Legge federale sulle attività informative (LAIn)

del 25 settembre 2015 (Stato 1° gennaio 2024)

L'Assemblea federale della Confederazione Svizzera,

visti gli articoli 54 capoverso 1, 123 capoverso 1 e 173 capoverso 2 della Costituzione federale[1];[2]

visto il messaggio del Consiglio federale del 19 febbraio 2014[3],

decreta:

Capitolo 1: Disposizioni generali e principi dell'acquisizione di informazioni

Art. 1 Oggetto

La presente legge disciplina:

a. l'attività del Servizio delle attività informative della Confederazione (SIC);

b. la collaborazione del SIC con altre autorità della Confederazione, con i Cantoni, con l'estero e con privati;

c. la direzione politica del SIC nonché il controllo e la vigilanza sulle attività informative.

Art. 2 Scopo

La presente legge ha lo scopo di tutelare interessi nazionali importanti; intende:

a. contribuire a garantire i fondamenti della democrazia e dello Stato di diritto della Svizzera e a proteggere i diritti di libertà della sua popolazione;

b. accrescere la sicurezza della popolazione della Svizzera e degli Svizzeri all'estero;

c. sostenere la capacità d'azione della Svizzera;

d. contribuire a tutelare gli interessi internazionali in materia di sicurezza.

RU **2017** 4095

1 RS **101**

2 Nuovo testo giusta l'all. n. II 1 del DF del 25 set. 2020 che approva e traspone nel diritto svizzero la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e il relativo Protocollo addizionale e potenzia il dispositivo penale contro il terrorismo e la criminalità organizzata, in vigore dal 1° lug. 2021 (RU **2021** 360; FF **2018** 5439).

3 FF **2014** 1885

Art. 3 Tutela di altri interessi importanti della Svizzera

Nel caso di una minaccia grave e incombente il Consiglio federale può impiegare il SIC per tutelare altri interessi nazionali oltre a quelli di cui all'articolo 2 allo scopo di:

a. proteggere l'ordinamento costituzionale;

b. sostenere la politica estera;

c. proteggere la piazza industriale, economica e finanziaria.

Art. 4 Autorità e persone soggette alla presente legge

La presente legge si applica alle autorità e alle persone seguenti:

a. autorità della Confederazione e dei Cantoni incaricate dell'esecuzione di attività informative;

b. autorità della Confederazione e dei Cantoni nonché organizzazioni e persone di diritto pubblico o privato che dispongono di informazioni rilevanti per le attività informative;

c. privati che secondo la presente legge sono tenuti a trasmettere informazioni rilevanti per le attività informative.

Art. 5 Principi dell'acquisizione di informazioni

1 Per adempiere i suoi compiti, il SIC acquisisce informazioni tanto da fonti accessibili al pubblico quanto da fonti non accessibili al pubblico.

2 A tale scopo il SIC ricorre sia a misure di acquisizione non soggette ad autorizzazione sia a misure di acquisizione soggette ad autorizzazione.

3 Il SIC sceglie di volta in volta la misura di acquisizione che:

a. è più idonea ed è necessaria per raggiungere un determinato obiettivo in materia di acquisizione; e

b. incide il meno possibile sui diritti fondamentali delle persone interessate.

4 Il SIC può acquisire dati personali all'insaputa delle persone interessate.

5 Il SIC non acquisisce e non tratta informazioni sull'attività politica e sull'esercizio della libertà di opinione, di riunione o di associazione in Svizzera.

6 Il SIC può eccezionalmente acquisire le informazioni di cui al capoverso 5 relative a un'organizzazione o a una persona e registrarle con riferimento alle persone se sussistono indizi concreti che tale organizzazione o tale persona esercita i propri diritti per preparare o eseguire attività terroristiche, di spionaggio o di estremismo violento.

7 Il SIC cancella i dati registrati con riferimento alle persone non appena possono essere escluse attività secondo il capoverso 6, ma al più tardi dopo un anno dalla registrazione, se fino a tale momento dette attività non sono confermate.

[8] Il SIC può acquisire e trattare anche le informazioni di cui al capoverso 5 relative a organizzazioni e gruppi della lista d'osservazione di cui all'articolo 72 o a loro esponenti se, in tal modo, è possibile valutare la minaccia rappresentata da tali organizzazioni e gruppi.

Capitolo 2: Compiti e collaborazione del SIC

Sezione 1: Compiti, misure di protezione e di sicurezza, dotazione di armi

Art. 6 Compiti del SIC

[1] Il SIC acquisisce e tratta informazioni al fine di:

a. individuare tempestivamente e sventare minacce per la sicurezza interna o esterna rappresentate:
   1. dal terrorismo,
   2. dallo spionaggio,
   3. dalla proliferazione di armi nucleari, biologiche o chimiche, compresi i loro sistemi vettori nonché tutti i beni e tutte le tecnologie a duplice impiego civile e militare necessari per la fabbricazione di tali armi (proliferazione NBC), o dal commercio illegale di sostanze radioattive, materiale bellico e altri beni d'armamento,
   4.[4] da attacchi a infrastrutture per l'approvvigionamento di acqua potabile e di energia, a infrastrutture nei settori dell'informazione, della comunicazione e dei trasporti nonché ad altri processi, sistemi e installazioni essenziali per il funzionamento dell'economia e il benessere della popolazione (infrastrutture critiche),
   5. dall'estremismo violento;
b. accertare, osservare e valutare fatti rilevanti sotto il profilo della politica di sicurezza che avvengono all'estero;
c. salvaguardare la capacità d'azione della Svizzera;
d. tutelare altri interessi nazionali importanti secondo l'articolo 3, su mandato concreto del Consiglio federale.

[2] Il SIC valuta la situazione di minaccia e informa costantemente i servizi federali interessati e le autorità d'esecuzione cantonali in merito a eventuali minacce nonché alle misure adottate e previste secondo la presente legge. Se necessario, allerta i servizi competenti dello Stato.

[3] Garantendo la protezione delle fonti, il SIC informa altri servizi della Confederazione e dei Cantoni sui fatti e riscontri che possono incidere sui compiti legali di tali servizi in materia di salvaguardia della sicurezza interna o esterna.

4 Nuovo testo giusta l'all. 1 n. 2 della L del 18 dic. 2020 sulla sicurezza delle informazioni, in vigore dal 1° gen. 2024 (RU **2022** 232; **2023** 650; FF **2017** 2563).

4 Il SIC cura le relazioni della Svizzera con servizi esteri in materia di attività informative.

5 Il SIC assicura un servizio di preallerta informativa per la protezione di infrastrutture critiche.

6 Il SIC realizza programmi di informazione e sensibilizzazione in merito alle minacce per la sicurezza interna o esterna.

7 Il SIC protegge i suoi collaboratori, le sue installazioni, le sue fonti e i dati che tratta.

Art. 7 Misure di protezione e di sicurezza

1 Il SIC adotta misure per garantire la protezione e la sicurezza dei suoi collaboratori, delle sue installazioni e dei dati che tratta. A tal fine può:

a. controllare, nei propri locali, le persone elencate di seguito e i loro effetti personali:
   1. collaboratori del SIC,
   2. persone al servizio del SIC a tempo determinato,
   3. collaboratori di aziende che forniscono prestazioni al SIC nei suoi locali;
b. eseguire controlli dei propri locali per verificare il rispetto delle prescrizioni sulla protezione di informazioni classificate;
c. provvedere alla videosorveglianza di archivi, camere blindate, magazzini e zone d'accesso ai locali del SIC;
d. esercitare, nei locali che utilizza, impianti di telecomunicazione che provocano interferenze ai sensi dell'articolo 34 capoverso 1ter della legge del 30 aprile 1997[5] sulle telecomunicazioni.

2 Il SIC gestisce una rete informatica protetta per impedire a persone non autorizzate di accedere ai propri sistemi d'informazione che necessitano di una protezione particolare.

Art. 8 Dotazione di armi

1 Per il loro impiego in Svizzera, i collaboratori del SIC possono essere dotati di armi se la loro funzione e i loro compiti li espongono a pericoli particolari.

2 I collaboratori armati del SIC possono impiegare la propria arma soltanto in caso di legittima difesa o di stato di necessità e unicamente in misura proporzionata alle circostanze.

3 Il Consiglio federale determina le categorie di collaboratori del SIC autorizzati a portare un'arma e disciplina la loro istruzione.

5 RS **784.10**

Sezione 2: Collaborazione

Art. 9 Autorità d'esecuzione cantonali

1 Ogni Cantone designa un'autorità che collabora con il SIC per l'esecuzione della presente legge (autorità d'esecuzione cantonale). Il Cantone provvede affinché l'autorità designata possa eseguire senza indugio i mandati del SIC.

2 Il SIC assegna i mandati alle autorità d'esecuzione cantonali per scritto; in casi urgenti può assegnare oralmente i mandati e confermarli successivamente per scritto.

Art. 10 Informazione dei Cantoni

1 Periodicamente e in caso di eventi particolari, il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) informa le conferenze governative intercantonali in merito alla valutazione della situazione di minaccia.

2 Il SIC informa le autorità d'esecuzione cantonali in merito ai fatti che possono incidere sull'esecuzione dei loro compiti.

Art. 11 Collaborazione con l'esercito

1 Il SIC informa le unità competenti del Servizio informazioni dell'esercito e del servizio di sicurezza militare in merito ai fatti che possono incidere sull'esecuzione dei loro compiti.

2 Nell'ambito dei contatti militari internazionali il SIC può collaborare con i servizi competenti dell'esercito, richiedere loro informazioni e assegnare loro mandati in materia di collaborazione internazionale.

3 Il Consiglio federale disciplina:

a. la collaborazione e lo scambio di informazioni tra il SIC e le unità competenti del Servizio informazioni dell'esercito;

b. la ripartizione dei compiti tra il SIC e il servizio di sicurezza militare durante un servizio di promovimento della pace, un servizio d'appoggio o un servizio attivo.

Art. 12 Collaborazione con l'estero

1 Nei limiti dell'articolo 70 capoverso 1 lettera f, il SIC può collaborare per l'esecuzione della presente legge con servizi delle attività informative e autorità di sicurezza esteri:

a. ricevendo o trasmettendo informazioni pertinenti;

b. organizzando congiuntamente colloqui specialistici e convegni;

c. svolgendo attività congiunte volte ad acquisire e analizzare informazioni e a valutare la situazione di minaccia;

d. acquisendo e trasmettendo informazioni allo Stato che le richiede per valutare se una persona può partecipare a progetti classificati esteri nel settore della

sicurezza interna o esterna oppure se può ottenere l'accesso a informazioni, materiali o impianti classificati esteri;

e. partecipando, nei limiti dell'articolo 70 capoverso 3, a sistemi d'informazione automatizzati internazionali.

2 D'intesa con il Dipartimento federale degli affari esteri (DFAE), il SIC può impiegare collaboratori nelle rappresentanze svizzere all'estero al fine di promuovere i contatti internazionali. Per l'esecuzione della presente legge, essi collaborano direttamente con le autorità competenti dello Stato ospite e di Stati terzi.

3 La collaborazione con servizi delle attività informative esteri per l'adempimento dei compiti informativi secondo la presente legge compete al SIC.

4 I Cantoni possono cooperare con le autorità di polizia estere competenti per le questioni di sicurezza nelle regioni di frontiera.

Capitolo 3: Acquisizione di informazioni

Sezione 1: Misure di acquisizione non soggette ad autorizzazione

Art. 13 Fonti d'informazione pubbliche

Sono fonti d'informazione pubbliche segnatamente:

a. i media accessibili al pubblico;

b. i registri accessibili al pubblico di autorità della Confederazione e dei Cantoni;

c.[6] i dati personali che privati rendono accessibili al pubblico;

d. le dichiarazioni rese in pubblico.

Art. 14 Osservazioni in luoghi pubblici e liberamente accessibili

1 Il SIC può osservare fatti e installazioni in luoghi pubblici e liberamente accessibili ed effettuarvi registrazioni su supporto audiovisivo. A tale scopo può impiegare aeromobili e satelliti.

2 Il SIC non è autorizzato a osservare e registrare su supporto audiovisivo fatti e installazioni rientranti nella sfera privata protetta. Le registrazioni audio e video rientranti nella sfera privata protetta che per motivi tecnici non è possibile evitare devono essere immediatamente distrutte.

Art. 15 Fonti umane

1 Per fonti umane si intendono persone che:

a. comunicano al SIC informazioni o riscontri;

6 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).

b. forniscono al SIC prestazioni utili per l'adempimento dei compiti secondo la presente legge;

c. sostengono il SIC nell'acquisizione di informazioni.

2 Il SIC può indennizzare adeguatamente le fonti umane per la loro attività. Se è necessario per la protezione delle fonti o per l'acquisizione di ulteriori informazioni, tali indennità non sono considerate né reddito imponibile né reddito ai sensi della legge federale del 20 dicembre 1946[7] sull'assicurazione per la vecchiaia e per i superstiti.

3 Il SIC adotta le misure necessarie per proteggere la vita e l'integrità fisica delle fonti umane. Tali misure possono essere adottate anche a favore di persone a loro vicine.

4 Al termine della collaborazione, il capo del DDPS può, in casi specifici, autorizzare il SIC ad assegnare alle fonti umane una copertura o un'identità fittizia se ciò è indispensabile per proteggerne la vita e l'integrità fisica.

5 Le misure di cui ai capoversi 3 e 4 sono limitate al periodo di tempo durante il quale sussiste un pericolo concreto. Eccezionalmente, è possibile rinunciare a una limitazione temporale o commutare una misura limitata nel tempo in una misura a tempo indeterminato se i rischi per gli interessati sono particolarmente elevati e si deve ritenere che perdureranno.

Art. 16 Segnalazioni per la ricerca di persone e oggetti

1 Il SIC può disporre la segnalazione, a scopo di ricerca, di persone e veicoli nel sistema di ricerca informatizzato di polizia di cui all'articolo 15 capoverso 1 della legge federale del 13 giugno 2008[8] sui sistemi d'informazione di polizia della Confederazione (LSIP) e nella parte nazionale del Sistema d'informazione Schengen di cui all'articolo 16 capoverso 2 LSIP.

2 La segnalazione di una persona o di un veicolo è ammessa unicamente se sussistono indizi fondati che:

a. la persona rappresenta una minaccia concreta per la sicurezza interna o esterna secondo l'articolo 6 capoverso 1 lettera a;

b. il veicolo è utilizzato da una persona di cui alla lettera a;

c. il veicolo è utilizzato per un'altra minaccia concreta per la sicurezza interna o esterna secondo l'articolo 6 capoverso 1 lettera a;

d. la determinazione del luogo in cui si trova una persona o un veicolo è necessaria per tutelare altri interessi nazionali importanti secondo l'articolo 3.

3 La segnalazione non è ammessa se è finalizzata a sorvegliare il veicolo di terzi appartenenti a uno dei gruppi professionali di cui agli articoli 171–173 del Codice di procedura penale (CPP)[9].

7 RS **831.10**
8 RS **361**
9 RS **312.0**

Sezione 2: Coperture e identità fittizie

Art. 17 Coperture

1 Il direttore del SIC può autorizzare l'assegnazione di una copertura a collaboratori del SIC per dissimularne l'appartenenza a tale Servizio.

2 D'intesa con un Cantone o a sua richiesta, può inoltre autorizzare il SIC ad assegnare una copertura anche a collaboratori delle autorità d'esecuzione cantonali.

3 Il SIC può allestire o modificare documenti per creare o conservare una copertura. Le autorità federali, cantonali e comunali competenti sono tenute a collaborare con il SIC.

4 Il direttore del SIC presenta annualmente al capo del DDPS un rapporto sulla gestione delle coperture.

5 La dissimulazione dell'appartenenza al SIC o a un'autorità d'esecuzione cantonale senza l'impiego di documenti allestiti o modificati espressamente per tale scopo non necessita di alcuna autorizzazione particolare.

Art. 18 Identità fittizie

1 Il capo del DDPS può autorizzare l'assegnazione di un'identità fittizia alle persone indicate di seguito per garantire la loro sicurezza o l'acquisizione di informazioni:

a. collaboratori del SIC;

b. collaboratori delle autorità d'esecuzione cantonali che operano su mandato della Confederazione, d'intesa con il Cantone o a sua richiesta;

c. fonti umane nel quadro di una determinata operazione.

2 L'identità fittizia può essere utilizzata fintanto che è necessaria per garantire la sicurezza della persona interessata o l'acquisizione di informazioni. L'utilizzazione è limitata:

a. a cinque anni al massimo per i collaboratori del SIC o degli organi di sicurezza dei Cantoni; se necessario, il termine può essere prorogato di volta in volta di tre anni al massimo;

b. a 12 mesi al massimo per le fonti umane; se necessario, il termine può essere prorogato di volta in volta di 12 mesi al massimo.

3 L'utilizzazione di un'identità fittizia per l'acquisizione di informazioni è ammessa soltanto se concerne uno dei compiti di cui all'articolo 6 capoverso 1 e se:

a. l'acquisizione di informazioni non ha dato esito positivo e, senza l'utilizzazione di un'identità fittizia, risulterebbe vana o eccessivamente difficile; oppure

b. un bene giuridico rilevante quale la vita o l'integrità fisica delle persone incaricate dell'acquisizione di informazioni o delle persone a loro vicine è minacciato.

4 Il SIC può allestire o modificare documenti d'identità, attestati e altri documenti nonché dati riferiti a persone per creare e conservare identità fittizie. Le autorità federali, cantonali e comunali competenti sono tenute a collaborare con il SIC.

5 Il SIC adotta le misure necessarie per prevenire lo smascheramento.

Sezione 3: Obbligo di informazione e di comunicazione

Art. 19 Obbligo di informazione in caso di minaccia concreta

1 Le autorità della Confederazione e dei Cantoni nonché le organizzazioni alle quali la Confederazione o i Cantoni hanno delegato l'adempimento di compiti pubblici sono tenute, in casi specifici, a fornire al SIC, sulla base di una domanda motivata, le informazioni necessarie per individuare o sventare una minaccia concreta per la sicurezza interna o esterna oppure per tutelare altri interessi nazionali importanti secondo l'articolo 3.

2 Una minaccia concreta per la sicurezza interna o esterna sussiste quando è a repentaglio un bene giuridico importante quale la vita, l'integrità fisica o la libertà delle persone oppure l'esistenza e il funzionamento dello Stato e la minaccia proviene:

a. da attività terroristiche, nel senso di azioni tendenti a influenzare o a modificare l'ordinamento dello Stato, che si intendono attuare o favorire commettendo o minacciando di commettere gravi reati o propagando paura e timore;

b. dallo spionaggio secondo gli articoli 272–274 e 301 del Codice penale (CP)[10] e 86 e 93 del Codice penale militare del 13 giugno 1927[11];

c. dalla proliferazione NBC o dal commercio illegale di sostanze radioattive, di materiale bellico e di altri beni d'armamento;

d. da un attacco a un'infrastruttura critica; oppure

e. da attività dell'estremismo violento nel senso di azioni di organizzazioni che negano i fondamenti della democrazia e dello Stato di diritto e che commettono, incoraggiano o approvano atti violenti allo scopo di raggiungere i loro obiettivi.

3 Le autorità e le organizzazioni di cui al capoverso 1 sono tenute al segreto nei confronti di terzi in merito alle domande del SIC e alle informazioni eventualmente fornite. Sono invece autorizzate a informare gli organi superiori e gli organi di vigilanza.

4 Esse possono comunicare spontaneamente informazioni quando constatano una minaccia concreta per la sicurezza interna o esterna secondo il capoverso 2.

5 Il Consiglio federale designa mediante ordinanza le organizzazioni tenute a fornire informazioni, segnatamente le organizzazioni di diritto pubblico o privato esterne all'Amministrazione federale, in quanto emanino atti normativi o decisioni di prima

10 RS **311.0**
11 RS **321.0**

istanza ai sensi dell'articolo 5 della legge federale del 20 dicembre 1968[12] sulla procedura amministrativa oppure svolgano compiti federali d'esecuzione loro attribuiti; sono eccettuati i Cantoni.

Art. 20 Obbligo speciale di informazione e di comunicazione

[1] Le seguenti autorità sono tenute a fornire al SIC le informazioni necessarie per l'adempimento dei suoi compiti:

a. tribunali, autorità di perseguimento penale e autorità preposte all'esecuzione delle pene e delle misure;

b. autorità incaricate dei controlli di frontiera e autorità doganali;

c. autorità competenti per la sicurezza militare, autorità del Servizio informazioni dell'esercito e autorità preposte ai controlli militari;

d. autorità della Confederazione e dei Cantoni competenti per l'entrata e il soggiorno di stranieri e per le questioni in materia d'asilo;

e. autorità che collaborano all'adempimento di compiti di polizia di sicurezza;

f. uffici del controllo abitanti;

g. autorità competenti per le relazioni diplomatiche e consolari;

h. autorità competenti per il rilascio dei permessi di trasporto di determinati beni;

i. autorità competenti per l'esercizio di sistemi informatici;

j. autorità di vigilanza sul mercato finanziario e autorità che, conformemente alla legge del 10 ottobre 1997[13] sul riciclaggio di denaro, ricevono comunicazioni concernenti il sospetto riciclaggio di denaro nei casi di finanziamento del terrorismo e di finanziamento di attività in materia di proliferazione NBC.

[2] Le autorità di cui al capoverso 1 sono tenute al segreto nei confronti di terzi in merito alle domande del SIC e alle informazioni eventualmente fornite. Sono invece autorizzate ad informare gli organi superiori e gli organi di vigilanza.

[3] Le autorità di cui al capoverso 1 comunicano spontaneamente informazioni al SIC quando constatano una minaccia concreta e grave per la sicurezza interna o esterna.[14]

[4] Il Consiglio federale stabilisce in un elenco non pubblico quali fatti e constatazioni devono essere comunicati spontaneamente al SIC. Definisce l'estensione dell'obbligo di comunicazione e la procedura per fornire le informazioni.

Art. 21 Segreto professionale

Per le informazioni di cui agli articoli 19 e 20 il segreto professionale tutelato dalla legge è garantito.

12 RS **172.021**
13 RS **955.0**
14 La correzione della Commissione di redazione dell'AF del 12 mar. 2020, pubblicata il 24 mar. 2020, concerne solamente il testo francese (RU **2020** 1057).

Art. 22 Procedura in caso di divergenze d'opinione in merito all'obbligo di informazione e di comunicazione

1 In caso di divergenze d'opinione tra il SIC e un'altra unità dell'Amministrazione federale riguardo all'obbligo di informazione secondo l'articolo 19 o 20 decide in via definitiva l'autorità di vigilanza comune.

2 In caso di divergenze d'opinione tra il SIC e un'organizzazione, un organo o un'autorità non appartenente all'Amministrazione federale riguardo all'obbligo di informazione secondo l'articolo 19 o 20 decide il Tribunale amministrativo federale (TAF) secondo l'articolo 36*a* della legge del 17 giugno 2005[15] sul Tribunale amministrativo federale.

Art. 23 Informazioni fornite o comunicate da terzi

1 Il SIC può ricevere comunicazioni da qualsiasi persona.

2 Il SIC può richiedere in modo mirato, per scritto o oralmente, le informazioni necessarie per l'adempimento dei suoi compiti. Può invitare per scritto persone ad audizioni.

3 Eccettuato il caso in cui l'acquisizione di informazioni avvenga sotto copertura, il SIC rende attenta la persona alla quale richiede informazioni che è libera di comunicarle o meno.

Art. 24 Identificazione e audizione di persone

1 Per l'adempimento dei compiti di cui all'articolo 6 capoverso 1 lettera a, il SIC può far fermare una persona per stabilirne l'identità e interrogarla brevemente a proposito della sua identità ai sensi dell'articolo 23.

2 Il fermo è eseguito da membri di un corpo di polizia cantonale.

3 Il SIC può obbligare la persona fermata a declinare le proprie generalità e a esibire i documenti d'identità.

Art. 25 Obbligo speciale di informazione dei privati

1 Se è necessario per individuare, scongiurare o sventare una minaccia concreta per la sicurezza interna o esterna secondo l'articolo 19 capoverso 2, in casi specifici il SIC può richiedere le informazioni o registrazioni indicate di seguito:

a. a persone fisiche o giuridiche che effettuano trasporti a titolo professionale o che mettono a disposizione o procurano mezzi di trasporto, informazioni su una prestazione da loro fornita;

b. a gestori privati di infrastrutture di sicurezza, in particolare di apparecchi per la registrazione e la trasmissione di immagini, registrazioni, comprese le registrazioni di fatti che si svolgono su suolo pubblico.

15 RS **173.32**

2 Il SIC può inoltre richiedere informazioni secondo l'articolo 15 della legge federale del 18 marzo 2016[16] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT).[17]

Sezione 4: Misure di acquisizione soggette ad autorizzazione

Art. 26 Generi di misure di acquisizione soggette ad autorizzazione

1 Le seguenti misure di acquisizione sono soggette ad autorizzazione:

a.[18] la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni nonché la richiesta di metadati postali e di metadati delle telecomunicazioni secondo la LSCPT[19];

a^bis.[20] l'impiego di apparecchi tecnici speciali di sorveglianza del traffico delle telecomunicazioni per registrare comunicazioni oppure identificare una persona o un oggetto o determinarne la posizione, se le misure di sorveglianza già attuate non hanno dato esito positivo oppure se altrimenti la sorveglianza risulterebbe vana o eccessivamente difficile e si dispone delle autorizzazioni necessarie per l'impiego di siffatti apparecchi conformemente al diritto delle telecomunicazioni;

b. l'impiego di apparecchi di localizzazione per determinare la posizione e i movimenti di persone o oggetti;

c. l'impiego di apparecchi di sorveglianza per intercettare o registrare comunicazioni o conversazioni private oppure per osservare o registrare fatti in luoghi privati o non accessibili al pubblico;

d. l'infiltrazione in sistemi e reti informatici per:

1. acquisire informazioni ivi disponibili o trasmesse da questi sistemi e reti,
2. perturbare, impedire o rallentare l'accesso a informazioni, se i sistemi e le reti informatici sono utilizzati per attacchi a infrastrutture critiche;

e. le perquisizioni di locali, veicoli o contenitori per acquisire gli oggetti o le informazioni ivi disponibili oppure le informazioni trasmesse da tali locali, veicoli o contenitori.

2 Le misure sono eseguite in segreto; la persona interessata non viene informata.

16 RS **780.1**
17 Nuovo testo giusta l'art. 46 n. 2 della LF del 18 mar. 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, in vigore dal 1° mar. 2018 (RU **2018** 117; FF **2013** 2283).
18 Nuovo testo giusta l'art. 46 n. 2 della LF del 18 mar. 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, in vigore dal 1° mar. 2018 (RU **2018** 117; FF **2013** 2283).
19 RS **780.1**
20 Introdotta dall'art. 46 n. 2 della LF del 18 mar. 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, in vigore dal 1° mar. 2018 (RU **2018** 117; FF **2013** 2283).

Art. 27 Principio

[1] Il SIC può ordinare una misura di acquisizione soggetta ad autorizzazione a condizione che:

a. sussista una minaccia concreta ai sensi dell'articolo 19 capoverso 2 lettere a–d oppure lo richieda la tutela di altri interessi nazionali importanti secondo l'articolo 3;

b. la gravità della minaccia giustifichi la misura; e

c. gli accertamenti informativi non abbiano dato esito positivo oppure risulterebbero altrimenti vani o eccessivamente difficili.

[2] Prima di eseguire la misura, il SIC deve disporre dell'autorizzazione del TAF e del nullaosta del capo del DDPS.

[3] Se per eseguire la misura è necessaria la collaborazione di altri servizi della Confederazione e dei Cantoni, il SIC trasmette loro un ordine scritto non appena dispone dell'autorizzazione del TAF e del nullaosta del capo del DDPS. La misura di acquisizione è tenuta segreta.

Art. 28 Misure di acquisizione soggette ad autorizzazione ordinate nei confronti di terzi

[1] Il SIC può ordinare una misura di acquisizione soggetta ad autorizzazione anche nei confronti di terzi se sussistono indizi fondati che la persona riguardo alla quale vengono acquisite informazioni utilizza locali, veicoli o contenitori oppure indirizzi postali, collegamenti di telecomunicazione, sistemi o reti informatici di terzi per trasmettere, ricevere o conservare informazioni.

[2] La misura non può essere ordinata se i terzi appartengono a uno dei gruppi professionali menzionati negli articoli 171–173 CPP[21].

Art. 29 Procedura di autorizzazione

[1] Se intende ordinare una misura di acquisizione soggetta ad autorizzazione, il SIC sottopone al TAF una domanda con:

a. l'indicazione dell'obiettivo specifico della misura di acquisizione e la giustificazione della sua necessità nonché le ragioni per cui gli accertamenti già svolti non hanno dato esito positivo oppure risulterebbero altrimenti vani o eccessivamente difficili;

b. i dati relativi alle persone interessate dalla misura di acquisizione;

c. l'esatta designazione della misura di acquisizione e della base legale;

d. la designazione di eventuali altri servizi che saranno incaricati dell'esecuzione della misura di acquisizione;

21 RS **312.0**

e. l'indicazione dell'inizio e della fine della misura di acquisizione nonché il termine entro il quale essa dev'essere eseguita;

f. i documenti essenziali ai fini dell'autorizzazione.

2 Il presidente della corte competente del TAF decide quale giudice unico entro cinque giorni lavorativi dal ricevimento della domanda del SIC motivando succintamente la sua decisione; può affidare questo compito a un altro giudice.

3 Il presidente della corte competente del TAF non autorizza una misura di acquisizione di cui è stata fatta domanda qualora tale misura sia già stata autorizzata sulla base di un procedimento penale contro le persone di cui al capoverso 1 lettera b e l'inchiesta penale presenti una correlazione con la minaccia concreta sulla quale la misura di acquisizione del SIC intende fare chiarezza. I competenti giudici dei provvedimenti coercitivi nonché il servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni forniscono al TAF le informazioni di cui ha bisogno.

4 Il presidente della corte competente del TAF può chiedere l'audizione di uno o più rappresentanti del SIC prima di decidere.

5 Il presidente della corte competente del TAF può concedere l'autorizzazione vincolandola a oneri oppure esigere un completamento degli atti o ulteriori accertamenti.

6 L'autorizzazione è valida per tre mesi al massimo. Può essere prorogata di volta in volta di tre mesi al massimo.

7 Se è necessaria una proroga, prima della scadenza della durata autorizzata il SIC presenta al TAF una domanda motivata secondo il capoverso 1.

8 Il presidente della corte competente del TAF redige ogni anno un rapporto d'attività all'attenzione della Delegazione delle Commissioni della gestione (DelCG).

Art. 30 Nullaosta

1 Se la misura di acquisizione è autorizzata, il capo del DDPS decide in merito al nullaosta per l'esecuzione previa consultazione del capo del DFAE e del capo del Dipartimento federale di giustizia e polizia (DFGP). I casi di particolare importanza possono essere presentati al Consiglio federale.

2 La procedura di consultazione si svolge in forma scritta.

Art. 31 Procedura in caso d'urgenza

1 In caso d'urgenza, il direttore del SIC può ordinare l'esecuzione immediata di misure di acquisizione soggette ad autorizzazione. Ne informa senza indugio il TAF e il capo del DDPS. Quest'ultimo può porre fine con effetto immediato alla misura di acquisizione.

2 Il direttore del SIC sottopone la domanda al presidente della corte competente del TAF entro 24 ore, motivandone l'urgenza.

3 Il presidente della corte competente del TAF comunica la sua decisione al SIC entro tre giorni lavorativi.

4 Se la misura di acquisizione è autorizzata, il capo del DDPS decide in merito al nullaosta per il proseguimento dell'esecuzione, previa consultazione del capo del DFAE e del capo del DFGP.

Art. 32 Fine della misura di acquisizione

1 Il SIC pone fine senza indugio alla misura di acquisizione soggetta ad autorizzazione se:

a. il termine è scaduto;

b. le condizioni per proseguirne l'esecuzione non sono più adempiute;

c. il TAF non concede l'autorizzazione o il capo del DDPS non rilascia il nullaosta.

2 Nei casi d'urgenza, il SIC provvede affinché i dati acquisiti siano distrutti senza indugio se:

a. il presidente della corte competente del TAF respinge la domanda;

b. il capo del DDPS pone fine con effetto immediato alla misura di acquisizione o nega il nullaosta per il proseguimento dell'esecuzione.

3 Se altri servizi collaborano all'esecuzione della misura di acquisizione soggetta ad autorizzazione, il SIC comunica loro la fine di detta misura.

4 Il SIC comunica la fine della misura di acquisizione al TAF e al capo del DDPS.

Art. 33 Obbligo di comunicazione nei confronti delle persone sorvegliate

1 Entro un mese dalla conclusione dell'operazione, il SIC comunica alla persona sorvegliata il motivo, il genere e la durata della sorveglianza cui è stata sottoposta mediante misure di acquisizione soggette ad autorizzazione.

2 Il SIC può differire la comunicazione oppure rinunciarvi se:

a. è necessario per non pregiudicare una misura di acquisizione in corso o un procedimento legale in corso;

b. è necessario a causa di un altro interesse pubblico preponderante per la salvaguardia della sicurezza interna o esterna oppure lo richiedono le relazioni della Svizzera con l'estero;

c. la comunicazione potrebbe esporre terzi a un considerevole pericolo;

d. la persona interessata non è raggiungibile.

3 Il differimento della comunicazione o la rinuncia alla comunicazione deve ottenere l'autorizzazione e il nullaosta secondo la procedura di autorizzazione di cui all'articolo 29.

Sezione 5: Collaborazione e protezione delle fonti

Art. 34 Collaborazione e mandati nell'ambito dell'acquisizione

1 Il SIC può eseguire esso stesso le misure di acquisizione, collaborare con servizi svizzeri o esteri oppure demandarne l'esecuzione a tali servizi, sempre che offrano la garanzia di eseguire l'acquisizione conformemente alle disposizioni della presente legge.

2 Il SIC può eccezionalmente collaborare anche con privati o assegnare loro mandati, se è necessario per motivi tecnici o di accesso all'oggetto dell'acquisizione ed essi offrono la garanzia di eseguire l'acquisizione conformemente alle disposizioni della presente legge.

Art. 35 Protezione delle fonti

1 Il SIC garantisce la protezione delle sue fonti e ne tutela l'anonimato; in particolare tutela l'anonimato dei servizi delle attività informative esteri e delle autorità di sicurezza estere nonché delle persone esposte a pericolo perché acquisiscono informazioni concernenti l'estero. Sono escluse le persone alle quali, nell'ambito di un procedimento penale, sono imputati gravi crimini contro l'umanità o crimini di guerra.

2 Il SIC comunica alle autorità di perseguimento penale svizzere l'identità di una fonte umana domiciliata in Svizzera se alla persona in questione è imputato un reato perseguibile d'ufficio o se è indispensabile per far luce su un reato grave.

3 Per la protezione delle fonti devono essere considerati:

a. l'interesse del SIC a continuare a utilizzare le fonti in ambito informativo;

b. la necessità di proteggere le fonti, segnatamente le fonti umane, nei confronti di terzi;

c. nel caso di fonti tecniche, la necessità di mantenere segreti i dati riguardanti l'infrastruttura, le prestazioni, i metodi operativi e le procedure di acquisizione di informazioni.

4 In caso di controversie decide il Tribunale penale federale. Per il rimanente si applicano le disposizioni determinanti in materia di assistenza giudiziaria.

Sezione 6: Acquisizione di informazioni riguardanti fatti che avvengono all'estero

Art. 36 Disposizioni generali

1 Il SIC può acquisire segretamente informazioni riguardanti fatti che avvengono all'estero.

2 Se acquisisce in Svizzera informazioni riguardanti fatti che avvengono all'estero, il SIC è vincolato alle disposizioni della sezione 4; è fatto salvo l'articolo 37 capoverso 2.

3 Il SIC provvede affinché i rischi in occasione dell'acquisizione non siano sproporzionati rispetto al valore atteso delle informazioni e affinché le ingerenze nei diritti fondamentali delle persone interessate rimangano limitate allo stretto necessario.

4 Il SIC documenta all'attenzione degli organi di vigilanza e di controllo l'acquisizione di informazioni riguardanti fatti che avvengono all'estero.

5 Il SIC può memorizzare separatamente dati provenienti da operazioni di acquisizione all'estero comparabili a misure di acquisizione soggette ad autorizzazione se il volume dei dati, la tutela del segreto o la sicurezza lo esige.

6 Durante il loro impiego all'estero, i collaboratori del SIC sono assicurati contro le malattie e gli infortuni secondo la legge federale del 19 giugno 1992[22] sull'assicurazione militare.

7 Il SIC provvede alla protezione dei suoi collaboratori impiegati all'estero.

Art. 37 Infiltrazione in sistemi e reti informatici

1 Se sistemi e reti informatici ubicati all'estero sono utilizzati per attacchi a infrastrutture critiche in Svizzera, il SIC può infiltrarvisi per perturbare, impedire o rallentare l'accesso alle informazioni. Il Consiglio federale decide in merito all'esecuzione di una simile misura.

2 Il SIC può infiltrarsi in sistemi e reti informatici ubicati all'estero per acquisire informazioni ivi disponibili o trasmesse da tali sistemi e reti riguardanti fatti che avvengono all'estero. Il capo del DDPS decide in merito all'esecuzione di tale misura previa consultazione del capo del DFAE e del capo del DFGP.

Art. 38 Esplorazione radio

1 La Confederazione può gestire un servizio per il rilevamento delle emissioni elettromagnetiche di sistemi di telecomunicazione ubicati all'estero (esplorazione radio).

2 L'esplorazione radio serve:

a. ad acquisire informazioni rilevanti sotto il profilo della politica di sicurezza riguardanti fatti che avvengono all'estero, in particolare in relazione al terrorismo, alla proliferazione di armi di distruzione di massa e ai conflitti all'estero che hanno ripercussioni sulla Svizzera;

b. a tutelare altri interessi nazionali importanti secondo l'articolo 3.

3 Il Consiglio federale disciplina gli ambiti di esplorazione, l'organizzazione e le procedure in materia di esplorazione radio. Stabilisce per quanto tempo il servizio addetto all'esplorazione può conservare le comunicazioni rilevate e i dati registrati relativi ai collegamenti.

4 Il Consiglio federale garantisce in particolare che sulla base delle comunicazioni rilevate il servizio addetto all'esplorazione trasmetta:

22 RS **833.1**

a. unicamente informazioni riguardanti fatti che avvengono all'estero rilevanti sotto il profilo della politica di sicurezza;

b. informazioni riguardanti persone che si trovano in Svizzera unicamente se sono necessarie per la comprensione di un fatto che avviene all'estero e sono state precedentemente anonimizzate.

5 Il servizio addetto all'esplorazione trasmette informazioni riguardanti fatti che avvengono in Svizzera se le comunicazioni rilevate contengono indizi di una minaccia concreta per la sicurezza interna secondo l'articolo 6 capoverso 1 lettera a.

6 Se nell'ambito della propria attività scopre comunicazioni rilevate che non contengono informazioni riguardanti fatti che avvengono all'estero rilevanti sotto il profilo della politica di sicurezza né indizi di una minaccia concreta per la sicurezza interna, il servizio addetto all'esplorazione le distrugge il più rapidamente possibile.

Sezione 7: Esplorazione di segnali via cavo

Art. 39 Disposizioni generali

1 Il SIC può incaricare il servizio addetto all'esplorazione di rilevare segnali transfrontalieri provenienti da reti filari per acquisire informazioni riguardanti fatti che avvengono all'estero rilevanti sotto il profilo della politica di sicurezza (art. 6 cpv. 1 lett. b) e per tutelare altri interessi nazionali importanti secondo l'articolo 3.

2 Se sia l'emittente che il ricevente si trovano in Svizzera, l'utilizzazione dei segnali rilevati secondo il capoverso 1 non è ammessa. Se non può scartare tali segnali già in occasione del rilevamento, il servizio addetto all'esplorazione distrugge i dati acquisiti non appena riconosce che provengono da detti segnali.

3 Il servizio addetto all'esplorazione può trasmettere al SIC i dati provenienti dai segnali rilevati soltanto se il loro contenuto corrisponde alle chiavi di ricerca definite per l'adempimento del mandato. Le chiavi di ricerca devono essere definite in modo tale che la loro applicazione determini per quanto possibile ingerenze minime nella sfera privata delle persone. Non è ammesso utilizzare come chiavi di ricerca dati riguardanti persone fisiche o giuridiche svizzere.

4 Il Consiglio federale disciplina:

a. gli ambiti di esplorazione ammessi;

b. l'organizzazione e i dettagli delle procedure in materia di esplorazione dei segnali via cavo;

c. la durata massima del periodo durante il quale il servizio addetto all'esplorazione dei segnali via cavo può conservare i dati relativi ai contenuti e ai collegamenti registrati nell'ambito dell'esplorazione.

Art. 40 Obbligo di autorizzazione

1 I mandati per l'esplorazione di segnali via cavo sottostanno ad autorizzazione.

2 Prima di assegnare un mandato per l'esplorazione di segnali via cavo, il SIC deve ottenere l'autorizzazione del TAF e il nullaosta del capo del DDPS.

3 Il capo del DDPS consulta preliminarmente il capo del DFAE e il capo del DFGP.

Art. 41 Procedura di autorizzazione

1 Se intende assegnare un mandato per l'esplorazione di segnali via cavo, il SIC presenta al TAF una domanda in cui figurano:

a. la descrizione del mandato assegnato al servizio addetto all'esplorazione;

b. la motivazione della necessità dell'impiego;

c. le categorie di chiavi di ricerca;

d. l'indicazione dei gestori di reti filari e dei fornitori di servizi di telecomunicazione che devono fornire i segnali necessari per l'esecuzione dell'esplorazione di segnali via cavo; e

e. l'indicazione dell'inizio e della fine del mandato.

2 Il seguito della procedura è retto dagli articoli 29–32.

3 L'autorizzazione è valida sei mesi al massimo. Può essere prorogata di volta in volta di tre mesi al massimo, applicando la medesima procedura.

Art. 42 Esecuzione

1 Il servizio addetto all'esplorazione riceve i segnali dai gestori e dai fornitori secondo l'articolo 41 capoverso 1 lettera d, li converte in dati e, sulla base del contenuto, valuta quali dati trasmettere al SIC.

2 Il servizio addetto all'esplorazione trasmette al SIC esclusivamente dati contenenti informazioni relative alle chiavi di ricerca definite per l'adempimento del mandato. Gli trasmette informazioni relative a persone che si trovano in Svizzera unicamente se sono necessarie per la comprensione di un fatto che avviene all'estero e se sono state precedentemente anonimizzate.

3 Se i dati contengono informazioni riguardanti fatti che avvengono in Svizzera o all'estero che possono costituire una minaccia concreta per la sicurezza interna secondo l'articolo 6 capoverso 1 lettera a, il servizio addetto all'esplorazione li trasmette al SIC senza modifiche.

4 Il servizio addetto all'esplorazione distrugge il più rapidamente possibile i dati che non contengono informazioni secondo i capoversi 2 e 3.

5 Il SIC è competente per l'analisi dei dati a fini informativi.

Art. 43 Obblighi dei gestori di reti filari e dei fornitori di servizi di telecomunicazione

1 I gestori di reti filari e i fornitori di servizi di telecomunicazione sono tenuti a comunicare al servizio addetto all'esplorazione o al SIC i dati tecnici necessari per l'esecuzione dell'esplorazione di segnali via cavo.

2 In presenza di un mandato e del relativo nullaosta, i gestori di reti filari e i fornitori di servizi di telecomunicazione sono tenuti a fornire i segnali al servizio addetto all'esplorazione. Sopprimono i criptaggi che hanno applicato.

3 I gestori di reti filari e i fornitori di servizi di telecomunicazione sono tenuti a mantenere il segreto riguardo ai mandati.

4 La Confederazione indennizza i gestori di reti filari e i fornitori di servizi di telecomunicazione. Il Consiglio federale stabilisce l'importo dell'indennità in funzione dei costi per la fornitura dei segnali al servizio addetto all'esplorazione.

Capitolo 4: Trattamento dei dati e archiviazione

Sezione 1: Principi, controllo della qualità e trattamento dei dati nei Cantoni

Art. 44 Principi

1 Il SIC e le autorità d'esecuzione cantonali sono autorizzati a trattare dati personali, compresi quelli necessari per valutare il grado di pericolosità di una persona, a prescindere dal fatto che si tratti o meno di dati personali degni di particolare protezione.[23]

2 Il SIC può continuare a trattare informazioni che si rivelano essere disinformazione o false informazioni, se ciò è necessario per la valutazione della situazione o di una fonte. Contrassegna i dati in questione come inesatti.

3 Il SIC può riversare i medesimi dati in più sistemi d'informazione. Si applicano le disposizioni specifiche di ogni sistema d'informazione.

4 Il SIC può correlare i dati all'interno di un sistema d'informazione e analizzarli in modo automatizzato.

Art. 45 Controllo della qualità

1 Il SIC valuta la rilevanza e l'esattezza dei dati personali prima di registrarli in un sistema d'informazione. Valuta nel loro insieme le informazioni che contengono più dati personali prima di registrarle nel sistema di ordinamento.

2 Il SIC registra unicamente i dati necessari per l'adempimento dei compiti di cui all'articolo 6, tenendo conto dell'articolo 5 capoversi 5–8.

3 Il SIC distrugge i dati che non è lecito registrare in alcun sistema d'informazione oppure li rinvia al mittente per ulteriori accertamenti o per il trattamento di competenza di quest'ultimo.

23 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).

4 Il SIC verifica periodicamente in tutti i sistemi d'informazione se gli insiemi di dati personali registrati sono ancora necessari per l'adempimento dei suoi compiti. Cancella gli insiemi di dati non più necessari. I dati inesatti sono immediatamente rettificati o cancellati; è fatto salvo l'articolo 44 capoverso 2.

5 L'organo interno di controllo della qualità del SIC assume i compiti seguenti:

a. verifica la rilevanza e l'esattezza dei dati personali nel sistema IASA-GEX SIC (art. 50);

b. verifica periodicamente la rilevanza e l'esattezza dei rapporti delle autorità d'esecuzione cantonali registrati nel sistema INDEX SIC (art. 51);

c. controlla a campione in tutti i sistemi d'informazione del SIC la legalità, l'adeguatezza, l'efficacia e l'esattezza del trattamento dei dati;

d. cancella nel sistema INDEX SIC i dati risultanti da accertamenti preliminari dei Cantoni e la cui registrazione risale a oltre cinque anni prima, nonché i dati che il Cantone propone di cancellare;

e. provvede alla formazione interna dei collaboratori del SIC in materia di protezione dei dati.

Art. 46 Trattamento dei dati nei Cantoni

1 Le autorità d'esecuzione cantonali non gestiscono alcuna banca dati propria in applicazione della presente legge.[24]

2 Se trattano dati entro le proprie competenze, i Cantoni provvedono affinché i dati cantonali non contengano indicazioni riguardo all'esistenza e al contenuto dei dati della Confederazione.

3 Le autorità d'esecuzione cantonali possono trasmettere valutazioni della situazione e dati ricevuti dal SIC se ciò è necessario alla valutazione di misure per la salvaguardia della sicurezza o per sventare una minaccia considerevole. Il Consiglio federale stabilisce a quali servizi possono essere trasmessi questi dati e in quale misura.

Sezione 2: Sistemi d'informazione per le attività informative

Art. 47 Sistemi d'informazione del SIC

1 Il SIC gestisce i sistemi d'informazione seguenti per adempiere i compiti di cui all'articolo 6:

a. IASA SIC (art. 49);

b. IASA-GEX SIC (art. 50);

c. INDEX SIC (art. 51);

d. GEVER SIC (art. 52);

24 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).

e. PES (art. 53);
f. Portale OSINT (art. 54);
g. Quattro P (art. 55);
h. ISCO (art. 56);
i. Memoria dei dati residui (art. 57).

2 Per ogni sistema d'informazione del SIC il Consiglio federale disciplina:

a. il catalogo dei dati personali;
b. le competenze in materia di trattamento dei dati;
c. i diritti d'accesso;
d. la frequenza del controllo della qualità, considerando la gravità dell'ingerenza nei diritti costituzionali che il trattamento dei dati comporta;
e. la durata di conservazione dei dati, considerando le esigenze specifiche del SIC riguardo ai vari compiti;
f. la cancellazione dei dati;
g. la sicurezza dei dati.

Art. 48 Assegnazione dei dati ai sistemi d'informazione

Il SIC assegna i dati che riceve come segue:

a. i dati con informazioni sull'estremismo violento, al sistema IASA-GEX SIC;
b. i dati con informazioni che servono esclusivamente per scopi amministrativi, al sistema GEVER SIC;
c. i dati con informazioni che riguardano esclusivamente misure di polizia di sicurezza, al sistema PES;
d. i dati provenienti da fonti accessibili al pubblico, al sistema Portale OSINT;
e. i dati provenienti da controlli di frontiera e doganali, al sistema Quattro P;
f. i dati che servono esclusivamente al controllo dei compiti e alla direzione dell'esplorazione radio e dell'esplorazione di segnali via cavo, al sistema ISCO;
g. i rimanenti dati, al sistema Memoria dei dati residui.

Art. 49 IASA SIC

1 Il Sistema di analisi integrale del SIC (IASA SIC) serve all'analisi dei dati a fini informativi.

2 IASA SIC contiene dati che riguardano i compiti di cui all'articolo 6 capoverso 1, eccettuati i dati relativi all'estremismo violento.

3 I collaboratori del SIC incaricati della registrazione, della ricerca, dell'analisi e del controllo della qualità dei dati hanno accesso a IASA SIC mediante procedura di richiamo. Con l'ausilio di IASA SIC possono intraprendere ricerche di dati in tutti i sistemi d'informazione del SIC ai quali sono autorizzati ad accedere.

Art. 50 IASA-GEX SIC

1 Il Sistema di analisi integrale dell'estremismo violento del SIC (IASA-GEX SIC) serve alla registrazione, al trattamento e all'analisi di informazioni che riguardano l'estremismo violento.

2 IASA-GEX SIC contiene dati che riguardano l'estremismo violento.

3 I collaboratori del SIC incaricati della registrazione, della ricerca, dell'analisi e del controllo della qualità dei dati hanno accesso a IASA-GEX SIC mediante procedura di richiamo.

Art. 51 INDEX SIC

1 Il sistema d'informazione INDEX SIC serve:

a. ad accertare se il SIC tratta dati relativi a una persona, un'organizzazione, un gruppo, un oggetto o un evento;

b. a registrare i rapporti redatti dalle autorità d'esecuzione cantonali;

c. a trattare i dati provenienti da accertamenti preliminari delle autorità d'esecuzione cantonali.

2 INDEX SIC consente alle autorità che non sono collegate alla rete particolarmente protetta del SIC di accedere ai dati necessari per l'adempimento dei loro compiti legali e di trasmetterli in modo sicuro.

3 INDEX SIC contiene:

a. i dati per l'identificazione delle persone, delle organizzazioni, dei gruppi, degli oggetti e degli eventi registrati nei sistemi d'informazione IASA SIC e IASA-GEX SIC;

b. i rapporti redatti dalle autorità d'esecuzione cantonali di propria iniziativa o su mandato del SIC;

c. i dati provenienti da accertamenti preliminari delle autorità d'esecuzione cantonali.

4 Le seguenti persone hanno accesso mediante procedura di richiamo ai dati di INDEX SIC indicati di seguito:

a. i collaboratori del SIC incaricati di individuare tempestivamente e sventare minacce contro la Svizzera e la sua popolazione, ai dati di cui al capoverso 3 lettere a e b;

b. i collaboratori delle autorità d'esecuzione cantonali per l'adempimento dei loro compiti secondo la presente legge nonché per il trattamento e la trasmissione al SIC e ad altre autorità d'esecuzione cantonali di dati risultanti da accertamenti preliminari e di rapporti; hanno accesso ai dati di cui al capoverso

3 lettera c unicamente i collaboratori dell'autorità d'esecuzione cantonale che ha eseguito gli accertamenti preliminari e i collaboratori dell'organo di controllo della qualità del SIC;

c. i collaboratori dell'Ufficio federale di polizia, ai dati di cui al capoverso 3 lettera a per l'esecuzione di compiti di polizia di sicurezza, di polizia giudiziaria e di polizia amministrativa, nonché per l'esame di casi di sospetto riciclaggio di denaro e finanziamento del terrorismo comunicati da istituti svizzeri;

d.[25] i collaboratori dei servizi specializzati competenti per l'esecuzione dei controlli di sicurezza relativi alle persone secondo l'articolo 31 capoverso 2 della legge del 18 dicembre 2020[26] sulla sicurezza delle informazioni, ai dati di cui al capoverso 3 lettera a per l'esecuzione di controlli di sicurezza relativi alle persone, per verifiche dell'affidabilità e per la valutazione del potenziale di violenza.

Art. 52 GEVER SIC

1 Il Sistema d'informazione per la gestione degli affari del SIC (GEVER SIC) serve a trattare e controllare gli affari, nonché a garantire processi di lavoro efficienti.

2 GEVER SIC contiene:

a. i dati riguardanti affari amministrativi;

b. tutti i prodotti informativi che il SIC trasmette all'esterno;

c. i dati che sono stati impiegati per allestire i contenuti di cui alle lettere a e b;

d. le informazioni necessarie per il controllo degli affari, in particolare nel settore dei controlli di sicurezza relativi alle persone.

3 I collaboratori del SIC hanno accesso a GEVER SIC mediante procedura di richiamo.

Art. 53 PES

1 Il Sistema d'informazione per la presentazione elettronica della situazione (PES) è uno strumento di condotta che serve alle competenti autorità della Confederazione e dei Cantoni per diffondere informazioni allo scopo di definire e attuare misure di polizia di sicurezza, segnatamente in occasione di eventi in cui si temono atti violenti.

2 PES contiene dati riguardanti eventi nonché dati riguardanti misure per la salvaguardia della sicurezza interna o esterna.

3 I collaboratori del SIC e delle competenti autorità della Confederazione e dei Cantoni incaricati della condotta in materia di politica di sicurezza o della valutazione e della gestione di eventi che incidono sulla situazione hanno accesso a PES mediante procedura di richiamo.

25 Nuovo testo giusta l'all. 1 n. 2 della L del 18 dic. 2020 sulla sicurezza delle informazioni, in vigore dal 1° gen. 2024 (RU **2022** 232; **2023** 650; FF **2017** 2563).
26 RS **128**

4 In occasione di eventi particolari, il SIC può concedere l'accesso temporaneo mediante procedura di richiamo anche a enti privati e ad autorità di sicurezza e di polizia estere. L'accesso è limitato ai dati del sistema necessari a tali enti e autorità per l'adempimento dei loro compiti in relazione con la gestione di un simile evento.

Art. 54 Portale OSINT

1 Il Portale «Open Source Intelligence» (Portale OSINT) serve al SIC per approntare dati provenienti da fonti accessibili al pubblico.

2 Il Portale OSINT contiene dati raccolti in occasione dell'utilizzazione di fonti accessibili al pubblico.

3 I collaboratori del SIC hanno accesso al Portale OSINT mediante procedura di richiamo.

4 Il SIC può accordare ai collaboratori delle autorità d'esecuzione cantonali l'accesso mediante procedura di richiamo a determinati dati del Portale OSINT.

Art. 55 Quattro P

1 Il SIC può gestire un sistema d'informazione per identificare determinate categorie di stranieri che entrano in Svizzera o escono dalla Svizzera e per stabilire le date della loro entrata e uscita (Quattro P).

2 Quattro P contiene dati raccolti nel quadro di controlli di frontiera e doganali presso i posti di confine e che servono a identificare le persone e a individuarne gli spostamenti.

3 I collaboratori del SIC incaricati di identificare persone nel quadro dell'adempimento dei compiti di cui all'articolo 6 hanno accesso a Quattro P mediante procedura di richiamo.

4 Il Consiglio federale stabilisce, in un elenco non pubblico, le categorie di persone da registrare in Quattro P; al riguardo, si fonda sulla situazione di minaccia del momento.

Art. 56 ISCO

1 Il Sistema d'informazione per l'esplorazione delle comunicazioni (ISCO) serve a controllare e dirigere l'esplorazione radio e l'esplorazione di segnali via cavo.

2 ISCO contiene dati che consentono di dirigere i mezzi d'esplorazione, di procedere a verifiche e di redigere rapporti.

3 I collaboratori del SIC incaricati della direzione dell'esplorazione radio e dell'esplorazione di segnali via cavo hanno accesso a ISCO mediante procedura di richiamo.

Art. 57 Memoria dei dati residui

1 La Memoria dei dati residui serve a memorizzare i dati che in occasione dell'assegnazione di cui all'articolo 48 non possono essere assegnati direttamente a un altro sistema.

2 Se un'entrata di informazioni da archiviare nella Memoria dei dati residui contiene dati personali, la valutazione della sua rilevanza ed esattezza secondo l'articolo 45 capoverso 1 avviene per l'entrata nel suo insieme e non in relazione ai singoli dati personali. I dati personali sono valutati singolarmente quando vengono riversati in un altro sistema d'informazione.

3 I collaboratori del SIC incaricati della registrazione, della ricerca, dell'analisi e del controllo della qualità dei dati hanno accesso alla Memoria dei dati residui mediante procedura di richiamo.

4 La durata di conservazione dei dati è di dieci anni al massimo.

Sezione 3: Dati provenienti da misure di acquisizione soggette ad autorizzazione

Art. 58

1 Il SIC memorizza in sistemi d'informazione distinti da quelli di cui all'articolo 47 i dati provenienti dalle misure di acquisizione soggette ad autorizzazione di cui all'articolo 26; i dati sono memorizzati con riferimento a casi specifici.

2 Il SIC provvede affinché i dati personali che provengono da misure di acquisizione soggette ad autorizzazione e che non hanno alcuna correlazione con la specifica situazione di minaccia non vengano utilizzati e siano distrutti al più tardi entro 30 giorni dalla fine delle misure.

3 Se la misura di acquisizione soggetta ad autorizzazione riguarda una persona appartenente ad una delle categorie professionali menzionate agli articoli 171–173 CPP[27], la cernita e distruzione dei dati non aventi alcuna correlazione con la specifica situazione di minaccia avvengono sotto la direzione[28] del TAF. Se la misura di acquisizione soggetta ad autorizzazione riguarda un'altra persona, vanno distrutti anche i dati in merito ai quali una persona può avvalersi della facoltà di non deporre secondo gli articoli 171–173 CPP.

4 In casi specifici e tenendo conto dell'articolo 5 capoversi 5–8, il SIC può memorizzare dati personali anche nel sistema d'informazione appositamente previsto di cui all'articolo 47 capoverso 1, sempre che contengano informazioni necessarie per l'adempimento dei compiti di cui all'articolo 6 capoverso 1.

5 I collaboratori del SIC incaricati dell'esecuzione di una misura di acquisizione e dell'analisi dei risultati hanno accesso ai corrispondenti dati mediante procedura di richiamo.

6 Il Consiglio federale disciplina:

a. il catalogo dei dati personali;

b. il diritto di trattare dati e i diritti d'accesso;

27 RS **312.0**
28 Testo rettificato dalla Commissione di redazione dell'AF (art. 58 cpv. 1 LParl; RS **171.10**)

c. la durata di conservazione dei dati e la procedura per la loro distruzione;

d. la sicurezza dei dati.

Sezione 4: Disposizioni particolari sulla protezione dei dati

Art. 59 Verifica prima della comunicazione

Prima di ogni comunicazione di dati personali o di prodotti, il SIC si assicura che i dati personali soddisfino le prescrizioni della presente legge, che la loro comunicazione sia prevista dalla legge e sia necessaria nel caso concreto.

Art. 60 Comunicazione di dati personali ad autorità svizzere

1 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.

2 Se i riscontri del SIC servono ad altre autorità per il perseguimento penale, per la prevenzione di reati gravi o per il mantenimento dell'ordine pubblico, il SIC le mette a loro disposizione, spontaneamente o su richiesta, garantendo la protezione delle fonti.

3 Il SIC comunica a un'autorità di perseguimento penale dati provenienti da misure di acquisizione soggette ad autorizzazione ogniqualvolta contengano indizi concreti di un reato il cui perseguimento può dar luogo a una misura di sorveglianza comparabile in virtù del diritto processuale penale.

4 Il SIC indica alle autorità di perseguimento penale la provenienza dei dati. Il seguito della procedura è retto dalle disposizioni del CPP[29] o della Procedura penale militare del 23 marzo 1979[30].

Art. 61 Comunicazione di dati personali ad autorità estere

1 Il SIC può comunicare dati personali o elenchi di dati personali all'estero. Prima di ogni comunicazione verifica che le condizioni legali siano soddisfatte.

2 Se la legislazione dello Stato destinatario non assicura una protezione adeguata dei dati, i dati personali possono essergli comunicati in deroga all'articolo 16 capoverso 1 della legge federale del 25 settembre 2020[31] sulla protezione dei dati (LPD) soltanto se la Svizzera intrattiene con detto Stato relazioni diplomatiche e se è soddisfatta una delle condizioni seguenti:[32]

a. la Svizzera è tenuta a comunicargli i dati personali in virtù di una legge o di un trattato internazionale;

29 RS **312.0**
30 RS **322.1**
31 RS **235.1**
32 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).

b. la comunicazione è necessaria per tutelare un interesse pubblico preponderante inerente alla sicurezza della Svizzera o dello Stato destinatario, quale prevenire o fare luce su un reato grave punibile anche in Svizzera;

c. la comunicazione è necessaria per motivare una domanda di informazioni avanzata dalla Svizzera;

d. la comunicazione è nell'interesse della persona e questa ha fornito il suo consenso preliminare per la comunicazione dei dati oppure le circostanze lasciano presumere senza alcun dubbio il consenso della persona;

e. la comunicazione è necessaria per proteggere la vita e l'integrità fisica di terzi.

3 Il SIC può, in casi specifici, comunicare dati personali a Stati con i quali la Svizzera intrattiene relazioni diplomatiche se lo Stato richiedente garantisce per scritto di avere il consenso della persona interessata e i dati in questione gli consentono di valutare se tale persona possa collaborare a progetti esteri classificati nel settore della sicurezza interna o esterna oppure accedere a informazioni, materiali o impianti esteri classificati.

4 Il SIC può comunicare dati personali, mediante procedura di richiamo, ad organi di sicurezza di Stati terzi se detti Stati assicurano una protezione adeguata dei dati e se con essi la Svizzera ha concluso un trattato secondo l'articolo 70 capoverso 3.

5 I dati personali non possono essere comunicati a un organo di sicurezza estero se ciò comporta per la persona interessata il pericolo di una doppia punizione o pregiudizi gravi per la vita, l'integrità fisica o la libertà ai sensi della Convenzione del 4 novembre 1950[33] per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali o di altri trattati internazionali ratificati dalla Svizzera.

6 Se i dati personali sono richiesti nel quadro di un procedimento legale, si applicano le disposizioni determinanti in materia di assistenza giudiziaria.

Art. 62 Comunicazione di dati personali a terzi

La comunicazione di dati personali a terzi è ammessa unicamente se:

a. la persona interessata vi ha acconsentito o la comunicazione è inequivocabilmente nel suo interesse;

b. è necessaria per sventare un grave pericolo immediato;

c. è necessaria per motivare una domanda di informazioni.

Art. 63 Diritto d'accesso

1 Il diritto d'accesso ai sistemi d'informazione PES, Portale OSINT e Quattro P, ai dati amministrativi di GEVER SIC, nonché ai dati dei sistemi di memorizzazione di cui agli articoli 36 capoverso 5 e 58 è retto dalla LPD[34].

2 Qualora una persona domandi al SIC se stia trattando dati che la concernono nei sistemi d'informazione IASA SIC, IASA-GEX SIC, INDEX SIC, ISCO e Memoria dei dati residui o in GEVER SIC, il SIC differisce tale informazione:

33 RS **0.101**
34 RS **235.1**

a. se e nella misura in cui interessi preponderanti, debitamente motivati negli atti, esigano il mantenimento del segreto riguardo ai dati concernenti il richiedente per:
   1. l'adempimento dei compiti di cui all'articolo 6, o
   2. il perseguimento penale o un altro procedimento istruttorio;
b. se e nella misura in cui interessi preponderanti di terzi lo rendano necessario; oppure
c. se il SIC non tratta dati riguardanti il richiedente.

3 Il SIC comunica al richiedente il differimento dell'informazione rendendolo attento al fatto che può domandare all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) di verificare se eventuali dati che lo concernono sono trattati in modo lecito e se interessi preponderanti al mantenimento del segreto giustificano il differimento.

4 Non appena viene meno l'interesse al mantenimento del segreto, ma al più tardi allo scadere della durata di conservazione dei dati, il SIC fornisce al richiedente le informazioni chieste in virtù della LPD purché ciò non comporti un onere di lavoro eccessivo.

5 Il SIC informa le persone di cui non ha trattato alcun dato entro tre anni dal ricevimento della loro domanda.

Art. 64 Verifica da parte dell'IFPDT

1 Su domanda del richiedente, l'IFPDT effettua la verifica di cui all'articolo 63 capoverso 3.

2 L'IFPDT comunica al richiedente che nessun dato che lo concerne è trattato in modo illecito oppure che sono stati riscontrati errori nel trattamento dei dati o riguardanti il differimento dell'informazione e che ha aperto un'inchiesta ai sensi dell'articolo 49 LPD[35].[36]

3 … [37]

4 Se riscontra errori nel trattamento dei dati o riguardanti il differimento dell'informazione, l'IFPDT ordina al SIC di correggere tali errori.[38]

5 Qualora il richiedente renda verosimile che il differimento dell'informazione gli arrecherebbe un danno rilevante e irreparabile, l'IFPDT può ordinare al SIC di fornire immediatamente, a titolo eccezionale, le informazioni richieste, sempre che ciò non pregiudichi la sicurezza interna o esterna.[39]

35 RS **235.1**
36 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).
37 Abrogato dall'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, con effetto dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).
38 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).
39 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).

Art. 65[40]

Art. 66 Forma della comunicazione ed esclusione dei rimedi giuridici

1 Le comunicazioni di cui agli articoli 63 capoverso 3 e 64 capoverso 2 hanno sempre lo stesso tenore e non vengono motivate.[41]

2 Non sono impugnabili.

Art. 67 Deroga al principio di trasparenza

La legge del 17 dicembre 2004[42] sulla trasparenza non si applica all'accesso a documenti ufficiali riguardanti l'acquisizione di informazioni secondo la presente legge.

Sezione 5: Archiviazione

Art. 68

1 Il SIC offre all'Archivio federale, per l'archiviazione, i dati e i documenti non più necessari o destinati alla distruzione. I dati e i documenti del SIC sono archiviati in locali particolarmente protetti. Essi sottostanno a un termine di protezione di 50 anni.

2 Il Consiglio federale può, conformemente all'articolo 12 della legge federale del 26 giugno 1998[43] sull'archiviazione, prorogare ripetutamente e per una durata limitata il termine di protezione applicabile agli archivi provenienti da servizi di sicurezza esteri se questi formulano riserve su una loro eventuale consultazione.

3 In casi specifici, il SIC può consultare, durante il termine di protezione, i dati personali che ha consegnato all'Archivio federale per l'archiviazione al fine di valutare minacce concrete per la sicurezza interna o esterna oppure per tutelare un altro interesse pubblico preponderante.

4 Il SIC distrugge i dati e i documenti che l'Archivio federale considera privi di valore archivistico.

40 Abrogato dall'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, con effetto dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).
41 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).
42 RS **152.3**
43 RS **152.1**

Capitolo 5: Prestazioni

Art. 69

1 Se sussiste un interesse informativo o un altro interesse pubblico, il SIC può fornire prestazioni ad altre autorità della Confederazione e dei Cantoni segnatamente negli ambiti seguenti:

a. sicurezza delle trasmissioni;

b. trasporto di merci o persone;

c. consulenza e valutazione della situazione;

d. protezione e difesa contro attacchi all'infrastruttura di informazione o di comunicazione oppure contro la tutela del segreto.

2 Se sussiste un interesse informativo, il SIC può fornire simili prestazioni anche a terzi in Svizzera o all'estero.

Capitolo 6: Direzione politica, controllo e tutela giurisdizionale

Sezione 1: Direzione politica e divieti

Art. 70 Direzione politica da parte del Consiglio federale

1 Il Consiglio federale assicura la direzione politica del SIC, assumendo in particolare i compiti seguenti:

a. assegna al SIC un mandato di base e lo rinnova almeno ogni quattro anni; il mandato di base è segreto;

b. approva ogni anno la lista d'osservazione di cui all'articolo 72 e la trasmette alla DelCG; la lista d'osservazione è confidenziale;

c. designa ogni anno i gruppi da considerare di matrice estremista violenta e prende atto del numero di estremisti violenti non ancora attribuibili ad un gruppo noto;

d. valuta ogni anno la situazione di minaccia e se necessario in caso di eventi particolari, e informa le Camere federali e il pubblico;

e. ordina le misure necessarie in caso di situazioni di minaccia particolari;

f. definisce ogni anno la collaborazione del SIC con autorità estere.

2 I documenti in relazione con i compiti di cui al capoverso 1 non sono accessibili al pubblico.

3 Il Consiglio federale può concludere autonomamente trattati internazionali riguardanti la collaborazione internazionale del SIC in materia di protezione delle informazioni o di partecipazione a sistemi d'informazione automatizzati internazionali secondo l'articolo 12 capoverso 1 lettera e.

Art. 71 Tutela di altri interessi nazionali importanti

1 Nel caso di una minaccia grave e incombente, il Consiglio federale può incaricare il SIC di eseguire misure secondo la presente legge, sempre che tali misure siano necessarie per tutelare altri interessi nazionali importanti secondo l'articolo 3.

2 Stabilisce nel caso specifico la durata, lo scopo, il genere e l'estensione della misura.

3 Le misure di acquisizione soggette ad autorizzazione sottostanno alla procedura di autorizzazione secondo gli articoli 26–33.

4 Se assegna un mandato secondo il capoverso 1, il Consiglio federale ne informa entro 24 ore la DelCG.

Art. 72 Lista d'osservazione

1 Nella lista d'osservazione figurano organizzazioni e gruppi che è fondato supporre minaccino la sicurezza interna o esterna.

2 La presunzione è considerata fondata se un'organizzazione o un gruppo figura in una lista delle Nazioni Unite o dell'Unione europea; in tal caso, l'organizzazione o il gruppo in questione può essere inserito nella lista d'osservazione.

3 Le organizzazioni e i gruppi sono stralciati dalla lista d'osservazione quando:

a. viene meno la presunzione che essi minaccino la sicurezza interna o esterna; o

b. non figurano più in alcuna delle liste di cui al capoverso 2 e non sussistono motivi particolari per supporre che minaccino la sicurezza interna o esterna.

4 Il Consiglio federale definisce in un'ordinanza i criteri per l'elaborazione della lista d'osservazione e stabilisce la frequenza della sua verifica.

Art. 73 Divieto di determinate attività

1 Il Consiglio federale può vietare a una persona fisica, a un'organizzazione o a un gruppo un'attività che minaccia concretamente la sicurezza interna o esterna e che direttamente o indirettamente serve a propagare, sostenere o favorire in altro modo attività terroristiche o di estremismo violento.

2 Il divieto è pronunciato per cinque anni al massimo. Se allo scadere del termine le condizioni continuano a essere adempiute, il divieto può essere prorogato di volta in volta di cinque anni al massimo.

3 Il dipartimento che ha richiesto il divieto verifica periodicamente se le condizioni sono ancora adempiute. Se non sono più adempiute, propone al Consiglio federale la revoca del divieto.

Art. 74 Divieto di organizzazioni

1 Il Consiglio federale può vietare un'organizzazione o un gruppo che direttamente o indirettamente propaga, sostiene o favorisce in altro modo attività terroristiche o di estremismo violento e che in questo modo minaccia concretamente la sicurezza interna o esterna.

2 Il divieto si fonda su una decisione delle Nazioni Unite che sancisce un divieto o sanzioni nei confronti dell'organizzazione o del gruppo; il Consiglio federale consulta le commissioni competenti in materia di politica di sicurezza.[44]

3 Il divieto è pronunciato per cinque anni al massimo. Se allo scadere del termine le condizioni continuano a essere adempiute, il divieto può essere prorogato di volta in volta di cinque anni al massimo.

4 Chiunque partecipa sul territorio svizzero a una delle organizzazioni o a uno dei gruppi vietati secondo il capoverso 1, mette a disposizione risorse umane o materiale, organizza azioni propagandistiche in suo favore o a sostegno dei suoi obiettivi, recluta adepti o promuove in altro modo le sue attività, è punito con una pena detentiva sino a cinque anni o con una pena pecuniaria.[45]

4bis Il giudice può attenuare la pena di cui al capoverso 4 (art. 48*a* CP[46]), se l'autore si sforza d'impedire la prosecuzione dell'attività dell'organizzazione o del gruppo.[47]

5 È punibile anche chi commette il reato all'estero, se è arrestato in Svizzera e non è estradato. È applicabile l'articolo 7 capoversi 4 e 5 CP[48].

6 Il perseguimento e il giudizio dei reati di cui ai capoversi 4 e 5 sottostanno alla giurisdizione federale.[49]

7 Le autorità competenti comunicano senza indugio e gratuitamente al SIC tutte le sentenze, i decreti penali e le decisioni di abbandono nella loro versione integrale.[50]

44 Nuovo testo giusta l'all. n. II 1 del DF del 25 set. 2020 che approva e traspone nel diritto svizzero la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e il relativo Protocollo addizionale e potenzia il dispositivo penale contro il terrorismo e la criminalità organizzata, in vigore dal 1° lug. 2021 (RU **2021** 360; FF **2018** 5439).

45 Nuovo testo giusta l'all. n. II 1 del DF del 25 set. 2020 che approva e traspone nel diritto svizzero la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e il relativo Protocollo addizionale e potenzia il dispositivo penale contro il terrorismo e la criminalità organizzata, in vigore dal 1° lug. 2021 (RU **2021** 360; FF **2018** 5439).

46 RS **311.0**

47 Introdotto dall'all. n. II 1 del DF del 25 set. 2020 che approva e traspone nel diritto svizzero la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e il relativo Protocollo addizionale e potenzia il dispositivo penale contro il terrorismo e la criminalità organizzata, in vigore dal 1° lug. 2021 (RU **2021** 360; FF **2018** 5439).

48 RS **311.0**

49 Nuovo testo giusta l'all. n. II 1 del DF del 25 set. 2020 che approva e traspone nel diritto svizzero la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e il relativo Protocollo addizionale e potenzia il dispositivo penale contro il terrorismo e la criminalità organizzata, in vigore dal 1° lug. 2021 (RU **2021** 360; FF **2018** 5439).

50 Nuovo testo giusta l'all. n. II 1 del DF del 25 set. 2020 che approva e traspone nel diritto svizzero la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e il relativo Protocollo addizionale e potenzia il dispositivo penale contro il terrorismo e la criminalità organizzata, in vigore dal 1° lug. 2021 (RU **2021** 360; FF **2018** 5439).

Sezione 2: Controllo e vigilanza del SIC

Art. 75 Autocontrollo da parte del SIC

Mediante adeguate misure di assicurazione della qualità e di controllo il SIC garantisce che tanto in seno al SIC quanto da parte delle autorità di sicurezza dei Cantoni l'esecuzione della presente legge sia conforme al diritto.

Art. 76 Autorità di vigilanza indipendente

1 Il Consiglio federale istituisce un'autorità indipendente incaricata di vigilare sul SIC.

2 Su proposta del DDPS, il Consiglio federale nomina il capo dell'autorità di vigilanza indipendente per un mandato di sei anni.

3 Il mandato del capo dell'autorità di vigilanza si considera tacitamente rinnovato per un nuovo mandato di sei anni, a meno che, al più tardi sei mesi prima della scadenza, il Consiglio federale decida di non rinnovarlo per motivi oggettivi sufficienti.

4 Con un preavviso di sei mesi, il capo dell'autorità di vigilanza può chiedere al Consiglio federale la cessazione del mandato per la fine di ogni mese.

5 Il Consiglio federale può destituire il capo dell'autorità di vigilanza prima della scadenza del mandato se:

a. intenzionalmente o per negligenza grave, ha violato gravemente i suoi doveri d'ufficio; oppure

b. ha durevolmente perso la capacità di esercitare il suo ufficio.

Art. 77 Statuto dell'autorità di vigilanza indipendente

1 L'autorità di vigilanza indipendente esercita la propria funzione in modo indipendente; non è vincolata a istruzioni. Sotto il profilo amministrativo è aggregata al DDPS.

2 L'autorità di vigilanza indipendente dispone di un proprio preventivo. Assume il proprio personale.

3 Si costituisce da sé. Definisce la propria organizzazione e i propri metodi di lavoro in un regolamento interno.

4 I rapporti di lavoro del capo dell'autorità di vigilanza e del personale sono retti dalla legge del 24 marzo 2000[51] sul personale federale. Al capo dell'autorità di vigilanza non si applica il sistema di valutazione di cui all'articolo 4 capoverso 3 della legge sul personale federale.[52]

51 RS **172.220.1**

52 La correzione della Commissione di redazione dell'AF del 12 mar. 2020, pubblicata il 24 mar. 2020, concerne solamente il testo francese (RU **2020** 1057).

Art. 78 Compiti, diritti d'informazione e raccomandazioni dell'autorità di vigilanza indipendente

1 L'autorità di vigilanza indipendente vigila sulle attività informative del SIC, delle autorità d'esecuzione cantonali nonché di terzi o di altri servizi da esso incaricati. Verifica la legalità, l'adeguatezza e l'efficacia delle attività.

2 Essa coordina la propria attività con le attività di vigilanza parlamentare e con altri servizi di vigilanza della Confederazione e dei Cantoni.

3 L'autorità di vigilanza indipendente informa il DDPS in merito alla propria attività in un rapporto annuale; il rapporto è pubblicato.

4 L'autorità di vigilanza indipendente ha accesso a tutte le informazioni e a tutti i documenti utili nonché a tutti i locali dei servizi sottoposti a vigilanza. Può esigere fotocopie dei documenti consultati. Nel quadro della propria attività di vigilanza può chiedere ad altri servizi della Confederazione e dei Cantoni di fornirle informazioni nonché l'accesso a documenti, sempreché vi sia un nesso tra tali informazioni e la collaborazione tra questi servizi e i servizi sottoposti a vigilanza.

5 Per adempiere la propria attività, l'autorità di vigilanza indipendente può accedere a tutti i sistemi di informazione e a tutte le banche dati dei servizi sottoposti a vigilanza; può altresì accedere a dati personali degni di particolare protezione. I dati rilevati possono essere memorizzati soltanto fino al termine della verifica. Il titolare del trattamento verbalizza gli accessi ai sistemi di informazione e alle banche dati.[53]

6 L'autorità di vigilanza indipendente comunica per scritto al DDPS il risultato delle proprie verifiche. Può formulare raccomandazioni.

7 Il DDPS provvede all'attuazione delle raccomandazioni. Se rifiuta una raccomandazione, il DDPS la sottopone al Consiglio federale per decisione.

Art. 79 Autorità di controllo indipendente per l'esplorazione radio e dei segnali via cavo

1 Un'autorità di controllo indipendente, interna all'Amministrazione, verifica la legalità dell'esplorazione radio e vigila sull'esecuzione dei mandati di esplorazione dei segnali via cavo che hanno ottenuto l'autorizzazione e il nullaosta. L'autorità di controllo adempie i propri compiti senza essere vincolata a istruzioni. I suoi membri sono nominati dal Consiglio federale.

2 L'autorità di controllo verifica i mandati assegnati al servizio addetto all'esplorazione nonché il trattamento e la trasmissione delle informazioni che quest'ultimo ha registrato. A tal fine i servizi competenti accordano all'autorità di controllo accesso a tutte le informazioni e a tutti gli impianti utili.

3 In base all'esito delle verifiche, l'autorità di controllo può formulare raccomandazioni e proporre al DDPS la sospensione di mandati per l'esplorazione radio e la cancellazione di informazioni. Le raccomandazioni, le proposte e i rapporti dell'autorità di controllo non sono pubblici.

53 Nuovo testo giusta l'all. 1 n. II 2 della LF del 25 set. 2020 sulla protezione dei dati, in vigore dal 1° set. 2023 (RU **2022** 491; FF **2017** 5939).

4 Il Consiglio federale disciplina la composizione e l'organizzazione dell'autorità di controllo, le indennità dei suoi membri e l'organizzazione della sua segreteria. La durata del mandato è di quattro anni.

Art. 80 Vigilanza e controllo da parte del Consiglio federale

1 Il DDPS informa periodicamente il Consiglio federale in merito alla situazione di minaccia e ai risultati delle attività del SIC.

2 Il Consiglio federale disciplina:

a. la vigilanza finanziaria sui settori d'attività del SIC che richiedono una particolare tutela del segreto;

b. i requisiti minimi che i controlli nei Cantoni devono soddisfare e le competenze degli organi di vigilanza della Confederazione.

3 Il Consiglio federale approva gli accordi amministrativi internazionali conclusi dal SIC che sono di una certa durata, hanno ripercussioni finanziarie sostanziali o dei quali il Consiglio federale dovrebbe essere a conoscenza per ragioni giuridiche o politiche. La riserva di approvazione vale anche per accordi amministrativi non scritti. Gli accordi divengono esecutivi soltanto dopo aver ottenuto l'approvazione.

4 Annualmente, o secondo necessità, il DDPS informa il Consiglio federale e la DelCG in merito allo scopo e al numero di identità fittizie utilizzate dai collaboratori del SIC o degli organi di sicurezza dei Cantoni. Il numero dei nuovi documenti d'identità rilasciati è presentato separatamente.

5 Annualmente, e secondo necessità, il Consiglio federale informa la DelCG in merito ai divieti di attività, ai risultati delle verifiche periodiche di cui all'articolo 73 capoverso 3 e ai divieti di organizzazioni.

Art. 81 Alta vigilanza parlamentare

1 L'alta vigilanza parlamentare sulle attività del SIC e sulle attività svolte dalle autorità d'esecuzione cantonali su mandato della Confederazione per l'esecuzione della presente legge incombe alla DelCG e alla Delegazione delle finanze nei rispettivi ambiti di competenza e conformemente alla legge del 13 dicembre 2002[54] sul Parlamento.

2 Gli organi di vigilanza parlamentare cantonali verificano l'esecuzione di cui all'articolo 85 capoverso 1.

Art. 82 Vigilanza cantonale

1 I collaboratori delle autorità d'esecuzione cantonali incaricate dai Cantoni dell'adempimento di compiti secondo la presente legge sottostanno al diritto cantonale sui rapporti di servizio e alla vigilanza dei loro superiori.

2 Nei Cantoni la funzione di autorità di vigilanza compete agli organi preposti al rispettivo organo esecutivo cantonale. Per rafforzare la vigilanza, questi ultimi possono

54 RS **171.10**

ricorrere a un organo di controllo separato dall'organo esecutivo cantonale e responsabile nei loro confronti.

3 Per i propri controlli, l'autorità di vigilanza cantonale riceve un elenco dei mandati assegnati dal SIC nonché la lista d'osservazione di cui all'articolo 72.

4 L'autorità di vigilanza cantonale può prendere visione dei dati trattati dal Cantone su mandato della Confederazione. La consultazione può essere negata ove lo richiedano interessi essenziali in materia di sicurezza.

5 Il Consiglio federale disciplina la procedura per prendere visione dei dati. In caso di controversie, è possibile promuovere un'azione davanti al Tribunale federale secondo l'articolo 120 capoverso 1 lettera b della legge del 17 giugno 2005[55] sul Tribunale federale.

6 Il Consiglio federale disciplina l'assistenza all'autorità di vigilanza cantonale da parte di servizi della Confederazione.

Sezione 3: Tutela giurisdizionale

Art. 83

1 Le decisioni pronunciate da organi federali in virtù della presente legge sono impugnabili con ricorso al TAF.

2 Il ricorso contro decisioni concernenti l'obbligo speciale d'informazione dei privati nonché il divieto di determinate attività e di organizzazioni non ha effetto sospensivo.

3 Il termine di ricorso contro l'ordine di eseguire una misura di acquisizione soggetta ad autorizzazione decorre dal giorno successivo a quello del ricevimento della comunicazione della misura.

4 Le decisioni su ricorso del TAF sono impugnabili con ricorso al Tribunale federale. La procedura è retta dalla legge del 17 giugno 2005[56] sul Tribunale federale.

Capitolo 7: Disposizioni finali

Art. 84 Disposizioni d'esecuzione

Il Consiglio federale emana le disposizioni d'esecuzione.

Art. 85 Esecuzione da parte dei Cantoni

1 I Cantoni acquisiscono e trattano di propria iniziativa o sulla base di un mandato particolare del SIC le informazioni secondo l'articolo 6 capoverso 1 lettera a. A tal

55 RS **173.110**
56 RS **173.110**

fine, le autorità d'esecuzione cantonali hanno la facoltà di mettere in atto autonomamente le misure di acquisizione non soggette ad autorizzazione di cui agli articoli 13–15, 19, 20, 23 e 25.

2 Le autorità d'esecuzione cantonali informano spontaneamente il SIC quando vengono a conoscenza di una minaccia concreta per la sicurezza interna o esterna.

3 Per l'esecuzione della presente legge, il SIC collabora con i Cantoni, in particolare mettendo a loro disposizione mezzi tecnici, adottando misure di protezione e di osservazione e allestendo offerte di formazione comuni.

4 Nell'ambito delle loro possibilità, i Cantoni sostengono il SIC nell'esecuzione dei suoi compiti, in particolare:

a. mettendo a disposizione i mezzi tecnici necessari;

b. disponendo le misure di protezione e di osservazione necessarie;

c. collaborando alla formazione.

5 La Confederazione indennizza i Cantoni, nei limiti dei crediti stanziati, per le prestazioni che forniscono ai fini dell'esecuzione della presente legge. Il Consiglio federale stabilisce un'indennità forfettaria sulla base del numero di persone attive prevalentemente per compiti della Confederazione.

Art. 86 Abrogazione e modifica di altri atti normativi

L'abrogazione e la modifica di altri atti normativi sono disciplinate nell'allegato.

Art. 87 Coordinamento con la modifica del 25 settembre 2015 della legge sul servizio civile

...[57]

Art. 88 Referendum ed entrata in vigore

1 La presente legge sottostà a referendum facoltativo.

2 Il Consiglio federale ne determina l'entrata in vigore.

Data data dell'entrata in vigore: 1° settembre 2017[58]

57 La mod. può essere consultata alla RU **2017** 4095
58 DCF del 16 ago. 2017.

Allegato
(art. 86)

Abrogazione e modifica di altri atti normativi

I

La legge federale del 3 ottobre 2008[59] sul servizio informazioni civile è abrogata.

II

Gli atti normativi qui appresso sono modificati come segue:

...[60]

59 [RU **2009** 6565; **2012** 3745 all. n. 1, 5525; **2014** 3223]
60 Le mod. possono essere consultate alla RU **2017** 4095.