Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

**Segreteria generale DDPS SG-DDPS**
Digitalizzazione e cibersicurezza DDPS

24 agosto 2022

# Diritto d'esecuzione relativo alla legge sulla sicurezza delle informazioni

## Rapporto esplicativo

Dossier: SG-DDPS-251.2-35/1/6/8

# Compendio

Il 18 dicembre 2020 l'Assemblea federale ha approvato la legge sulla sicurezza delle informazioni (LSIn). La nuova legge crea un quadro legale formale uniforme per la sicurezza delle informazioni in seno alla Confederazione.

Le ordinanze d'esecuzione della LSIn figuranti nel presente rapporto esplicativo sono state elaborate in collaborazione con rappresentanti delle altre autorità federali e dei Cantoni. Nel suo messaggio del 22 febbraio 2017 concernente la legge sulla sicurezza delle informazioni il Consiglio federale ha annunciato che avrebbe invitato le altre autorità federali e i Cantoni a esprimersi in merito a tutte le normative importanti. Da un lato, occorre raggiungere un livello di sicurezza il più possibile uniforme e, dall'altro, si deve tenere debitamente conto delle esigenze di tutte le autorità federali e dei Cantoni. Si svolge pertanto una procedura di consultazione.

Il diritto d'esecuzione relativo alla LSIn comprende complessivamente tre nuove ordinanze e una modifica di un'ordinanza esistente:

- ordinanza sulla sicurezza delle informazioni (OSIn): la nuova ordinanza disciplina la gestione della sicurezza delle informazioni, la protezione delle informazioni classificate, la sicurezza informatica e le misure adottate per la sicurezza personale e fisica dell'Amministrazione federale e dell'esercito. Essa definisce i compiti, le competenze e le responsabilità pertinenti. La modifica più importante è l'introduzione di un sistema di gestione della sicurezza delle informazioni (SGSI; *Information Security Management System, ISMS*) in tutte le unità amministrative;
- ordinanza sui controlli di sicurezza relativi alle persone (OCSP): la nuova ordinanza riassume le disposizioni esecutive concernenti i vari controlli di sicurezza relativi alle persone. Questi controlli sono ridotti al livello minimo indispensabile per individuare rischi considerevoli per la Confederazione. In tal modo si ridurrà notevolmente, in futuro, il numero di controlli effettuati;
- ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz): la nuova ordinanza disciplina i dettagli della procedura di sicurezza relativa alle aziende (PSA) introdotta dalla LSIn. Tale procedura si applica a tutti i mandati sensibili sotto il profilo della sicurezza aggiudicati dalla Confederazione;
- ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM): la revisione parziale di questa ordinanza comporta, oltre ad adeguamenti principalmente tecnici, un'estensione del campo d'applicazione dell'ordinanza alle unità amministrative dell'Amministrazione federale decentralizzata.

L'entrata in vigore della LSIn e delle disposizioni esecutive è prevista per la metà del 2023.

**Indice**

# Rapporto esplicativo

## 1 Situazione iniziale

Il 18 dicembre 2020 l'Assemblea federale ha approvato la legge sulla sicurezza delle informazioni (LSIn).[1] Il termine per il referendum è scaduto inutilizzato a metà aprile 2021. La nuova legge crea un quadro legale formale uniforme per la sicurezza delle informazioni in seno alla Confederazione.

La nozione di «sicurezza delle informazioni» comprende la totalità dei requisiti e delle misure con cui vengono protette la confidenzialità, l'integrità, la disponibilità e la tracciabilità di informazioni e di dati di ogni tipo, nonché la disponibilità e l'integrità di mezzi informatici. Dato che oggi le informazioni vengono perlopiù trattate elettronicamente, si pone l'accento sulla «cibersicurezza». La nozione di «sicurezza delle informazioni» comprende però tutti i processi di elaborazione, dunque anche documenti cartacei e affermazioni orali, e non soltanto il trattamento elettronico. Nell'uso colloquiale, tuttavia, spesso le due nozioni sono utilizzate quale sinonimo.

Le ordinanze d'esecuzione della LSIn figuranti nel presente rapporto esplicativo sono state elaborate in collaborazione con rappresentanti delle altre autorità federali e dei Cantoni. Nel messaggio del 22 febbraio 2017[2] concernente la legge sulla sicurezza delle informazioni (messaggio LSIn) il Consiglio federale ha annunciato che avrebbe invitato le altre autorità federali e i Cantoni a esprimersi in merito a tutte le normative importanti (cfr. n. 1.5., pag. 2621). Così, da una parte, si può raggiungere un livello di sicurezza il più possibile uniforme e, dall'altra, tenere debitamente conto delle esigenze di tutte le autorità federali e dei Cantoni. Si svolge pertanto una procedura di consultazione.

## 2 Analisi di diritto comparato, in particolare con il diritto europeo

In molti Paesi europei le basi giuridiche per la sicurezza delle informazioni vengono adeguate alla nuova realtà della società dell'informazione. Dato che in parte gli ordinamenti giuridici e le strutture statali dei diversi Paesi si distinguono sostanzialmente, la gerarchia normativa e il campo d'applicazione delle corrispondenti normative possono difficilmente essere confrontati. Si può invece affermare che, in linea di principio, le disposizioni della LSIn e delle sue ordinanze d'esecuzione corrispondono, o sono perlomeno in sintonia, con le normative degli Stati presi in esame. Sotto il profilo organizzativo, grazie al servizio specializzato della Confederazione per la sicurezza delle informazioni quest'ultima disporrà di un unico punto di contatto nelle relazioni internazionali. La collaborazione internazionale nell'ambito della sicurezza delle informazioni sarà quindi più semplice ed efficiente.

## 3 Punti essenziali degli atti normativi

### 3.1 Entità del diritto d'esecuzione relativo alla LSIn

Il diritto d'esecuzione relativo alla LSIn comprende quattro ordinanze:

- una nuova ordinanza sulla sicurezza delle informazioni (OSIn; cfr. n. 3.3);
- una modifica dell'attuale ordinanza del 19 ottobre 2016[3] sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM; cfr. n. 3.4);
- una nuova ordinanza sui controlli di sicurezza relativi alle persone (OCSP; cfr. n. 3.5);
- una nuova ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz; cfr. n. 3.6).

Il 12 gennaio 2022 il Consiglio federale ha avviato la procedura di consultazione concernente l'introduzione dell'obbligo di notifica dei ciberattacchi per i gestori di infrastrutture critiche. L'introduzione di un siffatto obbligo di notifica comporta il rimaneggiamento completo del capitolo 5 (Infrastrutture critiche) della LSIn. L'entrata in vigore di questa revisione della LSIn, ordinanza inclusa, è prevista per la fine del 2023. Non è quindi opportuno adottare una nuova ordinanza per le esigenze attuali che verrà completamente riveduta già pochi mesi dopo. Per tale motivo si rinuncia per ora a emanare disposizioni esecutive concernenti il capitolo 5 della LSIn.

[1] FF **2020** 8755
[2] FF **2017** 2563
[3] RS **172.010.59**

## 3.2 Condizioni generali e principi

Il Consiglio federale ha motivato nel messaggio LSIn la necessità formale e materiale della LSIn. Questa situazione iniziale e gli obiettivi e gli approcci di soluzione ivi connessi del Consiglio federale non hanno perso nulla quanto ad attualità. Fungono da base concettuale per il diritto d'esecuzione relativo alla LSIn. Lo stesso vale per la valutazione della minaccia, l'orientamento strategico della Svizzera e i principi operativi stabiliti dal Consiglio federale nell'aprile 2018 nella «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018-2022». Per l'attuazione della sicurezza delle informazioni nell'Amministrazione federale e nell'esercito occorre tenere conto di altre strategie, in particolare le strategie informatiche nazionali e interne alla Confederazione.

Per l'elaborazione del diritto d'esecuzione relativo alla LSIn sono stati definiti quali indicatori strategici i cinque principi seguenti:

*a. Responsabilità in materia di sicurezza interconnessa*

Conformemente all'articolo 45 della legge del 21 marzo 1997[4] sull'organizzazione del Governo e dell'Amministrazione (LOGA), i direttori delle unità amministrative sono responsabili dell'esecuzione dei compiti loro assegnati, compresa la protezione delle proprie informazioni e dei propri mezzi informatici. In un contesto interconnesso e digitalizzato questa responsabilità considerata separatamente non è tuttavia sufficiente. Le informazioni vengono scambiate, i sistemi interconnessi e le raccolte di dati rese disponibili per un uso condiviso secondo il cosiddetto principio *«once only»*. In tal modo, minacce e attacchi contro un'organizzazione o i suoi fornitori possono estendersi anche all'ambito di competenza di altre organizzazioni. La sicurezza delle informazioni è quindi necessariamente un compito interconnesso con responsabilità interconnessa che richiede obiettivi comuni, una procedura coordinata e standard minimi.

*b. Approccio basato sul rischio*

È risaputo che non è possibile raggiungere la sicurezza assoluta e che i rischi sono quindi inevitabili. Le direttive sulla protezione di base della Confederazione offrono una protezione in funzione dei rischi contro numerose minacce. Servono alla sicurezza delle informazioni interconnessa della Confederazione e devono essere rispettate. Per integrarle, nell'ambito della sicurezza delle informazioni i responsabili sono tenuti a esercitare una gestione del rischio attiva, nel contesto della quale punti deboli e minacce e le loro potenziali ripercussioni sull'adempimento dei compiti vengono consapevolmente considerati e resi prioritari. Ne risulta così una sicurezza adeguata. Con un siffatto approccio basato sul rischio, oltre che sui rischi, è possibile concentrarsi anche su possibilità e opportunità, nuove idee, applicazioni o tecnologie.

*c. Armonizzazione e standardizzazione*

Un'adeguata sicurezza delle informazioni è un presupposto per la fiducia nel Governo elettronico. Ciò vale non soltanto per l'ambito nazionale, ma anche per la crescente interconnessione delle autorità su scala internazionale. Occorre perciò perseguire un'armonizzazione nazionale e internazionale delle prescrizioni e una standardizzazione delle misure di sicurezza. Quest'ultima comporta ulteriori importanti vantaggi: da un lato, alle autorità responsabili dello sviluppo e ai servizi incaricati degli acquisti vengono indicati chiari requisiti di sicurezza, sui quali potranno fondarsi nell'implementazione della sicurezza nei mezzi informatici; dall'altro, consente di prevedere e pianificare in modo più semplice i costi della sicurezza nell'ambito dei progetti.

*d. Neutralità tecnologica*

Con l'avanzare della digitalizzazione emergono tecnologie, piani o forme di lavoro sempre nuovi rilevanti per la sicurezza. Le ordinanze devono essere in grado di tenere conto di sviluppi quali «nuvola informatica» (*«*cloud computing*»)*, «Internet delle cose» («Internet of Things»), «intelligenza artificiale» («artifical intelligence») o «computazione quantistica» («quantum computing») senza dovere essere continuamente adeguate. A livello di ordinanza occorre quindi stabilire innanzitutto principi, compiti, competenze e responsabilità. Le direttive imposte dalla tecnologia devono essere definite a livello delle istruzioni e degli standard tecnici.

[4] RS **172.010**

*e. Consentire la digitalizzazione*

Nei progetti legislativi si deve tenere conto fin dall'inizio delle esigenze della digitalizzazione. Quando compiti, processi e procedure vengono verificati da un punto di vista giuridico o ridefiniti, occorre garantire che le nuove prescrizioni consentano la digitalizzazione.

### 3.3 Ordinanza sulla sicurezza delle informazioni (OSIn)

*a. Oggetto*

La nuova ordinanza sulla sicurezza delle informazioni (OSIn) sostituisce l'ordinanza sui ciber-rischi del 27 maggio 2020[5] (OCiber) e l'ordinanza sulla protezione delle informazioni del 4 luglio 2007[6] (OPrI). L'OSIn disciplina la gestione della sicurezza delle informazioni, la protezione delle informazioni classificate, la sicurezza informatica e le misure adottate per la sicurezza personale e fisica. Essa definisce i compiti, le competenze e le responsabilità pertinenti nell'Amministrazione federale e nell'esercito.

*b. Campo d'applicazione*

L'OSIn si applica al Consiglio federale, all'Amministrazione federale e all'esercito. Le unità amministrative dell'Amministrazione federale decentralizzata di cui all'articolo 7*a* dell'ordinanza del 25 novembre 1998[7] sull'organizzazione del Governo e dell'Amministrazione (OLOGA) vengono assoggettate all'OSIn soltanto se i loro compiti sono sensibili sotto il profilo della sicurezza o possono rappresentare un rischio considerevole per l'Amministrazione federale centrale. Questi presupposti sono soddisfatti se le unità amministrative decentralizzate accedono a mezzi informatici dell'Amministrazione federale centrale del livello di sicurezza «protezione elevata» o «protezione molto elevata», se esse stesse impiegano siffatti mezzi informatici oppure se trattano informazioni classificate della Confederazione. La CaF e i dipartimenti possono inoltre chiedere al Consiglio federale di assoggettare ulteriori unità amministrative decentralizzate.

Le organizzazioni di cui all'articolo 2 capoverso 4 LOGA alle quali sono attribuiti compiti amministrativi ma che sono al di fuori dell'Amministrazione federale vengono completamente escluse dal campo d'applicazione della LSIn e di conseguenza anche dell'OSIn. Sono considerate terzi.

L'OSIn si applica, per analogia, all'Assemblea federale, ai tribunali della Confederazione, al Ministero pubblico della Confederazione e alla sua Autorità di vigilanza nonché alla Banca nazionale svizzera se non emanano proprie prescrizioni.

*c. Collaborazione con i Cantoni*

Ove i Cantoni trattino informazioni classificate della Confederazione, si applicano le relative prescrizioni della LSIn e dell'OSIn. Quando accedono a mezzi informatici della Confederazione, si applicano loro le direttive della LSIn e dell'OSIn sulla sicurezza informatica. In pratica, come avviene oggi, i Cantoni dovranno soddisfare i requisiti di sicurezza fissati dall'ufficio federale responsabile del mezzo informatico in applicazione di suddette direttive. Essi possono tuttavia esentarsi dalle direttive del diritto federale se garantiscono di propria iniziativa una sicurezza delle informazioni equivalente. Ciò presuppone che essi emanino proprie prescrizioni di sicurezza, allineate agli standard federali, che applicano nel proprio ambito di competenza. Gli standard federali determinanti sono le norme e i requisiti tecnici per la protezione di base dell'informatica nella Confederazione nonché per la protezione delle informazioni classificate. I Cantoni non sono tenuti ad attuare un sistema di gestione della sicurezza delle informazioni (SGSI).

*d. Gestione della sicurezza delle informazioni*

Tutte le unità amministrative devono essere tenute ad attuare la propria sicurezza delle informazioni tramite un sistema di gestione della sicurezza delle informazioni (SGSI). Un SGSI è uno strumento di gestione e serve alla pianificazione, all'attuazione, alla verifica e al miglioramento sistematici della sicurezza delle informazioni. Esso comprende le prescrizioni e le procedure necessarie a tal fine e mostra a chi, all'interno dell'organizzazione, sono riconducibili quali compiti, competenze e responsabilità. Con «SGSI» si rinvia implicitamente alla norma ISO/IEC 27001, che vale quale standard sia nel settore privato sia, sempre più, nelle amministrazioni pubbliche. Varie unità amministrative e vari dipartimenti hanno già deciso di attuare la propria sicurezza delle informazioni sistematica-

[5] RS **120.73**
[6] RS **510.411**
[7] RS **172.010.1**

mente secondo la norma ISO. Alcuni di essi sono certificati ufficialmente. Alle unità amministrative l'OSIn chiede unicamente un SGSI *light*: ciò significa che non devono attuare la norma ISO completa, ma soltanto i processi di gestione più importanti, che figurano nell'OSIn. Non è richiesta una certificazione esterna. Le unità amministrative e i dipartimenti possono tuttavia fissare un livello di ambizione più elevato.

*e. Protezione di informazioni classificate e sicurezza informatica*

I criteri per la classificazione delle informazioni e per l'attribuzione dei mezzi informatici ai vari livelli di sicurezza vengono allineati ai parametri della gestione dei rischi della Confederazione. Per loro stessa natura, questi criteri sono vaghi e devono essere interpretati. Per l'attuazione vengono realizzati ausili. In futuro la Confederazione procederà a un numero minore di classificazioni.

Per quanto riguarda le misure concrete adottate per la protezione delle informazioni classificate e per la garanzia della sicurezza informatica, l'OSIn riprende in gran parte le normative esistenti dell'OPrI e dell'OCiber. Le direttive dettagliate, compresi i requisiti tecnici, attualmente mancanti, per il trattamento elettronico delle informazioni classificate, verranno probabilmente elaborate entro la fine del 2023 adeguandole, ove possibile e opportuno, a standard internazionali.

*f. Accreditamento in materia di sicurezza di mezzi informatici*

Ora l'OSIn introduce un obbligo di accreditamento per un numero limitato di sistemi d'informazione sensibili sotto il profilo della sicurezza nei quali vengono trattate informazioni classificate CONFIDENZIALE o SEGRETO (p. es. un'applicazione per la videocomunicazione confidenziale). L'OSIn colma così una lacuna che oggi rende difficile la collaborazione internazionale nell'ambito della sicurezza. Un accreditamento di sicurezza viene richiesto all'estero e nella cooperazione internazionale se si intende trattare informazioni protette di un'autorità (o di uno Stato) in un sistema di un'altra autorità (o di un altro Stato). Un accreditamento dimostra che il sistema ricevente soddisfa i requisiti di sicurezza prestabiliti e che i rischi residui sono sostenibili secondo lo stato della tecnica. Se non può essere concesso un accreditamento di sicurezza, il Consiglio federale deve valutare i rischi residui e decidere in merito all'impiego del mezzo informatico.

*g. Sicurezza delle persone*

L'assunzione della responsabilità dei rischi per la sicurezza riferiti a persone è un compito direttivo permanente. Introdotto ora con la LSIn, l'articolo 20*a* della legge del 24 marzo 2000[8] sul personale federale (LPers) consente alle unità amministrative, se necessario per tutelare i propri interessi, di esigere dai candidati a un impiego e dagli impiegati che presentino un estratto del casellario giudiziale e del registro delle esecuzioni. La prassi ha mostrato che, dopo avere superato un controllo di sicurezza relativo alle persone (CSP), è piuttosto raro che si affronti di nuovo la questione dei rischi per la sicurezza riferiti a persone. Ai sensi di una gestione a posteriori (cosiddetta *«aftercare»*) usuale a livello internazionale, i collaboratori che sono stati sottoposti a CSP devono pertanto notificare al proprio datore di lavoro circostanze derivanti dal proprio contesto privato e professionale che possono minacciare la sicurezza (p. es. ricattabilità a causa di un forte indebitamento nel casinò). La gestione di un rischio eventualmente accresciuto è compito del datore di lavoro. Questi può esigere dai collaboratori anche durante il termine previsto per la ripetizione del CSP estratti ai sensi dell'articolo 20*a* LPers. A seconda del singolo caso una siffatta notifica può anche portare a una ripetizione straordinaria del CSP.

*h. Responsabili della sicurezza e incaricati della sicurezza delle informazioni*

Una novità importante nell'OSIn riguarda le direzioni. Nell'ordinanza verranno assegnati loro compiti, competenze e responsabilità concreti nell'ambito della sicurezza delle informazioni che, in caso di bisogno, possono delegare a un membro della loro direzione (responsabili della sicurezza). I responsabili della sicurezza vigilano sul SGSI dell'ufficio e prendono tutte le decisioni importanti nel suddetto ambito. Le attività di vigilanza operativa sono compito degli incaricati della sicurezza delle informazioni di cui all'articolo 37. Con l'OSIn gli odierni ruoli degli «incaricati della sicurezza informatica» e degli «incaricati della protezione delle informazioni» vengono uniti nel nuovo ruolo degli «incaricati della sicurezza delle informazioni». I loro compiti verranno precisati di conseguenza e integrati dall'esercizio del SGSI.

Ai sensi degli articoli 37–38 e 41–42 LOGA, i dipartimenti sono responsabili della direzione, del coordinamento e della vigilanza della sicurezza delle informazioni nel dipartimento stesso. Essi

[8] RS **172.220.1**

definiscono in particolare la politica in materia di sicurezza delle informazioni e l'organizzazione della sicurezza del dipartimento. La responsabilità operativa per la sicurezza va assunta dal segretario generale, sempreché il capo di dipartimento non decida altrimenti. Come è avvenuto finora, gli incaricati della sicurezza delle informazioni svolgono i compiti di coordinamento e di vigilanza operativi (cfr. l'art. 81 LSIn).

*i. Servizio specializzato della Confederazione per la sicurezza delle informazioni*

L'articolo 83 LSIn istituisce un servizio specializzato della Confederazione per la sicurezza delle informazioni. L'OSIn ne definisce i compiti per l'ambito di competenza del Consiglio federale. Fondandosi sull'articolo 85 LSIn, il servizio specializzato deciderà le necessarie direttive organizzative, tecniche, edili e riguardanti il personale per garantire la sicurezza delle informazioni secondo lo stato della tecnica. Nell'ambito delle relazioni internazionali assolverà il ruolo di autorità di sicurezza nazionale della Svizzera (cfr. in merito il messaggio LSIn, n. 5.2. e l'art. 41 cpv. 3 OSIn).

### 3.4 Modifica dell'ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

Con gli articoli 24–26 LSIn è stata creata la base legale formale necessaria al trattamento di dati personali degni di particolare protezione o di profili della personalità nei sistemi di gestione delle identità della Confederazione. Nella modifica, figurante nel presente rapporto esplicativo, dell'attuale OIAM si procede soprattutto ad adeguamenti formali e tecnici. Nondimeno, il campo d'applicazione dell'OIAM viene ora esteso alle unità amministrative dell'Amministrazione federale decentralizzata.

### 3.5 Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)

*a. In generale*

Con l'adozione della LSIn il legislatore ha trasposto in essa il disciplinamento dei CSP dalla legge federale del 21 marzo 1997[9] sulle misure per la salvaguardia della sicurezza interna (LMSI). Nel contempo le disposizioni legali sono state adeguate alle odierne esigenze della sicurezza delle informazioni. Per motivi inerenti ai controlli al di fuori della sicurezza delle informazioni (p.es. la lotta alla corruzione) sono state create basi in altre leggi. Questo ammodernamento del diritto dei CSP deve anche servire a ridurre al minimo indispensabile l'impiego dei controlli necessari all'identificazione di rischi notevoli per la Confederazione. Si persegue una riduzione di almeno il 30 per cento, così che i CSP possano essere gestiti in tempo utile con le risorse esistenti. Le principali modifiche al quadro giuridico dei CSP sono contenute nella stessa LSIn.

*b. Oggetto*

La nuova ordinanza sui controlli di sicurezza relativi alle persone (OCSP) riassume in un unico atto normativo le disposizioni esecutive concernenti i vari controlli di sicurezza riferiti a persone. Essa sostituisce l'attuale ordinanza del 4 marzo 2011[10] sui controlli di sicurezza relativi alle persone (OCSP), l'attuale ordinanza del 9 giugno 2006[11] sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari (OCSPN) e tutte le altre ordinanze dipartimentali sui controlli di sicurezza relativi alle persone[12].

Sotto il profilo materiale l'ordinanza disciplina sia i CSP secondo la LSIn, sia tutti gli altri controlli e tutte le altre valutazioni e verifiche che, pur non essendo previsti dalla LSIn, vengono però effettuati in base alla procedura dei CSP secondo quest'ultima. Tuttavia, a prescindere dalla loro denominazione o dal motivo del controllo, in tutti i controlli si valuta sempre se la persona interessata è affidabile nell'esercizio dell'attività di riferimento. All'interno degli stessi livelli di controllo vengono raccolti gli stessi dati e si applica lo stesso metodo di valutazione.

*c. Snellimento dei motivi del controllo*

La nuova normativa limita i motivi per l'esecuzione di CSP. Le funzioni attribuite al massimo livello di controllo, il controllo di sicurezza ampliato, devono rimanere l'eccezione. Vi è tuttavia il rischio che, in pratica, la soglia giuridica per i controlli venga abbassata se gli uffici non dispongono di alcun

[9] RS **120**
[10] RS **120.4**
[11] RS **732.143.3**
[12] RS **120.421**–**120.427**

altro strumento per verificare l'affidabilità dei loro dipendenti. Il nuovo articolo 20*a* LPers offre a tal fine ai datori di lavoro i mezzi appropriati.

*d. Elenchi delle funzioni*

Al fine di tenere il numero dei controlli entro il limite auspicato, nell'allestire e nell'aggiornare gli elenchi delle funzioni nei quali figurano le funzioni da controllare occorre controllare meglio di oggi la legalità delle iscrizioni. L'intento è quindi che il DDPS gestisca a livello centrale gli elenchi delle funzioni e che li aggiorni costantemente su richiesta dei dipartimenti e della Cancelleria federale (CaF).

Gli elenchi delle funzioni per i quali è necessario un CSP secondo la LSIn sono problematici dal punto di vista della sicurezza delle informazioni. Essi forniscono una panoramica dell'insieme delle funzioni svolte dall'Amministrazione e dall'esercito che hanno accesso a informazioni classificate o che gestiscono o amministrano sistemi critici della Confederazione. Sebbene gli elenchi [delle funzioni] non contengano alcun nome dei detentori delle funzioni, nell'era dei media sociali è semplice per un potenziale aggressore collegare una funzione a un nome ottenendo così un obiettivo di spionaggio o di sabotaggio. Nell'ambito dell'esercito gli elenchi delle funzioni dettagliati possono inoltre consentire di trarre conclusioni sulla sua organizzazione di dettaglio, non pubblicata. Pertanto, fondandosi sull'articolo 6 della legge sulle pubblicazioni ufficiali del 18 giugno 2004[13] (LPubb), non vanno pubblicati gli elenchi delle funzioni che contengono le funzioni da controllare secondo la LSIn. Per gli stessi motivi, anche gli elenchi delle funzioni secondo la legge del 23 marzo 2007[14] sull'approvvigionamento elettrico (LAEl) non vengono pubblicati. Per contro, devono continuare a essere pubblicati gli elenchi delle funzioni che vengono sottoposte a un controllo per proteggere dalla corruzione o da un danno reputazionale.

Gli elenchi delle funzioni saranno stilati soltanto a partire dall'avvio della consultazione sul diritto d'esecuzione relativo alla LSIn. In primo luogo, occorre garantire che i criteri di controllo siano ampiamente accettati. Si tratta infatti di varie migliaia di iscrizioni potenziali che devono essere verificate prima di essere inserite negli elenchi delle funzioni definitivi. Informazioni dettagliate sull'onere per i CSP saranno pertanto disponibili soltanto dopo il termine della consultazione.

### 3.6 Ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz)

*a. In generale*

La LSIn (cfr. gli artt. 49–72 LSIn) introduce la cosiddetta procedura di sicurezza relativa alle aziende (PSA). La PSA si occupa della tutela della sicurezza delle informazioni nell'ambito dell'assegnazione di mandati sensibili sotto il profilo della sicurezza da parte delle autorità federali ad aziende che non sottostanno direttamente alla loro vigilanza. La PSA serve a verificare l'affidabilità delle aziende alle quali si intende affidare un mandato. Le aziende che sono sotto l'influenza di servizi d'informazione esteri non devono ottenere l'accesso a informazioni sensibili sotto il profilo della sicurezza o a mezzi informatici critici della Confederazione. A seguito della nuova procedura di sicurezza relativa alle aziende sarà abrogato il metodo di gestione del rischio per ridurre lo spionaggio da parte dei servizi di intelligence. La PSA consente inoltre di controllare e imporre l'attuazione della sicurezza delle informazioni durante l'esecuzione del mandato.

*b. Oggetto e campo d'applicazione*

La nuova ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz) disciplina i dettagli della procedura e sostituisce l'attuale ordinanza sulla tutela del segreto del 29 agosto 1990[15], limitata a mandati con contenuto classificato dal punto di vista militare. L'OPSAz si applica all'insieme delle autorità e delle organizzazioni che rientrano nell'ambito di applicazione della LSIn. L'OPSAz si applica alle unità amministrative dell'Amministrazione federale decentralizzata soltanto se esse rientrano anche nel campo d'applicazione dell'OSIn (cfr. il n. 3.3 lett. b).

*c. Acquisti assoggettati*

Nell'ordinanza vengono definiti gli acquisti per i quali la procedura deve essere eseguita in ogni caso. Sono interessati i mandati nei quali vengono rese accessibili informazioni classificate SEGRETO nonché gli acquisti di sistemi sensibili nei quali vengono trattate informazioni classificate CONFIDENZIALE di più organizzazioni o che vengono impiegati in più uffici e dipartimenti. Per

[13] RS **170.512**
[14] RS **734.7**
[15] RS **510.413**

tutti gli altri acquisti, il servizio specializzato competente per l'esecuzione della procedura di sicurezza relativa alle aziende (servizio specializzato PSA) valuterà con il servizio che assegna il mandato (mandante) se l'esecuzione della procedura è opportuna.

*d. Armonizzazione con il diritto in materia di acquisti pubblici*

Come la stessa LSIn, la nuova ordinanza presenta numerose interfacce con la nuova legislazione della Confederazione in materia di acquisti pubblici. Durante l'elaborazione dell'avamprogetto esse sono state esaminate e rettificate dettagliatamente in collaborazione con rappresentanti degli uffici specializzati. La corretta esecuzione della PSA presuppone inoltre una stretta collaborazione tra il mandante, il servizio incaricato degli acquisti (servizio d'acquisto) e il competente servizio specializzato PSA. Tale collaborazione deve avere luogo quanto prima possibile nel processo d'acquisto. In tal modo è possibile individuare e ridurre precocemente i rischi legati agli acquisti.

### 3.7 Compatibilità tra compiti e finanze

Con la LSIn e le sue ordinanze d'esecuzione vengono create le basi per un miglioramento duraturo della sicurezza delle informazioni dell'Amministrazione federale e dell'esercito. In tale contesto ci si concentra sulle informazioni e sui mezzi informatici più critici. L'introduzione del SGSI assume un significato cruciale a tale scopo: esso connette, gestisce e verifica tutte le misure e tutti i processi del nuovo diritto. Una gestione efficiente della sicurezza delle informazioni migliora la sicurezza delle informazioni in modo più efficace, economico e duraturo rispetto a puri investimenti in misure tecniche.

Il livello di ambizione è stato definito garantendo un uso rispettoso delle risorse sia per il SGSI, sia per le altre misure. Nel complesso, quindi, le ripercussioni in materia di personale e le ripercussioni finanziarie della LSIn e delle sue ordinanze risulteranno minime. Spetta alle unità amministrative e ai dipartimenti decidere se per il proprio ambito di competenza vogliono avere una sicurezza delle informazioni più elevata e mettere a disposizione le risorse corrispondenti.

### 3.8 Attuazione

L'entrata in vigore della LSIn e delle sue ordinanze è prevista per la metà del 2023. Sia la LSIn (cfr. l'art. 90 LSIn) sia le sue ordinanze d'esecuzione (cfr. l'art. 48 OSIn, l'art. 38 OCSP e l'art. 25 OPSAz) prevedono termini transitori idonei a un passaggio riuscito al nuovo diritto.

Prima dell'entrata in vigore della LSIn e delle sue ordinanze devono essere elaborate o aggiornate ulteriori direttive, tra cui:

- direttive sulla gestione della sicurezza delle informazioni nella Confederazione (cfr. l'art. 15 OSIn);
- cataloghi di classificazione (cfr. l'art. 17 cpv. 2 e 3 OSIn);
- direttive sulla protezione di informazioni classificate (cfr. l'art. 21 cpv. 1 OSIn);
- direttive sull'accreditamento in materia di sicurezza di mezzi informatici (cfr. l'art. 23 cpv. 6 OSIn);
- direttive sui requisiti minimi per i relativi livelli di sicurezza della sicurezza informatica (cfr. l'art. 29 cpv. 1 OSIn);
- direttive sulla protezione fisica e sulle zone di sicurezza (cfr. gli art. 34 e 35 OSIn);
- gli elenchi delle funzioni per i controlli di sicurezza relativi alle persone (cfr. l'art. 3 OCSP).

Oltre all'emanazione di direttive giuridiche o tecniche devono essere adempiuti tre ulteriori presupposti:

- il servizio specializzato della Confederazione per la sicurezza delle informazioni (cfr. l'art. 83 LSIn) deve essere istituito e messo in funzione. Esso assumerà compiti e risorse dall'attuale ambito di competenza della Segreteria generale del DDPS (SG-DDPS) (Digitalizzazione e cibersicurezza DDPS [DCS DDPS]) e della Segreteria generale del DFF (Centro nazionale per la cibersicurezza [NCSC]). Il 18 maggio 2022 il Consiglio federale ha deciso di trasformare il NCSC in un ufficio federale. A tale scopo ha incaricato il DFF di elaborare entro la fine del 2022 proposte concernenti la struttura del nuovo ufficio e il dipartimento a cui sarà aggregato. Nel contempo verranno chiarite varie questioni sulle strutture di politica di sicurezza della Confederazione, incluse quelle nel settore ciber. L'esito di questi lavori in corso è determinante per

l’insediamento del servizio specializzato della Confederazione per la sicurezza delle informazioni e delle sue risorse. Il Consiglio federale deciderà in merito all’assegnazione amministrativa del servizio specializzato soltanto dopo la consultazione;

- gli incaricati della sicurezza delle informazioni e altri detentori dei ruoli devono ricevere una formazione;
- più sistemi d’informazione devono essere adeguati o introdotti. Ciò concerne in particolare SIBAD, il sistema informatizzato dei CSP, e i suoi sistemi circostanti, nonché FABS, il futuro sistema d’informazione della procedura di sicurezza relativa alle aziende. Per un esercizio efficace del SGSI da parte degli uffici la Confederazione lavora all’acquisizione e all’introduzione di un’applicazione SGSI standardizzata con la quale verranno digitalizzati i compiti e i processi dell’ordinanza sulla sicurezza delle informazioni. L’applicazione SGSI è intesa essere pronta per l’introduzione e l’utilizzo da parte degli uffici e dei dipartimenti entro la fine del 2024.

I lavori di attuazione verranno coordinati con le altre autorità federali e con i Cantoni. Se necessario, il Consiglio federale deciderà una messa in vigore scaglionata della LSIn e delle sue ordinanze.

# 4 Commento a singoli articoli

## 4.1 Ordinanza sulla sicurezza delle informazioni (OSIn)

### *Ingresso*

L'ingresso rimanda a tutte le norme di legge che conferiscono al Consiglio federale una competenza normativa nell'ambito dell'OSIn.

### *Sezione 1: Disposizioni generali*

### *Art. 1 Oggetto*

La nozione di «sicurezza delle informazioni» comprende la sicurezza di tutte le informazioni, inclusi i dati personali secondo la legislazione sulla protezione dei dati, della quale sono responsabili l'Amministrazione federale e l'esercito. L'OSIn disciplina i compiti, le responsabilità e le competenze nonché le procedure per garantire la sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito che sono necessari nell'ambito della gestione della sicurezza delle informazioni, della protezione di informazioni classificate, della sicurezza informatica e delle misure adottate per la sicurezza personale e fisica. Come nella stessa LSIn (cfr. messaggio LSIn, commento ad art. 1 LSIn), nell'OSIn non viene definito il termine «informazione». Quando si intendono dati personali ai sensi della legislazione sulla protezione dei dati, si utilizza ogni volta il termine «dati personali».

Il rapporto tra la LSIn e la legge del 19 giugno 1992[16] sulla protezione dei dati (LPD) è illustrato dettagliatamente nel messaggio concernente la LSIn (cfr. messaggio LSIn, n. 1.2.3 pag. 2589). Gli organi di sicurezza secondo gli articoli 36 segg. OSIn assicureranno il coordinamento con i competenti consulenti per la protezione dei dati nell'ambito del SGSI.

### *Art. 2 Campo d'applicazione*

Capoversi 1–5: nell'ambito di una lista positiva viene indicato a quali autorità e organizzazioni assoggettate (cfr. messaggio LSIn, commento ad art. 2 LSIn) e a quali condizioni si applica questa ordinanza.

Per l'applicazione della LSIn e dell'OSIn alle unità amministrative dell'Amministrazione federale decentralizzata secondo l'articolo 7*a* OLOGA nonché alle organizzazioni secondo l'articolo 2 capoverso 4 LOGA alle quali sono attribuiti compiti amministrativi ma che sono al di fuori dell'Amministrazione federale cfr. il numero 3.3 lettera b.

Questa ordinanza si applica, per analogia, alle autorità assoggettate di cui all'articolo 2 capoverso 1 lettere a nonché c–e LSIn (Assemblea federale, tribunali della Confederazione, Ministero pubblico della Confederazione e la sua Autorità di vigilanza nonché la Banca nazionale svizzera), sempreché suddette autorità non emanino proprie disposizioni esecutive. Se esse si avvalgono di tale possibilità, sono esentate dall'OSIn (ma non dalla LSIn).

Capoverso 6: quando i Cantoni trattano informazioni classificate della Confederazione, si applicano le disposizioni del capoverso 4 di questa ordinanza. Se essi accedono ai suoi mezzi informatici, si applicano loro le disposizioni riguardanti l'attribuzione ai livelli di sicurezza (art. 28), le misure di sicurezza (art. 29), la sicurezza durante l'esercizio (art. 30) e le misure per la protezione fisica (art. 35). I Cantoni possono tuttavia esentarsi dalle direttive del diritto federale se garantiscono di propria iniziativa una sicurezza delle informazioni equivalente. Ciò presuppone che essi emanino proprie prescrizioni di sicurezza, allineate agli standard federali, che applicano nel proprio ambito di competenza. Gli standard federali determinanti sono le norme e i requisiti tecnici per la protezione di base dell'informatica nella Confederazione nonché per la protezione delle informazioni classificate. I Cantoni non sono tenuti ad attuare un sistema di gestione della sicurezza delle informazioni (SGSI) secondo gli articoli 5 segg.

Vi è una «sicurezza delle informazioni equivalente» se misure di sicurezza diverse da quelle previste nell'OSIn, secondo lo stato della tecnica conformemente all'articolo 85 capoverso 1 LSIn producono un effetto comparabile e per lo meno altrettanto elevato o forte. I Cantoni valutano in primo luogo a propria discrezione se vi è una sicurezza delle informazioni equivalente.

[16] RS **235.1**

Nel termine «Cantoni», oltre ai Cantoni stessi ai sensi dell'articolo 3 della Costituzione federale (Cost.)[17], sono compresi enti, istituti o fondazioni di diritto pubblico assoggettati al diritto amministrativo del rispettivo Cantone. Da parte loro, i Cantoni devono valutare caso per caso se un'organizzazione o un istituto (ad es. un ospedale, una centrale elettrica o anche un istituto finanziario) è da considerarsi un «Cantone» ai sensi della LSIn o dell'OSIn. Se un Cantone non rientra nel campo d'applicazione della LSIn viene trattato come «terzo» ai sensi dell'articolo 9 LSIn (cfr. commento ad art 10).

Capoverso 6 lettera b: con «accesso a mezzi informatici» si intendono tutti i tipi di accessi tecnici da parte dei Cantoni ai mezzi informatici della Confederazione. La questione dell'accesso deve essere chiarita in ogni singolo caso. In ultima analisi, è la Confederazione a decidere se vi è un accesso.

### *Sezione 2: Principi*

### *Art. 3 Obiettivi in materia di sicurezza*

I mezzi informatici delle organizzazioni che sono assoggettate all'OSIn presentano sempre più interfacce tecniche comuni. In virtù di ciò i rischi o le minacce per la singola organizzazione o i rispettivi fornitori non possono essere considerati separatamente. La sicurezza delle informazioni è necessariamente un compito interconnesso che richiede un obiettivo comune e una procedura coordinata.

Capoverso 1: il Consiglio federale si adopera affinché la protezione di informazioni e mezzi informatici sia garantita secondo un approccio basato sul rischio. Oggi non basta più attuare la sicurezza semplicemente in base a una lista di controllo. I responsabili sono tenuti a esercitare una gestione del rischio attiva, a conoscere le minacce alla sicurezza delle informazioni e le loro potenziali ripercussioni sulle attività, ad adeguare l'onere per minimizzare i rischi alle loro dimensioni ovvero a concentrarsi sui rischi maggiori e ad applicare le misure più efficaci per minimizzare i rischi. Con l'approccio basato sul rischio occorre focalizzarsi non soltanto sui rischi (effetti negativi), ma anche sulle possibilità e opportunità (effetti positivi) di nuove idee, applicazioni o tecnologie. Con «resilienza» si intende la resistenza di un'organizzazione e la rapida ripresa del normale esercizio dopo un incidente legato alla sicurezza.

### *Art. 4 Responsabilità*

Capoversi 1 e 2: conformemente all'articolo 45 LOGA i direttori degli aggruppamenti e degli uffici sono responsabili nei confronti dei propri superiori per la direzione delle unità amministrative subordinate a loro nonché per l'adempimento dei compiti loro affidati. Ciò include la responsabilità per la sicurezza delle informazioni. Oggi il NCSC definisce direttive minime in materia di sicurezza delle informazioni che servono alla protezione dell'intera Amministrazione federale e che le unità amministrative, con margine di manovra limitato, devono attuare. Dette direttive non esentano tuttavia le unità amministrative dalla loro responsabilità di valutare costantemente i rischi e, se necessario, di adottare misure più estese. Riguardo alla competenza dei dipartimenti di suddividere diversamente taluni compiti, cfr. commento ad articolo 39 capoverso 3.

Capoverso 3: nel trattamento di informazioni o nell'utilizzo dei mezzi informatici della Confederazione i collaboratori devono rispettare le pertinenti prescrizioni di comportamento. L'assunzione di questa responsabilità presuppone che essi siano istruiti e formati di conseguenza (cfr. commento ad art. 4 cpv. 4 e ad art. 11).

Con «collaboratori dell'Amministrazione federale» si intendono i collaboratori interni ed esterni assoggettati alla facoltà di emanare istruzioni della Confederazione: i collaboratori «interni» sono impiegati della Confederazione ai sensi della LPers; i collaboratori «esterni» sono invece persone che sono impiegate mediante un contratto di fornitura di personale a prestito. Non sono per contro collaboratori della Confederazione persone esercitanti un'attività autonoma o collaboratori di imprese che, ad esempio, in base a un rapporto contrattuale operano a livello di consulenza per la Confederazione o le forniscono prestazioni di servizio o in natura (quali sviluppo di software, potenziamento della rete, costruzione di un locale dei server, assunzione della direzione del progetto ecc.). Siffatte persone sono considerate «terzi», cfr. commento ad articolo 10 OSIn. Nel caso di «terzi», la corretta manipolazione degli oggetti da proteggere deve essere assicurata, se del caso, mediante relativi contratti ai sensi dell'articolo 9 LSIn.

[17] RS **101**

Capoverso 4: anche nell'ambito della sicurezza delle informazioni i superiori di tutti i livelli hanno la responsabilità per l'istruzione e la formazione conformi alla funzione e improntate alla prassi dei propri collaboratori nonché per la verifica del rispetto delle prescrizioni. Incombe così ai superiori spiegare ai propri collaboratori in modo pratico come devono gestire le informazioni protette, renderli attenti all'impiego coerente e conforme alle direttive di software di crittografia o assicurarsi che frequentino le formazioni proposte. Riguardo alla responsabilità delle unità amministrative, cfr. commento ad articolo 11.

### *Sezione 3: Gestione della sicurezza delle informazioni*

Gli articoli 5–15 OSIn definiscono i requisiti minimi per la gestione della sicurezza delle informazioni nell'Amministrazione federale e nell'esercito. Definiscono per i compiti fondamentali della sicurezza delle informazioni le rispettive competenze degli uffici, dei dipartimenti e del servizio specializzato della Confederazione per la sicurezza delle informazioni. Quest'ultimo emanerà a tal fine direttive inerenti al trattamento (cfr. l'art. 21 cpv. 1 lett. c) o istruzioni generali e astratte (cfr. l'art. 29 cpv. 1), che considerano l'approccio basato sul rischio.

### *Art. 5 Sistema di gestione della sicurezza delle informazioni*

Capoverso 1: un SGSI comprende procedure e norme che illustrano com'è organizzata la sicurezza delle informazioni in un sistema e rende visibile quali compiti, competenze e responsabilità sono riconducibili a pertinenti persone. Con il termine «SGSI» si rinvia implicitamente alla norma ISO/IEC 27001, che vale quale standard sia nel settore privato sia, sempre più, nelle amministrazioni pubbliche. Alle unità amministrative si chiede però semplicemente un SGSI *light*, vale a dire che non devono attuare l'intera norma ISO, ma soltanto i processi di gestione più importanti definiti nell'OSIn, che saranno precisati da future direttive. Non è richiesta una certificazione esterna. Le unità amministrative e i dipartimenti sono tuttavia liberi di fissare un livello di ambizione più elevato.

Mentre i responsabili della sicurezza delle unità amministrative (cfr. l'art. 36) assicurano lo sviluppo, il funzionamento, la verifica e i miglioramenti continui del SGSI, l'esercizio vero e proprio del SGSI incombe all'incaricato della sicurezza delle informazioni dell'unità amministrativa (cfr. l'art. 37 cpv. 2 lett. a) su mandato dei detti responsabili. Secondo l'articolo 48 capoverso 4, un SGSI deve essere creato entro tre anni al massimo dall'entrata in vigore dell'OSIn.

Capoverso 2: lo scopo di un SGSI è di gestire e di migliorare la sicurezza delle informazioni nell'unità amministrativa. A tal fine occorrono obiettivi concreti in base ai quali la direzione dell'ufficio può valutare se il SGSI produce gli effetti desiderati Questa definizione e misurazione di obiettivi annuale è un compito direttivo della direzione dell'ufficio e deve essere distinta dall'elaborazione del piano annuale dei controlli e degli audit.

Capoverso 3: per garantire una certa obiettività e comparabilità nella valutazione dell'attuazione e dell'efficacia del SGSI, è richiesta una verifica effettuata periodicamente dal dipartimento o da un servizio indipendente dall'Ufficio. Tale verifica indipendente del SGSI crea fiducia per gli altri uffici e, allo stesso tempo, assicura i miglioramenti continui della sicurezza nell'ufficio stesso.

Anche se la periodicità di tre anni si basa sul ciclo di certificazione ufficiale della norma ISO, l'entità della verifica obbligatoria è tuttavia nettamente meno ambiziosa di quella prevista dallo Standard ISO: non si richiede necessariamente un audit formale ai sensi della norma ISO, sebbene tale audit andrebbe accolto favorevolmente. A seconda del mandato è inoltre possibile verificare l'intero SGSI o soltanto determinate sue parti. L'unità amministrativa interessata ha il potere decisionale sulla scelta di un servizio di controllo indipendente. Siffatti controlli possono essere effettuati dalle strutture di vigilanza interne dei dipartimenti o da un'impresa esterna (cfr. le spiegazioni nel messaggio LSIn, pag. 2631). È ipotizzabile anche l'impiego di un pool di auditori SGSI provenienti dalle unità amministrative di un dipartimento o della Confederazione. Il continuo processo di miglioramento è fondamentale per garantire la sicurezza delle informazioni. Si tiene conto di tale processo mediante siffatte verifiche.

Capoverso 4: esso evidenzia lo stretto legame tra il SGSI e la gestione dei rischi della Confederazione, la gestione della continuità operativa e la gestione delle crisi. Si tratta di compiti di gestione che esulano dal campo d'applicazione dell'OSIn, ma che le unità amministrative devono allineare e coordinare strettamente tra loro.

### *Art. 6 Cura delle basi legali e degli obblighi contrattuali*

Capoverso 1: un registro delle basi legali e degli obblighi contrattuali determinanti nel proprio settore di competenza nell'ambito della sicurezza delle informazioni serve a dimostrare il rispetto delle basi legali rilevanti che, ad esempio, occorre controllare nel contesto della misurazione dell'annuale raggiungimento degli obiettivi del SGSI (cfr. l'art. 5 cpv. 2 o la verifica SGSI secondo l'art. 5 cpv. 3). A causa delle crescenti catene di approvvigionamento nell'ambito della sicurezza delle informazioni, è imprescindibile disporre di un riepilogo degli obblighi da assolvere e dei diritti da rivendicare e, non da ultimo, favorire lo sfruttamento delle sinergie di altri contratti esistenti.

Capoverso 2: il servizio specializzato della Confederazione per la sicurezza delle informazioni ha carattere consultivo vincolante (obbligo di consultazione), ma non ha alcuna facoltà di impartire istruzioni sul piano del contenuto. Le valutazioni e le stime di un servizio specializzato della Confederazione assumono tuttavia un peso rilevante. Le deroghe dovrebbero essere sempre ben motivate e, in particolare, equivalenti. Questo obbligo di consultazione è retto da direttive rilevanti per la sicurezza (p. es. istruzioni e direttive) o progetti (p. es. progetti IT rilevanti sotto il profilo della sicurezza) delle unità amministrative o dei dipartimenti.

### *Art. 7 Inventariazione degli oggetti da proteggere*

Capoverso 1: un inventario contiene un elenco di tutti gli oggetti da proteggere di cui all'articolo 7 capoverso 2 in un dato momento (cosiddetta lista dell'inventario).

Capoverso 2: oggi nell'OCiber si trovano soltanto gli «oggetti informatici da proteggere» (cfr. l'art. 3 lett. h OCiber), che sono coperti dalla lettera b. Tuttavia, le informazioni non vengono sempre elaborate in un unico sistema d'informazione dedicato. Questo è il caso, ad esempio, quando un compito viene svolto nell'ambiente informatico generale della Confederazione o quando le informazioni vengono elaborate in un cloud esterno. Con l'oggetto da proteggere «informazioni» ai sensi della lettera a si esclude pertanto la dipendenza da un determinato mezzo informatico e si valuta soltanto la protezione delle informazioni elaborate per l'adempimento del compito. In linea di principio, però, vengono utilizzati gli stessi criteri e metodi per valutare la necessità di protezione degli oggetti informatici da proteggere. Con la nozione di «compito della Confederazione» non si sottintende ogni compito, bensì importanti processi operativi di un'unità amministrativa. Le direttive del servizio specializzato della Confederazione per la sicurezza dell'informazione (cfr. l'art. 15) preciseranno questo aspetto.

Capoverso 3: soltanto una lista dell'inventario aggiornata può fornire la prova costante di tutte le informazioni concernenti gli oggetti da proteggere di cui alle lettere a–g.

Capoverso 3 lettera c: la possibilità dell'utilizzo condiviso dei relativi oggetti da proteggere (cfr. lett. e) fa riferimento al principio *«once only»*. Le unità amministrative decidono a propria discrezione quali oggetti da proteggere vengono condivisi con altre unità amministrative.

Capoverso 3 lettera d: da un lato, il riepilogo dei vincoli contrattuali con terzi (cfr. commento ad art. 10 cpv. 1 OSIn), ad esempio con fornitori di tecnologie dell'informazione, serve a una gestione dei fornitori funzionante e consente di riconoscere precocemente le eventuali dipendenze della Confederazione dai fornitori (incl. valutazione del pericolo di grandi rischi). Dall'altro, esso permette di identificare rischi che per il tramite di questi fornitori possono avere ripercussioni sulla Confederazione.

Capoverso 3 lettera f: riguardo ai rischi residui, cfr. commento ad articolo 9.

Capoverso 3 lettera g: cfr. commento ad articolo 14 in combinazione con l'articolo 6 capoversi 2 e 3.

### *Art. 8 Gestione dei rischi*

Capoverso 1: la valutazione dei rischi è una delle basi per un'efficace gestione dei rischi e, di conseguenza, per una sicurezza delle informazioni funzionale ed economica (cfr. le spiegazioni nel messaggio LSIn, pag. 2631 seg.). Le direttive sulla protezione di base TIC della Confederazione offrono una protezione in funzione dei rischi contro un gran numero di minacce. Servono alla sicurezza delle informazioni in rete della Confederazione e devono essere rispettate. Consentono una manutenzione poco onerosa, dal punto di vista della sicurezza, di mezzi informatici che non sono particolarmente sensibili sotto il profilo della sicurezza. In tal caso le unità amministrative non devono neanche eseguire valutazioni dei rischi complesse.

Va da sé che la valutazione dei rischi deve avvenire in modo «comprovabile». La comprovabilità non è legata a una forma determinata. In tal modo si intende rendere possibile, nel contesto della digitalizzazione, l'impiego di metodi di comprovabilità tecnologicamente neutri.

Capoverso 1 lettera a: in tale contesto, la valutazione dei rischi quanto alle loro ripercussioni sugli oggetti da proteggere (cfr. l'art. 7 cpv. 2) è anche assai tecnico-operativa e dipende dall'esigenza di confidenzialità, disponibilità, integrità e tracciabilità delle informazioni e del sistema informatico.

Capoverso 1 lettera b: il controllo dell'efficacia può ad esempio avvenire mediante test di penetrazione o la raccolta di indicatori rilevanti.

Capoverso 1 lettera c: cfr. commento alla gestione delle direttive di cui all'articolo 6.

Capoverso 1 lettera d: si richiede una decisione consapevole da parte del responsabile della sicurezza, vale a dire l'accettazione comprovabile di rischi residui sulla base di un accurato processo di analisi e di decisione.

Capoverso 3: fanno fede le istruzioni sulla politica della Confederazione in materia di gestione dei rischi nonché le direttive e i manuali correlati.

### *Art. 9 Autorizzazione ed elenco delle deroghe*

Con gestione delle deroghe si intende la gestione delle eccezioni alle vigenti direttive in materia di sicurezza delle informazioni. Come avviene oggi con il NCSC, fondandosi sull'articolo 85 LSIn con l'OSIn il servizio specializzato della Confederazione per la sicurezza delle informazioni stabilirà quali requisiti minimi devono essere soddisfatti nel settore della sicurezza. Se un'unità amministrativa non è in grado di soddisfarli può chiedere una deroga. Il servizio specializzato può delegare la decisione sull'autorizzazione di deroghe. Il servizio specializzato della Confederazione per la sicurezza delle informazioni, il dipartimento o una determinata persona in seno all'Ufficio può decidere in merito alla deroga. In linea di principio, per il tramite della subdelega di cui al capoverso 2 è possibile riprendere l'odierna procedura relativa alle deroghe autorizzate secondo le attuali disposizioni dell'OCiber.

### *Art. 10 Collaborazione con terzi*

Capoverso 1: sono considerati «terzi» ai sensi della LSIn tutte le autorità, organizzazioni e persone di diritto pubblico o privato che non sono né autorità né organizzazioni assoggettate e che, in linea di principio, agiscono indipendentemente da queste ultime due. Sono considerate terzi anche le unità amministrative decentralizzate, sempreché non rientrino nell'ambito di applicazione della LSIn (cfr. messaggio LSIn, pag. 2625 seg. e 2632), o talune organizzazioni che gestiscono infrastrutture critiche (art. 2 cpv. 5 LSIn).

Capoverso 3: le clausole in materia di sicurezza delle informazioni inserite nei contratti devono soddisfare i presupposti di cui all'articolo 9 LSIn (cfr. messaggio LSIn, commento all'art. 9).

### *Art. 11 Formazione e sensibilizzazione*

Se l'Amministrazione federale e l'esercito vogliono migliorare in modo duraturo la propria sicurezza, devono sensibilizzare e formare i propri collaboratori e militari in modo che siano in grado di riconoscere autonomamente pericoli e minacce, di reagirvi correttamente e di presentare le pertinenti notifiche di sicurezza.

Le unità amministrative garantiscono la formazione generale concernente la sicurezza delle informazioni (p. es. campagne di sensibilizzazione e di consapevolezza o corsi di formazione introduttivi a intervalli regolari) per tutto il personale, nonché i fondi necessari, il tempo e le relative risorse (cfr. l'art. 4 cpv. 4). Ciò contrariamente ai superiori diretti, che secondo questa disposizione sono responsabili della formazione adeguata alla funzione dei propri collaboratori (cfr. commento ad art. 4 cpv. 4).

### *Art. 12 Gestione degli incidenti*

Capoverso 1: le unità amministrative sono responsabili della gestione degli incidenti legati alla sicurezza e delle lacune nella sicurezza. Con «incidente legato alla sicurezza» si intende un evento in cui la sicurezza delle informazioni o le pertinenti direttive di sicurezza vengono violate o sono state violate. Anche un «quasi incidente legato alla sicurezza» è considerato un incidente legato alla sicurezza. Si è in presenza di un siffatto incidente se la sicurezza delle informazioni avrebbe potuto essere violata. È invece considerata una «lacuna nella sicurezza» un difetto in un mezzo

informatico il cui utilizzo può violare la sicurezza delle informazioni. È importante stabilire in anticipo chi, in caso di emergenza, decide in merito a misure immediate e chi deve essere consultato o informato nel caso si adottino siffatte decisioni. Chi detiene la competenza decisionale riguardo a misure immediate deve avere la necessaria comprensione degli effetti di una siffatta misura.

Capoverso 2: questa disposizione è conforme all'attuale diritto (cfr. l'art. 14 cpv. 4 lett. c OCiber), salvo che ora devono essere notificati anche i «quasi incidenti legati alla sicurezza».

Capoversi 3 e 6: con la disposizione potestativa si sottolinea che il servizio specializzato della Confederazione per la sicurezza delle informazioni può fornire sostegno ma, appunto, non è tenuto a farlo. Il sostegno di suddetto servizio specializzato viene fornito, in linea di massima, su richiesta delle unità amministrative o dei dipartimenti e, oltre che dal significato e dall'importanza dell'incidente, dipende dalle loro risorse (cfr. anche il cpv. 6).

Capoverso 4: cfr. i nuovi obblighi di notifica per violazioni della sicurezza dei dati ai sensi della futura legge sulla protezione dei dati (nLPD, cfr. l'art. 24), la cui messa in vigore è prevista per il 1° settembre 2023.

Capoverso 5 lettere b e d: cfr. il messaggio LSIn, commento ad articolo 17 o ad articolo 88 LSIn.

Capoverso 5 lettera e: l'importanza politica elevata dipende dagli interessi politici coinvolti. Deve essere verificato caso per caso assieme alla persona responsabile della sicurezza del rispettivo dipartimento (cfr. l'art. 39).

Capoverso 7: con «direzione» si intende la competenza decisionale operativa. Tuttavia, l'unità amministrativa o il dipartimento interessato rimane responsabile della sicurezza (cfr. commento ad art. 4). Se il servizio specializzato della Confederazione per la sicurezza delle informazioni assume la direzione, può, ad esempio, disporre autonomamente misure immediate o ricorrere all'impiego di specialisti (incl. terzi di cui all'art. 10) a scopo di sostegno. I relativi costi sono interamente a carico dell'unità amministrativa responsabile o del dipartimento e assunti d'intesa con essi. L'assunzione della direzione deve avvenire in modo comprovabile (cfr. commento ad art. 8 cpv. 1).

### *Art. 13 Pianificazione dei controlli e degli audit*

Attualmente la mancanza di controlli e di audit è una lacuna significativa nella gestione della sicurezza delle informazioni dell'Amministrazione federale e dell'esercito. Soltanto con audit adeguati le organizzazioni possono conoscere lo stato della sicurezza delle proprie informazioni, quali sono i rischi e quali sono le eventuali misure correttive necessarie (cfr. messaggio LSIn, pag. 2590). La disposizione prevede pertanto che le unità amministrative e i dipartimenti stabiliscano annualmente quali controlli e audit basati sul rischio effettueranno l'anno successivo e per quale motivo. Se si pianifica una verifica del SGSI ai sensi dell'articolo 5 capoverso 3 OSIn, occorre inserirla nel piano dei controlli e degli audit. Quest'ultimo e le relative risorse sono approvati dai responsabili della sicurezza dell'unità amministrativa (cfr. l'art. 36 cpv. 3 lett. d). L'articolo 13 non specifica quanti controlli e audit devono essere effettuati; la decisione spetta unicamente all'unità amministrativa. Con il piano dei controlli e degli audit da allestire imperativamente la direzione dell'ufficio deve prendere una decisione positiva e comprensibile.

I «controlli» ai sensi della presente ordinanza sono verifiche precise che hanno un campo d'applicazione limitato, si possono svolgere in modo informale con risorse limitate e spesso sono più convenienti rispetto agli audit. Un'unità amministrativa può, ad esempio, pianificare il controllo dell'attualità della documentazione di sicurezza o la verifica del rispetto della *«Clean Desk Policy»*. Gli «audit» seguono invece una procedura formalizzata e vengono spesso svolti da un organismo indipendente. Durante un audit si esamina se sistemi, processi o sistemi di gestione rispettano le direttive vigenti o gli standard e le norme richiesti.

Capoverso 2: sempreché i contratti con terzi lo consentano, i controlli e gli audit possono anche contemplare il rispetto delle prescrizioni da parte di terzi, ad esempio di fornitori. Se è previsto un siffatto controllo e se il terzo dispone di una dichiarazione di sicurezza aziendale (cfr. gli art. 61 segg. LSIn), un coordinamento con il servizio specializzato PSA responsabile di quest'ultima è inteso servire a che la Confederazione non controlli più volte le stesse cose presso un partner.

Capoverso 3: su richiesta delle autorità federali, il servizio specializzato della Confederazione per la sicurezza delle informazioni può svolgere verifiche (cfr. l'art. 83 cpv. 1 lett. c LSIn). Il livello di ambizione viene consapevolmente mantenuto basso e per il momento si rinuncia a potenziare la capacità di audit di suddetto servizio specializzato. Da anni il Controllo federale delle finanze (CDF)

svolge infatti audit di elevata qualità ed esami trasversali nell'ambito della sicurezza delle informazioni. Tali audit prendono di mira i rischi su cui si focalizza il servizio specializzato e coprono così il fabbisogno a livello di Confederazione.

### *Art. 14 Rapporti*

Capoversi 1 e 2: il rapporto comprende, in particolare, lo stato e l'efficacia del SGSI delle unità amministrative; lo stato degli oggetti da proteggere, dell'attuazione delle misure di sicurezza e dell'assunzione dei rischi residui; lo stato della formazione; i dati concernenti i controlli di sicurezza relativi alle persone e le procedure di sicurezza relative alle aziende svolti per il Dipartimento o la CaF; i riscontri derivanti dagli incidenti legati alla sicurezza e dalle lacune nella sicurezza nonché le misure di miglioramento adottate e previste; i riscontri derivanti dai controlli e dagli audit nonché le misure di miglioramento adottate e previste.

Capoverso 3: per conseguire un miglioramento duraturo della sicurezza delle informazioni in seno alla Confederazione, sono necessari una verifica critica continua dell'efficacia della sicurezza delle informazioni e un costante adeguamento di opportune misure di sicurezza.

### *Art. 15 Direttive concernenti la gestione della sicurezza delle informazioni*

Questo articolo è retto dall'articolo 85 LSIn. Il servizio specializzato ha ricevuto dal Consiglio federale la competenza di emanare le direttive concernenti la gestione della sicurezza delle informazioni (artt. 5–14). Tali direttive si applicano ai servizi di cui all'articolo 2 capoversi 1–3 che si trovano nell'ambito di competenza del Consiglio federale.

## *Sezione 4: Informazioni classificate*

Gli articoli 18–20 descrivono i presupposti materiali per la classificazione delle informazioni (cfr. il messaggio LSIn, commento ad art. 13). Rispetto all'attuale OPrI sono stati innalzati i valori soglia per la classificazione AD USO INTERNO, CONFIDENZIALE e SEGRETO. Innalzando la soglia per le informazioni classificate AD USO INTERNO, CONFIDENZIALE e SEGRETO, in futuro dovrebbe essere possibile classificarle in modo più mirato. In futuro nell'Amministrazione federale dovrebbero così esserci complessivamente meno informazioni classificate, con conseguente impatto sulle risorse. Tale misura ha inoltre un impatto diretto sul numero di controlli di sicurezza relativi alle persone (CSP). Con l'innalzamento della soglia di classificazione in futuro dovrebbero esserci meno funzioni per il cui adempimento è necessario trattare informazioni classificate CONFIDENZIALE (cfr. OCSP nonché il relativo commento).

### *Art. 16 Principi*

Capoverso 1: la classificazione è obbligatoria, purché siano soddisfatti i pertinenti criteri secondo gli articoli 18 segg. OSIn. Deve essere rispettato rigidamente il principio del *«need-to-know»*, ossia della necessità di sapere di cui all'articolo 14 LSIn. La classificazione di materiale è un caso d'applicazione della classificazione di informazioni per la quale, in linea di principio, valgono gli stessi metodi di valutazione e le stesse misure di protezione (incl. prescrizioni ai sensi di OCSP e OPSAz; cfr. il messaggio LSIn, pag. 2633).

Capoverso 2: dall'aggregazione di informazioni classificate o informazioni non classificate o di supporti di dati (quali carta, hardware, apparecchi radio) può risultare una collezione che presenta una necessità di protezione superiore rispetto a un'informazione isolata contenuta in essa. Questo è il caso tipico delle banche dati (ad es. il prodotto *«deepl.com»* quale soluzione cloud) o nell'*hosting provider* dell'Intranet della Confederazione (poiché l'*hosting* può avvenire nel cloud). Inoltre, in futuro è possibile che, per prodotti sempre di più azionati da intelligenza artificiale, potranno risultare collezioni da classificare a partire da semplici informazioni isolate.

Capoverso 3: se, ad esempio, in base al principio di trasparenza un documento viene consegnato a un giornalista, ciò non dipende dall'eventuale menzione di classificazione di tale documento, bensì si determina unicamente in virtù dei criteri della legge del 17 dicembre 2004[18] sulla trasparenza (LTras).

### *Art. 17 Servizi incaricati della classificazione*

Capoverso 1: sono servizi incaricati della classificazione ai sensi di questa ordinanza tutti i collaboratori della Confederazione (cfr. l'art. 4 cpv. 3) e i militari. I terzi non sono servizi incaricati

[18] RS **152.3**

della classificazione. Le persone menzionate nelle lettere a, b e c sono competenti per la classificazione e anche per la declassificazione. Occorre tenere conto dei casi speciali, ad esempio nell'ambito di attività progettuali: secondo HERMES, il mandante del progetto (e non il capoprogetto) è ad esempio responsabile che raccolte di informazioni eventualmente risultanti vengano verificate riguardo a una collezione da classificare.

In generale, occorre garantire che l'informazione degna di protezione venga protetta (p. es. classificata) esattamente nel momento in cui è percepibile visivamente e/o acusticamente. Se ciò non avviene direttamente alla fonte, di solito è già troppo tardi. I superiori gerarchici o i mandanti dei servizi incaricati della classificazione possono adeguare la classificazione. Nel caso di una siffatta sollecitazione, che contempla un'assunzione di responsabilità riguardo alla correttezza della classificazione, detti superiori devono però identificarsi chiaramente quale servizio incaricato della classificazione. Se non è più possibile risalire a detto servizio, c'è la possibilità di individuare l'organizzazione subentrante per il tramite dell'Archivio federale svizzero (AFS).

Capoverso 2: le attuali istruzioni concernenti la classificazione (catalogo di classificazione) del 26 settembre 2011 (cfr. l'art. 8 OPrI) verranno rielaborate prima dell'entrata in vigore della LSIn.

Capoverso 4: questa disposizione è conforme all'attuale articolo 8 OPrI, salvo che la competenza viene trasferita dalla Conferenza dei segretari generali al servizio specializzato della Confederazione per la sicurezza delle informazioni.

### *Art. 18 Livello di classificazione «ad uso interno»*

Affinché si giustifichi una classificazione AD USO INTERNO sono necessari due presupposti cumulativi: la conoscenza di informazioni da parte di persone non autorizzate deve potere comportare un *potenziale* pregiudizio causale per gli interessi pubblici della Svizzera, ovvero il pregiudizio non può essere semplicemente trascurabile, senza che occorra fornire indicazioni concrete per un danno finanziario; ai sensi dell'OPrI è semplicemente richiesto un non meglio precisato «pregiudizio». Questi interessi pubblici vengono riportati nell'articolo 1 capoverso 2 lettere a–d LSIn; di per sé, la lettera e non costituisce appunto un interesse alla protezione proprio dell'istituzione federale (cfr. messaggio LSIn, pag. 2635 seg.). Siffatte informazioni sono protette per legge o convenzione; il segreto d'ufficio di cui all'articolo 321 del Codice penale svizzero del 21 dicembre 1937[19] (CP) o la LTras nei casi previsti in queste leggi assicurano, parimenti, la protezione di determinate informazioni.

### *Art. 19 Livello di classificazione «confidenziale»*

Affinché si giustifichi una classificazione CONFIDENZIALE sono necessari due presupposti cumulativi: la conoscenza di informazioni da parte di persone non autorizzate deve potere comportare un *considerevole* pregiudizio causale e potenziale per gli interessi pubblici della Svizzera. Questi interessi pubblici vengono riportati nell'articolo 1 capoverso 2 lettere a–d LSIn. Con «considerevole» si intende che per la Svizzera o per la Confederazione potrebbe derivarne un danno importante.

### *Art. 20 Livello di classificazione «segreto»*

Affinché si giustifichi una classificazione SEGRETO sono necessari due presupposti cumulativi: la conoscenza di informazioni da parte di persone non autorizzate deve potere comportare un *grave* pregiudizio causale e potenziale per gli interessi pubblici della Confederazione. Questi interessi pubblici vengono riportati nell'articolo 1 capoverso 2 lettere a–d LSIn. Con «grave» si intende che per la Svizzera potrebbe derivarne un danno catastrofico.

### *Art. 21 Direttive concernenti il trattamento*

Capoverso 1: fondandosi sull'articolo 85 LSIn il servizio specializzato della Confederazione per la sicurezza delle informazioni emana direttive inerenti al trattamento di informazioni classificate e i requisiti organizzativi, tecnici, edili e riguardanti il personale per la loro protezione. Tali direttive si applicano soltanto ai servizi di cui all'articolo 2 capoversi 1–3.

Capoverso 4: in applicazione dell'articolo 84 capoverso 1 LSIn il Consiglio federale delega alla Cancelleria federale la competenza di disciplinare il trattamento degli affari classificati del Consiglio federale.

[19] RS **311.0**

Capoverso 5: i trattati internazionali nell'ambito della sicurezza delle informazioni contengono, ad esempio, elenchi di concordanza sull'applicazione di classificazioni, standard di sicurezza nell'ambito dell'informatica o della sicurezza delle comunicazioni nonché normative sull'esecuzione di controlli reciproci (cfr. messaggio LSIn, commento ad art. 88).

### *Art. 22 Misure di sicurezza specifiche all'impiego*

Può succedere che l'esigenza di condividere rapidamente informazioni debba essere ritenuta superiore alla protezione della confidenzialità. Ciò si verifica, in particolare, negli impieghi delle forze di sicurezza o delle forze di polizia. In questi casi, una semplificazione mirata delle normali prescrizioni di sicurezza può agevolare l'adempimento dei compiti senza dovere correre rischi inaccettabili. Conformemente all'attuale diritto (cfr. l'art. 18 cpv. 3 OPrI), i servizi d'informazione e fedpol possono gestire in modo semplificato informazioni classificate. La medesima esigenza si riscontra in altre unità amministrative della Confederazione alle quali sono affidati compiti di sicurezza, in particolare l'Aggruppamento Difesa, motivo per cui il trattamento semplificato dovrebbe essere messo a disposizione di ulteriori servizi. Tuttavia, questa possibilità non deve portare al risultato assurdo che per gli uffici più critici sotto il profilo della sicurezza si applichino, *in generale*, requisiti di sicurezza inferiori rispetto agli altri uffici. Le condizioni e le modalità di trattamento semplificato verranno perciò inasprite leggermente rispetto a oggi.

### *Art. 23 Accreditamento in materia di sicurezza di mezzi informatici*

Capoverso 1: ora l'OSIn introduce un obbligo di accreditamento per un numero limitato di sistemi d'informazione sensibili sotto il profilo della sicurezza (cfr. lett. a–c) nei quali vengono trattate informazioni classificate CONFIDENZIALE o SEGRETO di più organizzazioni (p. es. un'applicazione per la videocomunicazione confidenziale). Il pertinente mezzo informatico non può essere impiegato prima del rilascio dell'accreditamento in materia di sicurezza. L'accreditamento in materia di sicurezza viene sempre richiesto all'estero e nelle relazioni internazionali ogniqualvolta si intende trattare informazioni protette di un'autorità (o di uno Stato) in un sistema di un'altra autorità (o di un altro Stato). L'OSIn colma così una lacuna che finora ha reso difficile la cooperazione internazionale nell'ambito della sicurezza.

Capoversi 2–4: l'accreditamento in materia di sicurezza è volto a creare fiducia sul fatto che un mezzo informatico soddisfa i requisiti della sicurezza delle informazioni della Confederazione. Se l'accreditamento in materia di sicurezza non può essere rilasciato, il Consiglio federale decide in merito all'assunzione dei rischi residui.

Capoversi 5 e 6: la giusta entità («portata») per l'accreditamento dovrà sempre essere definita nel singolo caso concreto. Tale compito verrà assegnato al servizio specializzato della Confederazione per la sicurezza delle informazioni in quanto futuro servizio di accreditamento; un'apposita subdelega nell'ambito dei sistemi militari è prevista alla lettera c.

### *Art. 24 Protezione in caso di pericolo per le informazioni classificate*

È diritto vigente (cfr. l'art. 15 OPrI). La notifica ai competenti organi di sicurezza avviene secondo la disposizione riguardante la gestione degli incidenti (art. 12).

### *Art. 25 Verifica della necessità di protezione e cerchia delle persone autorizzate*

È diritto vigente (cfr. l'art. 14 OPrI).

### *Art. 26 Archiviazione*

Capoverso 1: le disposizioni concernenti l'archiviazione disciplinano la tutela di documenti della Confederazione che hanno un valore archivistico (incl. i documenti classificati) e la loro comunicazione al pubblico, tenendo conto di interessi legittimi della protezione della personalità e della protezione dello Stato nonché della trasparenza e della tracciabilità.

Capoverso 2: l'AFS ha il compito di garantire la protezione degli archivi archiviati centralmente e classificati. Esso può derogare ai requisiti e alle misure standard del servizio specializzato della Confederazione per la sicurezza delle informazioni previsti all'articolo 85 LSIn. L'AFS deve tuttavia proteggere gli archivi classificati così che la sicurezza ottenuta sia conforme al rischio posto dagli archivi.

Capoverso 3: il termine di protezione degli archivi (incl. gli archivi classificati) non viene prorogato automaticamente alla sua scadenza. La classificazione decade invece automaticamente con

detta scadenza. Ciò significa che successivamente a essa vi sarà un diritto generale di consultare gli archivi (cfr. l'art. 10 cpv. 1 dell'ordinanza sull'archiviazione dell'8 settembre 1999[20] [OLAr]). La maggior parte delle informazioni classificate non necessitano di una proroga del termine di protezione di 30 o di 50 anni dopo che è scaduto. Per contro, ad esempio nel caso di edifici o progetti militari, può essere giustificato prorogare il termine di protezione prima che scada (cfr. l'art. 12 della legge sull'archiviazione del 26 giugno 1998[21] [LAr] in combinato disposto con l'art. 14 OLAr).

L'ufficio competente è responsabile dell'avvio tempestivo di una proroga del termine di protezione. I termini di protezione per i documenti versati figurano nell'elenco di versamento che l'unità amministrativa competente gestisce nei sistemi GEVER (ActaNova). I fondi i cui termini di protezione sono stati prorogati in virtù di interessi pubblici e privati preponderanti degni di protezione (cfr. l'art. 12 LAr e l'art. 14 OLAr) vengono elencati nell'allegato 3 dell'OLAr (cfr. l'art. 14 cpv. 5 OLAr).

### *Sezione 5: Sicurezza nell'impiego di mezzi informatici*

### *Art. 27 Procedura di sicurezza*

In linea di massima, viene ripresa l'attuale procedura di sicurezza di cui agli articoli 14*b*–14*e* OCiber.

Capoverso 1: l'attuale necessità di protezione deve essere rilevata mediante i criteri dei livelli di sicurezza di cui all'articolo 28.

Capoverso 2: le eccezioni alle direttive necessitano sempre di un'autorizzazione esplicita del servizio che le ha emanate (cfr. commento sull'autorizzazione di deroghe di cui all'art. 9).

Inserito attualmente nelle prescrizioni in materia di informatica, il metodo di gestione dei rischi per ridurre lo spionaggio da parte dei servizi d'informazione sarà disciplinato mediante le normative concernenti la procedura di sicurezza relativa alle aziende e non necessita più di una normativa separata (cfr. gli art. 55–58 LSIn).

Capoverso 3: in linea di massima, un rischio residuo può essere un rischio accettato o un rischio ignoto (cfr. manuale sulla gestione dei rischi della Confederazione). Unicamente il primo è un rischio residuo ai sensi dell'OSIn. Se il rischio originario viene ridotto a un livello ragionevole grazie a misure di gestione dei rischi (ad es. per evitare, ridurre o trasferire i rischi), si parla di rischio residuo.

Capoverso 4: l'accettazione «comprovabile» (cfr. commento ad art. 8 cpv. 2) di rischi residui è importante, in quanto conferma lo svolgimento di un processo di analisi e decisionale e quindi una decisione consapevole sui rischi residui ammessi. In linea generale, la delega di tale decisione consapevole può avvenire per il tramite di un'istruzione oppure, in casi specifici (ad es. nell'ambito di un progetto informatico), a un altro membro della direzione (parimenti comprovabile).

Capoversi 5 e 6: la presenza di una minaccia nuova o ricorrente può mettere in discussione, in tutto o in parte, un'analisi dei rischi esistente, motivo per cui il concetto in materia di rischi deve, se del caso, essere adeguato.

A causa dei rapidi progressi dello sviluppo tecnologico e di minacce sempre più complesse nel settore della sicurezza delle informazioni, è necessario verificare ogni anno se c'è stato un cambiamento rilevante per la sicurezza. In tal modo decade anche il termine di cinque anni per la ripetizione della procedura di sicurezza ai sensi dell'articolo 14*e* capoverso 1 OCiber.

### *Art. 28 Assegnazione ai livelli di sicurezza «protezione elevata» e «protezione molto elevata»*

I prodotti informatici (cfr. la definizione legale all'art. 5 lett. a in combinato disposto con l'art. 17 LSIn) vengono ora suddivisi in tre livelli di sicurezza: «protezione di base», «protezione elevata» e «protezione molto elevata», diversamente dall'attuale OCiber che ne prevede soltanto due: «protezione di base» e «protezione elevata». Ai fini dell'attribuzione a uno dei tre nuovi livelli di sicurezza sono determinanti gli interessi pubblici della Confederazione ai sensi dell'articolo 1 capoverso 2 lettere a–e LSIn. La protezione di base si applica ora anche ai Cantoni (cfr. l'art 3 LSIn), a condizione che rientrino nel campo di applicazione della LSIn.

Contrariamente a quanto avviene per i criteri di attribuzione delle informazioni classificate ai vari livelli di sicurezza, nell'ambito dell'attribuzione dei mezzi informatici ai vari livelli di sicurezza ci

[20] RS **152.11**

[21] RS **152.1**

si rifà a criteri finanziari. Ciò è dovuto al fatto che una violazione della disponibilità o dell'integrità delle informazioni trattate con mezzi informatici è meglio quantificabile rispetto, ad esempio, a una violazione della confidenzialità di un documento classificato. I criteri finanziari si rifanno ai criteri stabiliti nella matrice di valutazione della gestione dei rischi della Confederazione.

### *Art. 29 Misure di sicurezza*

Capoverso 1: fondandosi sull'articolo 85 LSIn, il servizio specializzato della Confederazione per la sicurezza delle informazioni emana direttive concernenti i requisiti minimi per i relativi livelli di sicurezza secondo l'articolo 17 LSIn. Tali direttive si applicano soltanto ai servizi di cui all'articolo 2 capoversi 1–3.

Capoverso 2: il servizio specializzato della Confederazione per la sicurezza delle informazioni si adopera per un coordinamento opportuno con l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) e i consulenti per la protezione dei dati (cfr. anche l'art. 82 cpv. 1 LSIn) quanto alle questioni relative alla protezione dei dati e alla sicurezza dei dati basata sul rischio. Riguardo all'approccio basato sul rischio, si veda il commento ad articolo 4 capoverso 1. Le istruzioni del servizio specializzato di cui al capoverso 1 devono essere allineate alle vigenti disposizioni in materia di protezione dei dati. In tale contesto occorre osservare che le nozioni di «protezione elevata» e «protezione molto elevata» di cui all'articolo 17 LSIn non corrispondono alle nozioni di «rischio», «rischio esiguo» o «rischio elevato» del diritto in materia di protezione dei dati.

Capoverso 3: con le lettere a e b si distingue tra due tipi di rischio che richiedono un'attenzione particolare quanto all'efficacia delle misure di sicurezza. Per tale motivo, occorre una verifica pertinente appena si delineano cambiamenti sostanziali dei rischi, al più tardi però ogni cinque anni. La base legale per la verifica periodica si trova nell'articolo 18 capoverso 3 LSIn.

Capoverso 4: si veda il commento ad articolo 5 capoverso 4.

### *Art. 30 Sicurezza durante l'esercizio*

Capoversi 1–4: i fornitori interni di prestazioni della Confederazione svolgono un duplice ruolo nell'attuazione della sicurezza delle informazioni. Da un lato, sono normali unità amministrative che devono attuare l'OSIn come tutte le altre unità amministrative. Dall'altro, hanno un'importanza cruciale anche per la sicurezza dei beneficiari di prestazioni. È quindi essenziale per la sicurezza che la ripartizione dei compiti e delle competenze sia chiara. I fornitori di prestazioni hanno un obbligo generale di fornire le proprie prestazioni informatiche secondo lo stato della tecnica e di mettere a disposizione dei propri beneficiari di prestazioni, a tempo debito, le necessarie informazioni rilevanti per la sicurezza. Incombe tuttavia alle unità amministrative (di norma in qualità di beneficiari) che nelle convenzioni sulle prestazioni vengano chiaramente definite le responsabilità per la sicurezza a livello operativo, incluso per la gestione delle vulnerabilità. Sono infatti responsabili della sicurezza dei propri dati e compiti.

Capoverso 5: questa vigilanza è una faccenda di mera sicurezza tecnica e non ha nulla a che vedere con un'eventuale sorveglianza dei collaboratori. I terzi, ad esempio, possono essere persone nell'ambito di un programma *bug bounty*.

## *Sezione 6: Misure relative alle persone e protezione fisica*

### *Art. 31 Verifica dell'identità di persone e macchine*

Capoverso 1: fondandosi sull'articolo 85 LSIn e previa consultazione del delegato alla trasformazione digitale e alla governance delle TIC (delegato TDT), il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni concernenti requisiti tecnici minimi per la verifica basata sui rischi dell'identità di persone e macchine che necessitano di avere accesso a informazioni, mezzi informatici, locali e altre infrastrutture della Confederazione. Tali direttive si applicano soltanto ai servizi di cui all'articolo 2 capoversi 1–3.

Qui si tratta di stabilire la qualità delle prove che una persona deve fornire per dimostrare la propria identità fisica o elettronica al fine di ottenere l'accesso a informazioni, mezzi informatici, locali e altre infrastrutture della Confederazione. Il livello di sicurezza richiesto (il cosiddetto «level of assurance») sarà più elevato nel caso dei sistemi sensibili sotto il profilo della sicurezza che per le applicazioni normali. Non soltanto le persone, ma anche i computer e addirittura i processi devono «identificarsi» di conseguenza.

### *Art. 32 Sicurezza delle persone*

Capoverso 1: le unità amministrative devono assicurare ogni anno di sensibilizzare i collaboratori soggetti a un CSP. I superiori devono assumersi attivamente la responsabilità dei rischi per la sicurezza riferiti a persone e integrarla nei compiti direttivi permanenti. Una siffatta sensibilizzazione potrebbe, ad esempio, avere luogo nell'ambito del colloquio con il collaboratore. Tale aspetto verrebbe così affrontato almeno una volta l'anno.

Capoverso 2: la prassi ha mostrato che, dopo il superamento di un CSP, soltanto in casi eccezionali la questione dei rischi per la sicurezza riferiti a persone viene affrontata di nuovo. Ai sensi di una gestione a posteriori (cosiddetta «aftercare»), usuale a livello internazionale, i collaboratori che sono stati sottoposti a CSP devono comunicare al proprio datore di lavoro le circostanze, nel proprio contesto privato e professionale, che pregiudicano la sicurezza. Siffatte circostanze possono consistere in incidenti che generano una ricattabilità realistica di un collaboratore (p. es. forte indebitamento nel contesto di una dipendenza da gioco, alcolismo o tossicodipendenza rivelato da un terzo, rapporto extraconiugale scoperto). In caso di comunicazione, si concorda con il servizio del personale come procedere.

### *Art. 33 Sospetto di reato*

Capoverso 1: la disposizione mira a garantire che eventuali reati siano deferiti il più rapidamente possibile alle competenti autorità preposte al perseguimento penale senza che i dipartimenti debbano fare considerazioni dettagliate di diritto penale o addirittura di diritto processuale penale. In tal senso, un reato «è già ipotizzabile» se primi indizi, anche non del tutto concludenti, suggeriscono un comportamento punibile.

Capoverso 2: qui si tratta di accertare rapidamente prove tangibili e in parte effimere. A tal fine, non possono essere eretti ostacoli eccessivi. È importante che nell'ambito dell'accertamento delle prove le unità amministrative non cancellino, lascino o addirittura causino tracce fisiche o elettroniche. Con ciò che qui si intende per «mettere al sicuro le prove» non si intende quindi anche la loro valutazione; ciò spetta, se del caso, alle autorità preposte al perseguimento penale su ordine del tribunale.

### *Art. 34 Misure di protezione fisica*

Capoverso 1: fondandosi sull'articolo 85 LSIn e previa consultazione dei servizi dell'Amministrazione federale e dell'esercito competenti per la sicurezza degli oggetti, il servizio specializzato della Confederazione per la sicurezza delle informazioni emana istruzioni concernenti le misure minime necessarie per la protezione fisica di informazioni e mezzi informatici. Tali direttive si applicano soltanto ai servizi di cui all'articolo 2 capoversi 1–3.

Capoversi 1 e 2: sono considerate misure di protezione fisica, ad esempio, l'allestimento di zone di sicurezza (cfr. l'art. 35 e il messaggio LSIn, pag. 2644 seg.), i controlli all'ingresso degli edifici, la sorveglianza mediante telecamere in determinate zone, i dispositivi di distruzione dei supporti di dati o i controlli sul posto di lavoro. Per l'attuazione di questi ultimi è ora competente l'incaricato della sicurezza delle informazioni delle unità amministrative (cfr. l'art. 37 cpv. 2 lett. j).

### *Art. 35 Zone di sicurezza*

Capoverso 1: la creazione di zone di sicurezza ha lo scopo di ridurre il potenziale di danni a seguito di spionaggio o sabotaggio in zone molto sensibili (come i locali dei server o i locali di condotta) (cfr. messaggio LSIn pag. 2628, 2644 seg.).

Capoverso 2: la conferma del requisito di sicurezza per le zone di sicurezza non significa un accreditamento di sicurezza di cui all'articolo 23. Le zone di sicurezza non vanno inoltre confuse con locali a prova d'intercettazione, per i quali occorrono misure edili e organizzative nettamente più ampie.

Capoverso 3: fondandosi sull'articolo 85 LSIn e previa consultazione dei servizi dell'Amministrazione federale e dell'esercito competenti per la sicurezza degli oggetti, il servizio specializzato della Confederazione per la sicurezza delle informazioni emana direttive concernenti i requisiti di sicurezza per le zone di sicurezza e la loro istituzione. Tali direttive si applicano soltanto ai servizi di cui all'articolo 2 capoversi 1–3.

### *Sezione 7: Organizzazione di sicurezza*

Una novità importante nell'OSIn riguarda le direzioni. Nell'ordinanza verranno assegnati loro compiti, competenze e responsabilità concreti nell'ambito della sicurezza delle informazioni che, in caso di bisogno, possono delegare a un membro della loro direzione (responsabili della sicurezza). I responsabili della sicurezza vigileranno sul SGSI dell'ufficio e prenderanno tutte le decisioni importanti nel suddetto ambito. Le attività di vigilanza operativa sono compito degli incaricati della sicurezza delle informazioni. Con l'OSIn gli odierni ruoli degli «incaricati della sicurezza informatica» e degli «incaricati della protezione delle informazioni» vengono uniti nel nuovo ruolo degli «incaricati della sicurezza delle informazioni». I loro compiti verranno precisati di conseguenza e integrati da compiti rilevanti per il SGSI.

A livello dei dipartimenti si applica un modello analogo. Ai sensi degli articoli 37, 38, 41 e 42 LOGA, i dipartimenti sono responsabili della direzione, del coordinamento e della vigilanza della sicurezza delle informazioni nel dipartimento stesso. Essi definiscono in particolare la politica in materia di sicurezza delle informazioni e l'organizzazione della sicurezza del dipartimento. La responsabilità operativa per la sicurezza va assunta dal segretario generale. Come è avvenuto finora, gli incaricati della sicurezza delle informazioni svolgono i compiti di coordinamento e di vigilanza operativi (cfr. l'art. 81 LSIn).

L'organizzazione di sicurezza nella sezione 7 descrive i vari ruoli e le varie funzioni previsti. Taluni ruoli, ad esempio quello degli incaricati della sicurezza delle informazioni delle unità amministrative (cfr. l'art. 37), possono essere occupati da più persone su temi specifici, a seconda delle esigenze di un ufficio. Lo stesso vale per tutti gli altri ruoli di cui agli articoli 37 segg. OSIn. Nessun ruolo è vincolato a una sola persona. Fa eccezione quello di cui all'articolo 35: il responsabile della sicurezza della CaF e delle unità amministrative può essere unicamente rappresentato da una sola persona.

I sostituti devono essere idonei per tutti i compiti del ruolo primario dal punto di vista tecnico e personale. Il sostituto deve essere istruito o formato in modo da essere in grado di supplire al ruolo primario in modo adeguato in qualsiasi momento e, soprattutto, in situazioni di emergenza.

### *Art. 36 Responsabili della sicurezza della Cancelleria federale e delle unità amministrative*

Capoverso 1: con «responsabile» si intende l'obbligo personale di rendere conto all'organo superiore. Esso presuppone che la persona responsabile abbia il potere, in particolare finanziario, di adottare, verificare o correggere misure. Da ciò occorre distinguere l'obbligo di attuare misure di vigilanza. In tal caso, la persona incaricata è responsabile dello svolgimento e l'unica tenuta a rispondere di esso.

Capoverso 2: con la delega della responsabilità per la sicurezza si delega anche l'obbligo personale di rendere conto. Per tale motivo, la delega dovrebbe essere comprovabile (cfr. commento ad art. 8 cpv. 2 lett. a).

Capoverso 3 lettera b: in linea di principio, tutte le decisioni importanti concernenti la sicurezza delle informazioni sono interessate da questo ruolo.

Capoverso 4: gli incaricati della sicurezza delle informazioni di cui all'articolo 37 OSIn possono, ad esempio, ricevere l'incarico per il tramite di istruzioni interne o della definizione di obiettivi annuali ai sensi dell'articolo 5 capoverso 2. Sul termine «conflitto d'interessi», si veda messaggio LSIn, commento ad art. 82 capoverso 3.

### *Art. 37 Incaricati della sicurezza delle informazioni delle unità amministrative*

La designazione di una supplenza ufficiale è una novità. Questo ruolo corrisponde ampiamente all'attuale incaricato della sicurezza informatica delle unità amministrative (ISIU).

### *Art. 38 Sicurezza delle informazioni nei servizi standard*

In linea di principio, questo ruolo nei servizi standard ha gli stessi compiti del ruolo degli incaricati della sicurezza delle informazioni delle unità amministrative di cui all'articolo 37.

### *Art. 39 Responsabilità in materia di sicurezza dei dipartimenti*

Capoversi 1 e 2: la gestione della sicurezza delle informazioni e la vigilanza su di essa sono compiti strategici, nonché compiti fondamentali dei dipartimenti (cfr. l'art. 38 LOGA, commento ad art. 5 cpv. 1).

Capoverso 3: questa disposizione consente ai dipartimenti aventi un'organizzazione più centrale (p. es. il DFAE) di attuare le proprie esigenze organizzative nel contesto dell'OSIn.

### *Art. 40 Incaricati della sicurezza delle informazioni dei dipartimenti*

La designazione di una supplenza ufficiale è una novità (cfr. l'art. 81 cpv. 1 LSIn). Questo ruolo unisce il ruolo degli attuali incaricati della sicurezza informatica dei dipartimenti (ISID) e quello degli incaricati della sicurezza delle informazioni dei dipartimenti.

Lettera e: poiché i ruoli di cui agli articoli 37 e 40 devono collaborare strettamente, il ruolo di cui all'articolo 40 dovrebbe essere coinvolto nella scelta di una nuova persona per il ruolo di cui all'articolo 37.

Lettera f: la procedura dell'attuale controllo dei documenti segreti è ripresa invariata.

Lettera g: questo ruolo ha ora un compito supplementare nell'ambito dei CSP. I dettagli vengono definiti a livello di istruzioni e i detentori dei ruoli ricevono una formazione adeguata.

Lettera h: oggi i rapporti annuali degli ISID devono essere inviati al NCSC. D'ora in poi, i detentori dei ruoli secondo questa disposizione dovranno fare rapporto alla persona responsabile in materia di sicurezza del dipartimento ai sensi dell'articolo 39 (cfr. l'art. 14). In seguito, quest'ultima invia il rapporto al servizio specializzato della Confederazione per la sicurezza delle informazioni affinché, a sua volta, esso possa redigere annualmente per il Consiglio federale un rapporto sullo stato della sicurezza delle informazioni [della Confederazione] (cfr. l'art. 83 cpv. 1 lett. h LSIn).

### *Art. 41 Servizio specializzato della Confederazione per la sicurezza delle informazioni*

Capoverso 1: i compiti generali del servizio specializzato della Confederazione per la sicurezza delle informazioni figurano nell'articolo 83 LSIn e nell'articolo 41 OSIn; i compiti specifici al contesto in ulteriori disposizioni dell'OSIn (p. es. direttive concernenti la gestione della sicurezza delle informazioni di cui all'art. 16, ulteriori direttive in vari settori di cui agli artt. 21, 29, 31, 34 e 35 cpv. 4).

Capoverso 3: la Conferenza degli incaricati della sicurezza delle informazioni di cui all'articolo 82 capoverso 2 lettera c LSIn offre consulenza al servizio specializzato della Confederazione per la sicurezza delle informazioni su tutte le questioni relative al coordinamento dell'esecuzione e su questioni di importanza strategica.

Capoverso 4: il ruolo dell'autorità di sicurezza nazionale è ora assegnato al servizio specializzato della Confederazione per la sicurezza delle informazioni. Attualmente il ruolo è assunto dal settore Digitalizzazione e cibersicurezza DDPS (DCS DDPS) nella Segreteria generale del DDPS (SG-DDPS). I compiti e le competenze di cui alle lettere d e f sono oggetto dei trattati internazionali di cui all'articolo 87 LSIn (cfr. messaggio LSIn, commento ad art. 88, pagg. 2683–2684; pag. 2703).

## *Sezione 8: Costi e valutazione*

### *Art. 42 Costi*

Le unità amministrative assumono i costi della propria sicurezza. Tali costi devono essere pianificati e riportati già in sede di pianificazione dei progetti. Ciò si verifica, in particolare, per i costi delle misure per la sicurezza informatica.

### *Art. 43 Valutazione*

Si veda messaggio LSIn, commento ad articolo 89 LSIn, pagina 2684.

## *Sezione 9: Trattamento di dati personali*

Gli articoli 44–46 disciplinano il trattamento di informazioni e di dati personali nell'ambito della gestione della sicurezza delle informazioni secondo l'ordinanza oggetto del presente rapporto esplicativo. La gestione degli incidenti legati alla sicurezza presuppone il trattamento di dati riguardanti potenziali autori che possono essere connessi a perseguimenti e sanzioni amministrativi o penali e che sono pertanto considerati dati personali degni di particolare protezione ai sensi dell'articolo 3 lettera c LPD. La legislazione sulla protezione dei dati esige a tal fine una base legale esplicita, oggi mancante, a livello di legge. Nell'ambito della corrente revisione della LSIn (cfr. n. 3.1) viene creata la necessaria base legale formale.

### *Art. 44 In generale*

Capoversi 1 e 2: le unità amministrative e i loro organi di sicurezza non sono in grado di adempiere i propri compiti senza un reciproco scambio di informazioni e di dati personali. Riguardo al trattamento di dati personali degni di particolare protezione nell'ambito della gestione degli incidenti cfr. il commento alla sezione 9.

### *Art. 45 Applicazione SGSI*

Questa disposizione crea la base legale per l'impiego di applicazioni SGSI con le quali vengono digitalizzati i compiti e i processi dell'OSIn (cfr. n. 3.8). Riguardo al trattamento di dati personali degni di particolare protezione cfr. il commento alla sezione 9.

### *Art. 46 Servizi di modulistica elettronica*

Capoverso 1: un servizio di modulistica è una semplice, piccola applicazione con la quale vengono compilati e inviati formulari. I servizi di modulistica di cui al capoverso 1 servono a emettere in modo automatizzato cosiddette richieste di visita (*«Request for Visit»*, cpv. 1 lett. a), attestazioni di sicurezza (cpv. 1 lett. b) e attestazioni internazionali di sicurezza aziendale (*«Facility Security Clearances»*, cpv. 1 lett. c).

Capoverso 2: i dati nell'allegato 2 sono dati personali che, analogamente a quanto avviene in un processo di autorizzazione di viaggio ESTA, vengono richiesti per viaggi negli Stati Uniti. I dati contrassegnati da un asterisco (*) nell'allegato 2 sono inoltrati ad autorità straniere. Vengono rispettate le disposizioni del diritto in materia di protezione dei dati sulla comunicazione di dati all'estero (in particolare l'art. 16 cpv. 1 e l'art. 17 nLPD). Senza l'indicazione di questi dati la persona richiedente non ottiene l'accesso al progetto classificato all'estero.

Capoversi 3–6: nel contesto di una notifica di sicurezza possono venire trattati informazioni classificate o dati personali. Con l'invio della notifica, questi ultimi finiscono subito nell'applicazione SGSI, nella quale vengono trattati la notifica e l'incidente. Per ragioni di sicurezza delle informazioni e di protezione dei dati, i dati potenzialmente sensibili non possono essere memorizzati per oltre 24 ore nel servizio di modulistica. Riguardo al trattamento di dati personali degni di particolare protezione nell'ambito della gestione degli incidenti cfr. il commento alla sezione 9

## *Sezione 10: Disposizioni finali*

### *Art. 47 Abrogazione e modifica di altri atti normativi*

L'OCiber e l'OPrI saranno abrogate.

### *Art. 48 Disposizioni transitorie*

Oltre alle disposizioni transitorie contenute in questa disposizione, se ne trovano ulteriori nella LSIn, nell'OCSP e nell'OPSAz. L'intento è che entro sei anni dalla messa in vigore del nuovo diritto le disposizioni transitorie ne consentano la pianificazione e l'attuazione sistematiche e regolari (cfr. anche l'art. 90 LSIn).

### *Art. 49 Entrata in vigore*

Si sta ancora verificando se è necessaria una messa in vigore parziale.

### *Allegato 1*

Il [dipartimento competente] terrà aggiornato l'allegato 1.

### *Allegato 2*

Cfr. commento ad art. 46.

### *Allegato 3*

Numero 1: modifica dell'ordinanza del 25 novembre 2020[22] sul coordinamento della trasformazione digitale e la *governance* delle TIC in seno all'Amministrazione federale (OTDI): l'OCiber viene sostituita dall'OSIn.

[22] RS **172.010.58**

Numero 2: ordinanza del 7 marzo 2003[23] sull'organizzazione del DDPS (OOrg-DDPS): con la LSIn e l'OSIn viene meno la nozione di «segreto militare». L'Organo di coordinamento per la protezione delle informazioni in seno alla Confederazione viene sciolto e i suoi compiti assunti dal servizio specializzato della Confederazione per la sicurezza delle informazioni.

Numero 3: ordinanza del 24 giugno 2009[24] sui contatti militari internazionali (OCMI): con la LSIn e le sue ordinanze d'esecuzione devono venire aggiornati gli organismi e le ordinanze rilevanti.

### 4.2 Modifica dell'ordinanza sui sistemi di gestione delle identità e sui servizi di elenchi della Confederazione (OIAM)

#### *Ingresso*

Con gli articoli 24–26 LSIn è stata creata una base legale formale specifica per l'attuale OIAM elevando a livello di legge le principali disposizioni dell'ordinanza. Finora l'ordinanza si basava sulla competenza organizzativa del Consiglio federale e, indirettamente, sulle basi legali di tutti i sistemi collegati ai sistemi IAM. In virtù dell'articolo 20 capoverso 2 LSIn, a determinate condizioni sarà inoltre consentito il trattamento di dati biometrici nei sistemi IAM. Secondo la nLPD, i dati biometrici sono considerati dati personali degni di particolare protezione (FF 2020 6695, art 5 lett. c n. 4). Viene così relativizzato il principio secondo cui questi ultimi non possono essere trattati nei sistemi IAM (art. 11 cpv. 3). Sulla base di disposizioni di legge specifiche al di fuori della LSIn, permane quindi la possibilità di trattare nei sistemi IAM dati personali degni di particolare protezione. I profili della personalità non sono più un criterio rilevante nella nLPD e pertanto non occorre più menzionarli. Una profilazione ai sensi dell'articolo 5 lettera f nLPD non è effettuata in sistemi IAM e servizi di elenchi in quanto essi non servono a *valutare* gli aspetti personali delle persone.

#### *Art. 2 Campo d'applicazione*

Il termine «Amministrazione federale» utilizzato nell'articolo 2 capoverso 2 lettera b LSIn comprende sia l'Amministrazione federale centralizzata, sia quella decentralizzata (cfr. messaggio LSIn, pag. 2625), per cui il campo d'applicazione va ora esteso alle unità amministrative dell'Amministrazione federale decentralizzata, sempreché abbiano accesso a sistemi informatici dell'Amministrazione federale centrale.

I contenuti dell'attuale capoverso 2 non costituiscono una lista positiva esaustiva e possono pertanto essere eliminati senza sostituzione (per un'autorità o un servizio è possibile impegnarsi volontariamente a rispettare l'OIAM senza una base giuridica esplicita).

#### *Art. 3 cpv. 1*

Finora le identità vengono offerte soltanto passivamente a sistemi IAM o a memorie d'identità a valle ai fini dell'autoreferenzialità – sistemi e memorie consumano le identità secondo la propria cadenza, il proprio ritmo e le proprie esigenze. Nell'ambito di misure di protezione più proattive (p. es. immediate modifiche delle autorizzazioni o blocchi di emergenza), non si può più fare affidamento sulla data di applicazione della registrazione alle applicazioni, bensì si devono approvvigionare in modo proattivo con queste informazioni rilevanti per la sicurezza i sistemi a valle alimentati da IAM. Questo nuovo tipo di approvvigionamento è importante e deve quindi essere inserito nell'OIAM. L'attuale formulazione, che prevede che un sistema IAM metta a disposizione di sistemi a valle e di altri sistemi IAM i dati soltanto «su richiesta», viene perciò adeguata di conseguenza stralciando la locuzione «su richiesta».

#### *Art. 5 Sistemi IAM*

Capoverso 1: oltre agli organi federali responsabili che già figurano in OIAM, vengono elencati altri organi federali responsabili (lett. c e g) di sistemi IAM.

Capoverso 2: attualmente non ha luogo alcun controllo del trattamento dei dati personali in sistemi IAM. L'articolo 26 lettera e LSIn – peraltro non soltanto riguardo ai sistemi IAM – chiede ora esplicitamente che sia previsto un controllo periodico del trattamento di dati personali da parte di un servizio esterno. Di conseguenza, nell'articolo 5 viene inserito un capoverso.

Capoverso 3: in virtù dell'articolo 84 capoverso 3 LSIn, l'OIAM si applica anche alle autorità assoggettate di cui all'articolo 2 capoverso 1 lettere a e c–e LSIn, sempreché queste non emanino

[23] RS **172.214.1**
[24] RS **510.215**

proprie disposizioni. Affinché tale costrutto funzioni, le altre autorità assoggettate devono quanto meno stabilire chi, nel loro ambito, detiene la responsabilità a livello di diritto in materia di protezione dei dati.

Capoverso 4: in virtù dei nuovi capoversi 2 e 3, l'attuale capoverso 2 diventa il capoverso 4, riprendendone in toto il relativo contenuto

### *Art. 11 cpv. 2 e 3*

Gli attuali capoversi 2 e 3, in base ai quali nei sistemi IAM non possono essere trattati profili personali e, in assenza di una base legale specifica in materia, non vi si possono trattare neanche dati personali degni di particolare protezione devono essere sottoposti a una duplice rielaborazione (cfr. le considerazioni al n. 3.4), da un lato, in virtù dell'articolo 20 capoverso 2 LSIn e, dall'altro, in virtù della nLPD. Primo, al divieto del trattamento di profili della personalità subentra un divieto di profilazione (cfr. art. 5 lett. f nLPD). Secondo, i dati biometrici, che identificano chiaramente una persona, sono ora considerati, genericamente, dati personali degni di particolare protezione. Per il loro trattamento si crea però una base generale nell'articolo 20 capoverso 2 LSIn. Secondo l'allegato (lett. a n. 11), siffatti dati biometrici possono quindi ora essere trattati in tutti i sistemi IAM nei quali ciò risulti necessario per l'identificazione in funzione dei rischi.

### *Art. 13 cpv. 4*

A fini di chiarezza, alla lettera a si afferma esplicitamente che la base legale in questione deve prevedere (anche) il trattamento dei dati da fornire.

### *Art. 14 cpv. 2*

Questa disposizione rimane invariata sotto il profilo materiale, tuttavia il rimando non va più fatto all'articolo 2*a* della legge federale del 3 ottobre 2008[25] sui sistemi d'informazione militari (LSIM), bensì alla LSIn.

### *Titolo prima dell'art. 18 nonché art. 18 cpv. 1 e 2*

La sicurezza delle informazioni e il rispetto delle relative direttive non devono applicarsi esclusivamente ai sistemi IAM, ma devono esserlo parimenti ai servizi di elenchi. Ciò vale anche per offerenti, esterni alla Confederazione, di servizi di elenchi, in particolare se detti offerenti non gestiscono già un sistema IAM. Il testo dell'ordinanza viene quindi integrato di conseguenza.

### *Art. 20 Sistema globale IAM*

Ai sensi dell'attuale articolo 20, i sistemi IAM dell'Amministrazione federale possono essere collegati in modo ottimale tra loro nonché con i sistemi IAM dei Servizi del Parlamento o dell'esercito per rendere possibile una ripartizione dei compiti efficiente. Ciò significa anche che i dati degli utenti possono essere scambiati tra loro nella modalità di una federazione. Ora i suddetti sistemi IAM devono potere essere collegati anche con sistemi IAM di cui all'articolo 21, per cui l'articolo 20 è integrato di conseguenza sotto il profilo materiale. La novità dal punto di vista formale è che tutti i sistemi IAM al di fuori dell'Amministrazione federale (sistemi IAM esterni), dunque anche i sistemi IAM dei Servizi del Parlamento e dell'esercito figuranti finora nell'articolo 20, vengono elencati assieme nell'articolo 21.

### *Art. 21 Condizioni per il collegamento di sistemi IAM esterni*

Frase introduttiva: se un sistema IAM esterno di cui all'articolo 21 deve essere collegato con i sistemi IAM dell'Amministrazione federale, dei Servizi del Parlamento o dell'esercito è, in particolare, imperativo per motivi di sicurezza che i gestori in questione si assoggettino all'OIAM. La frase introduttiva è pertanto integrata di conseguenza.

Lettere a e b: ora nell'enumerazione vengono elencati anche i sistemi IAM dei Servizi del Parlamento e dell'esercito figuranti finora nell'articolo 20.

Le lettere c–f corrispondono alle attuali lettere a–d.

### *Allegato*

A norma dell'articolo 20 capoverso 2 LSIn, i dati biometrici vengono trattati non soltanto per persone figuranti in sistemi gestiti dall'esercito, bensì per tutte quelle figuranti in sistemi IAM

[25] RS **510.91**

(oggi, in virtù dell'art. 2*a* LSIM, ciò è possibile soltanto per sistemi dell'esercito). Attualmente figuranti alla lettera g, i dati biometrici ora vengono quindi integrati nella lettera a; la lettera g può così essere abrogata.

Tuttavia, i dati biometrici non possono figurare sistematicamente in tutti i sistemi IAM ed essere impiegati per qualsivoglia caso di utilizzo. Piuttosto, occorre verificare per ogni sistema IAM e per ogni scenario d'utilizzo se l'impiego di dati biometrici è necessario ai fini dell'identificazione delle persone in funzione dei rischi. Inoltre, venuta meno l'autorizzazione di accesso, i dati biometrici devono essere distrutti (cfr. l'art. 20 cpv. 3 LSIn e l'art. 14 cpv. 2 OIAM).

Inoltre, vengono accorpate le colonne «servizi di elenchi» e «sistemi IAM con persone secondo gli articoli 8 e 9 lettera a». In passato, una distinzione tra i servizi di elenchi e i sistemi IAM in questione si è rivelata un notevole ostacolo nell'offerta di prestazioni IAM ai processi amministrativi e dunque in futuro, nel caso di un collegamento a servizi IAM, tutti i beneficiari di informazioni dovranno rendere pubblico l'insieme dei regolamenti inerenti al trattamento e all'elaborazione (finora ciò valeva soltanto per i sistemi IAM).

Per finire, conformemente al tenore della LSIn, nella lettera f (frase introduttiva e n. 2) si procede a due adeguamenti linguistici.

### 4.3 Ordinanza sui controlli di sicurezza relativi alle persone (OCSP)

#### *Titolo*

Oltre ai controlli di sicurezza relativi alle persone (CSP) ai sensi della LSIn, con la nozione di «controllo di sicurezza relativo alle persone» si riassumono tutti i controlli nonché tutte le valutazioni e le verifiche ai sensi di leggi diverse dalla LSIn a cui secondo queste disposizioni di legge, direttamente o per analogia, si applica la procedura di suddetti CSP.

#### *Ingresso*

L'ingresso rimanda a tutte le norme di legge che conferiscono al Consiglio federale una competenza normativa nell'ambito dei CSP.

#### *Sezione 1: Disposizioni generali*

#### *Art. 1 Oggetto*

Capoversi 1 e 2: con l'OCSP si intende emanare un'ordinanza per tutte le competenze esecutive di cui all'articolo 48 LSIn concernenti i CSP ai sensi della LSIn e i controlli, le valutazioni e le verifiche ai sensi di altre leggi.

Capoverso 3: in quanto autorità assoggettata di cui all'articolo 2 capoverso 1 LSIn, il Consiglio federale svolge compiti esecutivi specifici per l'Amministrazione federale.

#### *Art. 2 Campo d'applicazione*

L'articolo 2 LSIn viene reso concreto dal Consiglio federale nell'articolo 2 dell'OSIn. Questa disposizione è quindi determinante anche per il campo d'applicazione dell'OCSP.

#### *Sezione 2 Elenchi delle funzioni*

#### *Art. 3 Attribuzione*

Capoversi 1–3: per ogni tipo di CSP si emana un proprio elenco delle funzioni quale allegato all'ordinanza. Ai sensi dell'articolo 41*b* capoverso 2 della legge federale del 16 dicembre 2005[26] sugli stranieri e la loro integrazione e dell'articolo 6*a* capoverso 2 della legge sui documenti d'identità del 22 giugno 2001[27], nell'ambito del rilascio di documenti d'identità, anche per determinate persone potrebbero venire svolti controlli di sicurezza ai sensi dall'articolo 6 dell'attuale OCSP. Nella nuova OCSP non figurerà, volutamente, alcun elenco delle funzioni a tale scopo. In caso di necessità impellente di CSP questi sarebbero coperti attraverso una procedura di sicurezza relativa alle aziende presso le imprese interessate.

Gli elenchi non possono contenere funzioni che non rispettano i rigidi presupposti degli articoli 10–14.

[26] RS **142.20**
[27] RS **143.1**

Le autorità assoggettate di cui all'articolo 2 LSIn che non rientrano nell'ambito di competenza del Consiglio federale (p. es. il Ministero pubblico della Confederazione) devono emanare autonomamente i propri elenchi delle funzioni.

Capoverso 4: il contenuto di questo capoverso è conforme al vigente disciplinamento di cui all'articolo 1 capoverso 3 OCSPN.

### *Art. 4 Modifica*

Al fine di tenere il numero dei controlli entro i limiti perseguiti, nell'allestire e nell'aggiornare gli elenchi delle funzioni nei quali figurano le funzioni da controllare occorre controllare meglio di oggi la legalità delle iscrizioni. L'intento è quindi che il DDPS gestisca a livello centrale gli elenchi delle funzioni e che li aggiorni costantemente su richiesta dei dipartimenti e della CaF. Nel farlo occorre che il DDPS coinvolga il servizio specializzato della Confederazione per la sicurezza delle informazioni.

### *Art. 5 Pubblicazione, conservazione e comunicazione*

Riguardo alla sensibilità sotto il profilo della sicurezza degli elenchi delle funzioni cfr. il numero 3.5 lettera d. I servizi e le persone che per l'adempimento dei propri compiti devono potere consultare elenchi delle funzioni non pubblicati, potranno farlo tramite il DDPS. Si tratta in particolare dei servizi promotori e degli organi di sicurezza secondo l'OSIn.

### *Art. 6 Verifica dell'aggiornamento*

Capoverso 1: la verifica della correttezza degli elenchi delle funzioni richiede una considerevole mole di lavoro. Vi è però una chiara necessità di mantenere aggiornati gli elenchi delle funzioni e di interrogarsi sulle classificazioni delle funzioni, affinché siano sottoposte a controllo sempre soltanto le persone per la cui funzione è necessaria una verifica in virtù del rischio potenziale. Occorre quindi stabilire l'approccio pragmatico di verificare gli elenchi delle funzioni una volta a legislatura, in generale, e in caso di riorganizzazioni o modifiche di compiti, nello specifico.

Capoverso 2: alla luce delle esperienze acquisite, è necessario garantire che la verifica della correttezza degli elenchi delle funzioni abbia effettivamente luogo. Occorre pertanto che ci sia l'obbligo di presentare rapporto in tal senso al DDPS. Se dalla verifica della correttezza degli elenchi delle funzioni risulta una necessità di modifica di tali elenchi, questi ultimi devono essere rielaborati di conseguenza.

## *Sezione 3 Controlli senza elenchi delle funzioni*

### *Art. 7 Controllo straordinario*

Qualora una funzione adempia i criteri per un controllo, ma non sia ancora stata inserita nel relativo elenco delle funzioni, in virtù dell'articolo 29 capoverso 3 LSIn, è possibile svolgere un controllo purché l'autorità assoggettata lo consenta. Per l'Amministrazione federale occorre delegare la pertinente competenza decisionale per un controllo eccezionale al DDPS, che consulta il servizio specializzato della Confederazione per la sicurezza delle informazioni. Gli elenchi delle funzioni devono essere aggiornati di conseguenza. Le altre autorità assoggettate disciplinano le competenze autonomamente.

### *Art. 8 Controlli presso gli impiegati cantonali e i terzi*

Capoverso 1: in linea di principio, spetta ai Cantoni stabilire le funzioni di impiegati di un Cantone che sono soggette a un controllo di cui all'articolo 29 capoverso 1 lettera b LSIn. Affinché sia possibile assicurare una gestione uniforme, qui il DDPS va tuttavia dotato di una funzione regolatrice. Esso consulta il servizio specializzato della Confederazione per la sicurezza delle informazioni.

Capoverso 2: le funzioni dei terzi che eseguono un mandato per conto di un'autorità o un'organizzazione assoggettata che comporta l'esercizio di un'attività sensibile sotto il profilo della sicurezza, non possono essere predeterminate, bensì risultano dalle necessità dei singoli mandati. Per garantire anche in questo caso la necessità del controllo, le decisioni devono essere prese a livello centrale.

### *Art. 9 Controllo di affidabilità straordinario da parte dell'Ispettorato federale della sicurezza nucleare*

Il contenuto di questo articolo è conforme al vigente disciplinamento di cui all'articolo 5 OCSPN.

### *Sezione 4: Livelli di controllo*

L'attribuzione della verifica dell'affidabilità secondo la legge sull'asilo al livello di controllo di sicurezza di base viene già stabilita nell'articolo 29*a* della legge sull'asilo del 26 giugno 1998[28] e non deve quindi più essere disciplinata nell'ordinanza.

### *Art. 10 Controlli di sicurezza relativi alle persone secondo la LSIn*

Capoverso 1 lettera a: con «trattamento» si intende ogni gestione di informazioni, indipendentemente dai mezzi e dalle procedure applicati, in particolare la raccolta, la conservazione, la memorizzazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione o la distruzione di informazioni. È il trattamento periodico di informazioni classificate. Qualora siffatte informazioni vengano trattate soltanto eccezionalmente e il loro trattamento non appartenga alla funzione vera e propria, non è richiesto un CSP.

Capoverso 1 lettera b: con «l'amministrazione, l'esercizio, la manutenzione e la verifica di mezzi informatici» vengono considerate tutte le attività di cui all'articolo 5 lettera b LSIn che sono connesse a particolari diritti d'accesso ai mezzi informatici della Confederazione o esercitando le quali persone sono in grado di pregiudicare considerevolmente gli interessi di cui all'articolo 1 capoverso 2 LSIn, ad esempio attraverso il furto di dati o il sabotaggio. Se gli utilizzatori di mezzi informatici esercitano un'attività sensibile sotto il profilo della sicurezza, si decide unicamente in base ai contenuti delle informazioni trattate. Di conseguenza, vengono inclusi principalmente amministratori e responsabili delle applicazioni dei sistemi. Il termine «esercizio» si riferisce all'attività dei fornitori di prestazioni ai sensi dall'articolo 19 LSIn. Tale termine va chiaramente distinto dall'espressione «gestire sistemi d'informazione» utilizzata nella legislazione sulla protezione dei dati per disciplinare in realtà l'impiego di sistemi d'informazione da parte dei beneficiari di prestazioni (cfr. p. es. art. 24 cpv. 1 LSIn). Attività sensibili sotto il profilo della sicurezza nell'ambito dello sviluppo o della creazione di sistemi d'informazione sono incluse nella lettera b quale parte dell'amministrazione e dell'esercizio.

Capoverso 1 lettera c: la delimitazione di questi locali o settori quali zone di sicurezza rappresenta una misura fisica di sicurezza delle informazioni, in particolare per proteggere locali dei server o determinati locali di condotta. Una zona di sicurezza deve essere protetta adeguatamente. Le persone che devono avere accesso a siffatte zone di sicurezza vanno quindi assoggettate a un controllo di sicurezza di base.

Capoverso 1 lettera d: sempreché trattati internazionali prevedano un controllo, il livello di controllo si rifà alle pertinenti direttive del trattato. Se il trattato non contiene alcuna normativa specifica, il controllo avviene sempre soltanto al livello di controllo di sicurezza di base.

Capoverso 2 lettere a e b: cfr. commento al capoverso 1 lettere a e b.

Capoverso 2 lettere c e d: le persone che svolgono attività sensibili sotto il profilo della sicurezza per il Servizio delle attività informative della Confederazione (SIC) o per la sua Autorità di vigilanza, il Servizio informazioni militare (SIM) o il Centro operazioni elettroniche (COE) della Base d'aiuto alla condotta (BAC) lo fanno regolarmente in settori estremamente sensibili. Le loro attività vanno quindi attribuite al livello di controllo di sicurezza ampliato.

Capoverso 2 lettera e: cfr. commento al capoverso 1 lettera d.

### *Art. 11 Verifica dell'affidabilità secondo la LPers*

Capoverso 1 lettera a: nel caso delle attività sovrane di personale impiegato all'estero e di personale del DFAE soggetto all'obbligo di trasferimento (cfr. l'art. 3 lett. a e b dell'ordinanza del DFAE del 20 settembre 2022[29] concernente l'ordinanza sul personale federale; O-OPers–DFAE) possono essere pregiudicati considerevolmente interessi essenziali della Confederazione. Le persone che esercitano siffatte attività vanno controllate al livello di controllo di sicurezza di base.

Capoverso 1 lettera b: ai sensi della vigente matrice di valutazione della gestione dei rischi della Confederazione, una potenziale dimensione delle conseguenze finanziarie di 50–500 milioni di franchi corrisponde alla ripercussione «considerevole».

[28] RS **142.31**
[29] RS **172.220.111.343.3**

Capoverso 1 lettera c: a seconda dell'interpretazione di questi termini, la gamma di compiti di perseguimento penale o di polizia può essere assai ampia. Il campo di applicazione di questo motivo del controllo deve pertanto essere limitato ai compiti che possono pregiudicare considerevolmente gli interessi pubblici della Confederazione.

Capoverso 1 lettera d: in caso di esercizio non appropriato della propria funzione, le persone operanti nella cerchia ristretta di un capo di dipartimento oppure di una cancelliera o di un cancelliere della Confederazione possono causare regolarmente un danno considerevole. Vanno quindi assoggettate, senza eccezioni, a un controllo di sicurezza di base.

Capoverso 2 lettere a–c: i detentori delle funzioni per i quali, secondo l'articolo 2 capoverso 1 dell'ordinanza del 3 luglio 2001[30] sul personale federale (OPers), spetta al Consiglio federale o, secondo l'articolo 1$^{bis}$ di detta ordinanza, spetta al capo del dipartimento la competenza di costituire, modificare e risolvere il rapporto di lavoro, soddisfano regolarmente uno dei motivi del controllo di cui all'articolo 20*b* capoverso 1 lettere a e b LPers. Ciò vale anche per i detentori delle funzioni di cui all'articolo 2 capoverso 1 lettera e LPers. In virtù dell'elevato danno reputazionale ivi connesso in caso di inadempienze di suddetti detentori, essi vanno assoggettati al controllo di sicurezza ampliato.

Capoverso 2 lettera d: ai sensi della vigente matrice di valutazione della gestione dei rischi della Confederazione, una potenziale dimensione delle conseguenze finanziarie di oltre 500 milioni di franchi corrisponde alla ripercussione «elevata» e una di oltre 1 miliardo di franchi alla ripercussione «molto elevata».

Capoverso 2 lettera e: le attività degli impiegati dei servizi specializzati CSP di cui all'articolo 16 capoverso 1 vanno, parimenti, assoggettati al controllo di sicurezza relativo alle persone ampliato affinché ne sia garantita la credibilità nei confronti delle persone da controllare.

### *Art. 12 Controlli secondo la legge militare del 3 febbraio 1995[31] (LM)*

Capoverso 1 lettera a: non ogni attività normale di militari in uniforme all'estero rientra nella definizione della «rappresentanza sovrana» della Svizzera. La rappresentanza meramente visiva della Svizzera o attività nell'ambito di contingenti di truppe internazionali non devono bastare per una verifica dell'affidabilità. Sono necessarie attività che contemplano competenze decisionali sovrane con effetto esterno in rappresentanza della Svizzera.

Capoverso 1 lettera b: cfr. commento all'articolo 11 capoverso 2 lettera b.

Capoverso 1 lettera c: in caso di bisogno, per decidere se una persona soggetta all'obbligo di leva non debba essere reclutata, o se un militare debba essere degradato o escluso dall'esercito, è sufficiente un controllo di sicurezza di base.

Capoverso 2: oggi è possibile svolgere un controllo di sicurezza relativo alle persone per tutti gli aspiranti, a prescindere da un motivo del controllo materiale. Questa possibilità viene meno con la nuova OCSP. D'ora in poi essi potranno essere controllati soltanto in presenza di un suddetto motivo ai sensi della LSIn o della LM. Se la persona interessata dispone già di un CSP valido ed è aspirante a una funzione che ne presuppone uno, il CSP può essere ripetuto purché sia scaduto il termine minimo di cui all'articolo 43 capoverso 1 LSIn.

### *Art. 13 Controlli di affidabilità secondo la legge federale del 21 marzo 2003[32] sull'energia nucleare (LENu)*

Il contenuto di questo articolo è conforme al vigente disciplinamento di cui all'articolo 3 OCSPN.

### *Art. 14 Verifiche dell'affidabilità secondo la LAEl*

Sulla base della Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 sono «informazioni critiche» tutte le informazioni essenziali per il funzionamento della sicurezza d'approvvigionamento, delle applicazioni critiche o delle infrastrutture critiche. Sono «informazioni estremamente critiche» tutte le informazioni assolutamente essenziali per il funzionamento della sicurezza d'approvvigionamento, delle applicazioni critiche o delle infrastrutture critiche.

[30] RS **172.220.111.3**
[31] RS **510.10**
[32] RS **732.1**

### *Sezione 5: Esecuzione*

Nell'ambito dei lavori preparatori al presente avamprogetto di ordinanza è stato altresì suggerito di prevedere termini massimi per la durata della valutazione del rischio per la sicurezza, in modo che i risultati siano disponibili entro un termine più attuabile. Alla luce delle esperienze fatte, occorre rinunciare volutamente a siffatti termini. La durata della valutazione dipende in larga misura dalla possibilità di procurarsi i dati da acquisire e dal loro contenuto effettivo. Un termine assoluto, in particolare termini molto brevi, porterebbe a un aumento delle dichiarazioni di constatazione a causa dell'impossibilità di chiarire ulteriormente i segni di rischi o della mancanza di dati disponibili in tempo utile.

### *Art. 15 Servizi promotori e servizi decisori*

Capoverso 1: per l'Amministrazione federale i dipartimenti e la Cancelleria federale devono potere stabilire autonomamente l'assegnazione di competenze più idonea per la propria organizzazione.

Capoverso 3: il contenuto di questo capoverso è conforme agli attuali articoli 2 capoverso 2 e 4 capoverso 1 OCSPN.

Capoverso 5: affinché i servizi specializzati CSP possano sbrigare efficacemente il proprio lavoro devono sapere chi presso le singole autorità è responsabile della promozione di verifiche e della decisione sull'esercizio della funzione.

### *Art. 16 Servizi specializzati CSP*

Occorre mantenere il collaudato sistema di due servizi specializzati CSP con differenti competenze.

Ai sensi dell'articolo 16 capoverso 2 lettera d, il servizio specializzato CSP CaF deve verificare le «funzioni della segreteria generale DDPS con compiti di condotta nei confronti del servizio specializzato CSP DDPS». Tali funzioni sono, nello specifico, il segretario generale, il suo sostituto nonché il responsabile del servizio specializzato CSP DDPS. Oltre a queste tre funzioni della SG-DDPS, il servizio specializzato CSP CaF non verifica altre funzioni di cui alla lettera d.

### *Art. 17 Verifica delle condizioni per il controllo*

Le autorità assoggettate sono responsabili di valutare la sensibilità sotto il profilo della sicurezza delle funzioni. Per i servizi specializzati CSP gli elenchi delle funzioni sono quindi vincolanti. Non possono verificare per ogni CSP avviato se la funzione è effettivamente sensibile sotto il profilo della sicurezza. L'onere ivi connesso sarebbe sproporzionato. Per contro, possono e devono verificare se i controlli sono stati avviati correttamente. Incombe peraltro al servizio promotore provare che è disponibile il consenso della persona da controllare e che detto consenso soddisfa i requisiti posti all'articolo 4 capoverso 5 della LPD.

### *Art. 18 Collaborazione*

Se vi fosse la possibilità di eludere domande sull'abuso di alcol o stupefacenti, su debiti personali, su occupazioni accessorie o simili facendo appello ai diritti fondamentali e, grazie a questo espediente, le corrispondenti informazioni non potessero confluire nella valutazione del rischio per la sicurezza, ciò renderebbe illusorio l'intero controllo di sicurezza. Nell'ambito dell'obbligo di collaborazione, la persona sottoposta al controllo è quindi tenuta a cooperare all'accertamento dei fatti. La persona sottoposta al controllo ha il diritto di non volere rispondere a determinate domande. I servizi specializzati avranno però poi il compito di valutare il rifiuto di informare o anche di presentare ulteriori documenti quali referti medici e test antidroga, poiché per le domande sulla sfera segreta personale occorre pur concedere un certo margine. In tale contesto devono essere considerati eventuali obblighi di segretezza legali della persona da controllare.

### *Art. 19 Raccolta dei dati*

Capoverso 1: per entrambi i servizi specializzati CSP le consultazioni di banche dati avvengono, sostanzialmente, per il tramite del servizio specializzato CSP DDPS. I servizi specializzati CSP non devono per forza ricorrere a tutti i mezzi disponibili per valutare il rischio. Ciò è importante in particolare nel controllo ampliato poiché la riduzione dei livelli di controllo non deve comportare un aumento massiccio dei costi dei CSP. Occorre quindi anche rinunciare consapevolmente a stabilire quali dati e quando devono essere acquisiti e trattati. I servizi specializzati CSP possono valutare al meglio quali dati sono necessari per le loro valutazioni dei rischi.

Capoversi 2 e 3: l'audizione della persona interessata di cui all'articolo 34 capoverso 2 lettera d LSIn serve a discutere di fatti che non risultano, o risultano soltanto in modo poco chiaro, dalle rimanenti acquisizioni dei dati. Può essere eseguita anche in assenza di indizi relativi all'esistenza di un rischio per la sicurezza e non è limitata quanto alla sua portata. A causa dell'onere conseguente a detta audizione, questa deve essere limitata al minor numero di funzioni possibile. L'elenco è quindi esaustivo. In tutte le funzioni elencate i collaboratori interni ed esterni vengono equiparati. Nel caso di una ripetizione ordinaria del controllo di cui all'articolo 26 l'audizione non è per forza necessaria se la situazione di rischio non è praticamente mutata.

Capoverso 4: per il chiarimento di particolari circostanze rilevanti per la sicurezza o per ottenere dati supplementari su un periodo di tempo più lungo, i servizi specializzati CSP possono anche sentire terzi. Nelle sue lettere a–c il capoverso 4 menziona i gruppi di persone più importanti noti dalla prassi sinora applicata. Inoltre, a seconda del caso vi sono altre persone (p. es. familiari o ex partner commerciali) che dispongono di preziose informazioni. Queste persone vengono riassunte in una formulazione generale nella lettera d. Da più parti è stato proposto che con l'ordinanza si obblighino i terzi che possono essere interrogati a fornire informazioni veritiere. Le basi legali non prevedono tuttavia alcun obbligo di rispondere. Il terzo interessato può quindi rinunciare in ogni momento a fornire qualsivoglia informazione.

### *Art. 20 Assistenza amministrativa*

I servizi specializzati CSP non acquisiscono tutti i dati in modo autonomo. Ciò riguarda in particolare l'acquisizione di dati all'estero che, in linea di principio, avviene per il tramite di fedpol e del SIC. Soltanto questi servizi sono in grado di valutare l'affidabilità dei dati e delle fonti di dati.

### *Art. 21 Raggruppamento di procedure di controllo*

Le funzioni contemplano le attività più disparate che possono soddisfare differenti motivi del controllo. Se una persona deve essere controllata a causa di svariati motivi del controllo, i controlli vanno raggruppati per ragioni d'economia procedurale. Se, a causa di svariati motivi del controllo, una persona deve essere controllata da entrambi i servizi specializzati CSP, soltanto il servizio specializzato CSP CaF è inteso svolgere il controllo. Il motivo del controllo per quest'ultimo si trova all'articolo 16 capoverso 2, in virtù del quale esiste un elenco delle funzioni esaustivo che deve essere rispettato. Grazie al raggruppamento è possibile evitare onere supplementare inutile. I risultati dei controlli vanno riportati separatamente per il rispettivo motivo del controllo.

### *Art. 22 Condizioni*

I servizi specializzati CSP raccomandano ai servizi decisori condizioni adeguate per ridurre a un livello accettabile il rischio per la sicurezza valutato dai primi. I servizi decisori non sono vincolati a tali raccomandazioni. Possono accettare le condizioni raccomandate, prevederne altre o rinunciarvi.

### *Art. 23 Comunicazione*

Capoverso 1: se in virtù di vari motivi del controllo talune persone sono assoggettate a un controllo che non si svolge nello stesso momento, le constatazioni rilevanti in materia di rischi devono potere essere comunicate in un successivo controllo ai servizi decisori del controllo precedente affinché, in caso di bisogno, possano essere adottate misure di sicurezza. Ciò è importante, in particolare, per i controlli di cui all'articolo 113 LM ai quali sono assoggettati tutti i militari. Se nell'ambito di un altro controllo si constata un rischio in relazione all'arma dell'esercito, i servizi specializzati CSP possono comunicare la dichiarazione alla competente autorità militare.

Capoverso 2: in caso di riserva motivata riguardo alla sicurezza e se vi è urgenza, nell'ottica della prevenzione dai pericoli i servizi specializzati CSP possono informare i servizi competenti in merito alle proprie constatazioni prima che la procedura sia conclusa. Dopodiché il servizio competente può adottare misure di sicurezza preventive. Ciò è particolarmente importante per il reclutamento di persone soggette all'obbligo di leva, un processo che dura al massimo tre giorni. Le riserve riguardo alla sicurezza (p. es. l'uso precedente di droghe) possono essere essenziali anche per la valutazione dell'idoneità al servizio militare da parte dei medici e degli psicologi del reclutamento.

## *Sezione 6: Conseguenze della dichiarazione*

### *Art. 24 Esercizio dell'attività*

Capoverso 1: il servizio decisore ha la responsabilità delle attività delle persone controllate e decide pertanto in merito all'esercizio dell'attività. Eventuali condizioni raccomandate dai servizi specializzati CSP non sono vincolanti per i servizi decisori (cfr. l'art 22). Essi possono accettarle, prevederne altre o rinunciarvi del tutto. Se però l'esercizio dell'attività sensibile sotto il profilo della sicurezza è vincolato a condizioni da parte del servizio decisore, quest'ultimo deve disciplinare anche l'assunzione di eventuali costi legati a dette condizioni. A tal proposito occorre rispettare soprattutto eventuali prescrizioni in materia di diritto del lavoro o di diritto contrattuale. Tuttavia, la mancata osservanza di eventuali condizioni dovrebbe, in ultima analisi, comportare la revoca alla persona controllata dell'attività sensibile sotto il profilo della sicurezza, in quanto senza le condizioni non è possibile ridurre il rischio per la sicurezza a un livello accettabile.

Capoverso 2: la comunicazione della decisione in merito all'esercizio dell'attività è necessaria ai fini dell'accesso a opere militari o a zone di sicurezza. Essa è altresì determinante per il rilascio di un'attestazione di sicurezza nel contesto internazionale di cui all'articolo 30 capoverso 2 lettera b.

### *Art. 25 Uso plurimo di una dichiarazione*

Capoverso 1: se alla persona interessata è già stata rilasciata una dichiarazione ancora valida ed equivalente, di norma per ragioni di economicità non è opportuno eseguire un nuovo controllo. Nel singolo caso la decisione in merito spetta al portatore del rischio.

Capoverso 2: qualora per un nuovo controllo si utilizzi la dichiarazione di un controllo precedente, se è stato eseguito a un livello di controllo superiore, in un'ottica di diritto in materia di protezione dei dati ciò potrebbe portare alla situazione problematica che confluiscano nella valutazione i dati raccolti al livello di controllo più elevato, che non potrebbero essere raccolti a un livello inferiore. La richiesta in virtù del diritto in materia di protezione dei dati di ignorare questa informazione può, nel singolo caso, condurre a risultati sconcertanti dal punto di vista della politica di sicurezza. Per analogia con i disciplinamenti restrittivi applicabili allo sfruttamento di scoperte fortuite presenti in altre basi giuridiche, dovrebbe quindi essere possibile un'utilizzabilità chiaramente delimitata.

### *Art. 26 Ripetizione ordinaria*

La LSIn rinuncia a prescrivere intervalli fissi per la ripetizione ordinaria. Al riguardo, essa fissa unicamente principi generali. Onde potere gestire anche qui in modo adeguato la quantità dei controlli, in base all'esigenza di sicurezza occorre fissare chiare scadenze per la ripetizione. La LSIn, inoltre, conferisce al Consiglio federale la competenza di rinunciare a una ripetizione del controllo per quanto riguarda i militari o i militi della protezione civile. Ciò va applicato ai casi in cui la ripetizione appare sproporzionata rispetto al periodo di servizio residuo.

### *Art. 27 Ripetizione straordinaria*

Capoverso 1: per una ripetizione straordinaria possono essere determinanti soltanto i nuovi rischi essenziali per la valutazione dei rischi ai fini dell'esercizio delle attività. Non sono per contro un motivo per l'avvio di una ripetizione anticipata le violazioni delle condizioni di impiego. Per siffatte violazioni sono previste misure di diritto in materia di personale.

Capoverso 2: la LSIn prevede una ripetizione straordinaria soltanto in caso di fondato sospetto di nuovi rischi. Per il datore di lavoro può però avere rilevanza anche il fatto che vengano meno rischi accertati in precedenza, poiché così non sono più necessarie eventuali restrizioni all'esercizio di attività sensibili sotto il profilo della sicurezza. Anche in questi casi deve pertanto essere possibile avviare una ripetizione straordinaria.

### *Art. 28 Effetto della ripetizione*

L'effetto della ripetizione vale sia per una ripetizione ordinaria, sia per una ripetizione straordinaria. Dato che la ripetizione serve a una nuova valutazione della persona da controllare, in attesa della nuova valutazione quella precedente deve essere determinante per l'esercizio delle attività sensibili sotto il profilo della sicurezza. Tuttavia, se ancora durante la ripetizione del controllo si individuano nuovi rischi, il servizio decisore deve, se del caso, provvedere con misure adeguate affinché tali rischi non diventino concreti fino alla conclusione del controllo. Ciò può avvenire, in particolare, mediante la revoca provvisoria di talune attività o modifiche provvisorie dell'elenco dei compiti.

### *Art. 29 Tutela giurisdizionale*

Ai sensi dell'articolo 31 capoverso 2 LSIn, nell'effettuare la loro valutazione i servizi specializzati CSP non sono vincolati a istruzioni. Ciò deve valere anche per la promozione di procedure di

ricorso relative alle valutazioni, in modo tale che gli organi superiori ai servizi specializzati CSP non possano influenzare indirettamente le valutazioni negando la possibilità di interporre ricorso. I servizi specializzati CSP devono quindi potere decidere autonomamente se vogliono interporre ricorso avverso decisioni del Tribunale amministrativo federale.

### *Art. 30 Attestazione di sicurezza nel contesto internazionale*

Le autorità di sicurezza estere accordano unicamente a persone che sono state sottoposte al CSP l'accesso a informazioni e materiale classificati o a zone di sicurezza. Occorre stabilire la procedura per il rilascio della cosiddetta *«personnel security clearance»* (PSC; dichiarazione di sicurezza relativa alle persone). Per la *«clearance»* è determinante la decisione del servizio decisore di cui all'articolo 24 e non l'esito della valutazione da parte dei servizi specializzati CSP. Ove la *«clearance»* non avvenga nell'interesse della Confederazione, un'attestazione di sicurezza deve essere rilasciata a pagamento.

## *Sezione 7: Trattamento di dati personali*

### *Art. 31 Responsabilità della protezione dei dati e della sicurezza dei dati*

In applicazione dell'articolo 16 capoverso 2 LPD, l'organizzazione delle competenze e responsabilità per la protezione dei dati, che richiede anche la sicurezza dei dati, deve essere disciplinata in relazione con il sistema d'informazione di cui all'articolo 45 LSIn. A tal fine si applica il principio secondo cui la responsabilità incombe al rispettivo detentore dei dati.

### *Art. 32 Controllo periodico del trattamento dei dati personali*

Siccome i dati trattati nell'ambito dei controlli sono particolarmente sensibili, la legalità del loro trattamento deve essere controllata periodicamente da un organo indipendente dai servizi coinvolti nella procedura di controllo.

## *Sezione 8: Disposizioni finali*

### *Art. 33 Gestione elettronica degli affari*

In futuro la gestione degli affari avverrà, per quanto possibile, elettronicamente.

### *Art. 34 Riscossione di emolumenti*

I costi derivanti dai controlli dell'Amministrazione federale centrale vanno preventivati in modo centralizzato presso il DDPS. I costi derivanti dai controlli per servizi esterni all'Amministrazione federale centrale vanno assunti da questi in modo decentralizzato e compensati mediante emolumenti. Mediante l'assegnazione adeguata di risorse finanziarie e di personale al DDPS, il Consiglio federale deve fare in modo che vi sia in ogni momento un equilibrio tra dette risorse e il numero di controlli da effettuare.

### *Art. 35 Prestazioni dei servizi specializzati CSP a favore dei Cantoni*

Ai sensi dell'articolo 86 capoverso 4 LSIn e purché il Consiglio federale lo stabilisca, pagando un emolumento i Cantoni possono avvalersi, per la propria sicurezza delle informazioni, delle prestazioni dei servizi specializzati di cui alla LSIn. Mediante l'articolo 16 si evince che il servizio specializzato CSP DDPS è competente per tali controlli di sicurezza relativi alle persone. Per potersi avvalere di suddette prestazioni i Cantoni devono disporre di una propria base giuridica per i controlli e il servizio specializzato CSP DDPS deve essere tecnicamente in grado di procedere alle valutazioni richieste. Trattandosi, di fatto, di prestazioni di servizio commerciali della Confederazione, vanno applicati i presupposti usuali per esse, in particolare il principio della copertura dei costi. Il DDPS stipula con i rispettivi Cantoni un accordo sulle prestazioni affinché il quantitativo dei controlli e dunque l'onere per il DDPS sia prevedibile e pianificabile. Qualora le prestazioni da fornire dovessero richiedere risorse supplementari dei servizi specializzati, dette prestazioni potranno essere fornite soltanto se ai servizi verranno effettivamente concesse tali risorse. È esclusa una loro compensazione interna alla Confederazione.

### *Art. 36 Abrogazione di altri atti normativi*

Per mantenere il numero dei controlli entro limiti ragionevoli gli elenchi delle funzioni devono essere allestiti e aggiornati in modo conseguente. Il DDPS, che assume i costi dei CSP, gestirà pertanto detti elenchi a livello centrale. In quanto effettivi portatori del rischio, i dipartimenti e la CaF chiedono

su base continuativa le necessarie modifiche degli elenchi. Occorre pertanto abrogare le pertinenti attuali ordinanze dei dipartimenti. Deve parimenti essere abrogata la vigente ordinanza del 4 marzo 2011[33] sui controlli di sicurezza relativi alle persone (OCSP), soggetta a revisione totale con la presente ordinanza. Va inoltre abrogata l'ordinanza del 9 giugno 2006[34] sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari (OCSPN) in quanto i suoi contenuti, sempreché siano ancora necessari, verranno integrati nella presente ordinanza.

### *Art. 37 Modifica di altri atti normativi*

A causa dell'entità della modifica di altri atti normativi il relativo disciplinamento ha luogo nell'allegato 9. Il commento in merito si trova più avanti.

### *Art. 38 Disposizioni transitorie*

Le dichiarazioni riguardanti gli attuali controlli non hanno un termine di scadenza formale e il controllo viene semplicemente ripetuto dopo un determinato periodo. Il disciplinamento proposto offre continuità sia ai servizi promotori sia ai servizi specializzati CSP. Inoltre, concede un margine di manovra sufficiente per sottoporre a un nuovo controllo dapprima le funzioni della massima criticità. Per i controlli ai sensi della legge del 23 marzo 2007[35] sull'approvvigionamento elettrico (LAEI), che finora erano retti dal diritto privato, occorre poi un disciplinamento specifico affinché il contratto in essere possa giungere a scadenza come previsto.

### *Art. 39 Entrata in vigore*

Al momento, la data di entrata in vigore è un criterio di riferimento perseguito. Per la data effettiva sono fattori d'influenza rilevanti, tra gli altri, l'ulteriore iter legislativo e il tempo necessario all'attuazione tecnica delle nuove norme nel sistema d'informazione CSP.

### *Allegati 1–6 Elenchi delle funzioni*

Gli allegati 1, 4 e 6 non vengono pubblicati onde salvaguardare la sicurezza interna ed esterna della Svizzera (cfr. commento ad art. 5).

### *Allegato 7 Raccolta e trattamento di dati*

L'allegato 7 contiene la raccolta e il trattamento dettagliati dei dati per i controlli. Qui non vengono ripetuti i limiti legali che la LSIn fissa per il trattamento dei dati (cfr. p. es. l'art. 27 cpv. 3 o l'art. 34 cpv. 4 LSIn). L'elenco dei dati non è esaustivo, come evidenzia la locuzione «in particolare». In entrambi i numeri si tratta di disposizioni potestative. I servizi specializzati non devono quindi per forza avere accesso a tutti i mezzi disponibili per valutare il rischio. Non ha ad esempio molto senso raccogliere dati fiscali di persone soggette all'obbligo di leva, visto che in giovane età non hanno presentato dichiarazioni dei redditi o comunque non di significative. Ciò è particolarmente importante al livello di controllo di sicurezza ampliato poiché la riduzione dei livelli di controllo non dovrebbe comportare un aumento eccessivo dei costi dei CSP.

Quanto alla raccolta e al trattamento dei dati da fonti pubblicamente accessibili (le cosiddette Open Source Information [OSINF]), si può constatare che non si tratta mai di informazioni private o confidenziali. Di conseguenza, le indagini OSINF non toccano né la sfera privata, protetta dalla Costituzione, né il segreto delle telecomunicazioni. Non si tratta nemmeno di una misura di sorveglianza segreta. In mancanza di una presa di contatto diretta da parte dell'inquirente con la persona oggetto dell'indagine non si è neppure in presenza di un'indagine in incognito. Le indagini OSINF sono un metodo di raccolta e trattamento delle informazioni legittimo e, in virtù della progressiva digitalizzazione, sempre più importante.

### *Allegato 8 Modifica di altri atti normativi*

1. OOrg-DDPS

Ai sensi dell'articolo 31 capoverso 2 LSIn i servizi specializzati CSP sono vincolati a istruzioni soltanto nell'effettuare la propria valutazione. Secondo gli articoli 7 segg. OLOGA essi fanno parte dell'Amministrazione federale centrale e non possono essere aggregati amministrativamente. Deve pertanto essere abrogata l'aggregazione amministrativa del Servizio specializzato per i

[33] RS **120.4**
[34] RS **732.143.3**
[35] RS **734.7**

controlli di sicurezza relativi alle persone in seno al DDPS [alla Segreteria generale del DDPS] contenuta nell'articolo 6 lettera c OOrg-DDPS in virtù dell'articolo 21 capoverso 1 LMSI applicabile sinora.

2. OPers

***Art. 94e Estratto del casellario giudiziale e del registro delle esecuzioni***

La possibilità per il datore di lavoro di richiedere un estratto del casellario giudiziario e del registro delle esecuzioni esiste soltanto se questi ha un interesse legittimo ai sensi del capoverso 1. Con la nozione di «interesse politico» si contempla in particolare il buon nome dell'Amministrazione federale. La possibilità di cui all'articolo 94*e* OPers è da intendersi come lo strumento meno invasivo nei diritti personali degli interessati tra la gamma dei controlli di sicurezza. In linea di principio, questa disposizione si applica soltanto quando la funzione in questione non è già coperta da un controllo di cui all'OCSP. Detta disposizione può tuttavia essere applicata anche quando il CSP è stato effettuato molto tempo prima e il datore di lavoro ha un sospetto fondato che vi è un rischio. Non deve però sorgere un automatismo secondo cui, per le funzioni che non sono soggette ad altri controlli, vengono sistematicamente richiesti i suddetti estratti. Soltanto se in ragione del suo settore di compiti una funzione soddisfa chiaramente i presupposti del capoverso 1 il datore di lavoro può richiedere estratti. Per validi motivi quali un impiego concreto o un incarico particolare è possibile richiedere un nuovo estratto prima di cinque anni. È responsabilità del rispettivo datore di lavoro decidere se in ragione di un'iscrizione nel registro vi è un rischio e, se del caso, quali misure di diritto in materia di personale devono essere adottate.

***Art. 94f Verifica dell'affidabilità***

I presupposti di una verifica dell'affidabilità di cui all'articolo 20*b* LPers devono essere disciplinati nell'OPers. La procedura della verifica deve tuttavia essere completamente inclusa nell'OCSP.

3. OCMI

L'attuale riferimento all'OCSP vigente finora deve essere adeguato al nuovo diritto.

4. Ordinanza del 16 dicembre 2009[36] sui sistemi d'informazione militari (OSIM)

Con il disciplinamento del sistema d'informazione per i controlli di sicurezza relativi alle persone nella LSIn e nella presente ordinanza devono essere abrogati i relativi articolo 67 e allegato 30 OSIM. Inoltre, gli attuali riferimenti all'OCSP vigente finora devono essere adeguati al nuovo diritto.

5. Ordinanza del 22 novembre 2017[37]. concernente l'obbligo di prestare servizio militare (OOPSM)

Gli attuali riferimenti all'OCSP vigente finora devono essere adeguati al nuovo diritto.

6. Ordinanza del 10 dicembre 2004[38] sull'energia nucleare (OENu)

A seguito dell'abrogazione dell'ordinanza sui controlli di sicurezza relativi alle persone nell'ambito degli impianti nucleari (OCSPN) e della sua integrazione nell'OCSP, nell'OENu va inserito un riferimento all'OCSP, in modo che il lettore interessato al diritto possa trovare più facilmente le disposizioni corrispondenti. La copertura dei costi dovrebbe invece essere inserita direttamente nell'OENu.

## 4.4 Ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz)

***Osservazioni preliminari***

Per la comprensione della materia in questa sede appaiono brevi considerazioni almeno riguardo alle seguenti disposizioni della LSIn:

- quando si parla di mandati sensibili sotto il profilo della sicurezza, si deve fare riferimento alle definizioni giuridiche dell'articolo 5 lettera b LSIn. Di conseguenza, siffatti mandati contemplano il trattamento di informazioni classificate CONFIDENZIALE o SEGRETO ai sensi dell'articolo 13 LSIn, l'amministrazione, l'esercizio, e la verifica di mezzi informatici del livello di sicu-

[36] RS **510.911**
[37] RS **512.21**
[38] RS **732.11**

rezza «protezione elevata» o «protezione molto elevata» a norma dell'articolo 17 LSIn nonché l'accesso a zone di sicurezza, ivi compreso alle zone di protezione previste dalla legislazione sulla protezione di impianti militari. La forma giuridica dei mandati è irrilevante;

- sono considerate aziende ai sensi dell'OPSAz le imprese, le imprese subappaltatrici o loro parti che adempiono un mandato pubblico comportante l'esercizio di un'attività sensibile sotto il profilo della sicurezza (cfr. l'art. 49 LSIn);
- da mandanti ai sensi dell'OPSAz fungono le autorità o le organizzazioni assoggettate di cui all'articolo 2 LSIn (cfr. l'art. 50 cpv. 1 lett. a LSIn).

**Ingresso**

In seno al capitolo 4 della LSIn, la procedura di sicurezza relativa alle aziende (PSA) costituisce un complesso di norme a sé stante che a sua volta costituisce la base della relativa legislazione esecutiva. L'articolo 84 capoverso 1 LSIn stabilisce la competenza generale delle autorità assoggettate di emanare disposizioni esecutive relative alla LSIn. L'articolo 73 assegna concretamente al Consiglio federale i settori da disciplinare nel dettaglio.

***Sezione 1: Disposizioni generali***

***Art. 1 Oggetto e campo d'applicazione***

Capoverso 1: ai fini della descrizione della materia normativa dell'OPSAz la disposizione si rifà ai mandati di legiferare di cui all'articolo 73 LSIn imposti al Consiglio federale.

Capoverso 2: purché autorità e organizzazioni siano soggette al campo d'applicazione della LSIn o dell'OSIn, entrano in linea di conto anche quali mandanti per mandati sensibili sotto il profilo della sicurezza. Il campo d'applicazione dell'OPSAz deve quindi coincidere con quello della LSIn e dell'OSIn (cfr. anche il n. 3.6 lett. a).

***Art. 2 Aziende interessate***

Capoverso 1: l'aggiudicazione da parte di autorità e organizzazioni svizzere di mandati sensibili sotto il profilo della sicurezza ad aziende con sede in Svizzera costituisce la fattispecie di base per l'esecuzione della procedura di sicurezza relativa alle aziende. Le imprese subappaltatrici con sede in Svizzera vengono equiparate a dette aziende. Il termine «azienda» è da intendersi in senso lato. Né la forma giuridica, né le dimensioni hanno dunque importanza. Sono decisivi unicamente la sensibilità sotto il profilo della sicurezza del mandato e l'assoggettamento dell'azienda all'ordinamento giuridico svizzero.

Possono essere considerate aziende anche le unità amministrative decentralizzate dell'Amministrazione federale nonché organizzazioni e persone di diritto pubblico o privato alle quali sono attribuiti compiti federali, sempreché non siano soggette alla LSIn.

Capoverso 2: l'OPSAz contempla le fattispecie nazionali. L'esecuzione di procedure di sicurezza relative alle aziende per le aziende con sede all'estero è retta dai corrispondenti trattati internazionali.

***Art. 3 Autorità competente***

Capoverso 1: l'autorità «servizio specializzato competente per l'esecuzione della procedura di sicurezza relativa alle aziende» (servizio specializzato PSA) deve essere aggregata sotto il profilo organizzativo. La pertinente decisione viene presa contestualmente a quella sull'aggregazione amministrativa del servizio specializzato della Confederazione per la sicurezza delle informazioni (cfr. n. 3.8).

Capoverso 2: in relazione con le procedure di sicurezza transfrontaliere relative alle aziende, il servizio specializzato PSA dipende dalla collaborazione con l'autorità di sicurezza svizzera designata, l'unica attraverso la quale si tengono i contatti con l'estero. Il coordinamento della procedura di sicurezza relativa alle aziende (PSA) con gli iter procedurali della suddetta autorità incombe al servizio specializzato PSA.

***Sezione 2: Avvio della procedura di sicurezza relativa alle aziende***

***Osservazione preliminare sulla sezione 2***

L'avvio della procedura deve potere avere luogo quanto prima possibile nel processo d'acquisto. In questa prima fase occorre soprattutto chiarire se il mandato da aggiudicare è sensibile sotto il

profilo della sicurezza e se è quindi soddisfatto il presupposto processuale centrale. Non vengono creati elementi pregiudicanti per la procedura di aggiudicazione.

### *Art. 4 Domanda di avvio della procedura*

Capoverso 1 lettere a e b: gli incaricati della sicurezza delle informazioni garantiscono che aspetti inerenti alla sicurezza delle informazioni confluiscano già in una fase iniziale nelle considerazioni di un'aggiudicazione a terzi.

Capoverso 1 lettera c: le aziende che aggiudicano un subappalto assumono così a loro volta il ruolo di mandanti. Di conseguenza, purché vengano autorizzate a farlo dal proprio mandante, sono altresì tenute a presentare la domanda di avvio della procedura di sicurezza relativa alle aziende. È competente l'incaricato della sicurezza aziendale di cui all'articolo 12.

Capoverso 2: al Consiglio federale (salvo che per sé stesso) non spetta stabilire la competenza per l'avvio della procedura per le autorità assoggettate di cui all'articolo 2 capoverso 1 LSIn. Nell'OPSAz esso si limita pertanto a lasciare comunicare alle autorità assoggettate il servizio competente.

Capoverso 3 lettera a: la descrizione della prestazione edile, fornitura o prestazione di servizio serve al servizio specializzato PSA in particolare come indicatore di identificazione, specialmente poi se un'azienda esegue più mandati sensibili sotto il profilo della sicurezza.

Capoverso 3 lettera b: poiché la sensibilità sotto il profilo della sicurezza del mandato è il presupposto per l'avvio della PSA, si deve illustrare per lo meno con una motivazione sommaria fino a che punto sono soddisfatti i presupposti di cui all'articolo 5 lettera b LSIn. L'alleggerimento della prova grazie a una motivazione soltanto sommaria è inteso, in particolare, a consentire un avvio della procedura in una fase relativamente precoce al fine di toccare il meno possibile gli iter procedurali della procedura di aggiudicazione.

Capoverso 3 lettera c: nel singolo caso la PSA deve essere coordinata fin da subito con le disposizioni procedurali nel settore degli appalti pubblici. È pertanto propizio all'economia procedurale se già in questo stadio iniziale il mandante ha le idee chiare sulla procedura di aggiudicazione applicabile.

### *Art. 5 Esame della domanda*

Capoverso 1: per quanto riguarda l'avvio della procedura, il servizio specializzato PSA gode di un margine di discrezionalità relativamente ampio che, tuttavia, deve sempre esercitare d'intesa con il mandante estero (cfr. l'art. 53 cpv. 2 LSIn).

Capoverso 2: con questa disposizione il Consiglio federale limita il potere discrezionale del servizio specializzato PSA e stabilisce in via definitiva le fattispecie per le quali deve essere obbligatoriamente avviata la PSA. Si tratta delle quattro configurazioni seguenti:

- lettera a: le aziende che operano nell'ambito della massima necessità di protezione di informazioni e mezzi informatici devono sempre essere soggette alle disposizioni dell'OPSAz, a prescindere dal genere o dal luogo di adempimento del mandato;
- lettera b: qui il Consiglio federale stabilisce che il trattamento di informazioni classificate CONFIDENZIALE per le quali l'interesse a conservare il segreto è ripartito su più autorità o dipartimenti costituisce, senza eccezioni, un caso per la PSA;
- lettera c: per analogia con la lettera b, se i mezzi informatici del livello di sicurezza «protezione elevata» vengono impiegati per compiti che coinvolgono più autorità o compiti interdipartimentali, anche l'esercizio, la manutenzione e la verifica di detti mezzi informatici devono attivare, senza eccezioni, la PSA;
- lettera d: un'attestazione di sicurezza aziendale internazionale deve disporre di una base solida, per la quale unicamente l'esecuzione della procedura di sicurezza relativa alle aziende secondo la LSIn offre la garanzia necessaria e sufficiente. Sebbene debba sostenere i costi della procedura, l'azienda non può tuttavia semplicemente «acquistare» in tal modo un marchio di qualità statale. Il servizio specializzato PSA avvierà la procedura soltanto in presenza di una pertinente domanda di un'autorità estera o di un'organizzazione internazionale e se si tratta effettivamente di un mandato sensibile sotto il profilo della sicurezza.

Capoverso 3: questo termine ordinatorio è inteso fornire ai mandanti un orientamento per la pianificazione e il coordinamento della procedura di aggiudicazione e incitare il servizio specializzato PSA al rispetto dell'imperativo di celerità.

### *Art. 6 Esame della domanda con autorità di sicurezza estere*

Capoverso 1: se il mandante intende affidare a un'azienda estera, dunque non soggetta all'ordinamento giuridico svizzero, un mandato sensibile sotto il profilo della sicurezza (cfr. l'art. 49 LSIn), presenta la pertinente domanda contestualmente al servizio specializzato PSA. Le necessarie fasi procedurali sono ora svolte dal servizio specializzato della Confederazione per la sicurezza delle informazioni (cfr. l'articolo 83 LSIn) assieme all'autorità di sicurezza estera.

Capoverso 2: purché esista un pertinente trattato internazionale (cfr. l'art. 87 LSIn), su richiesta del servizio specializzato della Confederazione per la sicurezza delle informazioni l'autorità di sicurezza estera o confermerà che l'azienda dispone di una dichiarazione di sicurezza aziendale, oppure avvierà la PSA. La procedura è interamente disciplinata dal diritto dello Stato in cui ha sede l'azienda e anche il rilascio di una pertinente attestazione di sicurezza aziendale ha luogo in virtù del diritto estero.

### *Art. 7 Definizione dei requisiti di sicurezza*

Capoverso 1: con l'OSIn e l'OCSP si menzionano entrambi gli atti normativi determinanti che devono essere considerati nel definire i requisiti di sicurezza nel singolo caso.

Capoverso 2: nelle relazioni internazionali il trattato internazionale prevale sull'OSIn e sull'OCSP.

Capoverso 3: fatto salvo l'articolo 5 capoverso 2, il mandante e il servizio specializzato PSA possono trovare un'intesa sull'avvio della procedura. Una volta avviata la procedura, deve altresì essere possibile che si accordino su una ripartizione dei compiti sia nella procedura di aggiudicazione, sia nell'adempimento del mandato. Tale modo di procedere dovrebbe essere utile specialmente laddove, dopo il rilascio dell'attestazione di sicurezza aziendale, per l'intera durata di quest'ultima siano opportune misure di controllo di ampia portata o permanenti. È nell'interesse diretto del mandante (titolare del segreto) potere effettuare controlli indipendentemente dal servizio specializzato PSA. Le misure coercitive delle autorità non sono trasferibili al mandante.

Capoverso 4: nel rapporto tra la procedura di aggiudicazione e la procedura di sicurezza relativa alle aziende, è sempre la prima a costituire la procedura direttiva. In quanto strumento della sicurezza delle informazioni, la suddetta procedura di sicurezza segue sempre gli iter della procedura di aggiudicazione. Per quest'ultima, tuttavia, le fasi della procedura di sicurezza devono essere integrate nel piano procedurale. Ne consegue che i pertinenti compiti di coordinamento incombono alla parte principalmente interessata nella procedura direttiva, ossia al mandante.

## *Sezione 3: Valutazione delle aziende*

### *Art. 8 Notifica delle aziende idonee*

Capoverso 1: contrariamente all'esame del mero avvio della procedura, con la valutazione dell'idoneità il servizio specializzato PSA oramai compie atti ufficiali incomparabilmente più costosi e approfonditi. Per ragioni inerenti al diritto e all'economia procedurale, a questo stadio della procedura di sicurezza relativa alle aziende è quindi imprescindibile che a queste analisi vengano sottoposte soltanto le aziende che dal punto di vista del mandante sono ancora suscettibili di ottenere il mandato. In linea di principio, al servizio specializzato PSA non vanno annunciate più di cinque aziende per la valutazione dell'idoneità. Un'estensione deve potere avvenire soltanto in casi motivati. Questa clausola d'eccezione deve, in particolare, costituire una via d'uscita in caso di sviluppi imprevisti nella procedura di aggiudicazione e consentire annunci ulteriori.

Capoverso 2: il consenso dell'azienda all'esecuzione della procedura è il presupposto per l'avvio della PSA (cfr. l'art. 50 cpv. 2 LSIn) e deve pertanto essere verificato d'ufficio dal servizio specializzato PSA. Questo consenso può essere esplicito o risultare già dalle condizioni di partecipazione elencate nella documentazione del bando di gara e accettate dall'azienda.

Capoverso 3 lettera a: conformemente all'articolo 56 capoverso 1 lettera a LSIn, per valutare l'idoneità delle aziende il servizio specializzato PSA può acquisire autonomamente dati pertinenti presso di esse. Alle aziende incombe così un obbligo di collaborazione che viene delineato nell'articolo 9 capoverso 1 lettere a–g. Il fatto che un'azienda evidenzi una carente disponibilità alla collaborazione è equiparabile a un mancato consenso alla procedura. La procedura viene abbandonata per l'azienda in questione a causa della mancanza di un presupposto processuale.

Capoverso 3 lettera b: se, contrariamente alle indicazioni rifiutate (lett. a), le indicazioni errate non costituiscono un ostacolo alla procedura, devono però essere tenute da conto nelle considerazioni

sulla decisione in merito all'affidabilità e, di norma, fanno sì che l'azienda venga giudicata un rischio per la sicurezza.

Capoverso 4: per analogia con l'articolo 5 capoverso 3, questo termine ordinatorio è inteso fornire ai mandanti un orientamento per la pianificazione e il coordinamento della procedura di aggiudicazione e incitare il servizio specializzato PSA al rispetto dell'imperativo di celerità.

### *Art. 9 Raccolta dei dati*

Capoverso 1 lettere a–g: queste disposizioni rendono concreto l'articolo 56 LSIn ed elencano in un'enumerazione non esaustiva i punti reputati idonei per valutare l'azienda, in termini di sicurezza, quanto alla sua affidabilità nonché alle sue relazioni con Stati e organizzazioni esteri. Le acquisizioni vengono svolte dal servizio specializzato PSA.

Capoverso 2: l'acquisizione dei dati di cui all'articolo 6 capoverso 1 lettera a della legge federale del 25 settembre 2015[39] sulle attività informative (LAIn) è di competenza del SIC. A tal proposito si esamina se finora l'azienda si è manifestata in relazione a terrorismo, spionaggio, proliferazione, attacchi contro infrastrutture critiche o estremismo violento. Le acquisizioni vengono effettuate dal SIC.

Capoverso 3 lettera a: ai sensi dell'articolo 56 capoverso 1 lettera a LSIn, per la valutazione dell'idoneità delle aziende il servizio specializzato PSA può raccogliere di sua iniziativa dati presso di esse. Alle aziende incombe così un obbligo di collaborazione delineato all'articolo 9 capoverso 1 lettere a–g. Se un'azienda mostra una scarsa disponibilità a collaborare, ciò equivale a un mancato consenso alla procedura. La procedura viene interrotta a causa di un presupposto processuale mancante per la relativa azienda.

Capoverso 3 lettera b: se, contrariamente alle indicazioni rifiutate (lett. a), le indicazioni errate non costituiscono un ostacolo alla procedura, devono però essere tenute da conto nelle considerazioni sulla decisione in merito all'affidabilità e, di norma, fanno sì che l'azienda venga giudicata un rischio per la sicurezza.

### *Art. 10 Esclusione dalla procedura*

Capoverso 1: sia l'articolo 44 della legge federale del 21 giugno 2019[40] sugli appalti pubblici (LAPub), sia l'articolo 57 LSIn enumerano varie fattispecie in presenza delle quali il mandante può o deve escludere un'azienda dalla procedura di aggiudicazione. Affinché la procedura di aggiudicazione e la procedura di sicurezza relativa alle aziende non si blocchino inutilmente l'un l'altra, il fatto che vi siano soltanto indizi della presenza di motivi di esclusione di cui all'articolo 44 LAPub non deve dissuadere il mandante dall'annunciare una siffatta azienda al servizio specializzato PSA per lo svolgimento della valutazione dell'idoneità, senza che il mandante debba già decidere in merito a un'esclusione. Tuttavia, esso deve comunicare i propri riscontri in tal senso al servizio specializzato PSA ai fini di detta valutazione. D'altro canto, quest'ultimo deve a sua volta informare il mandante il più rapidamente possibile se, sulla base della propria acquisizione dei dati, emergono riscontri che possono indurre il mandante a escludere l'azienda.

Capoverso 2: in virtù di questo continuo scambio di informazioni, è giustificato che il servizio specializzato PSA per intanto continui a valutare un'azienda dubbia quanto alla sua idoneità finché il mandante non avrà deciso in merito a un'eventuale esclusione.

Capoverso 3: se nella procedura di aggiudicazione c'è già stata un'esclusione da parte del mandante, alla procedura di sicurezza relativa alle aziende manca l'oggetto della procedura. Si tratta quindi di un chiaro caso di cui all'articolo 51 capoverso 1 lettera c LSIn e la PSA va prontamente abbandonata per l'azienda in questione.

### *Art. 11 Scambio di informazioni*

Questa disposizione riguarda il contenuto dello scambio di informazioni reciproco. Per la valutazione dell'idoneità, ad esempio, si mettono a disposizione del servizio specializzato PSA e del mandante, rispettivamente, indicazioni utili dal punto di vista del diritto d'aggiudicazione e riscontri rilevanti per la sicurezza ai fini della sua decisione sull'esclusione di cui all'articolo 44 LAPub.

[39] RS **121**
[40] RS **172.056.1**

### *Sezione 4: Piano in materia di sicurezza*

### *Art. 12 Incaricati della sicurezza aziendale*

Capoverso 1: un'azienda annunciata dal mandante per la valutazione dell'idoneità deve designare un incaricato della sicurezza aziendale e annunciarlo al servizio specializzato PSA. Affinché i requisiti di sicurezza definiti possano produrre l'effetto necessario occorre che la direzione dell'azienda possa essere ritenuta responsabile al riguardo. L'incaricato della sicurezza aziendale deve quindi disporre di taluni diritti di impartire istruzioni in seno all'azienda, almeno nell'ambito della sicurezza. L'ideale sarebbe che l'incaricato sia membro della direzione e possa così intervenire nelle decisioni o che per lo meno agisca su mandato diretto di un membro.

Capoverso 2 lettera a: per esercitare un'influenza efficiente ed efficace sulla sicurezza delle informazioni dell'azienda, il servizio specializzato PSA necessita di un interlocutore attraverso il quale possano svolgersi tutti i contatti.

Capoverso 2 lettera b: l'incaricato della sicurezza risponde nei confronti del servizio specializzato PSA quanto all'attuazione del piano in materia di sicurezza. Il servizio specializzato PSA provvede affinché l'incaricato riceva una formazione e un perfezionamento adeguati.

Capoverso 2 lettera c: nei casi in cui l'azienda è stata autorizzata dal mandante a coinvolgere imprese subappaltatrici, l'incaricato della sicurezza aziendale è legittimato a presentare al servizio specializzato PSA la richiesta di avvio della procedura di sicurezza relativa alle aziende per suddette imprese (cfr. l'art. 4 cpv. 1 lett. c).

### *Art. 13 Comunicazione dell'aggiudicazione*

Capoverso 1: di norma, i contratti quadro dovrebbero essere l'elemento attivante per il rilascio di una dichiarazione di sicurezza aziendale. Viceversa, i singoli rapporti di mandato connessi al contratto quadro possono, eventualmente, incidere sul rischio per la sicurezza delle informazioni tanto da richiedere un adeguamento del piano in materia di sicurezza. È quindi essenziale che il servizio specializzato PSA sia sempre al corrente della situazione dei mandati nell'azienda quanto alla loro sensibilità sotto il profilo della sicurezza.

Capoverso 2: le indicazioni che deve fornire il mandante e che sono necessarie per l'allestimento del piano in materia di sicurezza comprendono in particolare:

- indicazioni sul livello della sensibilità sotto il profilo della sicurezza del mandato in base all'articolo 5 LSIn;
- la menzione delle persone alle quali è affidata l'esecuzione del mandato sensibile sotto il profilo della sicurezza (per lo svolgimento di controlli di sicurezza relativi alle persone);
- indicazioni sull'impiego di mezzi informatici aziendali, in particolare se vengono utilizzati in rete o se ne vengono isolati.

### *Art. 14 Contenuto ed esame del piano in materia di sicurezza*

Capoverso 1: il sopralluogo assicura che con il piano in materia di sicurezza si possono imporre in modo mirato all'azienda le misure necessarie, idonee e adeguate alla situazione nel suo complesso. In tal modo, da una parte, il sopralluogo serve alla sicurezza delle informazioni e, dall'altra, tutela però anche l'azienda da un onere sproporzionato.

Capoverso 2: ai fini dell'allestimento del piano in materia di sicurezza, il servizio specializzato PSA specifica per l'azienda un contesto nel quale essa deve adottare e documentare le misure di sicurezza adeguate alla situazione complessiva. Devono essere documentate misure organizzative (p. es. gestione delle chiavi, sorveglianza dei locali), di personale (controlli di sicurezza relativi alle persone), tecniche (p. es. impiego di mezzi informatici) e fisiche (protezioni antiscasso).

Capoverso 3: l'allestimento di piani in materia di sicurezza può rivelarsi complesso, in particolare poiché all'azienda vengono accordati, consapevolmente, anche taluni margini di discrezionalità. Se il piano in materia di sicurezza non supera al primo tentativo la verifica da parte del servizio specializzato PSA (cfr. l'art. 59 cpv. 2 LSIn), quest'ultimo deve accordare all'azienda un termine suppletorio per migliorare il piano, impartendo anche istruzioni concrete riguardo ai punti a cui si deve porre rimedio e a come farlo.

Capoverso 4: per analogia con l'articolo 6 capoverso 3, questo termine ordinatorio è inteso fornire ai mandanti un orientamento per la pianificazione e il coordinamento della procedura di aggiudicazione e incitare il servizio specializzato PSA al rispetto dell'imperativo di celerità.

### *Art. 15 Controlli di sicurezza relativi alle persone*

Capoverso 1: per eseguire un mandato sensibile sotto il profilo della sicurezza l'azienda deve organizzarsi in modo tale che a un CSP debba essere sottoposto soltanto un numero minimo di persone, strettamente necessario all'adempimento del mandato. Le domande di controlli per persone che svolgono attività soltanto potenzialmente sensibili sotto il profilo della sicurezza sono illecite e vengono respinte dal servizio specializzato PSA.

Capoverso 2: per ragioni di economia procedurale può avere senso che soprattutto grandi aziende siano autorizzate ad avviare autonomamente CSP. Ciò non cambia il fatto che il servizio specializzato PSA decide in via definitiva quali persone vengono effettivamente controllate.

## *Sezione 5: Dichiarazione di sicurezza aziendale e ripetizione della procedura*

### *Art. 16 Rilascio della dichiarazione di sicurezza aziendale*

Non prevista dalla legge, la limitazione della dichiarazione di sicurezza aziendale a singoli elementi di attività sensibili sotto il profilo della sicurezza ai sensi dall'articolo 5 lettera b LSIn appare tuttavia compatibile con gli obiettivi della LSIn stessa, se non addirittura imposta dal principio di proporzionalità. Da un lato, ha senso che, ad esempio per il trattamento di informazioni classificate CONFIDENZIALE, a un'azienda non vengano imposte misure di protezione onerose quanto quelle necessarie per il trattamento di informazioni classificate SEGRETO. Dall'altro, un piano in materia di sicurezza orientato alle informazioni classificate CONFIDENZIALE va obbligatoriamente adeguato se ora ne sono interessate anche informazioni classificate SEGRETO. Occorre garantire mediante decisione la certezza del diritto in merito al livello di trattamento ammesso.

### *Art. 17 Annunci dell'azienda*

Capoversi 1 e 2: questi elenchi non esaustivi rendono concreto l'articolo 63 capoverso 2 LSIn quanto al contenuto dell'obbligo di annuncio concernente i cambiamenti rilevanti sotto il profilo della sicurezza nell'azienda.

Capoverso 3: un intervento tempestivo può essere agevolato dal fatto di agire già in presenza di un sospetto iniziale, senza attendere le ripercussioni di un incidente. Già il solo sospetto di un incidente viene pertanto dichiarato soggetto all'obbligo di annuncio.

Capoverso 4: oltre all'azienda, i cambiamenti e gli incidenti possono riguardare imprese subappaltatrici o fornitori dell'azienda. Mentre le imprese subappaltatrici autorizzate sono soggette autonomamente all'obbligo di annuncio primario di cui ai capoversi 1 e 2, ciò non vale per i fornitori che entrano in contatto soltanto indirettamente con l'attività sensibile sotto il profilo della sicurezza. Sempreché siano interessati da un incidente che può avere ripercussioni sull'attività sensibile sotto il profilo della sicurezza, anche tale evento deve essere annunciato dall'impresa.

Capoverso 5: lo scopo di questa disposizione è di impedire che la validità della dichiarazione di sicurezza aziendale scada durante un mandato in corso e che a causa di ciò il rapporto di mandato venga d'un colpo dichiarato illegittimo e, in linea di massima, debba essere interamente annullato. Con l'avvio tempestivo di un rinnovo della dichiarazione di sicurezza aziendale si può evitare questa situazione (cfr. anche considerazioni sull'art. 20 cpv. 2).

### *Art. 18 Obblighi del mandante*

Capoverso 1: i mandanti sono naturalmente in contatto stretto e frequente con le aziende, per cui è anche assai probabile che si accorgano di eventuali irregolarità. Perciò, da una parte, l'obbligo di annuncio dell'azienda per cambiamenti o incidenti rilevanti sotto il profilo della sicurezza viene esteso al mandante se esso fa le relative constatazioni nell'azienda. Dall'altra, al mandante incombe inoltre l'adozione di misure immediate.

Capoverso 2 lettera a: le fattispecie di cui all'articolo 44 LAPub possono avere effetti negativi sull'attuazione del piano in materia di sicurezza e devono quindi, eventualmente, essere valutate anche alla luce della sicurezza delle informazioni. Se fa constatazioni in tal senso, il mandante assume quindi un obbligo di annuncio nei confronti del servizio specializzato PSA. Tale obbligo sussiste anche se il mandante non intende revocare l'aggiudicazione.

Capoverso 2 lettera b: i cambiamenti del mandato rilevanti per la sicurezza spesso incidono sul piano in materia di sicurezza, per cui il servizio specializzato PSA deve essere tenuto al corrente.

Capoverso 2 lettera c: ciò che vale per il cambiamento di un mandato vale, per analogia, anche per l'aggiudicazione di un nuovo mandato. Si rinvia alle precedenti considerazioni sulla lettera b.

### *Art. 19 Attestazione internazionale di sicurezza aziendale*

Capoverso 1: il rilascio di un'attestazione internazionale di sicurezza aziendale costituisce una procedura amministrativa priva di specificità e di oneri di rilievo e pertanto a tal fine è riscosso un emolumento forfettario di 100 franchi.

Capoverso 2: la situazione è diversa se l'azienda non dispone ancora di un'attestazione di sicurezza aziendale svizzera. L'esecuzione della procedura di sicurezza relativa alle aziende necessaria previamente rappresenta un onere che deve essere fatturato in funzione del tempo impiegato. La tariffa oraria varia a seconda dell'urgenza e della necessaria qualifica del personale che esegue la procedura.

Capoverso 3: il rilascio di un'attestazione internazionale di sicurezza aziendale è, in linea di massima, un atto amministrativo tra il servizio specializzato PSA e l'azienda. Spesso, tuttavia, per fare esaminare la validità delle attestazioni che le vengono presentate l'autorità di sicurezza estera si rivolgerà alla propria controparte svizzera. È pertanto opportuno che il servizio specializzato PSA comunichi o faccia comunicare su richiesta all'autorità di sicurezza estera, per il tramite del servizio specializzato della Confederazione per la sicurezza delle informazioni, il rilascio di un'attestazione internazionale di sicurezza aziendale.

### *Art. 20 Revoca della dichiarazione di sicurezza aziendale e ritiro del mandato*

Capoverso 1: purché la sicurezza delle informazioni non sia in grave pericolo, seguendo il principio di proporzionalità inizialmente va concessa all'azienda la possibilità di rettificare le irregolarità constatate. Poiché in tale procedura il mandante gode, in via eccezionale, dei diritti di una parte legittimata a ricorrere, deve essere sentito ogni volta prima che vengano emanate decisioni di procedura.

Capoverso 2: nei rari casi di una revoca della dichiarazione di sicurezza aziendale occorre notare che in tal modo si innescano due ulteriori circostanze giuridicamente contestabili. Da un lato, il mandante deve revocare l'aggiudicazione (decisione) e, dall'altro, fa seguito la rescissione di un contratto di diritto privato. Per garantire la sicurezza delle informazioni, fondandosi sull'articolo 55 capoverso 2 della legge federale del 20 dicembre 1968[41] sulla procedura amministrativa (PA) il servizio specializzato PSA, di norma, revocherà a titolo precauzionale l'effetto sospensivo a un ricorso contro la revoca di una dichiarazione di sicurezza aziendale. La decisione può quindi essere eseguita senza ritardi. Sempreché non invochi la clausola derogatoria dell'articolo 58 capoverso 3 LSIn, ora il mandante deve ritirare il mandato sensibile sotto il profilo della sicurezza e garantire che l'azienda sia immediatamente privata di ogni possibilità di incidere negativamente sulla sicurezza delle informazioni. Se si impugna la revoca della dichiarazione di sicurezza aziendale, lo stesso vale per la revoca dell'aggiudicazione. È da ritenersi che le due procedure di ricorso vengano riunite dal Tribunale amministrativo federale. Su richiesta di una parte, nello stesso procedimento possono essere giudicati anche diritti di carattere civile (cfr. l'art. 40 cpv. 1 della legge del 17 giugno 2005[42] sul Tribunale amministrativo federale [LTAF]).

Capoverso 3: questo termine ordinatorio è inteso consentire al servizio specializzato PSA di fare chiarezza, in tempo utile, sull'eliminazione di una minaccia per la sicurezza e di decidere se eventualmente è ancora necessario il proprio intervento sovrano.

### *Art. 21 Ripetizione della procedura*

Capoverso 1: la presente disposizione attribuisce al servizio specializzato, che agisce d'ufficio, la competenza per avviare la procedura di ripetizione. Contrariamente alla procedura semplificata (cfr. l'art. 65 LSIn), in questo caso si svolge l'intera procedura (incl. la valutazione dell'idoneità).

Capoverso 2: questa disposizione è intesa impedire che i mandati in corso debbano essere interrotti e annullati se la procedura di ripetizione si protrae oltre la data di scadenza della dichiarazione di sicurezza aziendale. Risultante agli atti, l'atto formale dell'apertura della procedura da parte del servizio specializzato PSA deve essere sufficiente a prorogare fino alla nuova decisione la durata di validità della dichiarazione di sicurezza aziendale in scadenza.

Capoverso 3: nel corso della procedura di ripetizione, il servizio specializzato PSA può giungere alla conclusione che non sussistono i presupposti per un rinnovo della dichiarazione di sicurezza aziendale o che la procedura deve essere abbandonata per altri motivi. Tutte queste decisioni

[41] RS **172.021**

[42] RS **173.32**

pongono fine alla durata di validità prorogata di cui al capoverso 2. L'annullamento dei rapporti giuridici è disciplinato dalle norme di revoca della dichiarazione di sicurezza aziendale (cfr. l'art. 20).

### *Sezione 6: Trattamento dei dati personali*

### *Art. 22 Sistema d'informazione sulla procedura di sicurezza relativa alle aziende*

I dati personali e i dati aziendali della procedura di sicurezza relativa alle aziende devono essere definiti a livello di ordinanza. Il relativo elenco si trova nell'allegato dell'OPSAz.

### *Art. 23 Controllo periodico del trattamento di dati personali*

Utilizzato nella procedura di sicurezza relativa alle aziende, il sistema d'informazione di cui all'articolo 70 capoverso 1 LSIn può eventualmente contenere dati personali degni di particolare protezione. È pertanto indicata una pertinente vigilanza indipendente. Il dipartimento competente dispone di una certa discrezionalità quanto alla scelta dell'organo di revisione.

### *Sezione 7: Disposizioni finali*

### *Art. 24 Abrogazione e modifica del diritto previgente*

Capoverso 1: applicabile unicamente nel DDPS, la procedura di tutela del segreto è disciplinata nell'ordinanza sulla tutela del segreto. La procedura di sicurezza relativa alle aziende in uso a livello federale copre il contenuto della materia normativa dell'ordinanza sulla tutela del segreto, per cui quest'ultima può essere abrogata senza sostituzione.

Capoverso 2: nell'articolo 5 capoverso 1 lettera d dell'OCMI si rinvia all'ordinanza sulla tutela del segreto, ciò che deve essere rettificato.

Capoverso 3: nell'articolo 56 capoverso 1 lettera b LSIn il SIC è menzionato esplicitamente quale fonte d'informazione del servizio specializzato PSA. Ai sensi dell'articolo 60 capoverso 1 LAIn, il SIC comunica dati personali ad autorità svizzere se ciò è necessario per la salvaguardia della sicurezza interna o esterna. Il Consiglio federale determina le autorità interessate. Lo fa nell'allegato 3 dell'ordinanza del 16 agosto 2017[43] sulle attività informative (OAIn), nel quale attualmente non figura ancora il servizio specializzato PSA. A ciò si pone rimedio con il presente numero 10.6.

Capoverso 4: negli articoli 3 e 6 dell'ordinanza del 21 novembre 2018[44] sulla sicurezza militare (OSM) agli organi della sicurezza militare vengono assegnati compiti specifici con riferimento all'industria che, in virtù del nuovo diritto, sono assunti in via esclusiva dal servizio specializzato PSA. Le pertinenti disposizioni devono quindi essere stralciate (cfr. l'art. 3 OSM) o riformulate (cfr. l'art. 6 OSM).

Capoverso 5: l'articolo 68 e l'allegato 31 dell'OSIM possono essere abrogati, Il loro contenuto è ripreso nell'articolo 22 e nell'allegato dell'OPSAz.

### *Art. 25 Disposizioni transitorie*

Un effetto retroattivo su mandati per i quali l'appalto è iniziato prima dell'entrata in vigore dell'OPSAz potrebbe eventualmente modificare i presupposti in base ai quali il mandato è stato messo a concorso o aggiudicato e, in ultima analisi, può persino comportarne la revoca e una loro riassegnazione. Non si giustifica questa incertezza del diritto, per cui in questi casi andrebbe mantenuta l'idoneità dal punto di vista del diritto d'aggiudicazione. Sotto il profilo materiale, ai pochi casi di procedure di tutela del segreto del DDPS pendenti al momento dell'entrata in vigore si applicano comunque già pertinenti direttive di sicurezza e dunque, per motivi di economia procedurale, è opportuno rinunciare alle nuove fasi procedurali sancite dall'OPSAz. Le dichiarazioni di sicurezza aziendale emesse in virtù del diritto previgente rimangono valide per cinque anni a decorrere dal loro rilascio (cfr. art. 90 cpv. 3 LSIn).

### *Art. 26 Entrata in vigore*

L'entrata in vigore avverrà in sintonia con quella dell'OSIn e dell'OCSP.

### *Allegato*

Nell'allegato si trovano ora i dati del sistema d'informazione sulla procedura di sicurezza relativa alle aziende che ai sensi dell'articolo 24 capoverso 5 vengono tolti dall'OSIM.

[43] RS **121.1**
[44] RS **513.61**

# 5 Ripercussioni finanziarie e sull'effettivo del personale

## 5.1 Ripercussioni per la Confederazione

*a. SGSI e gestione della sicurezza delle informazioni (cfr. gli artt. 5–15 OSIn)*

Lo sviluppo e l'introduzione del SGSI *light* da parte degli uffici (e della CaF) comporterà un moderato onere iniziale *una tantum* di, in media, circa 0,5 posti a tempo pieno. Tale «onere progettuale» viene ripartito su vari servizi nell'ufficio (direzione dell'ufficio, informatica, diritto, personale e responsabili dell'applicazione). La quota maggiore andrà comunque agli incaricati della sicurezza delle informazioni (cfr. l'art. 37 OSIn). Per un corretto funzionamento minimo del SGSI *light* negli uffici occorre prevedere un onere supplementare di circa 0,2 posti a tempo pieno presso gli incaricati della sicurezza delle informazioni. L'applicazione SGSI (cfr. n. 3.8) aumenterà l'efficienza operativa del SGSI.

Non tutti gli uffici avranno lo stesso onere supplementare. Da una parte, i dipartimenti e gli uffici possono fissare un livello di ambizione più elevato, con corrispondenti ripercussioni sui costi. Dall'altra, taluni uffici e dipartimenti adempiono già le direttive. Così, ad esempio, alcuni uffici quali armasuisse, swisstopo, UFSPO, UFIT e USTRA sono certificati ISO. Nel DDPS già da alcuni anni è stato attuato un SGSI nella sua totalità. Il DFI ha già deciso di esigere dai suoi uffici l'attuazione di un SGSI.

*b. Accreditamento in materia di sicurezza di mezzi informatici (cfr. l'art. 23 OSIn)*

Al momento non è possibile quantificare l'onere per l'accreditamento di mezzi informatici. Si tratta di un compito nuovo del quale l'Amministrazione federale non ha alcuna esperienza. Dopo l'avvio della procedura di consultazione il Consiglio federale esaminerà quali competenze e risorse sono necessarie per suddetto compito.

*c. Incaricati della sicurezza delle informazioni dei dipartimenti (cfr. l'art. 40 OSIn)*

Con il nuovo diritto, anche agli incaricati della sicurezza delle informazioni dei dipartimenti incombe un onere leggermente aumentato di 0,2 posti a tempo pieno. Questo onere supplementare è parzialmente riconducibile ai compiti direttivi e di coordinamento della stessa LSIn. Un'ulteriore ragione risiede nel fatto che, in futuro, gli incaricati autorizzeranno l'avvio di CSP presso terzi non contemplati dalla procedura di sicurezza relativa alle aziende. I dipartimenti che aggiudicano molti mandati sensibili sotto il profilo della sicurezza avranno un onere leggermente maggiore.

*d. Servizio specializzato della Confederazione per la sicurezza delle informazioni (cfr. l'art. 41 OSIn)*

Le risorse del servizio specializzato della Confederazione per la sicurezza delle informazioni verranno riportate soltanto dopo la consultazione (cfr. n. 3.8). Qualora fossero necessarie risorse supplementari, cosa al momento non ancora prevedibile, l'onere supplementare risulterà esiguo.

*e. Attuazione delle misure di sicurezza tecniche e suo controllo*

Come avviene già oggi, i costi per l'attuazione delle misure di sicurezza tecniche e per il suo controllo, in particolare nel settore della cibersicurezza, rappresentano normali costi dei progetti e costi di esercizio. Essi devono essere pianificati di conseguenza e assunti nell'ambito del preventivo ordinario (cfr. l'art. 42 OSIn). Ciò include i costi per lo svolgimento di controlli e audit di cui all'articolo 13 OSIn e le verifiche dell'efficacia di cui all'articolo 29 capoverso 3 OSIn (cfr. l'art. 18 cpv. 3 LSIn).

*f. Modifica dell'OIAM*

Il campo d'applicazione dell'OIAM viene esteso alle unità amministrative dell'Amministrazione federale decentralizzata. Se vogliono impiegare un sistema IAM, dovranno soddisfare i requisiti dell'OIAM. I relativi costi devono essere previsti in tale contesto e assunti nell'ambito del preventivo ordinario.

*g. Ordinanza sui controlli di sicurezza relativi alle persone*

Indicazioni dettagliate sull'onere per i CSP ci saranno soltanto dopo la procedura di consultazione, in quanto gli elenchi delle funzioni determinanti a tal fine verranno stilati a partire dall'avvio della procedura di consultazione.

*h. Ordinanza sulla procedura di sicurezza relativa alle aziende (OPSAz)*

Per l'esecuzione della procedura di sicurezza relativa alle aziende il DDPS ha già aumentato di 1,5 posti a tempo pieno le risorse del servizio specializzato PSA. Non sono necessarie risorse supplementari.

### 5.2 Ripercussioni per i Cantoni

I costi per l'attuazione nei Cantoni sono tuttora incerti. L'applicazione della LSIn e delle ordinanze è tuttavia limitata. I costi di attuazione verranno generati prevalentemente nell'ambito di progetti o per l'acquisto di prestazioni di servizio della Confederazione e devono essere valutati in tale contesto. Le sessioni di lavoro con i Cantoni hanno dimostrato che la prassi è eterogenea. Un obiettivo importante della consultazione è stimare l'onere finanziario per i Cantoni.

### 5.3 Ripercussioni per l'economia

Le ripercussioni per l'economia sono state individuate nel messaggio LSIn e sono estremamente esigue. La LSIn e le sue disposizioni esecutive incidono sull'economia in caso di aziende che lavorano per la Confederazione. Le autorità federali sono tenute a stabilire contrattualmente la sicurezza delle informazioni nell'ambito della collaborazione con terzi e a provvedere a un adeguato controllo del rispetto delle direttive. Inoltre, nell'ambito della procedura di sicurezza relativa alle aziende (cfr. n. 4.4, commento all'OPSAz), le aziende che adempiono mandati della Confederazione sensibili sotto il profilo della sicurezza vengono verificate quanto alla loro affidabilità e in seguito controllate periodicamente. I costi della procedura ammontano, di norma, a meno dello 0,5 per cento del volume dei mandati e, direttamente o indirettamente, vengono riversati sul mandante. Da questi controlli sono interessate in totale circa 700 aziende. Nel complesso, le ripercussioni per l'economia rimangono quindi assai esigue.

### 5.4 Altre ripercussioni

Le ordinanze non hanno alcuna ripercussione sulla società, sull'ambiente o su altri settori importanti. In senso positivo indicano però chiaramente quali misure di sicurezza sono necessarie nell'era digitalizzata per garantire la sicurezza della Confederazione e dunque della Svizzera.