. Per motivi legati alla protezione dei dati è importante che il legislatore sia consapevole di tale prolungamento di fatto dei termini. Pertanto SG suggerisce di menzionare ed eventualmente di valutare questa problematica nel rapporto sui risultati della consultazione e nel messaggio da allestire.

Per TG occorre inserire il capoverso 6 dopo il capoverso 2, garantendo in tal modo che i dati da distruggere non siano considerati tra quelli per i quali è fatta salva la trasmissione all'archivio di Stato.

Per il PS la riserva dell'archiviazione dei dati secondo le prescrizioni della legge sull'archiviazione proposta nel capoverso 6 è strutturata in maniera insufficiente. Poiché tale riserva non è menzionata direttamente dopo il capoverso 2 né nel titolo, potrebbe sorgere l'impressione che determinati documenti da distruggere non siano soggetti all'obbligo di archiviazione. Tuttavia, questa interpretazione contravverrebbe chiaramente all'obbligo di archiviazione secondo l'attuale legge sull'archiviazione. La riserva concernente la legge sull'archiviazione dovrebbe pertanto essere collocata direttamente dopo il capoverso 2 e menzionata esplicitamente nel titolo. Inoltre occorre una norma esplicita per evitare che l'obbligo di archiviazione previsto dall'attuale legge sull'archiviazione possa essere aggirato tramite una distruzione arbitraria di documenti. Occorre altresì concedere all'Archivio federale il diritto esplicito di verificare l'osservanza dell'obbligo di archiviazione. Pertanto il PS propone per l'articolo 54 il nuovo titolo seguente, i nuovi capoversi 2^{bis} e 2^{ter} e lo spostamento del capoverso 6 (nuovo: capoverso 2^{quater}):

> Articolo 54 Titolo (nuovo): «Obbligo di archiviazione nonché conservazione e distruzione dei dati».
>
> Capoverso 2^{bis} (nuovo) I servizi specializzati CSP offrono all'Archivio federale, a fini di archiviazione, i documenti non più necessari o destinati alla distruzione. I dati designati dall'Archivio federale come non degni di essere archiviati sono distrutti.
>
> Capoverso 2^{ter} (nuovo) I servizi specializzati CSP concedono all'Archivio federale, ai fini di garantire la tutela dei documenti a lungo termine, la consultazione dell'indice del sistema d'informazione di cui all'articolo 52.
>
> Capoverso 2^{quater} (nuovo) Sono fatte salve le prescrizioni per l'archiviazione dei dati della legge sull'archiviazione (RS *152.1*) e della legge federale sul servizio informazioni civile (RS *121*, art. 7*a*).

Clusis accoglie favorevolmente questo articolo che costituisce una base legale sufficiente per il trattamento dei dati personali, in particolare di quelli sensibili.

Articolo 55 Disposizioni completive del Consiglio federale

Per TG sarebbe eventualmente ammissibile, sotto il profilo della ricattabilità e della sicurezza, che si emanino disposizioni in materia di restrizioni di viaggio per persone che esercitano attività sensibili sotto il profilo della sicurezza. Ciò rappresenterebbe una limitazione per singole persone, ma anche, nel quadro di una valutazione più circostanziata, una protezione per tali persone e per la sicurezza dei dati.

Capitolo 4: Procedura di sicurezza relativa alle aziende

In generale

Riguardo alla procedura di sicurezza relativa alle aziende, economiesuisse rileva in particolare che la LSIn parla di una procedura di sicurezza relativa alle aziende e non di una procedura di sicurezza relativa alle imprese. In tal modo è possibile circoscrivere il settore da sottoporre al controllo, ciò che dovrebbe facilitare e rendere più economica l'applicazione delle misure di sicurezza necessarie. L'estensione del campo d'applicazione dell'attuale procedura di tutela del segreto, limitata ai mandati classificati provenienti dall'ambito militare, è un altro

fattore positivo. Poiché con la LSIn viene introdotta una procedura di sicurezza relativa alle aziende unitaria per il settore militare e civile e che il servizio specializzato potrà rilasciare attestazioni di sicurezza ufficiali relative alle aziende nel contesto internazionale, ciò rafforzerà la competitività delle imprese svizzere nell'ambito delle procedure di aggiudicazione all'estero.

Il CP e la CVAM constatano che, oltre a non costituire un ostacolo maggiore per gli attori economici, il capitolo 4 dell'avamprogetto della LSIn (art. 56 a 79) concernente la procedura di sicurezza relativa alle aziende tende a rafforzare i principi dell'obiettività, dell'equità, della trasparenza e della certezza del diritto, nonché a consolidare il diritto di essere sentito e la protezione giuridica delle aziende svizzere quando intendono ottenere l'assegnazione di un mandato sensibile sotto il profilo della sicurezza connesso a un acquisto pubblico della Confederazione. Infine, la possibilità prevista dall'articolo 57 capoverso 1 lettera b LSIn che le autorità federali competenti rilascino un'attestazione di sicurezza ufficiale alle aziende che hanno sede in Svizzera e si candidano per mandati di autorità estere o internazionali, rafforzerà la competitività delle aziende svizzere.

Insecor approva un disciplinamento chiaro e uniforme della procedura di sicurezza relativa alle aziende.

Per il Consiglio dei PF nell'avamprogetto della LSIn non è chiaro quando un mandato va considerato sensibile dal profilo della sicurezza e quando no: mentre nell'articolo 62 segg. LSIn si precisa che il servizio specializzato SA deve valutare l'idoneità di un'azienda, nell'avamprogetto non è chiaro quale autorità è incaricata di valutare se il mandato stesso va considerato sensibile o non sensibile dal profilo della sicurezza. L'assenza di una chiara ripartizione delle competenze a tale riguardo lascia troppo spazio a decisioni arbitrarie. Il tenore attuale dell'articolo 59 LSIn suggerisce, in particolare, che un'autorità o un'organizzazione assoggettata potrebbe decidere autonomamente se un determinato mandato è sensibile o non è sensibile dal profilo della sicurezza. Se si lascia loro tale valutazione, senza la possibilità di basarsi su un controllo da parte delle autorità federali di sicurezza, occorre garantire che non subiscano svantaggi nel caso in cui più tardi insorgano situazioni problematiche. Il Consiglio dei PF propone che nella legge si indichi chiaramente quale autorità procede alla valutazione e a chi un'organizzazione può rivolgersi per far verificare se un mandato va considerato sensibile o non sensibile dal profilo della sicurezza. La relativa decisione dovrebbe essere impugnabile nel caso in cui l'organizzazione interessata non possa decidere autonomamente e non dovesse essere d'accordo con detta decisione. I criteri che determinano l'assoggettamento all'esecuzione di una procedura di sicurezza relativa alle aziende vanno inoltre chiaramente stabiliti e occorre fissare una durata massima (breve) della procedura di sicurezza relativa alle aziende al fine di evitare ritardi sproporzionati nell'assegnazione dei mandati.

Articolo 62 segg. Idoneità delle aziende in relazione alla sicurezza delle informazioni

Per il Consiglio dei PF la valutazione dell'idoneità secondo l'articolo 62 segg. LSIn deve avvenire, idealmente, prima della messa a concorso di un mandato e la dichiarazione di sicurezza aziendale secondo l'articolo 69 LSIn dovrebbe essere parimenti rilasciata prima di tale messa a concorso secondo la legislazione in materia di appalti. In caso contrario, con uno svolgimento a posteriori di un controllo di sicurezza e dell'idoneità di un'azienda annunciatasi nell'ambito di un bando di concorso, sussiste il rischio che, se ottiene il mandato nell'ambito della procedura d'aggiudicazione, tale azienda non possa svolgerlo in caso di esito negativo del controllo di sicurezza. Pertanto, il Consiglio dei PF propone di integrare nella LSIn una disposizione di diritto specifica che stabilisca, nel caso di un controllo di sicurezza negativo e di un conseguente impedimento o scioglimento di un contratto, che l'azienda non ha alcun diritto a un'indennità, indipendentemente dal fatto che tale controllo abbia o non abbia avuto luogo prima o dopo una procedura d'aggiudicazione. Ciò deve valere anche quando, nel caso di un esito negativo di un controllo di sicurezza relativo alle persone, un contratto è sciolto o non può essere stipulato.

Articolo 62 Valutazione dell'idoneità

Considerato il rapporto delicato tra l'assegnazione di un'attività sensibile sotto il profilo della sicurezza e l'ordinamento nazionale e internazionale sugli acquisti pubblici (cfr. osservazioni generali) a LB appare un po' strano che secondo l'articolo 62 capoverso 1 dell'avamprogetto della LSIn il mandante ha il diritto e l'obbligo, prima o al di fuori della messa a concorso di progetti d'acquisto degli enti pubblici prescritta dal diritto in materia di acquisti pubblici, di comunicare al servizio specializzato SA quali aziende entrerebbero in considerazione per l'esecuzione del mandato, per cui tutte le altre aziende sarebbero escluse dall'assegnazione di tale mandato. Nella fattispecie, al mandante è accordata una competenza molto ampia di determinare a sua discrezione, in settori sensibili in materia di sicurezza, quali aziende invitare tra quelle che entrano in considerazione per l'esecuzione di mandati sensibili dal profilo della sicurezza.

Articolo 63 Acquisizione dei dati

Il SIC chiede che a livello di disposizioni d'esecuzione si stabilisca che lo scambio di informazioni debba svolgersi per il tramite del SIC quando il servizio estero è parte di un'organizzazione di intelligence.

Articolo 64 Rischio per la sicurezza

Per quanto concerne l'articolo 64 LSIn, Economiesuisse auspica in particolare che, nell'ordinanza che deve ancora essere varata, il margine discrezionale sia limitato da definizioni precise e da criteri di valutazione chiari. L'avamprogetto contiene numerose nozioni indeterminate ed eccessivamente generiche. Nel caso dell'articolo 64 (Rischio per la sicurezza), in mancanza di criteri di valutazione chiaramente definiti, l'autorità ha un margine discrezionale troppo ampio nell'ambito della verifica del rischio per la sicurezza inerente all'esecuzione di mandati da parte di un'azienda. La disposizione consente all'autorità di escludere offerenti indesiderati dalla procedura d'aggiudicazione senza che vi siano motivi oggettivi. Pertanto, essa racchiude potenziali disparità di trattamento e distorsioni della concorrenza a fini protezionistici. Qualsiasi riduzione artificiale del numero di offerenti porta tuttavia a prezzi più elevati. Ciò indebolirebbe la piazza economica svizzera.

Rinviando a una decisione incidentale del Tribunale amministrativo federale del 21 maggio 2014 (numero di dossier B-998/2014), la swico ritiene che la disposizione sia discutibile in termini di diritto della concorrenza e di diritto degli acquisti pubblici, poiché la probabilità di un'esecuzione contraria alle prescrizioni o non appropriata del mandato sensibile sotto il profilo della sicurezza può essere considerata elevata in particolare quando l'azienda è controllata da Stati esteri o da organizzazioni estere di diritto pubblico o privato oppure è sotto il loro influsso. Essa aggraverebbe ulteriormente la problematica legata agli acquisti e, come qualsiasi riduzione artificiale del numero di offerenti, porterebbe a prezzi più elevati. Ciò indebolirebbe l'economia e la piazza economica svizzere. Questa disposizione legale spalancherebbe la porta a interpretazioni arbitrarie o addirittura abusive da parte delle autorità. Con il margine di interpretazione e discrezionale sussiste il rischio che offerenti indesiderati siano tenuti alla larga. Pertanto, la swico chiede che, nell'ordinanza che deve ancora essere varata, il margine discrezionale sia chiaramente limitato e che si stabiliscano definizioni e criteri di valutazione chiari.

Come generalmente noto, le società madri di molte aziende attive nel settore del trattamento e della trasmissione di informazioni sono domiciliate all'estero e sono controllate da titolari di quote e azionisti stranieri. L'articolo 64 capoverso 2 lettera b LSIn potrebbe ora lasciare intendere che per tali aziende vi sarebbe a priori un'elevata probabilità di esecuzione contraria alle prescrizioni del mandato sensibile sotto il profilo della sicurezza. Pertanto, secondo l'articolo 65 capoverso 2 LSIn, andrebbero escluse dalla procedura di aggiudicazione. LB ritiene che l'ipotesi summenzionata potrebbe essere vista, dal profilo della legislazione in materia di acquisti pubblici, quale una discriminazione oggettivamente ingiustificata degli offerenti esteri attivi nel settore del trattamento e della trasmissione di informazioni. In ogni caso, nell'ambito della procedura legislativa occorrerebbe verificare tramite un servizio competente se e in quale misura l'articolo 64 capoverso 2 lettera b LSIn sia compatibile con le norme della legislazione internazionale in materia di acquisti. Inoltre, l'applicazione rigida

della disposizione dell'articolo 64 capoverso 2 lettera b LSIn potrebbe limitare in maniera eccessiva la cerchia delle aziende qualificate per l'esecuzione di mandati sensibili, al punto che sarebbero disponibili soltanto pochi offerenti qualificati o addirittura nemmeno uno. Pertanto, ciò potrebbe condurre a un conflitto tra, da un lato, una sicurezza ottimale e, dall'altro, la scelta dell'offerente più qualificato per una determinata applicazione.

Articolo 66 Concetto in materia di sicurezza

LB ritiene inopportuno e un'ingerenza inutile nell'autonomia aziendale che un servizio dell'amministrazione, ossia il servizio specializzato SA, allestisca un concetto in materia di sicurezza per un'azienda alla quale è stato affidato un mandato sensibile dal profilo della sicurezza. Sembrerebbe più appropriato un disciplinamento secondo cui l'azienda scelta per l'esecuzione di un mandato sensibile sotto il profilo della sicurezza allestisca un concetto di sicurezza da sottoporre alla verifica e all'approvazione del servizio specializzato SA.

Articolo 68 Dichiarazione di sicurezza aziendale / **Articolo 69** Esecuzione del mandato sensibile sotto il profilo della sicurezza

Per privatim si dovrebbe chiarire imperativamente per quale ragione nel caso della dichiarazione di sicurezza aziendale, si emana una decisione, mentre nell'ambito dei controlli di sicurezza relativi alle persone vengono unicamente formulate delle raccomandazioni. Questa differenziazione va spiegata.

Articolo 69 segg. Conseguenze della dichiarazione di sicurezza aziendale

Clusis osserva che, la problematica del subappalto non è stata trattata. Considerato il carattere sensibile dei mandati, il subappalto va escluso. In caso contrario, la legge deve prevedere condizioni severe.

Articolo 69 Esecuzione del mandato sensibile sotto il profilo della sicurezza

Per il Consiglio dei PF questa disposizione incide troppo sull'autonomia delle istituzioni nel settore dei PF. Inoltre, genera notevoli oneri amministrativi e ritardi sproporzionati, specialmente per le istituzioni nel settore dei PF, che non sottostanno all'Org-OAPub, in particolare se si tiene presente che parallelamente alle disposizioni della LSIn vanno rispettati i criteri in materia di diritto degli acquisti.

Articolo 76 Tutela giurisdizionale

Come già indicato all'articolo 51 dell'avamprogetto della LSIn, anche in questo caso TG non considera opportuno disciplinare il termine per la consultazione degli atti diversamente dal termine d'impugnazione. Secondo l'articolo 50 PA (RS *172.021*) i ricorsi contro le decisioni della Confederazione possono, di regola, essere inoltrati entro 30 giorni al tribunale amministrativo, per cui il previsto termine di 10 giorni va adeguatamente esteso.

Articolo 79 Conservazione e distruzione dei dati

Secondo TG i capoversi 2 e 3 vanno invertiti (e grammaticalmente adeguati), così da garantire che i dati da distruggere non siano considerati tra quelli per i quali è fatta salva la trasmissione all'archivio di Stato.

Per il PS occorre tener conto delle considerazioni espresse in merito all'articolo 54 anche nel caso dell'articolo 79 che tratta della conservazione e della distruzione dei dati acquisiti dal servizio specializzato (servizio specializzato SA) competente per l'esecuzione della procedura di sicurezza relativa alle aziende:

> Articolo 79 Titolo (nuovo): «Obbligo di archiviazione nonché conservazione e distruzione dei dati».
>
> Capoverso 2bis (nuovo) Il servizio specializzato SA offre all'Archivio federale, a fini di archiviazione, i documenti non più necessari o destinati alla distruzione. I dati designati dall'Archivio federale come non degni di essere archiviati sono distrutti.
>
> Capoverso 2ter (nuovo) Il servizio specializzato SA concede all'Archivio federale, ai fini di garantire la tutela dei documenti a lungo termine, la consultazione del suo sistema interno di registrazione.

Capoverso 2^{quater} (nuovo) Sono fatte salve le prescrizioni per l'archiviazione dei dati della legge sull'archiviazione (RS *152.1*) e della legge federale sul servizio informazioni civile (RS *121*, art. 7*a*).

Capitolo 5: Sicurezza delle informazioni nelle infrastrutture critiche

Il PS ritiene che l'intero capitolo 5 sulla sicurezza delle informazioni nelle infrastrutture critiche (art. 81-83 LSIn) debba essere sostanzialmente rielaborato. L'avamprogetto della LSIn contiene in questo capitolo autorizzazioni globali inammissibili inerenti alle attività di intelligence e non chiarisce in modo sufficiente le interfacce tra la garanzia di sicurezza delle informazioni nelle infrastrutture critiche e la protezione delle infrastrutture critiche stesse. Dal punto di vista della politica di sicurezza la protezione delle infrastrutture critiche costituisce un compito troppo importante per essere affrontato in modo così approssimativo e generale come nell'avamprogetto della LSIn.

Articolo 81 Compiti della Confederazione

Secondo il PS il capoverso 3 autorizza, attraverso formulazioni generali, lo scambio di informazioni non meglio definite tra gestori di infrastrutture critiche non meglio precisati e servizi della Confederazione non meglio definiti. Il PS chiede che venga fatta chiarezza in merito e che la densità normativa venga nettamente potenziata. Occorrerà perlomeno aggiungere un nuovo capoverso 4 del seguente tenore: «^{4} Sono fatte salve le disposizioni della legge sulla protezione dei dati».

It-rm è dell'avviso che «sostenere i gestori di infrastrutture critiche» sia di gran lunga insufficiente, poiché il sabotaggio delle infrastrutture critiche può provocare danni molto più gravi al benessere del nostro Paese rispetto all'eventuale rivelazione di informazioni confidenziali. L'attuazione di tali direttive necessita pertanto di prescrizioni minime ed eventualmente anche del sostegno finanziario della Confederazione. It-rm propone di inserire nella legge una legittimazione in merito.

Articolo 82 Trattamento di dati personali

SO sostiene che questa disposizione consenta il trattamento di dati personali senza che la persona interessata ne sia a conoscenza, il che rappresenta un'ingerenza sensibile nei diritti della personalità. Al più tardi una volta venuto meno il presunto pericolo, la persona dovrebbe essere informata. Urge quindi elaborare una normativa analoga a quella concernente l'osservazione e l'inchiesta mascherata contenuta negli articoli 283, 298 e 298*d* del Codice di procedura penale.

TG chiede di stralciare la disposizione dell'articolo 82 dell'avamprogetto della LSIn, in virtù della quale i servizi competenti delle infrastrutture critiche possono, per sventare pericoli, trattare e comunicare dati personali, in particolare elementi d'indirizzo nel settore delle telecomunicazioni, e questo addirittura all'insaputa delle persone interessate. Adducendo il pretesto della sicurezza delle informazioni, la disposizione crea uno strumento per consentire il trattamento di dati personali degni di particolare protezione di un gran numero di persone. Manca qualunque tipo di controllo o base legale per poter porre un freno a eventuali abusi. La legge federale sulla sicurezza delle informazioni deve garantire la gestione sicura di informazioni e non deve essere utilizzata come espediente per poter svolgere attività di intelligence.

TI propone di completare l'articolo 82 LSIn con un quarto capoverso che preveda, in caso di identificazione dell'utente, che questi ne sia informato e che i relativi dati possano essere comunicati alle autorità competenti. Nel caso in cui una persona venisse identificata sulla base dei dati personali secondo l'articolo 82, ne dovrebbe essere informata, quanto meno dal momento in cui non dovesse più sussistere un motivo di pericolo (analogamente alle procedure in materia di osservazione di persone, inchiesta mascherata e indagine in incognito, rette dagli art. 283, 298 e 298*d* CPP). «A questo riguardo la formulazione del capoverso 1 appare troppo blanda e la pur puntuale descrizione nel rapporto esplicativo non è sufficiente.»

Il PS chiede di stralciare l'articolo 82. Secondo questa disposizione i servizi competenti delle infrastrutture critiche possono, per sventare pericoli, trattare e comunicare dati personali, in particolare elementi d'indirizzo nel settore delle telecomunicazioni, e questo addirittura all'insaputa delle persone interessate. Adducendo così il pretesto della sicurezza delle informazioni, la disposizione creerebbe uno strumento per consentire il trattamento di dati personali degni di particolare protezione di un gran numero di persone. Mancherebbe qualunque tipo di controllo o base legale per poter porre un freno a eventuali abusi. La presente legge federale deve invece garantire la gestione sicura di informazioni e non deve essere utilizzata come espediente per poter svolgere attività di intelligence.

Tenendo conto del principio costituzionale della buona fede e di conseguenza anche del principio di trasparenza nell'ambito della protezione dei dati, secondo privatim il trattamento di dati personali all'insaputa delle persone interessate finalizzato a sventare pericoli è giustificato solo se, una volta venuto meno il presunto pericolo, la persona interessata riceve una comunicazione al riguardo, analogamente alle procedure perviste ad esempio per l'osservazione, l'inchiesta mascherata e l'indagine in incognito (art. 283, 298 e 298*d* CPP). L'articolo 82 LSIn deve quindi essere completato in tal senso.

LB non mette in dubbio che la protezione delle infrastrutture che secondo l'articolo 3 capoverso 3 LSIn sono indispensabili per il funzionamento della società, dell'economia e dello Stato rivesta grande importanza. Tuttavia, per quanto riguarda l'ingerenza nei diritti fondamentali garantiti dalla Costituzione, anche in questo ambito occorre rispettare il principio secondo cui l'attività dello Stato deve essere proporzionata allo scopo (art. 5 cpv. 2 Cost.). In un periodo in cui i cittadini esprimono forti dubbi verso le misure di sorveglianza statali è quindi difficile comprendere come l'avamprogetto della LSIn possa conferire ai gestori di infrastrutture critiche la competenza:

- di trattare (cfr. art. 3 lett. e/f LPD), ovvero raccogliere, memorizzare, utilizzare, analizzare e archiviare per un periodo di tempo indeterminato,
- dati personali, in particolare elementi d'indirizzo, ma anche dati degni di particolare protezione ai sensi dell'articolo 3 lettera c LPD, di tutto il settore delle telecomunicazioni,
- di propria iniziativa, senza un motivo specifico quale il sospetto di un crimine,
- senza autorizzazione da parte di un'autorità giudiziaria o perlomeno di un'autorità politica competente e responsabile,
- senza limitazioni temporali e materiali;
- di comunicare i dati raccolti alle autorità e organizzazioni assoggettate, ai servizi competenti dei Cantoni e addirittura a terzi (ovviamente nel quadro dell'adempimento dei rispettivi compiti) e
- di non informare in merito le persone interessate dopo la conclusione della sorveglianza, contrariamente a quanto stabilito dall'articolo 279 CPP,
- mentre per tali attività di sorveglianza detti gestori non devono essere sottoposti a controlli indipendenti di alcun tipo.

La protezione delle infrastrutture critiche è di fondamentale importanza per la società, l'economia e lo Stato. Tuttavia i principi basilari dell'attività dello Stato e la tutela dei diritti fondamentali non devono essere sacrificati in nome della protezione delle infrastrutture critiche. Occorre trovare un equilibrio tra sicurezza e tutela dei diritti fondamentali.

Articolo 83 Disposizioni completive del Consiglio federale

TG chiede, come nel commento all'articolo 82 dell'avamprogetto della LSIn, di prescindere dallo svolgimento di attività di intelligence.

Il PS rifiuta la delega di competenze al Consiglio federale prevista dall'articolo 83 LSIn. Una legge sulla sicurezza delle informazioni non ha il compito di autorizzare qualsivoglia servizio privato anonimo o autorità a svolgere attività di intelligence con un espediente. La ripartizione dei compiti e la collaborazione tra i servizi che assumono i compiti secondo l'articolo 81 e il Servizio delle attività informative della Confederazione deve essere disciplinata a livello legislativo. I servizi a cui viene delegata la competenza di scambiare informazioni di intelligence devono essere designati singolarmente per motivi inerenti alla protezione dei dati. Occorre inoltre specificare quali informazioni questi servizi possono scambiare con il Servizio delle attività informative della Confederazione. Dal momento che spesso si tratta di dati personali degni di particolare protezione, la LSIn deve rispettare la consueta ed elevata densità normativa. Se questo non dovesse essere possibile, l'articolo 83 dovrà escludere esplicitamente qualunque attività di intelligence.

Capitolo 6: Organizzazione ed esecuzione

Articolo 84 Incaricati della sicurezza delle informazioni / **Articolo 85** Conferenza degli incaricati della sicurezza delle informazioni

GL chiede che un rappresentante della Conferenza svizzera sull'informatica venga designato quale incaricato della sicurezza delle informazioni dei Cantoni. Questi potrebbe anche prender parte alla Conferenza degli incaricati della sicurezza delle informazioni secondo l'articolo 85.

ZG chiede di completare l'articolo 84 capoverso 1 con la lettera «g. i Cantoni». L'organizzazione flessibile con punti di contatto cantonali proposta nella LSIn non consentirebbe l'attuazione di un coordinamento e di un'armonizzazione efficaci tra Confederazione e Cantoni. Un coinvolgimento più diretto e istituzionalizzato dei Cantoni sarebbe necessario e più efficace. Tale coinvolgimento si potrebbe realizzare attraverso la partecipazione permanente di una rappresentanza cantonale alla Conferenza degli incaricati della sicurezza delle informazioni secondo l'articolo 85, analogamente a quanto succede ad esempio per la politica europea (rappresentanza permanente dei Cantoni nella Direzione degli affari europei). I Cantoni dovrebbero quindi designare di comune accordo degli incaricati della sicurezza delle informazioni come è previsto per i singoli organi federali (art. 84).

Per evitare doppie richieste relative a problemi di sicurezza, TG chiede di ampliare l'articolo 85 dell'avamprogetto della LSIn in modo tale che non solo la Conferenza degli incaricati della sicurezza delle informazioni provveda al coordinamento con l'incaricato federale della protezione dei dati e della trasparenza, ma che vi sia anche un coordinamento con gli incaricati cantonali della protezione dei dati di volta in volta interessati.

Nella misura in cui la legge è applicabile alle autorità cantonali designate dalla Confederazione, VD solleva la questione della rappresentazione di queste ultime nella Conferenza degli incaricati della sicurezza delle informazioni.

Secondo il PS la Conferenza degli incaricati della sicurezza delle informazioni non dovrebbe occuparsi soltanto del coordinamento con l'incaricato federale della protezione dei dati e della trasparenza (IFPDT), ma provvedere anche al coordinamento con gli incaricati cantonali della protezione dei dati di volta in volta interessati.

La Clusis accoglie con favore la nuova funzione di incaricato della sicurezza delle informazioni, ma si chiede al contempo perché non creare un nesso con la funzione di responsabile della protezione dei dati (prevista dalla LPD), precisando in particolare che «qualora necessario, l'incaricato della sicurezza delle informazioni collabora strettamente con il responsabile della protezione dei dati personali dell'azienda». Sarebbe inoltre opportuno coordinare meglio i compiti delle due funzioni.

Il SIC esige che i sistemi operativi e i dati di intelligence acquisiti con modalità operative vengano esclusi dalla verifica da parte degli incaricati della sicurezza delle informazioni del DDPS, poiché per garantire la protezione delle fonti il SIC applica misure di protezione speciali a questo tipo di informazioni. Tali misure vengono verificate periodicamente da un'autorità di vigilanza interna al DDPS (Vigilanza sulle attività informative).

Articolo 86 Servizio specializzato della Confederazione per la sicurezza delle informazioni

Per quanto riguarda la struttura unica centralizzata, secondo TI «i vari ruoli indicati per i servizi "inter-autorità" non sono chiaramente definiti e sembrano per certi versi contradditori o peggio ridondanti».

Articolo 87 Disposizioni esecutive

ZH teme che in virtù della clausola di esenzione («opting out») prevista dall'articolo 87 capoverso 3 LSIn, secondo la quale le autorità assoggettate possono emanare disposizioni esecutive proprie e i requisiti e le misure standard stabiliti dal Consiglio federale hanno solo valore di raccomandazioni, i concetti che risultano per certi versi molto vasti vengano interpretati e regolamentati diversamente nelle disposizioni esecutive delle varie autorità. ZH ritiene quindi che la legge, di per sé molto dettagliata, dovrebbe essere più specifica perlomeno in relazione agli interessi pubblici da proteggere definiti nell'articolo 1 capoverso 2 LSIn e ai livelli di classificazione previsti.

BE chiede di completare l'articolo 87 con un nuovo capoverso 5 del seguente tenore: «[5] Il Consiglio federale stabilisce per via di ordinanza le attività di cui all'articolo 2 capoverso 2 lettera f». Il messaggio relativo alla LSIn dovrebbe inoltre contenere una lista di tali attività rapportata al contesto attuale. Secondo l'articolo 2 capoverso 2 lettera f, la LSIn si applica anche alle autorità e ai servizi cantonali che, per incarico della Confederazione e sotto la sua vigilanza, esercitano attività sensibili sotto il profilo della sicurezza. Dal commento agli articoli non è però possibile evincere a quali attività si faccia riferimento. Queste devono essere stabilite in una lista a livello di ordinanza, in modo che i Cantoni e i Comuni comprendano chiaramente in quale misura sono assoggettati alla LSIn. Affinché sia possibile prevedere le ripercussioni della LSIn sui Cantoni e sui Comuni, il messaggio relativo alla LSIn dovrebbe già contenere una lista rapportata al contesto attuale. Dovrebbe altresì chiarire che cosa si intende per «sotto la vigilanza».

ZG mette in discussione l'efficacia della clausola di esenzione («opting out») proposta, secondo la quale ogni autorità esegue autonomamente l'atto normativo nel proprio ambito ed emana il relativo disciplinamento a livello di ordinanza. Se l'obiettivo è garantire la sicurezza delle informazioni per tutte le autorità interessate, la legge deve stabilire qualcosa in più di semplici standard minimi. In questo senso sarebbe necessario e importante definire standard e norme applicabili a tutte le autorità. In linea di principio sarebbe quindi ragionevole coinvolgere anche i Cantoni.

BS osserva che né il testo di legge proposto (art. 2 cpv. 2 lett. f LSIn) né il commento agli articoli illustra quali attività delle autorità cantonali rientrino nel campo di applicazione. BS propone di aggiungere all'articolo 87 LSIn una disposizione, secondo la quale il Consiglio federale deve stabilire per via di ordinanza le attività di cui all'articolo 2 capoverso 2 lettera f. Affinché sia possibile prevedere le ripercussioni sul Cantone, il messaggio dovrebbe già contenere una lista rapportata al contesto attuale. Il messaggio dovrebbe altresì chiarire che cosa si intende per «sotto la vigilanza».

Per quanto riguarda la clausola di esenzione («opting out»), TI constata che l'autonomia nell'emanare disposizioni esecutive, che per analogia deve essere applicata anche alle altre autorità federali, pone le basi per una difformità di esecuzione. Tale clausola non è quindi una soluzione ideale nell'ambito della sicurezza.

Il PPD accoglie con favore il fatto che il presente avamprogetto di legge non limiti l'autonomia delle autorità, consentendo alle autorità assoggettate di emanare le proprie disposizioni esecutive. Approva parimenti che le disposizioni esecutive del Consiglio federale siano applicate per analogia alle autorità assoggettate qualora queste non emanino disposizioni esecutive proprie.

L'AV-MPC prende atto del fatto che l'autorità di vigilanza, che rientra tra le autorità assoggettate di cui all'articolo 2 capoverso 2 lettera d, può emanare le proprie disposizioni esecutive secondo l'articolo 87 capoverso 1. Vista questa disposizione l'AV-MPC scioglie alcune delle riserve da lei stessa avanzate in occasione della consultazione degli uffici del 2 aprile 2013.

Secondo privatim né il testo dell'articolo 2 capoverso 2 lettera f LSIn né il commento agli articoli illustra quali attività delle autorità cantonali rientrino nel campo di applicazione. Privatim chiede pertanto di aggiungere all'articolo 87 LSIn una disposizione, secondo la quale il Consiglio federale deve stabilire per via di ordinanza le attività di cui all'articolo 2 capoverso 2 lettera f. Affinché sia possibile prevedere le ripercussioni sui Cantoni, il messaggio dovrà già contenere una lista rapportata al contesto attuale. Il messaggio dovrebbe altresì chiarire che cosa si intende per «sotto la vigilanza».

La CSI chiede di completare l'articolo 87 con un nuovo capoverso 5 del seguente tenore: «[5] Il Consiglio federale stabilisce per via di ordinanza le attività di cui all'articolo 2 capoverso 2 lettera f». Il messaggio relativo alla LSIn dovrà inoltre contenere una lista di tali attività rapportata al contesto attuale. Dal commento agli articoli non è possibile evincere quali attività delle autorità e dei servizi cantonali esercitate per incarico della Confederazione e sotto la sua vigilanza siano da considerarsi attività sensibili sotto il profilo della sicurezza secondo l'articolo 2 lettera f. Affinché i Cantoni e i Comuni comprendano chiaramente in quale misura saranno assoggettati alla LSIn, tali attività dovranno essere determinate in una lista a livello di ordinanza e il messaggio relativo alla LSIn dovrà già contenere una versione della lista rapportata al contesto attuale.

La BNS approva pienamente l'autonomia a livello di esecuzione di cui all'articolo 87 dell'avamprogetto di legge. Il commento agli articoli ha però messo in evidenza uno svantaggio di tale autonomia: «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». La BNS comprende perfettamente l'intento dell'avamprogetto di legge di disciplinare determinati requisiti organizzativi anche per le autorità assoggettate che, conformemente alla Costituzione, sono indipendenti. Ma è proprio in considerazione dell'autonomia di queste autorità sul piano dell'esecuzione, sancita dall'articolo 87 e sottratta alla competenza normativa del Consiglio federale, che si impone prudenza rispetto a quanto praticato a livello di avamprogetto, ovvero l'introduzione a livello legislativo di disposizioni che costituirebbero materia di ordinanza. Secondo la BNS questo andrebbe a ledere proprio la suddetta autonomia.

Il TF richiama l'attenzione sul fatto che questo articolo è essenziale per il TF e non dovrebbe quindi essere modificato a suo discapito.

Insecor reputa la procedura secondo la quale le autorità federali interessate possono emanare le proprie disposizioni esecutive solo parzialmente efficace. Per Insecor sono proprio le ordinanze a contenere le precisazioni del testo di legge importanti nel contesto specifico, e nell'ambito della sicurezza delle informazioni occorre evitare di creare ulteriore «dispersione» di tali precisazioni. In fin dei conti resta comunque la possibilità di emanare di volta in volta ordinanze dipartimentali o istruzioni che tengano conto delle esigenze specifiche di una determinata unità amministrativa.

Per il Consiglio dei PF occorrerà verificare da quali parti della legge le istituzioni del settore dei PF e il Consiglio dei PF potrebbero essere esclusi; perlomeno il capitolo concernente la verifica della sicurezza aziendale non dovrebbe essere applicabile né alle istituzioni del settore dei PF né al Consiglio dei PF (cfr. in particolare il parere precedente sull'art. 65 segg.).

Articolo 88 Requisiti e misure standard

BE chiede di completare l'articolo 88 con un nuovo capoverso 4 del seguente tenore: «[4] Il Consiglio federale disciplina per via di ordinanza quali autorità assoggettate sono competenti, singolarmente o congiuntamente, per dichiarare vincolanti i requisiti e le misure standard riguardanti attività eseguite o sistemi utilizzati congiuntamente da diverse autorità assoggettate. Nel caso in cui siano interessate autorità cantonali assoggettate, è necessario il loro consenso». BE osserva che in molti ambiti le autorità federali e cantonali collaborano strettamente oppure le autorità cantonali svolgono compiti della Confederazione, ad esempio nel settore della polizia. Inoltre per adempiere i compiti è spesso necessario creare una connessione tra le raccolte di dati o i sistemi TIC (ad esempio le reti) di diverse autorità. In questi

casi non è ragionevole che le autorità partner applichino livelli di sicurezza diversi. Un'autorità direttiva designata dal Consiglio federale dovrebbe quindi stabilire il livello di sicurezza applicabile per l'attività nel suo complesso. Al fine però di impedire che un'autorità federale stabilisca in modo univoco misure che produrrebbero elevati costi supplementari per i Cantoni, occorre sempre chiedere il consenso delle autorità cantonali eventualmente coinvolte.

Secondo il PPD è importante che il Consiglio federale stabilisca, secondo lo stato della dottrina e della tecnica, requisiti di sicurezza standardizzati nonché misure organizzative, di personale, tecniche ed edili standardizzate in materia di sicurezza delle informazioni, che abbiano carattere di raccomandazione per le autorità assoggettate.

Privatim raccomanda di verificare con la massima urgenza in quale misura i requisiti e le misure standard possano essere dichiarate vincolanti per tutte le autorità e le organizzazioni assoggettate alla LSIn. Se si rimane sul piano della raccomandazione e della dichiarazione volontaria del carattere vincolante non è possibile raggiungere un livello di protezione uniforme.

Dal momento che in molti ambiti le autorità federali e cantonali collaborano strettamente oppure le autorità cantonali e comunali svolgono compiti della Confederazione e che per adempiere i compiti è spesso necessario creare una connessione tra le raccolte di dati o i sistemi TIC di diverse autorità, non sarebbe ragionevole che le autorità partner applicassero livelli di sicurezza diversi. Un'autorità direttiva designata dal Consiglio federale dovrebbe quindi stabilire il livello di sicurezza applicabile per l'attività nel suo complesso. Al fine però di impedire che un'autorità federale stabilisca in modo univoco misure che produrrebbero elevati costi supplementari per i Cantoni, occorre sempre chiedere il consenso delle autorità cantonali eventualmente coinvolte. La CSI chiede quindi di completare l'articolo 88 con un nuovo capoverso 4 del seguente tenore:

> [4] Il Consiglio federale disciplina per via di ordinanza quali autorità assoggettate sono competenti, singolarmente o congiuntamente, per dichiarare vincolanti i requisiti e le misure standard riguardanti attività eseguite o sistemi utilizzati congiuntamente da diverse autorità assoggettate. Nel caso in cui siano interessate autorità cantonali assoggettate, è necessario il loro consenso.

Il TF richiama l'attenzione sul fatto che questo articolo è essenziale per il TF e non dovrebbe quindi essere modificato a suo discapito.

Per it-rm è assolutamente necessario creare un'istituzione (organo di coordinamento) che emani disposizioni esecutive vincolanti per tutte le autorità interessate dalla presente legge e alle quali tali autorità devono quindi attenersi (in contrapposizione con l'art. 88 cpv. 3 LSIn). In caso contrario questa disposizione può essere all'origine di disomogeneità nel dispositivo di sicurezza e in parte responsabile del fatto che venga conferita troppa poca importanza all'evoluzione della tecnica e al conseguente cambiamento delle esigenze in materia di sicurezza. Sarebbe antieconomico adottare misure differenti per la protezione degli stessi beni giuridici nello scambio di informazioni tra autorità. Una disomogeneità nel dispositivo di sicurezza è da considerarsi altresì controproducente per l'autorità che ha messo in atto le disposizioni più efficaci e quindi più costose. Come è noto, nel campo della sicurezza delle informazioni il livello di sicurezza dell'intera catena è pari a quello del suo anello più debole. Dovrebbe quindi essere possibile discostarsi da questo principio solo in casi eccezionali e su richiesta scritta e motivata.

Secondo il SIC è giustificato delegare al SIC l'elaborazione e l'adozione di standard di sicurezza (analogamente a fedpol, cfr. rapporto esplicativo, commento all'art. 88 cpv. 2 LSIn, pag. 73). Così come fedpol, il SIC ha esigenze specifiche per quel che riguarda il trattamento e la conservazione dei dati. In particolare lo scambio di dati tra diversi organi statali in Svizzera e all'estero è di primaria importanza per il SIC e non è paragonabile ad altri servizi federali. Anche per quanto concerne la protezione delle fonti gli standard di sicurezza specifici del SIC sono imprescindibili.

Articolo 89 Cantoni

Secondo l'articolo 89 LSIn le autorità e i servizi cantonali sono assoggettati alla legge solo se esercitano attività sensibili sotto il profilo della sicurezza su mandato della Confederazione e sotto la vigilanza diretta di quest'ultima. La legge non include le autorità e i servizi cantonali che, di loro competenza, attuano il diritto federale (rapporto esplicativo, pag. 38). Questa importante disposizione concernente il campo d'applicazione, per ZH solleva più dubbi di quanti non ne chiarisca. A quali attività dei Cantoni si fa riferimento? In quali ambiti i Cantoni si trovano sotto una vigilanza diretta? In che cosa consiste tale vigilanza? Dal momento che nel rapporto esplicativo non vengono menzionati esempi concreti, se ne deduce che anche alla Confederazione manchi chiarezza in merito. È però necessario poter prevedere se e in quale misura la legge sia applicabile alle attività cantonali e quali sarebbero le conseguenze – in particolare anche di natura finanziaria – della sua applicabilità. Almeno il messaggio indirizzato alle Camere federali dovrà fornire delucidazioni al riguardo.

ZH e BE chiedono di aggiungere all'articolo 89 LSIn una disposizione che preveda che le autorità e i servizi cantonali possano fare ricorso alle prestazioni dei servizi specializzati della Confederazione previsti dalla LSIn. ZH giustifica la richiesta osservando che la LSIn prevede misure (in particolare controlli di sicurezza relativi alle persone e procedure di sicurezza relative alle aziende) che a livello cantonale (e comunale) non sono disciplinate o sono disciplinate in modo diverso. Per questo motivo i Cantoni (e i Comuni) devono poter ricorrere ai servizi specializzati della Confederazione. BE avanza una proposta concreta di testo: «[4] Le autorità e i servizi cantonali possono fare ricorso alle prestazioni dei servizi specializzati della Confederazione previsti dalla presente legge. Il Consiglio federale può prevedere la riscossione di tasse a copertura delle spese per prestazioni a favore di autorità e servizi diversi da quelli di cui al capoverso 1». Non sarebbe ragionevole e in parte anche non realizzabile pensare di creare le conoscenze specialistiche necessarie per i compiti dei servizi specializzati CSP e SA in modo decentralizzato e per tutti i Cantoni e Comuni. Per questo i Cantoni devono poter usufruire delle prestazioni dei servizi specializzati della Confederazione. Nella misura in cui la LSIn assoggetta direttamente servizi cantonali e comunali (art. 2 cpv. 2 lett. f e art. 89 cpv. 1 LSIn) le rispettive prestazioni (ad esempio l'esecuzione di CSP) devono essere finanziate dalla Confederazione. Se invece i Cantoni applicano autonomamente la LSIn sotto la propria responsabilità, ad esempio attraverso l'introduzione di CSP per altri impiegati cantonali, sembra opportuno che si facciano carico dei relativi costi generati alla Confederazione.

Secondo ZH l'articolo 89 capoverso 2 lettera a LSIn autorizza il Consiglio federale a disciplinare i controlli di sicurezza relativi alle persone per determinati organi cantonali. Dal momento che un controllo di sicurezza relativo alle persone comporta un'ingerenza nei diritti fondamentali della persona interessata, il rispettivo disciplinamento deve avvenire a livello di legge, perlomeno per quanto concerne i principi fondamentali. L'avamprogetto di legge deve essere modificato di conseguenza.

OW ritiene ragionevole che, per le questioni inerenti alla sicurezza delle informazioni, i Cantoni debbano designare un servizio quale interlocutore delle autorità federali (art. 89 cpv. 3 LSIn). In questo modo è possibile garantire che lo scambio di informazioni abbia luogo sistematicamente e che l'applicazione delle misure avvenga in modo coordinato.

NW disciplinerà la designazione di un servizio cantonale quale interlocutore in una ordinanza di applicazione della LSIn. Nel Cantone la sicurezza informatica è attribuita all'Informatikleistungszentrum ILZ OVV/NW con sede a Sarnen.

GL designa l'Informatikdienst, Rathaus, 8750 Glarona, quale interlocutore delle autorità federali per le questioni inerenti alla sicurezza delle informazioni.

ZG chiede di modificare e completare l'articolo 89 capoverso 1 e 3 come di seguito:

> «[1] I Cantoni provvedono affinché le autorità e i servizi cantonali che esercitano attività sensibili sotto il profilo della sicurezza in collaborazione con la Confederazione ~~su mandato della Confederazione e sotto la vigilanza di quest'ultima~~ applichino le misure secondo la presente legge.

[2] …

[3] Per le questioni inerenti alla sicurezza delle informazioni, i Cantoni designano ciascuno un servizio quale interlocutore delle autorità federali e degli organi di coordinamento cantonali.».

A loro volta i Cantoni dovranno designare un organo centrale quale organo di contatto e di coordinamento, ad esempio la Conferenza dei Governi cantonali (CdC). In questo modo sarebbe possibile affrontare in modo tempestivo e adeguato le ripercussioni sui Cantoni e le questioni concernenti la collaborazione e il coordinamento tra Confederazione e Cantoni. In generale ZG propone quindi che la Confederazione cerchi preventivamente la collaborazione con i Cantoni, come previsto dal punto 3 del Rahmenordnung über die Arbeitsweise der KdK und der Direktorenkonferenzen bezüglich der Kooperation von Bund und Kantonen (Regolamento quadro sulle modalità di lavoro della CdC e delle Conferenze dei direttori cantonali per la cooperazione tra Confederazione e Cantoni, *non tradotto in italiano*) del 28 settembre 2012.

SO prevede che solo pochissimi impiegati cantonali rientrerebbero nel campo di applicazione della legge. Dal rapporto esplicativo non è tuttavia possibile desumere informazioni più precise al riguardo. Anche se solo singoli impiegati cantonali dovessero assumere compiti per la Confederazione, questo significherebbe che la totalità dei sistemi TIC del Cantone dovrebbe essere conforme ai requisiti della LSIn. Questo comporterebbe un elevato onere finanziario. SO chiede pertanto di verificare la possibilità di delegare ai Cantoni la competenza per la sicurezza delle informazioni a patto che questi rispettino determinati standard minimi, analogamente a quanto previsto dall'articolo 37 capoverso 1 della legge sulla protezione dei dati. Gli standard minimi dovrebbero essere enumerati in maniera esaustiva nella LSIn o nell'ordinanza.

BS si reputa interessato dalla LSIn solo nel caso in cui per incarico della Confederazione vengano esercitate, secondo l'articolo 2 capoverso 2 lettera f LSIn, attività sensibili sotto il profilo della sicurezza ai sensi dell'articolo 2 capoverso 3 LSIn. In questo caso occorrerebbe applicare le misure conformemente all'articolo 89 capoverso 1 LSIn. La divisione Informatiksteuerung und Organisation (ISO) ha già svolto lavori preliminari con la preparazione sistematica dell'ISMS.BS (sistema di gestione della sicurezza delle informazioni) per poter applicare la legge e le misure nel Cantone di Basilea Città. I Cantoni sarebbero obbligati a designare un servizio per le questioni inerenti alla sicurezza delle informazioni (art. 89 cpv. 3 LSIn). Questo servizio fungerebbe da interlocutore delle autorità federali. Tale compito può essere svolto dal responsabile cantonale in materia di sicurezza IT presso l'ISO.

AI chiede di stabilire nell'articolo 89 che la Confederazione risarcisca interamente i Cantoni per le attività sensibili sotto il profilo della sicurezza esercitate su mandato della Confederazione e sotto la vigilanza di quest'ultima, comprese le infrastrutture necessarie per lo svolgimento di tali attività. Gli oneri finanziari sostenuti dai Cantoni per le attività esercitate su mandato della Confederazione devono essere completamente risarciti. Questo principio dovrebbe essere stabilito in modo esplicito e inequivocabile nella legge. Per le prestazioni previste nella legge federale sulla sicurezza delle informazioni i Cantoni dovrebbero inoltre poter usufruire direttamente e gratuitamente dei rispettivi servizi specializzati della Confederazione. Anche questa aggiunta deve essere inserita nell'articolo 89.

TG chiede che l'articolo 89 capoverso 2 dell'avamprogetto della LSIn venga stralciato senza sostituzione. I Cantoni sono autonomi nella scelta del proprio personale. Non è ammissibile che la Confederazione prescriva al Cantone come questo debba scegliere il proprio personale. Anche quando, come nel presente caso, per i Cantoni si tratta solo di esercitare attività sensibili sotto il profilo della sicurezza su mandato della Confederazione, la scelta del personale da impiegare e dei rispettivi compiti deve rimanere di competenza dei singoli Cantoni. Grazie al contatto diretto con il proprio personale, il Cantone si trova altresì in una condizione decisamente migliore per poter valutare i potenziali di pericolo tra le proprie fila. Si invita la Confederazione a rispettare la sovranità cantonale.

VD vuole apportare una precisazione al capoverso 2 «Il Consiglio federale, in collaborazione con i Cantoni, disciplina:..». L'ordinanza federale dovrebbe tener conto del fatto che un ente

indipendente quale il Controllo cantonale delle finanze (cfr. commento precedente all'art. 11 cpv. 2), può essere abilitato, su mandato speciale dell'autorità esecutiva cantonale, a effettuare il controllo delle misure.

Conformemente alla rispettiva richiesta (art. 89 cpv. 3) GE designa la Direction générale des systèmes d'information (DGSI) quale interlocutore cantonale per la sicurezza delle informazioni.

La CSI chiede di completare l'articolo 89 con un nuovo capoverso 4 del seguente tenore:

> [4] Le autorità e i servizi cantonali possono fare ricorso alle prestazioni dei servizi specializzati della Confederazione previsti dalla presente legge. Il Consiglio federale può prevedere la riscossione di tasse a copertura delle spese per prestazioni a favore di autorità e servizi diversi da quelli di cui al capoverso 1.

Non sarebbe ragionevole e in parte anche non realizzabile pensare di sviluppare le conoscenze specialistiche necessarie per i compiti dei servizi specializzati CSP e SA in modo decentralizzato e per tutti i Cantoni e Comuni. Per questo i Cantoni dovrebbero poter usufruire delle prestazioni dei servizi specializzati della Confederazione. Nella misura in cui la LSIn assoggetta direttamente i servizi cantonali e comunali (art. 2 cpv. 2 lett. f e art. 89 cpv. 1 LSIn) le rispettive prestazioni (ad esempio l'esecuzione di CSP) devono essere finanziate dalla Confederazione. Se invece i Cantoni applicano autonomamente la LSIn sotto la propria responsabilità, ad esempio attraverso l'introduzione di CSP per altri impiegati cantonali, sembra opportuno che si facciano carico dei relativi costi generati alla Confederazione. Se questa richiesta non dovesse essere accolta occorrerà stralciare l'articolo 2 lettera f e l'articolo 89, prediligendo invece la soluzione della legge sulla protezione dei dati, secondo la quale i Cantoni sono competenti per la protezione dei dati anche nel quadro dell'adempimento di compiti della Confederazione, ammesso che vengano rispettati determinati standard minimi (art. 37 LPD).

Articolo 90 Trattati internazionali

Il SIC segnala che lo scambio di informazioni di intelligence è retto dall'articolo 12 del disegno di legge sulle attività informative.

Capitolo 7: Disposizioni finali

Articolo 93 Disposizioni transitorie

BE e la CSI chiedono di completare l'articolo 93 con un nuovo capoverso 3 del seguente tenore: «[3] Le autorità assoggettate dei Cantoni applicano la presente legge al più tardi entro cinque anni dalla sua entrata in vigore, sempre che il Consiglio federale non stabilisca termini transitori più lunghi». In particolare nel settore dei sistemi TIC l'applicazione di misure di sicurezza può comportare costi elevati, dal momento che richiede l'adeguamento di hardware e software. Spesso non conviene adeguare un vecchio sistema ai nuovi requisiti di sicurezza, perché l'acquisto di un nuovo sistema risulta più economico. L'adeguamento può inoltre rivelarsi impossibile a causa della cessazione del servizio di assistenza o della chiusura dell'azienda produttrice. Teoricamente l'applicazione dei requisiti e delle misure secondo la LSIn dovrebbe quindi consistere nella sostituzione di vecchi sistemi con sistemi nuovi. I termini transitori devono pertanto essere fissati in base al ciclo di vita abituale dei sistemi TIC. La CSI vorrebbe altresì aggiungere una seconda frase: «Nel caso in cui un'applicazione immediata dovesse comportare costi eccessivamente elevati, il diritto cantonale può, in deroga alle prescrizioni della Confederazione, prevedere un periodo transitorio massimo di dieci anni».

Secondo l'AV-MPC manca ancora una soluzione soddisfacente per le persone che al momento non sono oggetto di controlli di sicurezza relativi alle persone, mentre stando alle nuove disposizioni dovrebbero esserlo. Attualmente tali persone rivestono funzioni che prevedono attività sensibili sotto il profilo della sicurezza. Non sarebbe necessario adottare un disciplinamento espressamente per queste persone? Se queste persone dovessero essere

sottoposte a un CSP a posteriori, occorrerebbe fissare il rispettivo termine nelle disposizioni transitorie.

5.2 Modifica di altri atti normativi

Insecor segnala l'assenza nell'avamprogetto di un'ampia armonizzazione con le leggi federali contenenti riferimenti alla sicurezza delle informazioni (ad es. LPD, FiEle, LTC o Codice penale svizzero), in particolare per quanto riguarda i pericoli e le minacce attuali. Insecor suggerisce di verificare questo aspetto, valutando soprattutto se sia eventualmente necessario trattare a livello di legge determinati contenuti delle ordinanze (in particolare OIAF, OPrl, OLPD).

Insecor reputa contradditoria la seguente affermazione (cfr. rapporto esplicativo, pag. 16): «Solo raramente, infine, i responsabili di incidenti o di violazioni delle prescrizioni vengono chiamati a renderne conto». Il presente avamprogetto non contiene né disposizioni penali né una corrispondente modifica del Codice penale svizzero (CP; RS 311.0). Insecor propone di esaminare questa possibilità.

6 Pareri in merito alle ripercussioni illustrate nel rapporto esplicativo

Qui di seguito vengono riportati i pareri concernenti le ripercussioni illustrate nel rapporto esplicativo. Sono indicate soltanto le ripercussioni in merito alle quali è stato esplicitamente o implicitamente espresso un parere.

In generale

TI evidenzia come le conseguenze sui processi dei livelli istituzionali, segnatamente le implicazioni di ordine procedurale nei vari livelli istituzionali coinvolti, ancorché non direttamente legati al tema della sicurezza, non vengano sufficientemente messe in rilievo, senza peraltro che vi siano indicazioni specifiche.

Il PS si aspetta che le conseguenze organizzative, finanziarie e in materia di personale della LSIn vengano accuratamente illustrate nel messaggio e che la Confederazione garantisca la presenza, presso tutte le autorità assoggettate, di una sufficiente disponibilità di risorse per un'esecuzione appropriata della legge. Secondo il PS, oggi le principali lacune nell'ambito della sicurezza delle informazioni e della protezione delle strutture TIC non si riscontrano tanto a livello concettuale e legislativo quanto piuttosto sul piano delle carenze organizzative, segnatamente nella sottodotazione finanziaria e di personale dei servizi competenti.

6.1 Ripercussioni per la Confederazione

Il PPD chiede che, come annunciato nel rapporto esplicativo, il Consiglio federale spieghi dettagliatamente nel messaggio quali saranno i costi derivanti dalla legge, con particolare riferimento a quelli relativi alla Conferenza degli incaricati della sicurezza delle informazioni e al servizio specializzato della Confederazione per la sicurezza delle informazioni. Il PPD chiede inoltre che l'allestimento e l'esercizio del nuovo sistema non comportino un ulteriore aumento dell'effettivo di personale.

Il PLR sottolinea che non è ancora possibile valutare i costi reali che la presente legge potrebbe generare a livello tecnico e organizzativo e che una stima in tal senso non potrà essere effettuata prima della fine della procedura di consultazione. Per il PLR è importante che si trovi un equilibrio tra il livello di sicurezza e i costi necessari per ottenerlo, al fine di evitare un'esplosione delle spese.

Il PS ritiene che, nella ripartizione delle risorse, occorra attribuire una netta priorità al settore civile e alle attività quotidiane. A suo avviso, infatti, i dipartimenti civili competenti non dispongono delle risorse finanziarie e di personale necessarie per far sì che agli annunci seguano i fatti. Per il PS è chiaro: la competenza principale dovrà rimanere decentralizzata ed essere attribuita anche in futuro ai dipartimenti civili. Inoltre, occorrerà procedere a un trasferimento delle risorse da settori della politica di sicurezza militare divenuti ormai obsoleti a

questi nuovi ambiti di una politica di sicurezza civile che deve essere attuata con urgenza. Secondo il PS, se si vuole ottenere un aumento effettivo della sicurezza, occorre impiegare le risorse liberate al DDPS dopo il «no» al Gripen, pari a circa 250-300 milioni di franchi l'anno, nel settore dei rischi della società dell'informazione, dei cyber-rischi e della protezione delle infrastrutture critiche. Il PS sottolinea inoltre come la criticità della questione delle risorse sia dimostrata anche dal rapporto esplicativo concernente la LSIn, in cui si evita accuratamente di quantificare i costi e i posti supplementari derivanti dalla legge. Tuttavia, senza una risposta chiara a tale questione, neanche la migliore delle nuove leggi potrebbe garantire un aumento effettivo della sicurezza.

In relazione a questa nuova e controversa legge, il PS conferma la sua richiesta di fornire le necessarie risorse all'IFPDT, che, a suo avviso, svolge un ruolo chiave nell'affermazione di una buona prassi giuridica per quanto concerne la classificazione e il principio di trasparenza. Il PS ritiene infatti che non gioverebbe a nessuno limitarsi, per via delle scarse risorse, a emanare raccomandazioni superficiali per la composizione delle controversie. Nella misura in cui la LSIn affida nuovi compiti all'IFPDT, la Confederazione deve preoccuparsi di fornire risorse finanziarie e di personale supplementari. Il PS si aspetta che il messaggio concernente la LSIn indichi di quanti posti supplementari sarà dotato l'IFPDT per far fronte a questo compito importante ma pur sempre aggiuntivo.

Per swico, il fatto che nel rapporto non possano essere quantificate le ripercussioni finanziarie e di personale (cfr. pag. 78 del rapporto esplicativo) indica chiaramente che il presente avamprogetto di legge è ancora incompleto.

6.2 Ripercussioni su Cantoni e Comuni

ZH chiede che le incertezze sulle ripercussioni e sul coinvolgimento dei Cantoni vengano eliminate al più tardi al momento dell'attuazione della legge e dell'emanazione delle relative disposizioni esecutive. Ritiene inoltre che, in tale contesto, sia assolutamente necessario tenere debitamente conto, in generale, degli interessi dei Cantoni e, in particolare, dell'autonomia amministrativa che spetta a questi ultimi.

Affinché i Cantoni e i Comuni sappiano con chiarezza in quale misura sono assoggettati alla LSIn, BE chiede di definire tale questione per via di ordinanza con un apposito elenco. A suo avviso, inoltre, per poter stimare le ripercussioni della LSIn sui Cantoni e sui Comuni, una versione attuale di questo elenco dovrebbe essere contenuta già nel messaggio concernente la LSIn, il quale dovrebbe anche chiarire che cosa si debba intendere per «sotto la vigilanza».

BE si aspetta uno stretto coinvolgimento dei Cantoni e delle relative autorità specializzate nell'elaborazione delle disposizioni esecutive della Confederazione, in particolare nella misura in cui tali disposizioni riguardano anche i Cantoni.

In relazione ai costi, per LU non è chiaro quale sarà l'ammontare a carico dei Cantoni. Finché non sarà nota l'ordinanza del Consiglio federale con le relative disposizioni esecutive, a suo avviso sarà difficile stimare le conseguenze per i Cantoni in termini di costi. LU chiede pertanto di illustrare con chiarezza, prima di licenziare la presente legge, i costi che quest'ultima comporterà per i Cantoni e di impostare la legge stessa e le relative ordinanze d'esecuzione in modo tale da garantire ai Cantoni un'esecuzione senza consistenti oneri amministrativi.

UR ritiene che i costi previsti a carico dei Cantoni nel quadro della gestione dei rischi e delle necessarie misure di sicurezza e di protezione siano difficili da stimare. Considera tuttavia indispensabile, soprattutto da parte della Confederazione, procedere con il dovuto senso della misura per far sì che gli oneri legati alla sicurezza delle informazioni possano essere sostenuti anche dai Cantoni finanziariamente più deboli. Qualora la Confederazione avesse già alcune idee in merito ai costi da prevedere e al finanziamento in genere, sarebbe necessario comunicarle.

Dopo aver esaminato il rapporto esplicativo e l'avamprogetto, SZ giunge alla conclusione che, in linea di principio, la LSIn non ha ripercussioni sul Cantone. È tuttavia dell'avviso che

le successive disposizioni esecutive potrebbero comportare alcune conseguenze per quanto riguarda il controllo di sicurezza ampliato secondo l'articolo 39 capoverso 2 lettera a in combinato disposto con l'articolo 40 capoverso 1 LSIn. Quando verrà il momento, SZ conta di essere invitato a esprimere un parere anche nell'ambito della procedura di consultazione sulle disposizioni esecutive.

Vista la situazione attuale, OW non può ancora valutare né le ripercussioni concrete che la nuova legge avrà sul Cantone né gli oneri supplementari da prevedere. È tuttavia dell'avviso che, considerata la quota piuttosto esigua di compiti federali sulla totalità dei compiti che i propri servizi sono tenuti ad adempiere, gli oneri supplementari per questi ultimi dovrebbero essere abbastanza contenuti. OW fa notare che, nell'esercizio della loro attività, le autorità di perseguimento penale cantonali dipendono spesso dalle informazioni fornite da autorità federali. Affinché le informazioni che giungono alle autorità cantonali mantengano il livello di protezione previsto dall'avamprogetto, è possibile che sia necessario ampliare le misure di sicurezza, il che potrebbe determinare oneri supplementari soprattutto per le autorità di dimensioni più piccole. Ciò andrà verificato in un secondo momento.

NW parte dal presupposto che, qualora la LSIn entrasse in vigore nella versione inviata in consultazione, le ordinanze emanate per la sua esecuzione potrebbero comportare un onere operativo considerevole per il Cantone. A tale proposito, fa notare la presenza di alcuni articoli che, a seconda del campo d'applicazione e del coinvolgimento di singoli uffici o dell'intero Cantone, potrebbero comportare diversi adeguamenti di leggi, ordinanze e istruzioni. NW conta di essere invitato a partecipare anche alla procedura di consultazione sulle disposizioni esecutive.

Secondo GL, la legge sulla sicurezza delle informazioni garantisce chiarezza alle autorità federali. A suo avviso, anche per i Cantoni sarebbe utile una sintesi dei compiti più importanti nonché delle principali competenze e responsabilità. GL ritiene inoltre che alcune nozioni debbano essere ulteriormente concretizzate. In particolare, per GL non è chiaro in quale forma specifica i singoli Cantoni saranno interessati da eventuali condizioni e dalla necessità di misure di formazione.

ZG ritiene che nell'avamprogetto di legge e nel rapporto esplicativo non siano state sufficientemente ponderate le ripercussioni sui Cantoni.

SO presuppone che siano pochissimi i collaboratori cantonali interessati dalla legge, ma sottolinea come dal rapporto esplicativo non si evincano dati più precisi in merito. Anche nel caso in cui soltanto singoli collaboratori cantonali svolgessero compiti per incarico della Confederazione, tutti i sistemi TIC del Cantone dovrebbero soddisfare i requisiti sanciti dalla LSIn, il che, secondo SO, comporterebbe oneri particolarmente elevati. SO chiede pertanto di valutare la possibilità di trasferire ai Cantoni la competenza in materia di sicurezza delle informazioni analogamente a quanto previsto dall'articolo 37 capoverso 1 della legge sulla protezione dei dati, purché i Cantoni soddisfino determinati standard minimi che dovrebbero essere elencati esaustivamente nella LSIn o nella relativa ordinanza.

Secondo BS, né dal testo di legge proposto (art. 2 cpv. 2 lett. f LSIn) né dal rapporto esplicativo si evince con chiarezza quali siano le attività delle autorità cantonali che rientrano nel campo d'applicazione dell'atto normativo. BS suggerisce pertanto di integrare l'articolo 87 LSIn con una disposizione in cui si stabilisca che il Consiglio federale deve fissare per via di ordinanza le attività di cui all'articolo 2 capoverso 2 lettera f. Inoltre, affinché sia possibile stimare le ripercussioni sul Cantone, una versione attuale dell'elenco di tali attività dovrebbe a suo avviso essere contenuta già nel messaggio, il quale dovrebbe anche chiarire che cosa si debba intendere per «sotto la vigilanza».

BL ritiene che l'assoggettamento alla nuova legge non debba generare costi per i Cantoni, visto che tali costi non sono documentati nel rapporto esplicativo.

Poiché la nuova legge federale fornisce un quadro normativo per l'esercizio di attività sensibili sotto il profilo della sicurezza ma lascia margini di manovra per quanto concerne l'esecuzione, secondo AI è ancora più importante che anche le ordinanze d'esecuzione ven-

gano sottoposte ai Cantoni per consultazione. In particolare, AI si aspetta di essere interpellato anche in merito all'ordinanza del Consiglio federale.

GR ritiene che l'avamprogetto non disciplini con sufficiente chiarezza le interfacce tra Confederazione e Cantoni. A suo avviso manca una descrizione esatta delle attività dei Cantoni che rientrano nel campo d'applicazione della legge e non viene precisato in quale misura i Cantoni stessi sono interessati da quest'ultima. GR ritiene che tali aspetti vadano disciplinati in modo differenziato già a livello di legge per evitare eventuali difficoltà in termini di competenze nell'ambito dell'attuazione pratica. Secondo GR, se i Cantoni applicano la LSIn, direttamente in qualità di autorità assoggettate o nel quadro della ripresa di prescrizioni della LSIn nel diritto cantonale, è necessario accordare loro la possibilità di assegnare incarichi anche ai servizi specializzati centrali della Confederazione previsti dalla LSIn (tra cui in particolare i servizi specializzati per i controlli di sicurezza relativi alle persone e il servizio specializzato per la sicurezza aziendale). GR sottolinea inoltre i costi elevati che potrebbero derivare dall'adattamento dei sistemi alle misure di sicurezza. Fa infine notare che il ciclo di vita dei sistemi TIC è in genere di cinque-dieci anni, motivo per cui ritiene indispensabile prevedere, per l'attuazione della legge, adeguati periodi transitori che abbiano almeno una durata compresa tra i cinque e i dieci anni.

AG sottolinea come, nel settore di maggiore rilevanza per i Cantoni, esistano attualmente diverse questioni aperte. Il modo con cui la Confederazione intende disciplinare il controllo di sicurezza relativo alle persone per gli impiegati cantonali sarà ad esempio disciplinato soltanto nel diritto esecutivo, motivo per cui, secondo AG, attualmente non è possibile dedurre né le modalità di attuazione né le ripercussioni concrete dei controlli di sicurezza relativi alle persone sul personale cantonale. AG fa anche notare che non è ancora stata definita con chiarezza nemmeno la verifica, da parte della Confederazione, dell'applicazione delle prescrizioni nei Cantoni e non è chiaro in che modo verranno impostati il procedimento e, in particolare, il flusso di dati in questa procedura di vigilanza. AG osserva inoltre che dal presente avamprogetto di atto normativo non emerge praticamente alcuna interfaccia tra il diritto in materia di sicurezza delle informazioni e la vigilanza cantonale sulla protezione dei dati, ma ritiene che non sia comunque possibile esprimere un giudizio definitivo sulla questione in quanto il rapporto esplicativo indica soltanto marginalmente, o per nulla, le interazioni tra la protezione dei dati e la sicurezza delle informazioni. Sottolinea in ogni caso come nel rapporto esplicativo venga implicitamente formulata una riserva a favore del diritto federale in materia di protezione dei dati (cfr. numero 1.3.1.2, pag. 29) e presuppone che tale riserva si applichi a maggior ragione al diritto cantonale in tale ambito, segnatamente in quei settori dell'esecuzione cantonale del diritto federale che saranno assoggettati alla LSIn. Per AG, le suddette questioni ancora aperte dovrebbero essere chiarite nell'ambito della procedura legislativa e spiegate nel messaggio.

Per TI, naturalmente la promulgazione della LSIn comporterà delle conseguenze operative a livello cantonale: andranno infatti verificate le conseguenze che la nuova legge, in particolare per quanto attiene alla classificazione delle informazioni, avrà sui sistemi utilizzati dall'Amministrazione cantonale e sulle procedure in uso; i sistemi interconnessi Cantone – Confederazione dovranno probabilmente essere adattati per soddisfare le nuove norme. A suo avviso dovrà inoltre essere approfondita l'eventuale modifica di leggi settoriali negli ambiti in cui i servizi dell'Amministrazione cantonale forniscono informazioni a servizi dell'Amministrazione federale. Esempio: le norme sulla sicurezza relativa alle aziende dovranno essere applicate per la scelta di prodotti informatici utilizzati in modo interconnesso con la Confederazione? Vi sono riferimenti della legge cantonale sull'archiviazione verso il diritto sovraordinato (Legge federale sull'archiviazione) che richiedono delle modifiche?

6.3 Ripercussioni sull'economia

La maggior parte delle conseguenze economiche della presente legge è conforme alle esigenze del PLR. La legge lascia infatti prevedere un rafforzamento della competitività delle imprese e una migliore protezione dei segreti economici che esse porranno sotto la protezione del Governo.

Il CP e la CVAM ritengono che sia difficile, in questa fase, pronunciarsi sull'efficacia delle misure proposte, ma considerano incoraggiante il fatto che, al posto di un considerevole numero di norme e misure diverse per i vari servizi federali, in futuro sarà applicato un unico dispositivo legale di riferimento. Secondo il CP e la CVAM, in questo modo si garantirà una maggiore sicurezza dei flussi di informazioni, che saranno al contempo facilitati, si rafforzerà la certezza del diritto e, paradossalmente, si favorirà il principio di trasparenza dell'amministrazione, che è appunto fatto salvo qualora non trovino applicazione misure di sicurezza basate sulla LSIn o su una delle altre leggi speciali (art. 3 cpv. 1 LSIn).

7 Pareri in merito agli aspetti giuridici

TI ritiene necessario che il futuro messaggio precisi, eventualmente con riferimento all'articolo 89 dell'avamprogetto, che la vigilanza della Confederazione non intacca le competenze dell'Autorità cantonale di vigilanza e controllo in materia di protezione dei dati personali, che rimangono quindi garantite. A suo avviso è importante rilevare come, indipendentemente dal tipo di atto giuridico che attribuisce o demanda loro un compito pubblico federale (mandato o delega di funzione), gli organi pubblici cantonali non diventano organi federali e rimangono pertanto assoggettati, oltre che al diritto federale speciale che ne definisce e delimita il rispettivo mandato o la delega di funzione, anche al diritto cantonale, in particolare a quello sulla protezione dei dati.

Per il CP e la CVAM, l'avamprogetto della LSIn non solleva alcun problema né in materia di costituzionalità né dal punto di vista del federalismo.