14.022

Messaggio concernente la legge sulle attività informative

del 19 febbraio 2014

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di legge sulle attività informative.

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

19 febbraio 2014

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Didier Burkhalter
La cancelliera della Confederazione, Corina Casanova

Compendio

Il presente progetto intende istituire una base legale formale unitaria per il servizio informazioni civile della Svizzera, ovvero il Servizio delle attività informative della Confederazione (SIC). Il SIC acquisisce informazioni, le analizza, le valuta e diffonde i risultati allo scopo di mettere a disposizione dei decisori di ogni livello le informazioni di cui hanno bisogno per poter adempiere il loro compito di condotta in modo tempestivo e adeguato alla situazione.

Conformemente all'attuale Rapporto sulla politica di sicurezza, il SIC fa parte, come la politica estera, l'esercito e la polizia, degli strumenti della politica di sicurezza della Confederazione.

L'obiettivo principale del progetto consiste nel disciplinare a livello di legge formale l'attività, i mandati e il controllo del servizio informazioni. In tal modo il SIC sarà in grado, in un'ottica preventiva, di fornire un contributo sostanziale alla sicurezza della Svizzera e della sua popolazione.

Situazione iniziale

Quasi contemporaneamente all'approvazione della legge federale del 3 ottobre 2008 sul servizio informazioni civile (LSIC), il Consiglio federale ha deciso, in una prima fase, di trasferire al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), con effetto dal 1° gennaio 2009, le componenti del Servizio di analisi e prevenzione (SAP) che si occupavano di compiti informativi. In una seconda fase ha riunito il Servizio informazioni strategico (SIS) e il Servizio di analisi e prevenzione (SAP) nel SIC. Quale terza fase, il Consiglio federale ha infine incaricato il DDPS di elaborare entro la fine del 2013 un messaggio per una nuova legge unitaria sul servizio informazioni (decisione del Consiglio federale del 27 novembre 2009).

Secondo la volontà del Consiglio federale la nuova legge istituirà una base legale per i compiti, i diritti, gli obblighi e i sistemi d'informazione del servizio informazioni civile. Il disegno di legge non rappresenta un ulteriore sviluppo delle basi legali vigenti, bensì costituisce un nuovo disciplinamento che tiene conto per quanto possibile delle preoccupazioni e delle riserve nei confronti delle attività attuali dei servizi informazioni svizzeri (in particolare per quanto riguarda la raccolta di dati personali) e prende meglio in considerazione i mutamenti sul fronte dei rischi e delle minacce.

Contenuto del progetto

Il presente disegno di legge comprende essenzialmente le seguenti novità:

– base legale unitaria per il SIC: *l'attuale suddivisione delle basi legali tra la LSIC e la legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI) viene meno;*

– nuovo orientamento dell'acquisizione di informazioni: *non si distingue più in primo luogo tra minacce provenienti dall'interno e minacce provenienti dall'estero, ma tra estremismo violento con riferimento alla Svizzera da un lato e rimanenti ambiti di minacce e compiti dall'altro;*

– introduzione di nuove misure di acquisizione di informazioni nei settori del terrorismo, dello spionaggio, della proliferazione e degli attacchi a infrastrutture critiche oppure per la tutela di altri interessi nazionali essenziali: *i mezzi speciali di acquisizione di informazioni come la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni o l'impiego di apparecchi tecnici di sorveglianza nel settore privato. previsti nel progetto LMSI II e respinti dal Parlamento, sono proposti in forma rielaborata e completati. Secondo il parere del Consiglio federale le nuove misure di acquisizione di informazioni sono necessarie. Alla luce della crescente aggressività degli attori che minacciano la sicurezza interna o esterna della Svizzera e delle forme di minaccia sempre più complesse, gli attuali strumenti non sono più sufficienti affinché il SIC continui ad adempiere i suoi compiti preventivi. Un'autorità giudiziaria e un'autorità politica decideranno nel singolo caso in merito all'autorizzazione di queste misure;*

– conservazione e registrazione differenziate dei dati: *il disegno di legge prevede che le informazioni acquisite dal SIC o da esso ricevute siano archiviate, in funzione della tematica, della fonte e del grado di sensibilità dei dati, in una rete integrata di sistemi d'informazione. Prima che esplichino effetti all'esterno in quanto utilizzati in un prodotto del SIC (p. es. rapporto di analisi, comunicazione a un servizio informazioni estero, valutazione della situazione), i dati personali del SIC devono essere esaminati per quanto riguarda l'esattezza e la rilevanza. I dati che il SIC ottiene mediante una misura di acquisizione soggetta ad autorizzazione sono trattati separatamente e sono a disposizione soltanto degli specialisti in seno al SIC;*

– regime di controllo*: le attività del SIC sottostanno a un controllo e a una vigilanza triplice: da parte del Dipartimento preposto, del Consiglio federale e della Delegazione delle Commissioni della gestione del Parlamento. L'esplorazione radio sottostà inoltre a una verifica tecnica separata da parte dell'autorità di controllo indipendente. Le misure soggette ad autorizzazione e l'esplorazione dei segnali via cavo sono applicabili solo se il Tribunale amministrativo federale ha autorizzato tali misure e il capo del DDPS, dopo aver consultato la Delegazione Sicurezza del Consiglio federale, ha dato il nullaosta per lo svolgimento dell'impiego. Con questi meccanismi si intende garantire la legalità e la proporzionalità delle attività del SIC.*

Indice

Messaggio

1 Punti essenziali del progetto

1.1 Situazione iniziale

Il presente progetto intende istituire una base legale formale unitaria per il Servizio delle attività informative della Confederazione (SIC). Il SIC acquisisce informazioni, le analizza, le valuta e diffonde i risultati allo scopo di mettere a disposizione dei decisori di ogni livello le informazioni di cui hanno bisogno per poter adempiere il loro compito di condotta in modo tempestivo e adeguato alla situazione.

Conformemente al nostro Rapporto all'Assemblea federale del 23 giugno 2010[1] sulla politica di sicurezza della Svizzera (di seguito: Rapporto sulla politica di sicurezza), il SIC fa parte – come la politica estera, l'esercito, la protezione della popolazione, la politica economica, l'amministrazione delle dogane, la polizia e la protezione civile – degli strumenti di politica di sicurezza della Svizzera. Esso è un elemento dell'architettura di sicurezza del nostro Paese.

Il Rapporto sulla politica di sicurezza definisce il ruolo del SIC come segue:

«Il SIC è il Centro di competenza per tutte le questioni di intelligence relative alla sicurezza interna ed esterna. Appoggia la condotta politica e militare nonché altri servizi della Confederazione e dei Cantoni e, con le sue conoscenze e valutazioni, contribuisce all'adozione di decisioni ampiamente condivise e conformi alla minaccia. Il SIC orienta l'impiego dei suoi mezzi alle necessità e alle aspettative dei suoi partner e dei beneficiari delle sue prestazioni. Genera così un prodotto in materia di intelligence con l'ausilio del quale viene allestito, all'attenzione dei decisori dei rispettivi livelli, un quadro globale delle informazioni rilevanti per la condotta».

Con questa definizione abbiamo contemporaneamente stabilito i limiti che la Costituzione prevede per i compiti del SIC.

L'obiettivo principale di questo progetto consiste nel disciplinare a livello di legge formale l'attività, i mandati e il controllo del servizio informazioni. In tal modo il SIC sarà in grado, in un'ottica preventiva, di fornire un contributo sostanziale alla sicurezza della Svizzera e della sua popolazione.

Antefatti e mandato del Consiglio federale

Nel rapporto del 29 febbraio 2008[2] sull'iniziativa parlamentare «Trasferimento dei compiti dei servizi informazioni civili a un dipartimento», la Commissione della gestione del Consiglio degli Stati si era espressa come segue in merito all'attività dei servizi informazioni:

«Le attività dei due servizi [nota: si intendono il Servizio di analisi e prevenzione (SAP) e il Servizio informazioni strategico (SIS)] si sovrappongono in taluni settori, sia a causa della natura della missione loro affidata, sia a causa della definizione legale dei loro compiti. Da un lato, non è sempre possibile distinguere in modo netto la sicurezza interna da quella esterna. Dall'altro, l'attività del SIS presuppone in una certa misura lo svolgimento di attività all'interno dei confini nazionali, mentre

1 FF **2010** 4511
2 FF **2008** 3439

l'adempimento dei compiti che la legge assegna al SAP implica anche contatti con l'estero. La cooperazione tra i due servizi è dunque il presupposto di un'attività efficiente ed efficace. …

Nel mese di giugno del 2005 il Consiglio federale ha deciso di sopprimere la funzione di coordinatore della raccolta informazioni, preferendo puntare su una collaborazione più intensa tra i servizi informazioni civili del DFGP [Dipartimento federale di giustizia e polizia] e del DDPS [Dipartimento federale della difesa, della protezione della popolazione e dello sport]. Si trattava in particolare di intensificare la collaborazione tra SAP e SIS nella lotta alle minacce internazionali. A tal fine, il Consiglio federale ha deciso di istituire piattaforme per lo scambio di informazioni e ha disposto di condurre analisi congiunte nei settori del terrorismo, della criminalità organizzata e della proliferazione di armi di distruzione di massa.

Nell'ambito della sua attività di vigilanza sui servizi e nel settore della protezione dello Stato, la Delegazione delle Commissioni della gestione (DelCG) aveva segnalato da lungo tempo ai Dipartimenti e al Consiglio federale le carenze in materia di coordinamento tra SIS e SAP. La DelCG ha pertanto accolto con favore la summenzionata decisione del Consiglio federale di istituire piattaforme per lo scambio di informazioni, ritenendola una prima, pragmatica tappa di una più ampia riforma. Nel contempo, la DelCG ha nondimeno sottolineato che tali provvedimenti non avrebbero migliorato la conduzione politica dei servizi, e ha quindi reiterato la richiesta, avanzata una prima volta nel 2004, di subordinare i servizi di intelligence a un solo dipartimento e di affidarne quanto prima la direzione a un ente unico. La DelCG si è detta tuttavia disposta a seguire le riforme avviate dal Consiglio federale e ad attendere sino alla fine del 2006 per valutarne gli effetti. …

… A suo giudizio, non si era infatti posto rimedio alle carenze sottolineate nei rapporti annuali del 2004, 2005 e 2006. In particolare, la DelCG aveva avuto modo di constatare, a seguito di numerose indagini conoscitive e di tre ispezioni senza preavviso delle piattaforme, che i provvedimenti adottati non avevano migliorato a dovere la collaborazione tra SAP e SIS. …

La DelCG ha perciò ritenuto che occorresse legiferare con urgenza. La collaborazione tra servizi informazioni non doveva più essere lasciata alla discrezionalità di due dipartimenti: occorreva dunque subordinare l'attività dei due servizi a un unico dipartimento. La DelCG ha quindi deciso all'unanimità di presentare un'iniziativa parlamentare che prevedesse di trasferire a un solo dipartimento i compiti dei due servizi informazioni civili. …».

La legge federale del 3 ottobre 2008[3] sul servizio informazioni civile (LSIC), elaborata in seguito all'iniziativa parlamentare, è entrata in vigore il 1° gennaio 2010.

Dopo l'approvazione della LSIC il nostro Collegio ha deciso, in una prima fase, di trasferire al DDPS con effetto dal 1° gennaio 2009 le componenti del SAP che si occupavano di compiti informativi. In una seconda fase abbiamo deciso, nel marzo del 2009, di riunire il SIS e il SAP nel SIC, con effetto dal 1° gennaio 2010.

In una terza fase abbiamo infine incaricato il DDPS di elaborare entro la fine del 2013 un messaggio per una legge unitaria sul servizio informazioni (decisione del Consiglio federale del 27 novembre 2009):

3 RS **121**

«Il DDPS è incaricato di presentare al Consiglio federale,

… entro la fine del 2013, un messaggio corredato del disegno di una nuova legge sul servizio informazioni, creando così una base legale per i diritti, obblighi e sistemi d'informazione dei servizi informazioni civili svizzeri. Nel nuovo disegno di legge occorrerà ridisciplinare i punti controversi del messaggio del 15 giugno 2007 concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI)[4] *e le disposizioni vigenti».*

Scaglionamento dei lavori legislativi secondo la decisione del Consiglio federale del 27 novembre 2009

Nella primavera del 2009, il Consiglio nazionale e il Consiglio degli Stati hanno rinviato al Governo il progetto legislativo LMSI II del 15 giugno 2007[5] (Mezzi speciali per la ricerca di informazioni), ai fini dell'esame di alcune questioni in campo costituzionale relative a misure di acquisizione dei servizi informazioni previste dal disegno di legge, le quali erano simili a misure coercitive del diritto processuale penale. In quell'occasione si era giunti all'esame dei contenuti dei singoli articoli unicamente in seno al Consiglio degli Stati; il dibattito parlamentare al Consiglio nazionale si era limitato alla questione dell'entrata in materia. Indicazioni precise sul consenso politico di allora in merito a singoli elementi del progetto legislativo sono quindi deducibili solo in maniera limitata.

Successivamente abbiamo fatto esaminare per mezzo di una perizia tali questioni in campo costituzionale e abbiamo deciso uno scaglionamento dei lavori legislativi (decisione del Consiglio federale del 27 novembre 2009): nell'ambito di un primo progetto legislativo urgente occorreva concretizzare nella LMSI le richieste non contestate dalla maggioranza e pronte per essere sottoposte a una decisione. Questa parte è stata nel frattempo realizzata con il messaggio aggiuntivo del 27 ottobre 2010[6] concernente la modifica della legge sulle misure per la salvaguardia della sicurezza interna («LMSI II ridotta») e approvata dal Parlamento il 23 dicembre 2011. La LMSI riveduta è entrata in vigore il 16 luglio 2012.

Il secondo progetto legislativo doveva incentrarsi sulla legge sul servizio informazioni, trattata in questa sede, la quale disciplina l'intero servizio informazioni.

Genesi del presente disegno di legge

Per preparare la nuova legge il SIC ha istituito un gruppo di lavoro interdipartimentale (GLID) composto di rappresentanti del DDPS, del Dipartimento federale degli affari esteri (DFAE), del DFGP, del Ministero pubblico della Confederazione, dei Cantoni e del SIC. Un collaboratore dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) era a disposizione per le questioni in materia di diritto sulla protezione dei dati.

Il GLID ha iniziato i suoi lavori alla fine del mese di ottobre 2010 e entro il mese di luglio 2011 ha elaborato un documento strategico e un concetto normativo. Sulla base dei lavori preliminari del GLID, il SIC ha in seguito avviato la redazione del

4 Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI), RS **120**

5 Messaggio del 15 giugno 2007 concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI; FF **2007** 4613)

6 FF **2010** 6923

presente disegno di legge. Nel corso dei lavori, i progetti di legge sono stati di volta in volta sottoposti al GLID per parere.

Laddove è stato ritenuto opportuno, nel disegno di legge sono state integrate le regolamentazioni affermate della LMSI e della LSIC nonché le nuove regolamentazioni della «LMSI II ridotta». Pertanto, ad esempio, l'obbligo speciale d'informazione e di comunicazione e il divieto di determinate attività corrispondono di principio alle pertinenti disposizioni nel messaggio «LMSI II ridotta».

La nuova legge sulle attività informative non rappresenterà un ulteriore sviluppo delle basi legali vigenti (non sarà quindi una «LMSI III» o «LSIC II»), bensì costituirà un nuovo disciplinamento che tiene conto per quanto possibile delle preoccupazioni e delle riserve nei confronti delle attività attuali dei servizi informazioni svizzeri e prende meglio in considerazione i mutamenti sul fronte dei rischi e delle minacce.

Sia nella procedura di consultazione concernente l'avamprogetto di legge del 2007, sia nei dibattiti politici pubblici e nei resoconti dei media, l'introduzione di mezzi speciali per l'acquisizione di informazioni ha rappresentato la misura di gran lunga più controversa.

Per questo motivo nel nostro progetto «LMSI II ridotta» avevamo rinunciato essenzialmente ai seguenti mezzi per l'acquisizione di informazioni soggetti ad autorizzazione:

- sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni;
- osservazione in luoghi non liberamente accessibili, anche mediante apparecchi tecnici di sorveglianza;
- accesso segreto a un sistema per il trattamento dei dati.

In linea di principio questi punti sono stati ripresi nel presente disegno di legge.

L'8 marzo 2013 il nostro Collegio ha licenziato l'avamprogetto di legge sul servizio informazioni (LSI) e ha autorizzato il DDPS a svolgere una procedura di consultazione, la quale si è tenuta dall'8 marzo al 30 giugno 2013. Il 23 ottobre 2013 abbiamo preso atto dell'esito della consultazione e incaricato il DDPS di procedere con i lavori legislativi.

1.2 Il nuovo disciplinamento proposto

Punti principali del disegno di legge:

Base legale unitaria per il SIC

Nuovo orientamento dell'acquisizione di informazioni

Per quanto riguarda l'acquisizione di informazioni, il disegno di legge prevede una novità nella misura in cui la distinzione non è più operata in primo luogo tra minacce provenienti dalla Svizzera e dall'estero, bensì tra estremismo violento con riferimento alla Svizzera e rimanenti ambiti di minacce e compiti. Una conseguenza di questa concezione è il fatto che, nel caso dell'estremismo violento, le misure di acquisizione soggette ad autorizzazione non possono essere applicate. In questo modo si intendono lasciare definitivamente alle spalle gli avvenimenti prodottisi in seno al

DFGP (Rapporto della Commissione parlamentare d'inchiesta del 22 novembre 1989[7] in merito agli avvenimenti in seno al DFGP), tracciando una linea di demarcazione tra terrorismo ed estremismo violento. Come nel caso della conservazione dei dati, anche l'acquisizione di informazioni nel settore dell'estremismo violento che presenta prevalentemente riferimenti alla Svizzera o ad attori svizzeri deve sottostare a condizioni più rigorose per quanto riguarda le ingerenze nei diritti fondamentali. Conformemente all'articolo 69 capoverso 1 lettera c del disegno della LAIn, il Consiglio federale stabilisce annualmente in un elenco quali gruppi devono essere considerati di matrice estremista violenta.

Introduzione di nuove misure di acquisizione di informazioni negli ambiti del terrorismo, dello spionaggio, della proliferazione e degli attacchi alle infrastrutture critiche oppure per la tutela di interessi nazionali essenziali secondo l'articolo 3

I mezzi speciali di acquisizione di informazioni menzionati nella LMSI II, sottoposti al Parlamento per esame e respinti dallo stesso, sono stati oggetto di una perizia sotto il profilo della conformità con il diritto costituzionale e il diritto internazionale pubblico (perizia del prof. Giovanni Biaggini del giugno 2009[8]). Nel presente disegno di legge, il catalogo dei mezzi speciali di acquisizione di informazioni contenuto nella LMSI II è stato rielaborato e nel contempo completato. Il nostro Collegio chiede l'introduzione delle seguenti nuove misure soggette ad autorizzazione per l'acquisizione di informazioni in Svizzera:

- sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni conformemente alle disposizioni della legge federale del 6 ottobre 2000[9] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT), incluse le informazioni in merito alle comunicazioni per mezzo della corrispondenza postale o del traffico delle telecomunicazioni delle persone sorvegliate nonché le informazioni sull'ubicazione di antenne con le quali è collegato il telefono cellulare di una persona sorvegliata;
- impiego di apparecchi tecnici di localizzazione per stabilire la posizione e i movimenti di persone o oggetti;
- impiego di apparecchi tecnici di sorveglianza per captare o registrare conversazioni private e osservare o registrare fatti in luoghi non pubblici;
- introduzione in sistemi e reti di ordinatori per acquisire informazioni o, in rari specifici casi eccezionali, per disturbare, impedire o rallentare l'accesso a informazioni;
- perquisizioni di locali, veicoli o contenitori portati con sé da persone.

Per l'impiego di queste misure è necessaria l'autorizzazione preliminare del Tribunale amministrativo federale e il successivo nullaosta del capo del DDPS, previa consultazione della Delegazione Sicurezza del Consiglio federale.

7 FF **1990** I 473
8 La perizia è consultabile, soltanto in tedesco, al seguente indirizzo Internet: www.bk.admin.ch > Documentazione > Giurisprudenza delle autorità amministrative della Confederazione (GAAC) > 2009.14 (pagg. 238–330)
9 RS **780.1**

Queste nuove misure di acquisizione di informazioni vengono proposte in quanto, alla luce delle forme di minaccia sempre più aggressive e complesse, gli attuali strumenti (art. 14 LMSI) non sono più sufficienti affinché il servizio informazioni possa svolgere i suoi compiti preventivi nell'ambito della sicurezza interna. Del rimanente si rinvia ai commenti agli articoli 25 segg. (Misure di acquisizione soggette ad autorizzazione).

Sfruttamento delle possibilità offerte dal progresso tecnico nel quadro delle misure di acquisizione non soggette ad autorizzazione

Anche le misure di acquisizione non soggette ad autorizzazione (art. 13 segg.) vengono ampliate. Occorre rendere sfruttabili le possibilità tecniche esistenti (ad es. impiego di mezzi di ricognizione aerea). Per l'impiego di tali mezzi non esisteva finora una base legale formale, ciò che rendeva poco chiara la situazione giuridica.

Trattamento dei dati differenziato

Il disegno di legge prevede che le informazioni acquisite dal SIC o le comunicazioni da esso ricevute siano archiviate in una rete integrata di sistemi d'informazione in funzione della tematica, della fonte e della sensibilità dei dati. Prima che i dati personali del SIC esplichino effetti all'esterno in quanto utilizzati in un prodotto del SIC (per es. rapporto di analisi, comunicazione a un servizio informazioni estero, valutazione della situazione), devono essere valutati per quanto riguarda l'esattezza e la rilevanza. I dati che il SIC ottiene mediante una misura di acquisizione soggetta ad approvazione oppure sulla base di controlli di frontiera sono trattati separatamente e sono a disposizione soltanto degli specialisti in seno al SIC.

Regime di controllo

Le attività del SIC sottostanno a un controllo e a una vigilanza triplice: da parte del Dipartimento preposto, del Consiglio federale e della Delegazione delle Commissioni della gestione delle Camere federali. L'esplorazione radio continua a sottostare inoltre a una verifica tecnica separata da parte dell'autorità di controllo indipendente.

Possibilità di ricorso

Per quanto riguarda le decisioni e le misure di acquisizione soggette ad autorizzazione del SIC, la LAIn prevede la possibilità di interporre ricorso al Tribunale amministrativo federale e, in seconda istanza, al Tribunale federale.

1.3 Motivazione e valutazione della soluzione proposta

Fornitura di un contributo sostanziale alla sicurezza della Svizzera

Per tutelare i propri interessi e proteggere i cittadini, la Svizzera deve poter fare affidamento su un servizio informazioni efficiente. Contemporaneamente, è necessario tenere conto dei diritti di libertà della popolazione.

Il SIC e le autorità d'esecuzione cantonali hanno il compito di fornire un contributo sostanziale alla salvaguardia degli interessi svizzeri e della sicurezza interna ed esterna del nostro Paese, rispettando le libertà dei cittadini. Essi devono acquisire le informazioni necessarie con mezzi e metodi propri dei servizi di intelligence (vale a

dire utilizzando fonti di informazioni pubblicamente accessibili e non pubblicamente accessibili nonché fonti umane), trattarle, analizzarle e trasmetterle in forma adeguata in particolare ai decisori statali (Confederazione e Cantoni). Per tale scopo è indispensabile una valutazione globale della situazione di minaccia. Con gli attuali mezzi legali di acquisizione di informazioni previsti dalla LMSI per il settore della sicurezza interna e che si limitano sostanzialmente all'acquisizione da fonti accessibili al pubblico, alla richiesta di informazioni e all'osservazione in luoghi pubblici e liberamente accessibili (art. 14 LMSI), il SIC può adempiere il suo compito soltanto in misura limitata. Il disegno di legge completa pertanto le misure di acquisizione attuali nel settore della sicurezza interna tramite l'introduzione di misure di acquisizione soggette ad approvazione. Esso disciplina altresì l'acquisizione di informazioni da parte dei Cantoni, ossia da parte delle autorità d'esecuzione cantonali.

Il SIC nel suo insieme provvede ad approvvigionare e assistere i suoi clienti in modo mirato e tempestivo con informazioni e valutazioni, non ottenibili in altro modo.

Uno sguardo al contesto internazionale

Anche nel XXI secolo, l'ambito dell'intelligence è in larga misura di competenza degli Stati nazionali e pertanto uno strumento della direzione politica del rispettivo Paese. Questa considerazione si applica in particolar modo alla Svizzera, che, in quanto Stato indipendente e neutrale, per molti aspetti deve fare affidamento solo su se stessa. La maggior parte dei nostri partner europei sono membri dell'Organizzazione del Trattato del Nord Atlantico (NATO) e/o dell'Unione europea (UE). Anche in seno a organismi come il G20 vengono adottate decisioni di ampia portata che interessano anche la Svizzera, ma per le quali il nostro Paese non viene praticamente consultato. Proprio i membri dell'UE e della NATO sono strettamente interconnessi anche nell'ambito dello scambio d'informazioni. Lo statuto di membro consente di beneficiare di un quadro della situazione ampio e costantemente aggiornato. Grazie alle sue relazioni con i servizi di intelligence di Stati esteri e alle informazioni ottenute per il loro tramite, il SIC sostiene la politica estera della Svizzera.

Riscontri sul «caso Snowden»

Le recenti rivelazioni fatte ai media da Edward Snowden, ex collaboratore del servizio segreto statunitense (NSA), hanno fornito nuove informazioni in merito alle prassi adottate dai grandi servizi informazioni internazionali, in particolare nell'ambito della sorveglianza delle comunicazioni. Se sono disponibili i mezzi tecnici per introdursi in sistemi di comunicazione, questi servizi non rispettano nemmeno i Paesi fondamentalmente «amici». Tali misure di sorveglianza hanno ormai raggiunto una copertura quasi totale e vengono eseguite con un notevole onere finanziario, tecnologico e di personale. Ciò ha aumentato la consapevolezza dell'opinione pubblica per quanto riguarda i pericoli di un utilizzo quasi illimitato e incontrollato delle tecnologie moderne.

La LAIn intende creare un quadro giuridico chiaro che limiti rigorosamente l'impiego di tali mezzi da parte del SIC, lo vincoli al principio di proporzionalità e alla necessità e lo sottoponga a controlli giudiziari, politici e democraticamente legittimati. Sarebbe tuttavia sbagliato rinunciare completamente a tali mezzi. È proprio in questo modo che si lascerebbe il campo libero agli interessi esteri e gli organi di difesa svizzeri continuerebbero a non essere in grado di identificare e chiarire anche solo parzialmente le attività sopracitate, poiché non disporrebbero dell'accesso ai canali di dati in questione.

Riteniamo che per salvaguardare la sicurezza della Svizzera siano necessari, oltre agli sforzi diplomatici a livello internazionale, anche propri mezzi di esplorazione e di difesa efficaci. Tra tali mezzi figura anche l'acquisizione di informazioni in ambiti che finora non erano accessibili ai servizi informazioni svizzeri.

Emanazione di una normativa globale

Il presente disegno di legge attua la decisione del Consiglio federale del 27 novembre 2009 e costituisce una normativa globale che funge da base legale per il SIC. Le disposizioni concernenti l'acquisizione di informazioni in Svizzera e all'estero, sinora contenute in due leggi separate, vengono riunite in un unico atto normativo.

Non si distingue più in primo luogo tra minacce provenienti dalla Svizzera e dall'estero, bensì tra l'estremismo violento con riferimento alla Svizzera e i rimanenti ambiti di minacce e compiti. Alla luce delle attuali forme di minaccia (ad es. il terrorismo), spesso non è più possibile operare una chiara distinzione tra Svizzera ed estero.

Il disegno di legge disciplina i compiti principali del SIC e contiene le disposizioni che, per motivi costituzionali, necessitano di una base legale formale. All'interno del quadro legale abbiamo definito dettagliatamente i settori di compiti del SIC in un mandato fondamentale che si orienta agli interessi specifici della Svizzera e all'evoluzione della situazione di minaccia.

Si tiene altresì conto del fatto che l'attività informativa sottostà a condizioni quadro particolari sia sul piano nazionale sia su quello internazionale (tutela del segreto riguardo a metodi applicati, informazioni, connessioni e processi tecnici, fonti, collaboratori e sensori impiegati). Si tratta in particolare anche di disciplinare chiaramente inevitabili ingerenze nei diritti fondamentali.

Eliminazione delle lacune e dei punti deboli del diritto vigente

Le lacune del diritto vigente sono dovute principalmente all'impostazione della LMSI. Quest'ultima è stata influenzata dalle conoscenze emerse a suo tempo nel quadro del rapporto della Commissione parlamentare d'inchiesta in merito agli avvenimenti in seno al DFGP, la cui percezione da parte del pubblico e degli ambienti politici ha in parte ripercussioni fino a oggi.

In occasione dell'emanazione della LMSI, il legislatore aveva consapevolmente preso in considerazione un rischio in materia di sicurezza adottando il principio in base al quale il trattamento delle informazioni preliminarmente al perseguimento penale doveva essere previsto dalla legge soltanto in misura molto limitata. Tuttavia questo rischio doveva essere minimizzato seguendo attentamente gli sviluppi ed effettuando periodicamente nuove valutazioni della situazione. L'acquisizione, il trattamento e la diffusione di dati particolarmente degni di protezione sono stati disciplinati e limitati in disposizioni esaustive. In tal modo la LMSI è stata resa conforme anche alle severe esigenze della legge federale del 19 giugno 1992[10] sulla protezione dei dati (LPD). Poco dopo l'entrata in vigore della LMSI, gli attacchi terroristici dell'11 settembre 2001 hanno modificato radicalmente la situazione di minaccia. Diversi interventi parlamentari depositati in seguito sollecitavano un rafforzamento del ruolo degli organi di protezione dello Stato e dei servizi informazioni, come pure un ampliamento dei mezzi e degli strumenti a loro disposizione.

10 RS **235.1**

Essi richiedevano inoltre rapporti circostanziati sulla situazione in materia di sicurezza. Nel mese di novembre 2001 il nostro Collegio ha incaricato il DFGP di sottoporgli un rapporto e delle proposte sulle misure per migliorare la situazione e per la lotta contro il terrorismo. Nel mese di giugno del 2002 esso ha approvato il rapporto «Analisi della situazione attuale e dei rischi per la Svizzera dopo gli attacchi terroristici dell'11 settembre 2001»[11] e nel contempo ha preso conoscenza del progetto legislativo che, per mezzo di una revisione della LMSI, intendeva colmare, tra l'altro, le lacune negli strumenti per l'accertamento delle minacce.

Dopo diversi anni di lavori preparatori, il 15 giugno 2007 il Governo ha presentato al Parlamento un messaggio concernente la modifica della LMSI (Mezzi speciali per la ricerca di informazioni; LMSI II), il quale illustrava la situazione in materia di sicurezza e le lacune riscontrate nel dispositivo preventivo di difesa per tutti gli ambiti di minaccia rilevanti.

Come già menzionato in precedenza, nella primavera del 2009 il Parlamento ha rinviato al Collegio governativo il progetto LMSI II. Le lacune e i punti deboli principali della LMSI sono pertanto rimasti immutati fino a oggi.

Per esempio, secondo il diritto in vigore la corrispondenza postale e il traffico delle telecomunicazioni non possono essere oggetto di accertamenti per valutare la minaccia sulla base della LMSI. Laddove manca questo tipo di fonte di informazioni, le autorità di intelligence devono cercare di ottenere informazioni, con un onere notevolmente superiore, entrando in contatto mediante agenti sotto copertura con i gruppi e le persone in questione. Sebbene l'accesso ai settori protetti da password di ordinatori e reti in cui si discutono ad esempio azioni terroristiche sia tecnicamente possibile, ciò è vietato in quanto detti settori sono attribuibili alla sfera privata. Ne derivano lacune a livello di conoscenze nell'individuazione tempestiva e nella cooperazione internazionale.

Qualora dovessero essere raccolte informazioni su attività di spionaggio, il diritto in vigore esclude di principio da ogni accertamento in materia di minacce i luoghi non liberamente accessibili (ad es. camere d'albergo). Le spie sfruttano consapevolmente questa lacuna, in quanto sono sovente tutelate dall'immunità diplomatica e vengono addestrate per acquisire informazioni sotto copertura. A ciò si aggiungono le ricerche effettuate da agenzie investigative private attive su scala internazionale che non di rado agiscono su incarico (non dichiarato) di uno Stato. La conseguenza dell'attuale situazione giuridica è che per esempio anche l'attività di controspionaggio si ferma di principio letteralmente sulla soglia della sfera privata. Di conseguenza possono sorgere gravi lacune nel dispositivo di difesa.

I tentativi di procurarsi armi estere di distruzione di massa sono intrapresi attraverso reti internazionali di estrema complessità. Al riguardo, la Svizzera ottiene ad esempio da terzi indicazioni su ditte e istituti finanziari coinvolti. Se non è possibile sorvegliare in modo mirato la sfera segreta o privata, esattamente come nel caso del terrorismo e dello spionaggio anche nel settore della proliferazione gli accertamenti da parte del SIC in caso di situazioni sospette risultano poco promettenti.

11 FF **2003** 1657

Nel frattempo le lacune e i punti deboli del diritto vigente sono stati tematizzati anche in una serie di interventi parlamentari:

- si è riscontrata una necessità di regolamentazione nel settore dell'impiego di mezzi di esplorazione elettronica (11.3862, Interpellanza Amherd, «Potenziare la sorveglianza di Internet»; 11.3471, Interpellanza Malama, «Sorveglianza in ambienti privati. Correlare la protezione dei dati e la sicurezza»);
- lo stesso dicasi del settore della lotta contro l'estremismo (11.4076, Interpellanza Eichenberger-Walther, «Futuro disciplinamento delle attività di protezione dello Stato»; 11.4059, Interpellanza Geissbühler, «Controllo dell'estremismo di destra in Svizzera»);
- anche nel settore della protezione della piazza finanziaria svizzera è stata riscontrata la necessità di regolamentazione (10.3028, Interpellanza Gruppo Unione democratica di centro, «Furto di dati bancari. Provvedimenti del Consiglio federale ai fini dell'applicazione dello Stato di diritto»; 09.4146, Interpellanza Wehrli, «Strategia piazza finanziaria svizzera»).

Procedura di consultazione

Pareri nel quadro della procedura di consultazione

L'8 marzo 2013 il nostro Collegio ha licenziato l'avamprogetto di legge sul servizio informazioni e ha autorizzato il DDPS a svolgere una procedura di consultazione.

La procedura di consultazione è durata dall'8 marzo al 30 giugno 2013. Sono stati invitati alla consultazione 72 destinatari; il DDPS ha ricevuto 68 risposte (Cantoni: 26, partiti: 8, organizzazioni e altre cerchie interessate: 34).

Di principio il progetto è sostenuto dai Cantoni responsabili in prima linea per la sicurezza interna. Essi sottolineano principalmente la necessità di precisazioni sulla collaborazione con la Confederazione, in particolare per quanto riguarda le questioni relative alla vigilanza. In alcuni casi l'approvazione dell'avamprogetto è subordinata alla riserva dell'elaborazione di una nuova base costituzionale.

Tutti i grandi partiti politici (ad eccezione dei Verdi e del Partito Pirata, contrari) sono sostanzialmente favorevoli al progetto, con alcune riserve e richieste di adeguamento.

Per quanto riguarda le associazioni mantello dell'economia, i pareri variano dall'approvazione al rifiuto; la critica formulata dagli ambienti delle telecomunicazioni concerne principalmente dubbi riguardanti i costi, i quali dipendono in gran parte dalle regolamentazioni già esistenti nella LSCPT. Essa si trova in fase di revisione e gli aspetti relativi ai costi dovranno essere esaminati in primo luogo in tale sede.

Le reazioni delle altre cerchie interessate sono ripartite in maniera più o meno equilibrata, ovvero variano da una tendenziale o completa approvazione a posizioni critiche e di completo rifiuto.

Parallelamente alla valutazione dei pareri ricevuti sono stati svolti colloqui chiarificatori con la Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS) nonché con i rappresentanti del settore delle telecomunicazioni, nel quadro dei quali sono state appianate alcune divergenze e sono state cercate soluzioni per un disciplinamento più preciso.

Adeguamento dell'avamprogetto di legge posto in consultazione

Il 23 ottobre 2013 il nostro Collegio ha preso conoscenza del rapporto sui risultati della procedura di consultazione[12] e ha incaricato il DDPS di elaborare un messaggio entro la fine del 2013.

Le decisioni più importanti scaturite nel quadro della valutazione dei risultati della procedura di consultazione sono le seguenti:

- rinuncia all'elaborazione di una base costituzionale separata per il SIC (ulteriori indicazioni al n. 5.1);
- precisazione del disciplinamento della collaborazione con i Cantoni (unitamente alla CCPCS) e ampliamento dei diritti di vigilanza cantonali per evitare lacune dei controlli (cfr. commenti ai rispettivi articoli);
- mantenimento del disciplinamento in materia di esplorazione dei segnali via cavo (cfr. commenti ai rispettivi articoli);
- formulazione più chiara del disciplinamento relativo alla protezione giuridica.

Numerose osservazioni sono state trattate mediante integrazioni o precisazioni nei commenti.

Valutazione globale

Sotto molteplici aspetti il presente disegno di legge è di considerevole importanza sul piano della politica istituzionale. Tratta questioni delicate e importanti riguardanti la ponderazione dei diritti fondamentali, in particolare il rapporto tra il diritto della popolazione alla tutela della libertà individuale e il diritto a essere protetta dalle minacce che esulano dai singoli casi di competenza delle autorità di polizia e di perseguimento penale. Di conseguenza, nell'articolo sullo scopo la priorità è data alla garanzia dei fondamenti democratici e dello Stato di diritto della Svizzera e alla protezione della sua popolazione. Lo Stato non è quindi protetto in quanto tale, ma si tratta di concretizzare gli scopi fondamentali definiti nella Costituzione.

La LAIn parte dal presupposto che le misure in materia di servizi informazioni devono essere strettamente orientate alle minacce effettive e ai loro autori, mentre la maggior parte della popolazione non deve essere esposta alle osservazioni di intelligence. Per i casi importanti, nei quali si prevedono minacce di grandissima portata per la sicurezza interna o esterna e che quindi coinvolgeranno molte persone, devono essere a disposizione misure incisive, ma mirate, affinché sia possibile identificare e valutare per tempo la situazione. Condizioni legali più severe, procedure di approvazione e strumenti di controllo e di vigilanza efficaci hanno lo scopo di far rispettare tali linee direttrici. I nuovi diritti di ricorso permetteranno inoltre di valutare per via giudiziaria se le disposizioni di legge sono state rispettate.

La LAIn disciplina anche l'acquisizione di informazioni all'estero, per la quale prevede i medesimi principi per quanto riguarda la proporzionalità e il rispetto dei diritti fondamentali, sebbene le regolamentazioni di dettaglio riguardanti l'acquisizione siano diverse. L'acquisizione di informazioni all'estero o concernenti l'estero avviene per lo più in una zona grigia del diritto internazionale. Essa è praticata da

12 www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione ed indagini conoscitive concluse > 2013 > Dipartimento federale della difesa, della protezione della popolazione e dello sport > Legge sul servizio informazioni

tutti gli Stati e nel contempo tutti questi Stati la puniscono quando è diretta contro di loro. Anche la LAIn non può sottrarsi a tale paradosso, ma stabilisce chiaramente che l'acquisizione deve rispettare il principio di proporzionalità. L'essenza dei diritti fondamentali deve essere tutelata anche all'estero. La LAIn si attiene in questo modo sia alla Costituzione che agli imprescindibili impegni di diritto internazionale della Svizzera.

È inoltre importante sottolineare che il servizio informazioni non è un organo di polizia ausiliaria o un fornitore primario di informazioni per le autorità di perseguimento penale, ma rappresenta un'organizzazione autonoma i cui compiti sono focalizzati sull'individuazione tempestiva delle minacce in materia di politica di sicurezza e non hanno alcun carattere penale. I suoi resoconti sono quindi orientati alla prevenzione di minacce e non al perseguimento di reati già avvenuti.

Il nostro Collegio ritiene che in questo progetto ha adottato soluzioni equilibrate e limitate al minimo necessario per quanto riguarda la ponderazione degli interessi. Ciò è stato già parzialmente confermato dall'esito della consultazione; inoltre sono state effettuate ulteriori precisazioni. Grazie a questo progetto è possibile un concreto e fondato dibattito politico pubblico sul rapporto tra libertà e sicurezza, tra trasparenza e necessaria segretezza nonché sui ruoli della Confederazione e dei Cantoni.

1.4 Compatibilità di compiti e finanze

La garanzia della sicurezza è tra i compiti primari di uno Stato. Per salvaguardare gli interessi del Paese, proteggere la popolazione e adottare le misure necessarie, la Svizzera deve poter fare affidamento su un servizio informazioni efficace, in grado di individuare e impedire attività che minacciano la sicurezza.

L'evoluzione sociale e tecnologica, nonché le attuali minacce di portata sempre più globale (p. es. estremismo, terrorismo, criminalità economica, proliferazione di armi nucleari o chimiche), richiedono un'individuazione migliore e più tempestiva rispetto al passato nonché una reazione rapida ed efficace. Inoltre, il servizio informazioni civile deve essere in grado di impiegare le tecnologie e i metodi più moderni.

In considerazione di quanto esposto riteniamo che i costi derivanti dall'attuazione siano sostenibili, tanto più che anche dopo il richiesto aumento dell'effettivo il SIC continuerà ad avere un organico nettamente inferiore rispetto ai servizi di Paesi europei comparabili.

1.5 Diritto comparato, con particolare riferimento al contesto europeo

Nel compendio tabellare vengono comparati taluni aspetti di diversi sistemi di intelligence operativi nel contesto europeo. Per la scelta dei Paesi sono stati applicati i criteri seguenti:

- Germania e Francia sono Paesi limitrofi importanti e presentano una tradizione giuridica simile a quella della Svizzera;
- analogamente al SIC, gli attuali servizi informazioni di Spagna e Paesi Bassi sono anch'essi nati da una fusione di precedenti servizi di intelligence;

– Austria e Belgio sono Paesi di dimensioni comparabili a quelle della Svizzera.

	Germania *Bundesamt für Verfassungsschutz (BfV)* *Bundesnachrichtendienst (BND)*
Posizione nell'architettura di sicurezza	*BfV:* il servizio informazioni interno (unitamente agli uffici dei Länder incaricati della tutela della Costituzione) è subordinato al **Ministero dell'interno**. *BND:* il servizio informazioni concernente l'estero è direttamente subordinato al **Governo federale**. Oltre a questi due servizi, soltanto il Militärischer Abschirmdienst (*MAD)* ha lo statuto di un servizio informazioni.
Compiti	*BfV:* – raccogliere e valutare notizie, informazioni e documenti relativi a mene contro l'ordinamento fondamentale liberale e democratico oppure contro la stabilità o la sicurezza della Repubblica federale o di un Land, oppure mene che mediante l'uso della forza o atti preparatori orientati a tal fine minacciano gli interessi esterni della Repubblica federale o mene contro il principio della comprensione tra i popoli, segnatamente contro la convivenza pacifica dei popoli; – controspionaggio; controproliferazione; protezione dell'economia; collaborazione nell'ambito dei controlli di sicurezza relativi alle persone per la tutela del segreto e la protezione da sabotaggi. *BND:* – raccogliere e valutare le informazioni necessarie per acquisire conoscenze sull'estero rilevanti per lo Stato in materia di politica estera e di politica di sicurezza; – fornire informazioni politiche, economiche, militari e scientifico-tecnologiche sull'estero.
Competenze (impiego di mezzi di intelligence)	*BfV:* l'impiego di mezzi di intelligence da parte del *BfV* è disciplinato nella legislazione. Per adempiere i propri compiti, nel rispetto degli oneri legali al *BfV* è consentito: – impiegare metodi, oggetti e mezzi per acquisire segretamente informazioni (p. es. informatori, osservazioni, registrazioni di immagini e suoni, documenti o contrassegni di copertura);

– richiedere informazioni a istituti finanziari, aziende postali, compagnie aeree e aziende di telecomunicazione;

– accedere a diverse banche dati gestite dalla Repubblica federale (p. es. al registro centrale degli stranieri del *Bundesamt für Migration und Flüchtlinge*, ai dati in materia di asilo del *Bundesamt für die Anerkennung ausländischer Flüchtlinge* oppure al registro dei veicoli).

Per quanto riguarda l'osservazione di organizzazioni e individui sono necessari indizi concreti tali da far sospettare attività che minacciano la Costituzione o la sicurezza.

BND:

i mezzi di intelligence utilizzati all'estero o concernenti l'estero (soprattutto HUMINT e l'esplorazione delle telecomunicazioni) non sono disciplinati nella legislazione, mentre lo sono le attività del *BND* sul territorio tedesco.

In sintonia con la legge tedesca sulla protezione dei dati può registrare, trattare e utilizzare le informazioni necessarie, compresi i dati riferiti a persone:

– per proteggere i propri collaboratori, le proprie installazioni, i propri beni e le proprie fonti contro attività che minacciano la sicurezza o contro lo spionaggio;

– per il controllo di sicurezza relativo a persone che sono o saranno attive in seno al *BND*;

– per la verifica degli accessi alle informazioni necessari all'adempimento dei compiti;

– per l'acquisizione di informazioni su fatti all'estero rilevanti in materia di politica estera e di politica di sicurezza per la Repubblica federale di Germania, se sono ottenibili unicamente in questo modo e nessun'altra autorità è competente per la loro registrazione.

Se è necessario per adempiere i compiti, il *BND* può nel singolo caso richiedere informazioni su dati a operatori postali e di teleservizi, compagnie aeree e istituti di credito. Inoltre, può impiegare metodi, oggetti e mezzi per acquisire segretamente informazioni (p. es. impiego di persone di fiducia o informatori, osservazioni, registrazioni di immagini e suoni, documenti o contrassegni di copertura).

Per quanto riguarda la sorveglianza della corrispondenza postale e delle telecomunicazioni, il *BfV* e il *BND* sottostanno alla *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*. Pertanto, misure incisive in questo ambito possono necessitare dell'autorizzazione dell'Organo di controllo parlamentare oppure della Commissione G-10.

Entrambi i servizi non hanno né poteri di polizia né facoltà di impartire istruzioni.

Vigilanza	*BfV/BND:* – l'**Organo di controllo parlamentare** ha diritto, per il controllo attivo, di consultare atti e dati dei servizi informazioni, interrogare collaboratori, effettuare visite e, in singoli casi, ricorrere all'assistenza di esperti. Inoltre, il Governo federale è tenuto a informare l'Organo in merito alle attività dei servizi informazioni, eccetto se vi sono i presupposti per rifiutare l'informazione, ad esempio per motivi imperativi di protezione delle fonti. L'Organo partecipa anche alla procedura decisionale relativa alle misure nell'ambito della cosiddetta sorveglianza strategica. – Possono essere istituite **Commissioni parlamentari d'inchiesta** per chiarire fatti gravi nel campo dell'intelligence, sempre che siano richieste da un quarto dei deputati del Bundestag. Questo strumento non serve ad esercitare una funzione di controllo costante. Vi è però un obbligo di presentare esaustivamente gli atti per tutti gli organi pubblici nonché un obbligo di testimoniare per i rappresentanti governativi e i collaboratori dei servizi informazioni. – I servizi informazioni sono controllati anche nel quadro dell'«Artikel-10-Gesetz». L'Organo parlamentare e la **Commissione G-10** si completano nel controllo della sorveglianza della corrispondenza postale e delle telecomunicazioni. Inoltre, la Commissione G-10 decide in merito all'ammissibilità e alla necessità di misure di limitazione nell'ambito del controllo individuale e strategico. Di conseguenza, informa il ministero responsabile del rispettivo servizio informazioni in merito alle misure previste per la sorveglianza strategica delle telecomunicazioni. La Commissione può anche verificare nella loro totalità la registrazione, il trattamento e l'utilizzo dei dati riferiti a persone acquisiti grazie alla sorveglianza della corrispondenza postale e delle telecomunicazioni, non da ultimo grazie al diritto all'informazione, alla consultazione di documenti e all'accesso a tutti i locali di servizio. – Il **Comitato parlamentare di fiducia** è competente per il controllo del bilancio dei servizi informazioni. – La **Corte federale dei conti** verifica i conti annuali nonché la gestione del bilancio e la gestione economica. – L'**Incaricato federale per la protezione dei dati e la libertà d'informazione** verifica sia per quanto riguarda il servizio informazioni interno sia per il servizio informazioni concernente l'estero l'osservanza della legge tedesca sulla protezione dei dati e delle altre prescrizioni per la protezione dei dati.

Protezione dei dati	*BfV/BND:* la gestione dei dati riferiti a persone da parte dei servizi e i diritti delle persone interessate sono disciplinati nella legislazione in materia di servizi informazioni. Le regolamentazioni per il *BfV* e il *BND* sono pressoché identiche. Il *BfV* può memorizzare, modificare e utilizzare dati riferiti a persone se vi sono indizi concreti per sospettare attività che minacciano la Costituzione o la sicurezza, il *BND* può fare altrettanto sempre che l'adempimento dei propri compiti lo richieda. In caso di inesattezze, i dati devono tuttavia essere corretti e in caso di illiceità, oppure se non sono più necessari, cancellati. Ciò viene verificato in singoli casi oppure entro i termini stabiliti (*BfV*: dopo cinque anni; *BND*: dopo dieci anni). I dati riferiti a persone che pregiudicano interessi degni di protezione delle persone in questione e non sono più necessari per il futuro adempimento dei compiti devono essere bloccati. Una persona che può riferirsi a fatti concreti e far valere un particolare interesse a un'informazione riceve gratuitamente informazioni in merito ai dati che la concernono. A determinate condizioni i dati riferiti a persone possono essere comunicati ad autorità estere, a servizi delle forze armate di stazionamento nonché a organi sovranazionali e internazionali. A determinate condizioni il *BND* può ottenere dati riferiti a persone da altre autorità tedesche.
	Francia *Direction centrale du renseignement intérieur (DCRI)* *Direction générale de la sécurité extérieure (DGSE)* Il libro bianco francese del 2008 prevede l'elaborazione di un quadro legale per le attività dei servizi informazioni francesi, tuttavia le loro attività sinora non sono praticamente state disciplinate.
Posizione nell'architettura di sicurezza	*DCRI:* il servizio informazioni interno è subordinato al **Ministero dell'interno**. *DGSE:* il servizio informazioni concernente l'estero è subordinato al **Ministero della difesa**. In Francia la comunità dell'intelligence comprende diversi servizi complementari. Oltre alla *DCRI* e alla *DGSE* vi sono altri sei servizi.

Compiti	*DCRI:* – prevenire e perseguire attività ispirate, svolte o sostenute da potenze e organizzazioni estere e tali da minacciare la sicurezza del Paese; – contribuire a prevenire e perseguire atti di terrorismo o azioni che minacciano l'autorità dello Stato, il segreto di Stato oppure gli interessi economici del Paese; – contribuire alla sorveglianza delle radiocomunicazioni e delle comunicazioni elettroniche che minacciano la sicurezza dello Stato nonché contribuire alla lotta contro la criminalità nel settore delle tecnologie dell'informazione e della comunicazione; – partecipare alla sorveglianza di persone, gruppi, organizzazioni e fenomeni sociali che per il loro carattere radicale, il loro orientamento o i loro effetti minacciano la sicurezza nazionale. *DGSE:* – acquisire e valutare informazioni rilevanti per la sicurezza della Francia a favore del Governo e in collaborazione con altre organizzazioni; – individuare o ostacolare le attività di spionaggio che al di fuori del territorio francese sono dirette contro interessi francesi (nel senso di una misura preventiva); – al riguardo, la *DGSE* assicura i collegamenti necessari con altri servizi e organizzazioni rilevanti, esegue le operazioni che le sono assegnate dal Governo nell'ambito delle proprie competenze e presenta le informazioni raccolte sotto forma di sintesi; – in tale contesto, la *DGSE* considera in particolare la lotta al terrorismo e la lotta contro la proliferazione delle armi di distruzione di massa, ma anche il servizio informazioni militare e il servizio informazioni strategico.
Competenze (impiego di mezzi di intelligence)	*DCRI:* la *DCRI* collabora con gli Esecutivi delle regioni e le prefetture della Polizia nazionale. Le sue competenze non sono ancora disciplinate nella legislazione. *DGSE:* la *DGSE* acquisisce informazioni tramite tutti i metodi informativi: HUMINT, SIGINT, OSINT e mezzi operativi. Collabora con servizi informazioni francesi ed esteri. Effettua operazioni segrete tramite operatori paramilitari. Metodi e competenze non sono disciplinati nella legislazione.

Vigilanza	*DCRI/DGSE:* – la **Délégation parlementaire au renseignement (Delegazione parlamentare per i servizi informazioni)** vigila sulle attività e sui mezzi. La Delegazione riceve informazioni sul budget, sulle attività generali e sull'organizzazione dei servizi informazioni, tuttavia non riceve informazioni sulle attività operative, sulle disposizioni governative, sul relativo finanziamento e sugli scambi con servizi esteri o organizzazioni internazionali. Non rientrano tra le informazioni accessibili quelle che potrebbero compromettere l'anonimato, la sicurezza o la vita di una persona o quelle che rivelerebbero specifici metodi operativi per raccogliere informazioni. Il lavoro della Delegazione parlamentare sottostà al segreto di Stato. Formula raccomandazioni e osservazioni e redige un rapporto annuale. – Altre autorità di controllo: – la **Commission nationale de contrôle des interceptions de sécurité** per la sorveglianza delle intercettazioni ambientali; – la **Commission nationale de l'informatique et des libertés** per il controllo della protezione dei dati; – la **Commission de vérification des fonds spéciaux** per l'assegnazione di risorse finanziarie speciali ai servizi informazioni.
Protezione dei dati	*DCRI/DGSE:* per i servizi informazioni non sono state definite condizioni specifiche in materia di protezione dei dati. I servizi informazioni sottostanno tuttavia alle disposizioni generali in materia di protezione dei dati e al controllo della *Commission nationale de l'informatique et des libertés*. Quest'ultima controlla l'osservanza della legge sulla protezione dei dati e la gestione dei dati riferiti a persone da parte dei servizi informazioni e, su incarico dei cittadini interessati, esercita il loro diritto di visionare gli atti, che nel contesto dei servizi informazioni francesi può essere concretizzato soltanto in questa maniera indiretta.
	Spagna *Centro Nacional de Inteligencia (CNI)*
Posizione nell'architettura di sicurezza	Il *CNI* è subordinato al **Ministero della difesa**. Dirige la comunità dell'intelligence spagnola. È completato da un servizio informazioni militare e da altri servizi informazioni minori.
Compiti	– Raccogliere, valutare e trattare informazioni in Spagna e all'estero per proteggere e promuovere gli interessi politici, economici e industriali, commerciali e strategici del Paese;

– prevenire, scoprire e neutralizzare attività di servizi esteri, gruppi o persone che minacciano, violano o costituiscono un rischio per l'ordinamento costituzionale, i diritti o le libertà dei cittadini spagnoli, la sovranità, l'integrità o la sicurezza dello Stato, la stabilità delle istituzioni, gli interessi economici nazionali o il benessere della popolazione;

– promuovere i rapporti e la collaborazione con i servizi informazioni di altri Paesi e con le organizzazioni internazionali;

– eseguire l'acquisizione, la valutazione e l'interpretazione in ambito SIGINT;

– coordinare i diversi servizi, utilizzare i metodi di criptaggio e garantire la sicurezza delle tecnologie dell'informazione in questo settore. Inoltre, acquistare materiale per la crittologia e provvedere alla formazione del personale;

– controllare l'osservanza delle regolamentazioni per la protezione di informazioni segrete;

– garantire la sicurezza e la protezione delle proprie installazioni, informazioni e risorse materiali e di personale.

Competenze (impiego di mezzi di intelligence)

Le competenze del *CNI* sono soltanto in parte disciplinate nella legislazione, l'impiego dei mezzi di intelligence sottostà al controllo giudiziario.

Il *CNI* adempie i suoi compiti raccogliendo informazioni mediante mezzi di intelligence sia in Spagna che all'estero. Può svolgere indagini di sicurezza su persone ed entità e al riguardo può contare sulla necessaria collaborazione di organizzazioni e istituzioni pubbliche e private.

L'uso dei mezzi di intelligence non è disciplinato in maniera univoca, tuttavia un suo disciplinamento risulta dall'autorizzazione che può essere ottenuta per l'impiego di mezzi che incidono sull'inviolabilità della sfera privata o la confidenzialità del traffico di dati (per es. sorveglianza e intercettazione).

Il *CNI* può ottenere questa autorizzazione mediante richiesta del direttore al giudice competente della Corte suprema, sempre che l'impiego dei mezzi sia necessario per l'adempimento dei compiti. La richiesta deve avvenire in maniera formale e scritta e specificare le misure necessarie, le circostanze, gli obiettivi e i motivi di tali misure. Inoltre, deve contenere indicazioni concernenti le persone interessate e il luogo in cui saranno impiegate le misure. Il giudice competente è tenuto a decidere entro 72 ore oppure, in casi urgenti, entro 24 ore.

Il *CNI* dispone di mezzi per inchieste mascherate e può ottenere dalle autorità competenti le identità, le immatricolazioni e i documenti necessari alle sue missioni.

	Agli agenti del *CNI* è consentito il porto d'armi in conformità con le relative esigenze e le prescrizioni legali. A prescindere dal personale addetto alla sicurezza, il servizio informazioni spagnolo non dispone tuttavia di alcun potere di polizia.
Vigilanza	Il **comitato parlamentare per la vigilanza sui fondi segreti** è competente per il controllo parlamentare. Verifica gli obiettivi assegnati dal Governo e il rapporto annuale del direttore del *CNI* sulle attività e sulla situazione per quanto riguarda gli obiettivi assegnati. Il comitato ha accesso unicamente alle informazioni che non si riferiscono a fonti o risorse del *CNI* oppure che non provengono da servizi informazioni esteri o da organizzazioni internazionali. Inoltre, il comitato non può appropriarsi di alcun documento, nemmeno di copie. L'impiego dei mezzi di intelligence sottostà al **controllo giudiziario**.
Protezione dei dati	I testi di legge che concernono il *CNI* non menzionano questioni relative alla protezione dei dati né rimandano a una legge nazionale sulla protezione dei dati a cui si dovrebbe attenere il servizio informazioni spagnolo.
	Paesi Bassi *Algemene Inlichtingen- en Veiligheidsdienst (AIVD)*
Posizione nell'architettura di sicurezza	L'*AIVD* è subordinato al **Ministero dell'interno**. È completato dal servizio informazioni militare.
Compiti	– Indagini su persone e organizzazioni per le quali sussiste un sospetto fondato che rappresentino un serio pericolo per l'ordinamento democratico, la sicurezza nazionale o altri importanti interessi dei Paesi Bassi; – esame dei candidati a posizioni con obbligo del segreto; – appoggio alle istituzioni responsabili della sicurezza delle infrastrutture private e statali di importanza vitale per il mantenimento della struttura sociale dei Paesi Bassi; – indagini su Paesi in conformità con attività affidate per incarico congiunto del Primo ministro, del ministro dell'interno e del ministro della difesa; – elaborazione di analisi dei rischi e dei pericoli relative a immobili, prestazioni e individui per il sistema nazionale di sicurezza.

Competenze (impiego di mezzi di intelligence)	Le competenze dell'*AIVD* sono disciplinate in maniera relativamente chiara nella legislazione, l'impiego dei mezzi di intelligence da parte dell'*AIVD* è regolamentato da una moltitudine di condizioni nella legge sui servizi informazioni e sul servizio di sicurezza. Per l'acquisizione di informazioni dispone delle competenze seguenti: – contattare tutte le autorità o persone che sembrano in grado di fornire le informazioni necessarie; – sorvegliare persone e opere con o senza ausili tecnici per effettuare registrazioni, seguire tracce o procedere alla localizzazione; – impiegare agenti infiltrati; – perquisire opere e settori chiusi; – aprire lettere e invii di merci senza il consenso del mittente o del destinatario (è però necessario il mandato del Tribunale distrettuale dell'Aia); – penetrare in sistemi informatici con o senza mezzi tecnici o segni, password e identità falsi; – intercettare, registrare o sorvegliare qualsiasi forma di conversazione, telecomunicazioni o trasferimento di dati con l'ausilio di apparecchi tecnici; – rivolgersi a operatori pubblici di reti di telecomunicazione per ottenere informazioni su un utente. Queste competenze sottostanno a rigorose condizioni legali e necessitano spesso di istruzioni del ministro competente o del direttore del servizio informazioni. L'*AIVD* non ha alcun potere di polizia e non gli è consentito di occuparsi di reati.
Vigilanza	– Un **comitato parlamentare di vigilanza sui servizi informazioni e sui servizi di sicurezza** controlla l'osservanza della legge sui servizi informazioni e di sicurezza da parte del servizio informazioni civile e militare. Tutti i partecipanti al processo di intelligence sono tenuti a collaborare con il comitato. Inoltre, il comitato ha accesso a tutte le informazioni di intelligence e ha il diritto di interrogare testimoni ed esperti e di avviare un'inchiesta. – L'**ombudsman nazionale** è competente per i ricorsi della popolazione concernenti il comportamento dei servizi informazioni e dei servizi di sicurezza. Decide in merito a tali ricorsi e motiva la sua posizione, sempre che la sicurezza e altri interessi dello Stato non vi si oppongano. Successivamente informa il ministro interessato in merito alla sua decisione. L'ombudsman può anche formulare raccomandazioni. Il ministro trasmette

poi le raccomandazioni e le sue conclusioni al Parlamento dei Paesi Bassi.

– La **Corte dei conti** verifica le uscite dell'*AIVD* per le operazioni segrete e presenta annualmente al Parlamento un rapporto al riguardo.

– I ministri responsabili dei servizi informazioni e dei servizi di sicurezza presentano al Parlamento un rapporto annuale sulle attività dell'*AIVD*.

Protezione dei dati

L'*AIVD* può utilizzare o trattare i dati personali di una persona unicamente nei casi seguenti:

– se sussiste un serio sospetto che questa persona costituisca un pericolo per l'ordinamento democratico, la sicurezza o altri interessi vitali del Paese;

– se la persona ha dato il proprio consenso per effettuare un controllo di sicurezza;

– se ciò è necessario nell'ambito di ricerche su altri Paesi;

– se le informazioni sono state raccolte da un altro servizio informazioni o da un altro servizio di sicurezza;

– se i dati sono necessari al servizio affinché questo possa adempiere i propri obblighi;

– se la persona è stata impiegata presso il servizio o lo è attualmente; oppure

– se i dati sono necessari all'allestimento di analisi dei rischi.

I dati riferiti a persone i quali non hanno più alcuna importanza per lo scopo per il quale sono stati raccolti devono essere eliminati. Anche le informazioni che si sono rivelate errate o che sono state trattate illecitamente devono essere corrette o eliminate.

Il ministro, altre persone e autorità rilevanti, i servizi informazioni e i servizi di sicurezza rilevanti di altri Paesi nonché le organizzazioni di sicurezza, le organizzazioni SIGINT e le organizzazioni di intelligence internazionali rilevanti possono essere informati in merito alle informazioni trattate dall'*AIVD*.

Per quanto riguarda il diritto di consultare dati personali, il ministro competente è tenuto a informare appena possibile il richiedente in merito a quali dati personali sono stati trattati dal servizio o per il servizio. Successivamente il richiedente ha il diritto di consultare i dati.

Austria

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)

Heeresnachrichtenamt (HNaA)

Posizione nell'architettura di sicurezza	*BVT:* il servizio informazioni interno è subordinato, in quanto parte della polizia di sicurezza, alla Direzione generale della sicurezza pubblica in seno al **Ministero federale dell'interno**. Il *BVT* è appoggiato da nove uffici dei Länder per la tutela della Costituzione e la lotta al terrorismo. *HNaA:* il servizio informazioni strategico concernente l'estero è subordinato, in seno al **Ministero federale della difesa e dello sport**, al capo di Stato maggiore generale. Oltre al servizio informazioni interno e al servizio informazioni concernente l'estero vi è un solo altro servizio, il Servizio per le informazioni e la sicurezza militare, che svolge la funzione di servizio informazioni militare.
Compiti	*BVT:* – acquisizione di informazioni, indagini e analisi nei settori del terrorismo, dell'estremismo, del controspionaggio, del traffico illegale di armi e della proliferazione; – protezione di persone e di opere a favore degli esponenti di istituzioni costituzionali; – protezione di rappresentanti di Stati esteri, organizzazioni internazionali e altri oggetti tutelati dal diritto internazionale pubblico; – protezione di infrastrutture critiche; – controlli di sicurezza. *HNaA:* attività informativa: acquisizione, trattamento, valutazione e presentazione di informazioni concernenti l'estero o organizzazioni internazionali oppure altri enti internazionali in relazione con fattispecie militari e altri fatti, fenomeni o progetti connessi.
Competenze (impiego di mezzi di intelligence)	L'impiego di mezzi di intelligence è disciplinato chiaramente dalla legge per entrambi i servizi. *BVT:* il *BVT* acquisisce le sue informazioni tramite l'analisi OSINT nonché da fonti non pubblicamente accessibili. In questo ambito (ricerca ampliata in materia di pericoli) dispone delle seguenti competenze: – sorveglianza di gruppi di persone, se sulla base delle circostanze e degli sviluppi è possibile prevedere un serio pericolo per la sicurezza pubblica e a causa della criminalità ad esso correlata, segnatamente la violenza a sfondo religioso o ideologico;

– impiego segreto di apparecchi per riconoscere le targhe dei veicoli e impiego visibile di apparecchi per registrare immagini e suoni nelle aree critiche in materia di criminalità;

– impiego segreto di apparecchi per registrare immagini e suoni e la trasmissione di registrazioni private di suoni e immagini alle autorità di sicurezza a determinate condizioni;

– osservazioni e impiego di agenti infiltrati.

A seconda dell'entità dell'impatto dei mezzi di intelligence, il loro utilizzo presuppone l'informazione del garante dei rimedi giuridici del Ministero federale dell'interno e l'autorizzazione preliminare del suddetto garante.

Il *BVT* è un servizio di polizia e quindi, in quanto parte della polizia di sicurezza, ha poteri di polizia conformemente alla *Sicherheitspolizeigesetz*.

HNaA:

secondo la *Militärbefugnisgesetz* l'*HNaA* ha le seguenti competenze in materia di intelligence:

– richiesta di informazioni a persone, organi di enti territoriali e di altri enti di diritto pubblico nonché a fondazioni, istituti e fondi gestiti da questi enti e agli operatori pubblici di servizi di telecomunicazione;

– registrazione di dati sulla base di osservazioni, se altrimenti l'adempimento dei compiti fosse impedito o ostacolato in maniera considerevole;

– inchiesta mascherata, se ciò è urgentemente necessario nell'interesse della sicurezza nazionale, in particolare nell'interesse della garanzia della prontezza all'impiego dell'esercito austriaco e se altrimenti sarebbe impedito l'adempimento dei compiti;

– registrazione di dati mediante apparecchi per registrazioni audiovisive, se ciò è indispensabile nell'interesse della sicurezza nazionale, in particolare nell'interesse della garanzia della prontezza all'impiego dell'esercito austriaco, e se altrimenti l'adempimento dei compiti sarebbe in gran parte impedito.

Prima di una registrazione dei dati sulla base di osservazioni, inchieste mascherate o mediante apparecchi per registrazioni audiovisive, l'*HNaA* deve informare il garante dei rimedi giuridici per la verifica della legalità delle misure in materia di intelligence o di controspionaggio, indicando i motivi principali della registrazione, nonché darne comunicazione al ministro federale della difesa. Una simile registrazione può essere avviata unicamente dopo il pertinente consenso del garante dei rimedi giuridici. Se un'ulteriore attesa dovesse però comportare un grave danno per la sicurezza nazionale a cui non è più possibile rimediare, segnatamente per la prontezza all'impiego dell'esercito

austriaco o per la sicurezza delle persone, la registrazione potrà essere avviata ed effettuata immediatamente dopo la presa di conoscenza da parte del garante della tutela giurisdizionale, sempre che quest'ultimo non vi ponga fine con un veto.

Vigilanza

BVT:

– controlli nel quadro dell'*Interpellationsrecht,* il diritto del Parlamento di controllare la gestione dell'Esecutivo.

– Controlli da parte dello **Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Massnahmen zum Schutz der verfassungsmässigen Einrichtungen und ihrer Handlungsfähigkeit (sottocomitato permanente della Commissione per gli affari interni incaricata della verifica delle misure volte alla protezione delle istituzioni costituzionali e della loro capacità di agire)**. Esso è competente per la verifica dell'adempimento dei compiti conforme alla Costituzione da parte del *BVT*. È autorizzato dal ministro federale dell'interno a richiedere informazioni e a consultare documenti.

– Controllo sostanzialmente amministrativo da parte della **Corte dei conti** e della **Difesa civica (Volksanwaltschaft**).

– Controlli da parte del **garante della tutela giurisdizionale del Ministero federale dell'interno**. Nel quadro delle competenze speciali del *BVT* il suo coinvolgimento spazia, a seconda dell'intensità dell'impatto delle misure, dalla semplice presa di conoscenza all'autorizzazione preliminare per le misure. Allestisce annualmente un rapporto sull'adempimento dei propri compiti.

– Controlli da parte del **Comitato per i diritti dell'uomo** (**Menschenrechtsbeirat**). Esso consiglia il ministro federale dell'interno in caso di questioni concernenti la tutela dei diritti dell'uomo e in questa funzione vigila anche sul *BVT*. Questo è tenuto ad assisterlo nella sua attività; inoltre il ministro federale gli mette a disposizione le risorse necessarie all'adempimento dei compiti.

HNaA:

– controlli nel quadro dell'*Interpellationsrecht,* il diritto del Parlamento di controllare la gestione dell'Esecutivo.

– Controlli da parte dello **Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Massnahmen zur Sicherung der militärischen Landesverteidigung (sottocomitato permanente della Commissione per la difesa nazionale incaricato della verifica delle misure di intelligence volte alla sicurezza della difesa nazionale militare)**. Esso può esigere dall'*HNaA* tutte le informazioni e i documenti pertinenti. Ai fini della protezione delle fonti non è tuttavia autorizzato a richiedere

informazioni o documenti, in particolare sulle fonti, la cui conoscenza potrebbe minacciare la sicurezza nazionale o la sicurezza delle persone.

– Controlli da parte del **garante della tutela giurisdizionale per verificare la legalità delle misure in materia di intelligence o di controspionaggio**. Esso è competente per l'autorizzazione e il controllo dell'impiego dei mezzi di intelligence. Gli deve essere concesso in ogni momento il diritto di consultare tutti i documenti e le registrazioni necessari e gli devono essere fornite le informazioni che gli occorrono. Ciò non vale tuttavia per le informazioni e i documenti, relativi all'identità di persone o a fonti, la cui conoscenza potrebbe minacciare la sicurezza nazionale o la sicurezza delle persone. Deve anche poter sorvegliare in ogni momento l'attuazione delle misure che deve controllare e accedere a tutti i locali in cui sono conservati registrazioni o altri risultati della sorveglianza. Inoltre, il garante dei rimedi giuridici vigila sull'osservanza dell'obbligo di rettifica o cancellazione conformemente alle disposizioni in materia di protezione dei dati. Allestisce un rapporto annuale sulle proprie attività.

BVT/HNaA:

controlli da parte della **Commissione per la protezione dei dati**. Nel quadro della legge sulla protezione dei dati la Commissione è competente per la protezione giuridica di una persona fisica in caso di sospette violazioni del diritto fondamentale alla protezione dei dati. Essa giudica i ricorsi per sospetta violazione del diritto all'informazione, alla tutela del segreto, alla rettifica o alla cancellazione.

Protezione dei dati

BVT:

La gestione dei dati riferiti a persone e i diritti delle persone interessate sono disciplinati dalla *Sicherheitspolizeigesetz*.

I dati riferiti a persone possono essere registrati e utilizzati, per quanto ciò sia necessario per l'adempimento dei compiti. I dati possono essere richiesti anche agli operatori di servizi di telecomunicazione o ad altri fornitori di servizi.

I dati inesatti o registrati in maniera imprecisa devono essere rettificati e i dati riferiti a persone non più necessari devono essere cancellati. I dati trattati riferiti a persone devono essere verificati se non sono più stati modificati per sei anni.

Un interessato ha il diritto di ricevere gratuitamente informazioni in merito ai dati registrati concernenti la propria persona. Il *BVT* non deve tuttavia fornire alcuna informazione se ciò è necessario alla protezione del fornitore delle informazioni o se legittimi interessi preponderanti del mandante o di un terzo, segnatamente interessi pubblici preponderanti (p. es. la protezione delle istituzioni costituzionali della Repubblica d'Austria) si oppongono alla comunicazione delle informazioni.

	HNaA: la *Militärbefugnisgesetz* non prevede regolamentazioni speciali relative alla protezione dei dati, ma rimanda alla legge sulla protezione dei dati. Il diritto all'informazione corrisponde a quello del *BVT*.
	Belgio *Sûreté de l'Etat (SE)* *Service générale du renseignement et de la sécurité des Forces armées (SGRS)* (In Belgio la *SE* è di carattere civile, il *SGRS* di orientamento militare. Entrambi sono competenti per l'intelligence sia interna sia esterna, tuttavia la *SE* si occupa essenzialmente dell'interno mentre il *SGRS* si concentra piuttosto sull'estero.)
Posizione nell'architettura di sicurezza	*SE:* il servizio informazioni civile è di principio subordinato al **Ministro della giustizia**, per le questioni che riguardano al sicurezza pubblica e la protezione delle persone è tuttavia competente anche il **Ministro dell'interno**. *SGRS:* il servizio informazioni militare è subordinato al **Ministro della difesa**. Anche il servizio delle dogane e la polizia si occupano dell'acquisizione informativa, ma non sono servizi informazioni veri e propri e quindi non sottostanno alle relative leggi. I servizi informazioni collaborano sia tra di loro sia con servizi esteri e possono fornire appoggio alle autorità giudiziarie e amministrative.
Compiti	*SE:* – ricercare, analizzare e trattare informazioni su attività che minacciano o potrebbero minacciare la sicurezza dello Stato o l'esistenza dell'ordinamento democratico o costituzionale, la sicurezza esterna dello Stato o le relazioni internazionali, il potenziale scientifico o economico o tutti gli altri interessi fondamentali del Paese (spionaggio, terrorismo, estremismo, proliferazione delle armi di distruzione di massa, organizzazioni settarie nocive o organizzazioni criminali, interferenze); – controlli di sicurezza; – protezione delle persone; – altri compiti secondo la legge.

SGRS:

– ricercare, analizzare e trattare informazioni su attività che minacciano o potrebbero minacciare l'integrità del territorio nazionale, i piani di difesa militari, l'esecuzione dei compiti delle Forze armate, la sicurezza dei cittadini belgi o altri interessi fondamentali del Paese; informare il ministro competente;

– consigliare il Governo nelle questioni di politica estera e di difesa;

– garantire la sicurezza militare del personale del Ministero della difesa, delle installazioni militari, delle armi, dei piani, dei sistemi informatici, delle comunicazioni e di altre opere militari;

– tutela del segreto;

– controlli di sicurezza.

Competenze (impiego di mezzi di intelligence)

L'impiego dei mezzi di intelligence è disciplinato in maniera chiara per entrambi i servizi nella legislazione.

SE/SGRS:

secondo la legge, i servizi possono ricercare, raccogliere, ricevere e trattare dati riferiti a persone, sempre che ciò sia necessario per adempiere i propri compiti. Inoltre, per ottenere informazioni possono ricorrere a autorità giudiziarie, funzionari e impiegati del servizio pubblico nonché a persone o organizzazioni del settore privato, entrare in locali e luoghi pubblicamente accessibili, visitare alberghi e altri alloggi nonché utilizzare fonti umane.

Se questi metodi usuali non sono sufficienti per ottenere informazioni, entrambi i servizi possono utilizzare anche metodi specifici o metodi straordinari.

Metodi specifici:

– osservazione mediante ausili tecnici in spazi pubblici o privati accessibili al pubblico oppure osservazione con o senza ausili tecnici di spazi privati non accessibili al pubblico;

– controlli, mediante ausili tecnici, di spazi pubblici e di spazi privati accessibili al pubblico nonché di opere chiuse che si trovano al loro interno;

– identificazione del mittente o del destinatario di un invio postale o del titolare di una casella postale;

– identificazione dell'abbonato o dell'utente abituale di un servizio di comunicazione elettronica o del mezzo di comunicazione elettronica utilizzato;

– localizzazione dei dati relativi alle chiamate di mezzi di comunicazione elettronica e localizzazione della provenienza o della destinazione della comunicazione elettronica.

Questi metodi possono essere utilizzati soltanto se la commissione amministrativa istituita per la sorveglianza e in parte anche per l'autorizzazione dei metodi è stata informata al riguardo dal direttore del rispettivo servizio.

Metodi straordinari:

– osservazione e controllo di spazi privati non accessibili al pubblico;
– costituzione e utilizzazione di una persona giuridica per appoggiare le attività operative e l'impiego di agenti del servizio informazioni;
– apertura e lettura della posta;
– raccolta di dati relativi a conti bancari e transazioni bancarie;
– introduzione in sistemi informatici;
– intercettazione e registrazione di comunicazioni.

Questi metodi possono essere utilizzati soltanto se sono stati autorizzati dalla commissione amministrativa competente.

I servizi informazioni belgi possono appoggiare le autorità giudiziarie, ma non hanno poteri di polizia (per lo meno la legge non si esprime al riguardo).

Vigilanza

SE/SGRS:

– **commissione permanente per i servizi informazioni e i servizi di sicurezza** (autorità di controllo parlamentare): vigila sui servizi informazioni e può svolgere indagini (inoltre dispone del diritto di visionare gli atti e può disporre convocazioni, perquisizioni e sequestri).
– **Commissione amministrativa**: sorveglia l'applicazione delle misure specifiche e delle misure straordinarie dei servizi informazioni.
– **Ombudsman federale**: è competente per i ricorsi di singoli individui, può svolgere indagini e visionare atti; non sussiste però alcun obbligo di trasmettergli informazioni segrete.
– **Commissione per la protezione dei dati**: verifica su incarico dei cittadini le informazioni riferite a persone registrate dai servizi, può però formulare unicamente raccomandazioni e non può fornire informazioni in merito al contenuto degli atti.

Protezione dei dati

SE/SGRS:

alla *SE* e al *SGRS* si applicano le stesse regolamentazioni. La gestione da parte dei servizi dei dati riferiti a persone e i diritti delle persone interessate sono disciplinati nella legislazione in materia di attività informative.

Le informazioni e i dati riferiti a persone possono essere ricercati, raccolti, ricevuti e trattati. Possono anche essere comunicati a

determinate persone, autorità, servizi di polizia o a tutti gli altri organi competenti, sempre che questi siano oggetto di una minaccia oppure le informazioni riferite a persone siano necessarie per l'adempimento dei rispettivi compiti. Questi dati possono essere conservati soltanto finché sono necessari per lo scopo per cui sono stati registrati, ad eccezione dei dati considerati di importanza storica dall'Archivio di Stato. La distruzione avviene soltanto dopo la scadenza di un termine stabilito dal Re e basato sull'ultimo trattamento dei dati.

I cittadini non hanno alcun diritto di visionare gli atti personali che li concernono e devono rivolgersi alla commissione per la protezione dei dati.

1.6 Attuazione

Le misure potranno essere attuate facendo quasi completamente ricorso alle strutture federali (SIC, Tribunale amministrativo federale, Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, rappresentanze svizzere ecc.) e cantonali (autorità di polizia e di sicurezza cantonali) esistenti.

2 Commento alle singole disposizioni

Nota introduttiva circa il termine «minaccia»

Secondo la definizione data dal Consiglio federale nel RAPOLSIC 2010, il termine «minaccia» presuppone «*la volontà di danneggiare la Svizzera o i suoi interessi o per lo meno di considerare un simile danneggiamento*». Il termine «pericolo» non presuppone invece alcuna volontà di danneggiare (per es. pericoli naturali e tecnologici)[13].

Nel presente disegno di legge si è scelto di utilizzare il termine «minaccia» onde distinguere nettamente la nozione da quella di pericolo naturale, benché taluni sviluppi in materia di politica di sicurezza compresi nel settore di compiti del servizio informazioni non siano orientati direttamente contro la Svizzera, o per lo meno non ancora, oppure possano rappresentare un fattore in grado di impedire o allontanare una minaccia.

Ingresso

Conformemente alla recente prassi in materia di legislazione, l'ingresso della legge non fa più menzione della competenza costituzionale implicita della Confederazione di legiferare sulla salvaguardia della sicurezza interna o esterna. Secondo l'attuale interpretazione, la competenza normativa in materia è contemplata nell'articolo 173 capoverso 2 della Costituzione federale (l'Assemblea federale tratta le questioni rientranti nella competenza della Confederazione e non attribuite ad altre autorità).

13 FF **2010** 4511 4523

Da questa competenza costituzionale deriva in particolare la competenza (limitata) della Confederazione di legiferare sui compiti dei Cantoni, ossia delle autorità d'esecuzione cantonali, in materia di sicurezza interna. In proposito si rimanda al commento agli articoli 9 (Autorità d'esecuzione cantonali) e 81 (Esecuzione da parte dei Cantoni).

Art. 1 Oggetto

Nell'articolo 1 è riassunto il contenuto della legge.

Art. 2 Scopo

L'importanza del presente disegno di legge in quanto disciplinamento globale del servizio informazioni svizzero giustifica l'introduzione di una disposizione sullo scopo. L'articolo 2 riprende elementi della LMSI. Esso definisce gli scopi sui quali si concentrano le attività informative e serve da linea guida per l'esecuzione della legge, senza tuttavia fissare alcuna competenza.

Art. 3 Impiego in situazioni particolari

La LAIn disciplina la salvaguardia degli interessi essenziali della Svizzera nell'ambito della politica di sicurezza. L'articolo 3 conferisce al Consiglio federale la facoltà di incaricare il SIC, in situazioni particolari, di acquisire e analizzare informazioni e se del caso di svolgere attività operative che vanno oltre i limiti del mandato legale ordinario del Servizio. A tal fine è necessaria una decisione del Consiglio federale ai sensi dell'articolo 70. Non sono sufficienti né il mandato fondamentale assegnato dal Consiglio federale (art. 69 cpv. 1 lett. a) né la lista d'osservazione emanata dal Consiglio federale (art. 71). Per salvaguardare interessi nazionali essenziali ai sensi dell'articolo 3, il SIC non può dunque agire né di sua iniziativa né in virtù degli strumenti ordinari di condotta «Mandato fondamentale» e «Lista d'osservazione». La decisione del Consiglio federale non conferisce al SIC competenze particolari più estese di quelle definite dalla LAIn. Pertanto, le attività di acquisizione sono rette dalle norme stabilite dalla legge, in particolare per quanto riguarda l'applicazione di misure soggette ad autorizzazione (art. 25 segg.), le quali devono essere proposte e motivate seguendo la procedura normale. Nella propria decisione il Consiglio federale può invece assoggettare a condizioni l'attività del SIC, limitando ad esempio all'estero le attività di intelligence oppure escludendo determinate misure di acquisizione (per es. quelle soggette ad autorizzazione).

Di norma, quando saranno invocati interessi nazionali essenziali ai sensi dell'articolo 3 non ancora contemplati nel mandato generale che la legge assegna al SIC, si tratterà di attività di intelligence all'estero. Detti interessi nazionali essenziali dovranno rientrare nella sfera di competenza della Confederazione sancita dalla Costituzione federale. In via aggiuntiva, è possibile che un Cantone o più Cantoni facciano richiesta di un impiego del SIC affinché siano tutelati interessi svizzeri rientranti in primo luogo nella sfera di competenza dei Cantoni, ma che, se minacciati, possono essere considerati interessi essenziali di livello nazionale. Il disegno di legge menziona tra gli altri interessi nazionali essenziali la protezione dell'ordinamento costituzionale della Svizzera (nella misura in cui va oltre il mandato del SIC definito all'articolo 6), il sostegno alla politica estera svizzera (per es. in caso di situazioni di crisi a livello di politica di sicurezza, negoziati particolarmente difficili o pressioni

diplomatiche) e la protezione della piazza industriale, economica e finanziaria svizzera (per es. in caso di pressioni esercitate per motivi politico-economici contro determinati rami economici di importanza nazionale).

Eventuali particolari risorse di personale o finanziarie necessarie per l'adempimento di un simile impiego dovranno essere di volta in volta assegnate al SIC dal Consiglio federale nel quadro della pertinente decisione. È fatta salva la sovranità delle Camere federali in materia di preventivo.

L'articolo 3 non limita la competenza del Consiglio federale a emanare ordinanze fondate sugli articoli 184 capoverso 3 e 185 capoverso 3 della Costituzione federale (cfr. anche art. 7*a*–7*d* della legge del 21 marzo 1997[14] sull'organizzazione del Governo e dell'Amministrazione, LOGA).

Art. 5 Principi dell'acquisizione di informazioni

Il compito principale del servizio informazioni consiste nell'acquisire e valutare informazioni nonché nel trasmetterle ai destinatari autorizzati sotto forma di prodotti informativi come pure nel concretizzare i riscontri acquisiti in prestazioni operative di carattere preventivo atte a ridurre le minacce nei confronti della sicurezza. L'articolo 5 del disegno definisce dunque i principi dell'acquisizione di informazioni che governano l'applicazione di tutte le altre disposizioni. L'articolo si rivolge in primo luogo al SIC, in quanto autorità d'esecuzione federale competente, ma in secondo luogo anche alle autorità d'esecuzione cantonali che agiscono direttamente in esecuzione della LAIn o per mandato speciale del SIC.

I contenuti dei singoli capoversi sono disciplinati e in parte precisati in altre disposizioni della legge.

Il *capoverso 1* precisa che il SIC acquisisce informazioni sia da fonti accessibili al pubblico sia da fonti non accessibili al pubblico. La conoscenza delle fonti accessibili al pubblico (cfr. art. 13) è importante in questo contesto per poter valutare quali informazioni devono essere acquisite, confermate o eventualmente smentite con mezzi di intelligence.

Il *capoverso 2* rimanda al sistema di misure di acquisizione soggette e non soggette ad autorizzazione disciplinato nel capitolo 3. Le misure non soggette ad autorizzazione (art. 13 segg.) vengono applicate dal SIC sotto la propria responsabilità e non necessitano di autorizzazione (per es. osservazioni in luoghi pubblici). Esse corrispondono in gran parte al catalogo di misure già contemplato nel vigente articolo 14 capoverso 2 LMSI.

Le misure di acquisizione soggette ad autorizzazione (art. 25 segg.) sono applicabili soltanto nei casi previsti dalla legge; esse presuppongono un'autorizzazione da parte del Tribunale amministrativo federale e il nullaosta del capo del DDPS.

Il *capoverso 3* esplicita l'applicazione del principio generale di proporzionalità al campo di attività del servizio informazioni: l'essenza di questo principio è un rapporto adeguato tra lo scopo perseguito e l'ingerenza nei diritti fondamentali che il suo raggiungimento impone. Il principio di proporzionalità prescrive ad esempio al SIC, nell'adempimento del proprio mandato, di adottare di volta in volta la misura più mite, ossia la misura che presumibilmente comporta la minor ingerenza nei

14 RS **172.010**

diritti fondamentali della persona interessata. Se è possibile acquisire un'informazione con una misura non soggetta ad autorizzazione, questa dovrà essere preferita a una misura soggetta ad autorizzazione.

Il *capoverso 4* è necessario per derogare al principio generale previsto in materia di protezione dei dati, secondo il quale la raccolta di dati personali deve essere riconoscibile da parte della persona interessata (art. 4 cpv. 4 LPD). La disposizione corrisponde agli attuali articoli 5 capoverso 1 LSIC e 14 capoverso 1 LMSI. Se la persona interessata fosse al corrente dell'acquisizione e del trattamento di dati personali, lo scopo del trattamento ne sarebbe in genere compromesso. È riconosciuto invece un diritto d'accesso, disciplinato negli articoli 62 e seguenti.

Nei *capoversi 5–8* sono ripresi in sostanza i collaudati principi già previsti dalla LMSI per proteggere le attività politiche dalle osservazioni di intelligence, con le relative eccezioni. Durante la procedura di consultazione singoli partecipanti hanno richiesto un inasprimento di tali disposizioni. Il nostro Collegio ritiene per contro adeguato l'attuale sistema, aggiornato alle nuove circostanze soltanto nel 2001. L'attuale sistema è mantenuto nel quadro della LAIn, così da garantire la medesima protezione già assicurata nel quadro della LMSI per il trattamento a livello di intelligence di eventi occorsi in Svizzera. Per l'estero una simile riserva non avrebbe senso, poiché renderebbe praticamente impossibile l'osservazione e la valutazione di sviluppi di tipo egemonico.

Gli esempi di seguito illustrano l'esercizio abusivo di diritti fondamentali ai sensi del capoverso 6 per svolgere attività che minacciano la sicurezza:

– un'associazione costituita per fini di culto gestisce una sala riunioni per i propri membri. Questa sala è regolarmente frequentata da una persona che cerca di convincere i membri dell'associazione a unirsi alla lotta religiosa armata all'estero o a partecipare a un addestramento al combattimento armato all'estero. Gli accertamenti e il trattamento dei dati da parte del servizio informazioni si riferiscono a questa persona, ma non ai membri dell'associazione in generale;

– un gruppo di persone appartenenti a una minoranza etnica che nel Paese d'origine conduce una lotta armata contro il governo gestisce in Svizzera un locale per fini apparentemente culturali. Una serata folcloristica con spettacoli musicali non serve però allo scopo annunciato, bensì per una «commemorazione di martiri» alla quale intervengono oratori che inneggiano alla lotta armata e raccolgono fondi a tale scopo.

I *capoversi 6 e 7* corrispondono alle disposizioni entrate in vigore nel 2012 a precisazione dell'articolo 3 LMSI. Il SIC è tenuto a proporre all'Archivio federale i dati che devono essere cancellati. I dati privi di valore archivistico devono essere definitivamente distrutti.

Il *capoverso 8* chiarisce che il SIC può trattare tutte le informazioni rilevanti per la valutazione della minaccia che riguardano organizzazioni e gruppi della lista d'osservazione secondo l'articolo 71. Nella LMSI questa disposizione era sinora integrata nelle norme sulla lista d'osservazione, dove la sua applicazione ha dato adito ad alcune incertezze. La nuova collocazione sistematica ovvierà a questo problema.

Capitolo 2, sezione 1

Il contributo del SIC alla sicurezza del Paese è soprattutto di carattere preventivo. Nondimeno esso deve poter coadiuvare con i mezzi speciali di cui dispone anche altri servizi federali nell'adempimento dei loro compiti (cfr. art. 68).

L'attività preventiva del SIC deve essere chiaramente distinta dall'attività repressiva delle autorità di perseguimento penale. Il mandato fondamentale del SIC consiste nell'individuare tempestivamente le minacce in materia di politica di sicurezza che incombono sulla Svizzera e nel riferire su di esse, principalmente all'indirizzo delle competenti autorità, affinché sia possibile minimizzare i rischi. Il SIC non svolge però compiti di polizia o inerenti alla procedura penale (p.es. indagini, arresti ecc.). Le attività del servizio informazioni e delle autorità di perseguimento penale sono complementari, tuttavia le une non sono preliminari alle altre e pertanto sottostanno a due regimi separati anche in materia di vigilanza (il servizio informazioni sottostà alla vigilanza degli organi politici, il perseguimento penale a quella dei tribunali). Di conseguenza, il reciproco scambio di informazioni tra SIC e autorità di perseguimento penale deve essere disciplinato in modo chiaro.

Art. 6 Compiti del SIC

Nel *capoverso 1* la legge menziona soltanto il SIC come autorità incaricata dell'esecuzione. Tuttavia, i settori di compiti di cui alla lettera a sono determinanti anche per l'esecuzione da parte dei Cantoni (cfr. art. 81). A livello di contenuto essi corrispondono ai noti settori di competenza della LMSI. A questi settori vengono ora ad aggiungersi per esplicita menzione gli attacchi a infrastrutture critiche, che a seguito degli sviluppi tecnici intervenuti dall'epoca dell'adozione della LMSI hanno assunto una nuova rilevanza. Se sono ad esempio connessi ad attività terroristiche o di spionaggio, gli attacchi di questo genere rientrano come sinora anche tra i compiti definiti nel numero 1 o nel numero 2. Ma poiché spesso questi retroscena non sono riconoscibili, o lo diventano semmai dopo approfonditi accertamenti, è indispensabile assicurare sin dall'inizio la collaborazione del SIC, onde consentire al Servizio di poter svolgere il ruolo assegnatogli nell'ambito della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi. Le reti delle infrastrutture critiche devono essere protette contro gli attacchi degli hacker. In questo campo il SIC continuerà ad acquisire le informazioni necessarie sugli attacchi incombenti o già avvenuti per i servizi che si occupano dei cyber-attacchi e a contribuire alla difesa da questi attacchi. A questo scopo il SIC può anche contare su contatti internazionali esclusivi.

La nozione di «infrastrutture critiche» si fonda sulla terminologia in uso nel settore della protezione della popolazione. Essa è da intendersi in senso generale e comprende, ad esempio, anche le infrastrutture di importanti organizzazioni internazionali con sede in Svizzera.

Alla *lettera b*, l'espressione «fatti rilevanti in materia di politica di sicurezza che avvengono all'estero» sta a designare fatti e sviluppi all'estero suscettibili di compromettere l'autodeterminazione della Svizzera, i fondamenti della democrazia e dello Stato di diritto, di arrecarle gravi danni nel campo della politica di sicurezza o danni di altra natura o di pregiudicare la capacità di agire delle sue autorità. In questo ambito il SIC fornisce soprattutto prestazioni a favore del Dipartimento federale degli affari esteri (DFAE), sotto forma di rapporti di analisi e di comunicazione di informazioni specifiche.

La *lettera c* fa riferimento al compito fondamentale del SIC, il quale consiste nel fornire tempestivamente al Governo federale le informazioni necessarie all'adempimento dei suoi compiti. Il compito di sostenere la capacità di agire della Svizzera è stato pertanto espressamente incluso nel catalogo dei compiti del SIC.

Costituisce una novità anche il compito di salvaguardare interessi essenziali della Svizzera (cfr. commento all'art. 3).

L'elenco dei compiti del SIC e degli obiettivi perseguiti è distinto dalle competenze concrete del Servizio, disciplinate nelle successive disposizioni della legge.

L'acquisizione e il trattamento di dati allo scopo di valutare la situazione di minaccia ai sensi del *capoverso* 2 è disciplinata in modo particolareggiato nei capitoli 3 e 4. Il SIC si occupa soltanto delle allerte che rientrano nel settore di compiti della legge. Per altri tipi di allerta sono competenti altri organi (per es. per le catastrofi naturali la Centrale nazionale d'allarme dell'Ufficio federale della protezione della popolazione).

In caso di eventi di particolare importanza dal profilo della sicurezza (per es. l'incontro annuale del World Economic Forum oppure grandi conferenze internazionali quali il Vertice della Francofonia), per adempiere i compiti previsti ai capoversi 2 e 3 il SIC allestisce una rete informativa integrata. Questa coordina l'acquisizione e la disseminazione delle informazioni e consente ai servizi competenti interessati di seguire costantemente l'evoluzione della situazione mediante il sistema di presentazione elettronica della situazione (PES, art. 52).

L'informazione di altri servizi della Confederazione e dei Cantoni secondo il *capoverso 3* è oggetto di precisazioni negli articoli 58 e seguenti che disciplinano in particolare la trasmissione di dati personali.

Il *capoverso 4* assegna al SIC il ruolo di servizio responsabile in materia di contatti di intelligence con l'estero, già sancito nel vigente articolo 8 LMSI. La disposizione è intesa a evitare doppioni e incoerenze nelle relazioni con servizi informazioni o autorità di sicurezza esteri. Il compito di servizio responsabile assunto dal SIC è ulteriormente precisato nell'articolo 12.

Il *capoverso 5* riprende i compiti preventivi svolti attualmente dalla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, unità operativa e informativa già integrata nel SIC. Oggi MELANI gestisce già un sistema di preallerta per una ristretta cerchia di gestori di infrastrutture critiche. Questa importante funzione va oltre il mero trattamento di informazioni ai sensi del capoverso 1 lettera a numero 4 e pertanto è espressamente disciplinata in questo capoverso.

Il *capoverso 7*, infine, riveste una particolare importanza per la sicurezza del SIC, dei suoi collaboratori e delle sue informazioni. L'articolo 7 disciplina la questione in modo più particolareggiato. Contemporaneamente alla LAIn, la Confederazione prepara anche una base legale per la protezione delle informazioni e delle opere. Tale base legale introdurrà se necessario norme di portata generale, applicabili a tutta l'Amministrazione federale, che copriranno determinate esigenze di sicurezza del SIC. Al momento attuale, tuttavia, la LAIn deve garantire al SIC una protezione sufficiente.

Il SIC può fornire anche prestazioni di supporto nell'ambito dell'assistenza amministrativa. Questa funzione non rientra però tra i suoi compiti fondamentali e pertanto è disciplinata separatamente nell'articolo 68.

Art. 7 Misure di protezione e di sicurezza

Le misure di protezione e di sicurezza enumerate completano gli atti normativi federali in materia di sicurezza integrale, segnatamente negli ambiti della protezione delle persone, delle informazioni e delle opere. Tali misure mirano a imporre l'applicazione di prescrizioni per la tutela del segreto di servizio e, pertanto, incrementano la sicurezza e la credibilità del SIC per quanto concerne la gestione di dati classificati.

Per garantire la sicurezza, la formazione e le misure di sensibilizzazione hanno la priorità rispetto ad altre misure. Tuttavia anche le misure tecniche e la verifica del rispetto delle prescrizioni rientrano in una gestione dei rischi efficace e credibile.

Lettera a: i controlli di borse e persone sono eseguiti esclusivamente per motivi di sicurezza e nel rispetto della proporzionalità. Il SIC può affidarne l'esecuzione a terzi. Tale misura è volta alla protezione dei beni di proprietà del datore di lavoro e al rispetto delle prescrizioni per la protezione di informazioni classificate. È applicabile nei confronti dei collaboratori del SIC, ma anche del personale impiegato a tempo determinato, come i praticanti. Possono essere controllati anche collaboratori di aziende che forniscono prestazioni all'interno dei locali del SIC o eseguono lavori artigianali. I membri degli organi di vigilanza e i visitatori non sono oggetto di controlli. Nei locali del SIC essi sono sempre accompagnati.

Lettera c: i sistemi di videosorveglianza non sono utilizzati per sorvegliare costantemente il comportamento delle persone. Il loro impiego avviene all'esterno degli edifici, nei parcheggi, nelle zone d'accesso, d'entrata o di transito, nei locali dove sono custodite casseforti, negli archivi contenenti dati classificati o degni di particolare protezione, nonché nei magazzini contenenti beni preziosi.

Lettera d: i locali in cui si svolgono conversazioni con contenuti altamente sensibili o classificati sono dotati, per quanto possibile, di misure di protezione passive (schermatura e isolamento acustico) che impediscono una fuga di informazioni per esempio via telefoni cellulari. Laddove ciò non è possibile, si può ricorrere all'impiego temporaneo di impianti di telecomunicazione che provocano interferenze per impedire le comunicazioni telefoniche cellulari. In tale contesto occorre prestare attenzione a non ledere eccessivamente altri interessi pubblici o interessi di terzi. Per non interferire con le telecomunicazioni di terzi, l'impiego di disturbatori di frequenza è limitato al locale utilizzato e avviene esclusivamente durante le conversazioni sensibili o classificate «segreto». Gli apparecchi in questione devono essere conformi alle prescrizioni dell'UFCOM ed essere omologati.

Il *capoverso 2* costituisce la base legale per la rete separata gestita già oggi dal SIC per la maggior parte delle proprie applicazioni informatiche e dei propri sistemi d'informazione. Poiché il SIC elabora una grande quantità di dati sensibili e classificati, la sicurezza informatica riveste un'importanza particolare. L'accesso alla rete è limitato ai collaboratori del SIC, ai collaboratori degli organi di vigilanza sulle attività informative nonché, in maniera molto restrittiva, a pochi collaboratori del Servizio informazioni militare, che attualmente non dispone di una propria rete protetta da analoghe misure di sicurezza.

Art. 8 Armamento

Nell'ambito dell'acquisizione di informazioni in materia di terrorismo, spionaggio, estremismo violento, commercio illecito di armi o di armi di distruzione di massa chimiche, biologiche o nucleari, i collaboratori incaricati devono talvolta operare in ambienti pericolosi e violenti, per esempio quando devono instaurare e mantenere contatti con fonti umane. I collaboratori del SIC attivi in tale ambito in Svizzera devono essere armati per poter proteggere se stessi, le fonti umane o terze persone quando incombe un pericolo immediato per la vita e l'integrità fisica. Nei casi descritti, l'attività di un collaboratore incaricato dell'acquisizione di informazioni in Svizzera è comparabile a quella di un responsabile delle persone di fiducia nell'ambito della polizia.

L'arma deve essere impiegata soltanto in caso di legittima difesa (art. 15 seg. del Codice penale[15] [CP]) o di stato di necessità (art. 17 seg. CP). Nell'impiego dell'arma occorre rispettare in particolare la proporzionalità (cpv. 2).

La disposizione riprende ampiamente il vigente articolo 5*a* LMSI. Oltre ad applicare le prescrizioni d'esecuzione del Consiglio federale, come sinora il SIC disciplinerà mediante istruzioni i dettagli relativi alle armi di servizio (tra cui le prescrizioni sull'attestazione di un addestramento sufficiente e sull'abilitazione al porto di armi da fuoco, l'allenamento obbligatorio al tiro).

Art. 9 Autorità d'esecuzione cantonali

Secondo il presente disegno, la Confederazione e i Cantoni assumono congiuntamente l'esecuzione dei compiti di intelligence (cfr. art. 81). Le autorità d'esecuzione cantonali acquisiscono nel territorio sottoposto alla loro giurisdizione le informazioni che sono tenute a raccogliere in virtù della LAIn o su mandato speciale del SIC. Come sinora, i Cantoni designeranno un servizio specializzato per l'adempimento di questi compiti. In genere questo servizio fa parte del corpo di polizia.

Altre prescrizioni riguardanti i Cantoni sono contemplate dai capitoli 4 (trattamento dei dati) e 6 (controllo e vigilanza).

Art. 10 Informazione dei Cantoni

La nuova legge attribuirà ancora grande importanza all'attuale stretta collaborazione tra Confederazione e Cantoni. Essa impone pertanto alla Confederazione di informare, come finora, le competenti autorità cantonali in merito a eventi particolari nel settore di compiti del SIC e in merito alla situazione di minaccia. L'informazione avviene soprattutto attraverso la Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS) e la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP). Inoltre, il SIC è in contatto permanente con le autorità d'esecuzione cantonali, alle quali è così garantita la possibilità di adempiere i propri compiti sul territorio cantonale in sintonia con le esigenze della Confederazione. L'articolo 45 capoverso 3 disciplina in via complementare l'utilizzazione presso i Cantoni delle valutazioni della situazione e degli ulteriori dati trasmessi dal SIC.

15 RS **311.0**

Art. 11 Collaborazione con l'esercito

La collaborazione con il Servizio informazioni dell'esercito (in special modo con il Servizio informazioni militare) e con la Sicurezza militare, praticata sin dall'istituzione del SIC, sarà mantenuta.

Il Servizio informazioni dell'esercito e la Sicurezza militare coprono entrambi le necessità dell'esercito negli ambiti tematicamente affini della valutazione delle minacce e della sicurezza. In tale contesto, l'articolo 11 disciplina l'obbligo del SIC di informare i competenti servizi dell'esercito in merito a fatti militarmente rilevanti. Gli obblighi d'informazione dei due servizi militari sono invece disciplinati negli articoli 19 e 20 (obbligo d'informazione generale e speciale). I dettagli della collaborazione saranno definiti (in sostanza come già previsto dalla vigente normativa) nell'ordinanza d'esecuzione.

Il *capoverso 2* è inteso a consentire al SIC di continuare a incaricare gli addetti alla difesa di acquisire in determinati casi informazioni per suo conto e di curare i contatti con servizi informazioni o autorità di sicurezza esteri. In questi casi, le informazioni vengono sempre acquisite nel rispetto dell'ordinamento giuridico dello Stato ospite, vale a dire utilizzando i contatti ufficiali con le sue autorità o la rete delle relazioni diplomatiche. Gli addetti alla difesa non sono dunque persone a cui è attribuito un ruolo di «spie in uniforme», bensì persone di collegamento con il SIC annunciate presso i servizi informazioni interessati dei rispettivi Stati di accreditamento. Questo modo di procedere si è dimostrato molto valido ad esempio in casi di rapimento o per l'osservazione degli sviluppi in atto nel contesto della cosiddetta «Primavera araba». La collaborazione e la suddivisione dei compiti avranno luogo anche in futuro in stretta intesa con il settore Relazioni internazionali dell'esercito.

Art. 12 Collaborazione con l'estero

A titolo introduttivo va detto che il nostro Collegio rinuncia a evocare espressamente nella LAIn il principio secondo cui per le questioni di sicurezza i Cantoni possono cooperare con le autorità di sicurezza estere competenti per la regione di frontiera (cfr. art. 8 cpv. 2 LMSI). Questo ordinamento vige comunque già in forza di quanto disposto dall'articolo 56 capoverso 3 della Costituzione federale. Per quanto riguarda l'esecuzione da parte dei Cantoni non vi sono dunque cambiamenti rispetto a quanto già disciplinato nella LMSI vigente.

Quanto al *capoverso 1,* occorre menzionare che in materia di servizio informazioni non esistono attualmente convenzioni internazionali vincolanti. In quest'ambito gli accordi vengono piuttosto conclusi sotto forma di accordi (agreement) o eventualmente di memorandum d'intesa, senza effetto vincolante. Questa prassi si spiega con il fatto che il servizio informazioni serve principalmente gli interessi di carattere nazionale del singolo Paese. Una collaborazione può concretizzarsi negli ambiti in cui questi interessi coincidono con quelli di altri Paesi. Oggi il SIC collabora con servizi informazioni e autorità di sicurezza di numerosi Paesi, per esempio nei campi della lotta contro il terrorismo, lo spionaggio, l'estremismo violento, oppure su questioni di politica egemonica e militari. Tuttavia, gli Stati vogliono essere liberi di adeguare i propri interessi in materia di servizio informazioni alle loro necessità senza essere vincolati da convenzioni. La Svizzera non costituisce un'eccezione.

La comunicazione di dati personali ad autorità estere è disciplinata in maniera più dettagliata nell'articolo 60.

In avvenire un'eccezione potrebbe essere rappresentata soprattutto dalla gestione di sistemi d'informazione internazionali comuni (lett. e). Si tratta di una crescente rivendicazione espressa dai servizi informazioni europei, che tuttavia non ha potuto essere pienamente realizzata, poiché nella maggior parte degli Stati mancano le necessarie basi legali nazionali e non esistono nemmeno accordi internazionali al riguardo. Il Consiglio federale propone ora di sancire nella LAIn il diritto per il SIC di partecipare a sistemi d'informazione automatizzati. Trattandosi di una forma particolare di collaborazione internazionale, per ragioni inerenti alla protezione dei dati essa dovrebbe essere disciplinata nell'ambito di un accordo tecnico scritto. Tuttavia, la competenza di concludere simili accordi non spetta al SIC ma al Consiglio federale (art. 69 cpv. 3).

Secondo il *capoverso 2* in futuro sarà possibile distaccare persone di collegamento del SIC nelle rappresentanze svizzere all'estero, analogamente a quanto previsto per gli addetti alla migrazione, alla difesa e di polizia, qualora la collaborazione internazionale lo richiedesse. Il personale del SIC sarà impiegato soltanto d'intesa con il DFAE. I collaboratori del SIC in questione opereranno in missione ufficiale. Saranno regolarmente annunciati ai competenti servizi dello Stato ospite e di eventuali Stati terzi in caso di accreditamento collaterale e opereranno esclusivamente come persone di collegamento ufficiali con i competenti servizi. Non essendo incaricati dell'acquisizione segreta di informazioni di intelligence, non violano il diritto degli Stati ospiti. Considerati gli elevati costi, siamo del parere che soltanto poche persone di collegamento del SIC potranno essere impiegate in tal modo, e ciò soltanto dopo un potenziamento del Servizio a lungo termine. Questi collaboratori del SIC potrebbero essere impiegati per colmare eventuali lacune nel dispositivo degli addetti alla difesa oppure per completare tale dispositivo nel caso in cui gli addetti alla difesa non siano in grado di assumere determinate funzioni indispensabili. Le risorse finanziarie e di personale necessarie saranno messe a disposizione nel quadro del preventivo ordinario.

Il *capoverso 3* è volto a garantire che i contatti in materia di intelligence della Svizzera con altri Paesi si svolgano esclusivamente secondo le norme previste dalla LAIn. Lo stesso principio è già oggi applicabile in forma analoga in virtù dell'articolo 8 LMSI ed è precisato nell'articolo 11 capoversi 1 e 2 dell'ordinanza del 4 dicembre 2009[16] sul Servizio delle attività informative della Confederazione (O-SIC). Il ruolo di «leading agency» assegnato al SIC riguarda però unicamente i contatti con servizi informazioni veri e propri e con altre autorità estere quando si tratta di contenuti in materia di intelligence. La limitazione riguarda soprattutto le relazioni con autorità estere che svolgono diverse funzioni (per es. polizia giudiziaria e servizio informazioni interno). In questi casi, i contatti con contenuti di polizia (giudiziaria) sono di competenza delle autorità svizzere di polizia.

Nel quadro della collaborazione con l'estero secondo l'articolo 69 del disegno, il Consiglio federale ha del rimanente compiti particolari e può emanare al riguardo ulteriori regolamentazioni a livello di ordinanza.

16 RS **121.1**

Capitolo 3

Secondo l'esauriente definizione del trattamento di dati contemplata dalla LPD, l'acquisizione (raccolta) è senz'altro compresa nella nozione di trattamento (cfr. art. 3 lett. e LPD). Tuttavia, il fatto che per ogni servizio informazioni la raccolta di dati rivesta un'importanza primordiale e che essa può essere connessa, per le persone interessate, a gravi ingerenze nei diritti fondamentali, giustifica il disciplinamento dell'acquisizione e dell'ulteriore trattamento in capitoli indipendenti.

Le disposizioni di questo capitolo menzionano soltanto il SIC come servizio incaricato dell'acquisizione. Tuttavia, esse si applicano anche alle autorità d'esecuzione cantonali nell'ambito dei loro compiti d'esecuzione in virtù degli articoli 9 e 81.

Durante la procedura di consultazione, taluni partecipanti hanno espresso il parere che le misure di acquisizione della nuova legge non sarebbero sufficientemente in sintonia con il Codice di procedura penale[17] (CPP). Al riguardo va osservato che, conformemente al principio dell'unità della materia, nel quadro del presente disegno va disciplinato unicamente il settore del servizio informazioni e che non possono confluirvi tematiche inerenti al CPP. Poiché è una nuova legge, la LAIn deve contemplare i recenti sviluppi tecnici (per es. in relazione a misure di acquisizione nel cyberspazio). Inoltre rammentiamo che il servizio informazioni adempie un compito a sé stante e non costituisce un'istanza preliminare rispetto al perseguimento penale o una sua forma meno severa. Relativamente alle misure di acquisizione per le quali è necessaria un'autorizzazione, si è tenuto conto del fatto che la legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) è attualmente in fase di revisione. Per facilitare l'armonizzazione con la revisione della LSCPT e per evidenziare che la LAIn non deve permettere di attuare un maggior numero di misure o altre misure, il presente disegno fa esplicito riferimento alla LSCPT. Tale riferimento consentirà di ridurre al minimo gli oneri di coordinamento tra i due disegni di legge.

All'auspicio di alcuni Cantoni di poter disporre delle medesime competenze del SIC è stato dato seguito soltanto in misura limitata. È il caso, in parte, delle misure di acquisizione per le quali non è necessaria un'autorizzazione. Per contro, le misure che necessitano di un'autorizzazione secondo la LAIn possono essere adottate unicamente dalla Confederazione. I Cantoni che dovessero avere necessità proprie in materia dovranno legiferare al riguardo a livello cantonale.

Capitolo 3, sezione 1

In questa sezione sono enumerate le misure di acquisizione che il SIC può adottare autonomamente senza necessitare di una specifica autorizzazione esterna, poiché comportano un'ingerenza di intensità relativamente limitata nei diritti fondamentali. Queste misure corrispondono sostanzialmente alle possibilità di acquisizione contemplate nell'articolo 14 capoverso 2 LMSI. Il terzo capitolo menziona tutti i mezzi classici di intelligence per l'acquisizione di informazioni, dall'«open source intelligence» (OSINT, art. 13) all'«imagery intelligence» (IMINT, art. 14 cpv. 2) e dalla «human intelligence» (HUMINT, art. 15) alla «communication intelligence» (COMINT, art. 27 e 37 segg.). Per l'applicazione di queste misure la LAIn prevede norme specifiche in funzione dell'intensità dell'ingerenza nei diritti fondamentali.

17 RS **312.0**

In occasione della consultazione, alcuni partecipanti hanno proposto anche di disciplinare nella LAIn l'accesso ai dati delle reti sociali, poiché tali dati possono essere di elevato interesse per un servizio informazioni. Il nostro Collegio ha però rinunciato a un tale disciplinamento in quanto il termine «reti sociali» è poco determinato e potrebbe essere applicato a una quantità pressoché infinita di dati. In questo caso vanno piuttosto applicate le regolamentazioni generali: se si tratta di dati resi accessibili al pubblico, allora si applicano le normative corrispondenti. Per le misure di acquisizione nell'ambito protetto dal segreto delle telecomunicazioni si applica per contro l'obbligo dell'autorizzazione del giudice e del nullaosta dell'autorità politica secondo gli articoli 25 e seguenti.

Secondo l'articolo 81 capoverso 1, nel quadro dell'esecuzione autonoma della LAIn, i Cantoni sul loro territorio possono impiegare la maggior parte delle misure non soggette ad autorizzazione.

Art. 13 Fonti d'informazione accessibili al pubblico

I servizi informazioni reperiscono molte informazioni nella sfera pubblica. Procedendo in questo modo, possono limitarsi a ricorrere a specifici strumenti di intelligence per colmare in maniera mirata le lacune residue oppure per confermare o smentire informazioni pubblicamente accessibili.

Questa forma di acquisizione rappresenta la forma più lieve di ingerenza nei diritti fondamentali, poiché sfrutta informazioni pubbliche, vale a dire praticamente a disposizione di chiunque. Il carattere pubblico di queste informazioni non cambia neppure se si tratta di informazioni offerte, soprattutto da privati, soltanto a pagamento. In questo contesto, le collezioni di dati elettroniche accessibili dietro pagamento non devono essere considerate diversamente dai media tradizionali, quali i giornali o le pubblicazioni specializzate, che di norma vengono pure offerti a pagamento.

Rispetto all'avamprogetto posto in consultazione, le informazioni contenute nei registri pubblici delle autorità sono state spostate in questo articolo, poiché la loro acquisizione corrisponde più a un accesso a fonti d'informazione pubbliche che a un obbligo d'informazione dell'autorità che gestisce il registro.

La qualità delle informazioni accessibili al pubblico può essere molto variabile e di conseguenza è importante valutarle al momento della loro utilizzazione. Il disegno prevede pertanto che le informazioni provenienti da fonti pubbliche siano messe a disposizione all'interno del SIC in un apposito sistema d'informazione (art. 53). In seguito, se necessario, possono essere valutate e trasferite in ulteriori sistemi in vista di una loro utilizzazione per prodotti di intelligence.

Art. 14 Osservazioni in luoghi pubblici e liberamente accessibili

Il *capoverso 1* corrisponde sostanzialmente alla vigente normativa prevista dall'articolo 14 capoverso 2 lettera f LMSI. L'osservazione e la registrazione di fatti che avvengono in luoghi pubblici e liberamente accessibili fanno parte dei compiti standard di ogni servizio informazioni. Gli incontri tra gestori (case officer) appartenenti a servizi informazioni esteri e i loro agenti avvengono spesso in luoghi pubblici e liberamente accessibili, ad esempio in una stazione ferroviaria, un aeroporto o in altri spazi pubblici. I luoghi pubblici e liberamente accessibili comprendono anche i corrispondenti spazi di ristoranti e alberghi.

Esempio pratico: un agente straniero di stanza a Ginevra che aveva assunto l'identità fittizia di diplomatico andava spesso a prendere con la propria autovettura il suo informatore nel centro città. L'agente cercava in tal modo di far credere di essere un normale diplomatico.

Per documentare questo tipo di incontri è indispensabile osservare i luoghi pubblici e liberamente accessibili, anche con l'ausilio di registrazioni audiovisive.

L'articolo 14 disciplina più in dettaglio il campo dell'elaborazione di immagini (Imagery Intelligence,IMINT). Per adempiere i compiti legali, in taluni casi può essere necessario impiegare mezzi aerei adeguati quali velivoli, elicotteri o aeromobili senza pilota, ossia aeromobili telecomandati dal suolo. Anche mezzi spaziali come i satelliti posso essere strumenti adeguati per acquisire immagini (per es. in occasione di rapimenti di cittadini svizzeri all'estero). L'osservazione mediante immagini satellitari consente per esempio di sorvegliare adeguatamente i progressi nella realizzazione di impianti per programmi esteri riguardanti armi di distruzione di massa. Il SIC non dispone di mezzi propri di questo genere, ma per il loro impiego può far capo a terzi. Il Servizio informazioni militare svizzero dispone di un Centro IMINT in grado di acquisire e interpretare questo tipo di informazioni. Le immagini satellitari provengono soprattutto da operatori commerciali, poiché anche in questo ambito la Svizzera non dispone di mezzi propri.

Una valutazione indipendente e autonoma dei fatti rilevanti in materia di politica di sicurezza non può prescindere da questo tipo di osservazioni. Le valutazioni del SIC servono direttamente da base per la politica estera svizzera, consentendo ad esempio di elaborare previsioni sul tempo che ancora rimane per negoziare con uno Stato proliferatore.

Si considera che fatti in corso al suolo non avvengono in luoghi pubblici se si svolgono ad esempio all'interno di un'abitazione privata o su terreno privato. Se è necessario osservare simili fatti, per l'acquisizione di informazioni il SIC deve proporre una misura soggetta ad autorizzazione secondo gli articoli 25 e seguenti. Se non è stato possibile evitare l'osservazione di uno spazio privato (per es. mediante provvedimenti di carattere tecnico o una limitazione della risoluzione che non consenta di riconoscere i dettagli attribuibili alla sfera privata), i dati raccolti devono essere distrutti. Questa situazione può essere paragonata a un aereo passeggeri che sorvola una zona abitata: anche in questo caso non si può impedire che i passeggeri guardino dal finestrino e osservino o fotografino gli eventi che si svolgono al suolo in aree private. Tuttavia, l'utilizzazione di simili immagini sarebbe legalmente impugnabile.

Con questo chiaro riferimento alla protezione della sfera privata, il nostro Collegio ritiene che la tutela dei diritti fondamentali sia sufficientemente garantita. Contemporaneamente, al SIC non è vietato l'accesso a mezzi di osservazione che, in seguito al progresso tecnico, sono diventati in parte beni di dominio pubblico.

Nella legge militare del 3 febbraio 1995[18] (LM) è integrata una disposizione analoga per l'ambito militare (art. 99 cpv. 1^{quater}, cfr. modifica di altri atti normativi).

18 RS **510.10**

Art. 15 Fonti umane

La definizione delle «fonti umane» di cui al *capoverso* 1 si ispira a quella di «informatore» data nell'articolo 14*a* LMSI, la quale, tuttavia, si riferisce piuttosto al settore della polizia. L'espressione scelta nel disegno è pertanto più adatta al gergo del servizio informazioni unificato.

Il termine «fonte umana» (in inglese *human intelligence, HUMINT)*, è un termine consacrato sul piano internazionale nel gergo dei servizi informazioni per designare le persone che hanno accesso a titolo esclusivo a informazioni specifiche e sono disposte a fornire al SIC tali informazioni. La legge belga del 4 febbraio 2010 sui metodi di acquisizione di dati da parte dei servizi informazioni e dei servizi di sicurezza, ad esempio, impiega anch'essa il termine corrispondente a «fonti umane» («sources humaines»,«menselijke bronnen»).

Si tratta di persone che per motivi propri o su richiesta del SIC sono disposte a fornire informazioni a quest'ultimo.

Se per esempio un gruppo terroristico basato in Svizzera o all'estero progetta attentati terroristici in Svizzera o contro cittadini o interessi svizzeri all'estero, le relative informazioni spesso possono essere acquisite soltanto attraverso persone che hanno contatti diretti o indiretti con questo gruppo. Frequentemente, per motivi di sicurezza questi gruppi non redigono né scambiano scritti sui loro piani e sulle loro attività, ma ne discutono soltanto a voce in una ristretta cerchia all'interno del gruppo.

Le fonti umane, e in particolare le fonti umane all'estero, possono talvolta fornire informazioni al SIC anche a loro insaputa. Il fatto che ignorino di agire come informatori può servire a proteggere queste fonti.

Le indennità ai sensi del *capoverso 2* possono consistere nella rifusione di esborsi che vengono rimborsati a titolo di spese previo accordo o nel pagamento di informazioni di grande utilità per l'adempimento dei compiti del SIC. In particolare le fonti all'estero richiedono facilmente denaro per le informazioni in loro possesso. Se viene scoperto, il pagamento di fonti umane può costituire un grave rischio, tanto nel Paese d'origine quanto negli ambienti di cui esse fanno parte. Il sospetto di introiti provenienti da rapporti con servizi informazioni e da attività informative può danneggiare una fonte sul piano professionale, rovinare la sua reputazione e, a dipendenza del Paese e dell'ambiente di cui fa parte, anche metterne in pericolo l'integrità fisica e la vita. Per questi motivi, nella maggior parte dei casi le indennità versate alle fonti non possono essere dichiarate e tassate né essere assoggettate ai relativi obblighi in materia di contributi sociali, altrimenti la sicurezza di molte fonti non potrebbe essere garantita e una collaborazione sarebbe impossibile. Soltanto in casi speciali è talvolta possibile ufficializzare i redditi per il tramite di strutture di copertura, per esempio qualora una fonte debba assicurarsi il proprio sostentamento quasi esclusivamente con le indennità del SIC e di conseguenza non dispone di alcuna altra sicurezza sociale sufficiente. In Svizzera simili casi costituirebbero comunque un'assoluta eccezione.

Capoversi 3–5

A causa delle informazioni di cui dispone e che trasmette al SIC, una fonte umana può rischiare in determinate circostanze la propria integrità fisica e la vita. Questo rischio incombe in particolare nell'ambito delle cellule terroristiche e dei gruppi di estremisti violenti provenienti dall'estero, ma anche negli ambiti in cui operano organizzazioni statali e servizi informazioni. Le fonti estere che operano per il SIC

possono essere in grave pericolo nei loro Paesi d'origine. Nel caso estremo, lo smascheramento potrebbe addirittura significare una condanna a morte, per la fonte umana stessa o per i suoi familiari:

- gli scienziati nucleari di Paesi asiatici che forniscono informazioni a un servizio informazioni estero, nel loro Paese possono essere condannati a morte;
- durante i tumulti della «Primavera araba», il SIC ha appreso da diverse fonti che gli oppositori residenti in Svizzera venivano regolarmente spiati o vessati da persone fedeli al regime provenienti dal loro Paese d'origine. Se un'eventuale collaborazione con il SIC di fonti appartenenti agli ambienti dell'opposizione venisse alla luce, le fonti o i loro familiari nei Paesi d'origine potrebbero rischiare la vita o l'integrità fisica.

Il SIC ha l'obbligo di garantire nel migliore dei modi l'incolumità delle proprie fonti umane. Nella gestione delle fonti, veglia costantemente a garantire loro la massima protezione. Le misure atte a garantire tale protezione comprendono, in casi straordinari, la concessione di permessi di dimora in Svizzera a fonti umane e ai loro familiari, ma anche l'assegnazione di una copertura o di un'identità fittizia. Mentre è impiegata attivamente, una fonte umana può ottenere dal SIC un'identità fittizia ai sensi dell'articolo 18, se tale misura risulta necessaria per proteggerla.

Una fonte umana che abbia operato per il SIC può continuare a rischiare l'integrità fisica o la vita anche dopo aver terminato la sua attività. Anche in casi del genere la legge prevede la possibilità di assegnare una copertura o un'identità fittizia. In questi casi, tuttavia, non è più previsto un termine di verifica di 12 mesi come nell'impiego attivo; si tratta invece di una misura di lunga durata. Essa dura fintanto che perdura il rischio per la fonte umana ed eventualmente per i suoi familiari. Poiché in questi casi la fonte umana e il SIC di regola non mantengono più contatti tra loro, il disegno prevede che l'assegnazione di una copertura o di un'identità fittizia sia autorizzata dal capo del DDPS, affinché anche in questo caso possano essere ponderati i rischi politici.

Gli organi di vigilanza sulle attività informative (cfr. art. 74 segg.) hanno accesso a tutte le informazioni concernenti la gestione di fonti umane; già secondo la prassi in vigore ricevono ogni anno un rapporto esaustivo su tutte le operazioni di questo tipo e possono consultare liberamente i dossier che desiderano.

Art. 16 Segnalazioni per la ricerca di persone e oggetti

I *capoversi 1 e 2* introducono una regolamentazione analoga a quella definita nella prevista e non realizzata legge federale sui compiti della Confederazione in materia di polizia (titolo quarto, capitolo 3: Misure per prevenire possibili reati). A differenza della legge sui compiti di polizia, il presente disegno non è incentrato sulla prevenzione di possibili reati, bensì sull'acquisizione di informazioni per sventare minacce nei confronti della sicurezza interna o esterna della Svizzera e per salvaguardare interessi nazionali essenziali secondo l'articolo 3. Perciò, la segnalazione di persone e veicoli da parte del SIC presuppone l'esistenza di una minaccia per la sicurezza interna o esterna (cfr. cpv. 2 lett. a) oppure una decisione del Consiglio federale riguardante la salvaguardia di interessi essenziali della Svizzera (cfr. art. 3 in combinato disposto con l'art. 70). A tale riguardo, solo una delle condizioni del capoverso 2 dev'essere adempiuta.

La legge sancisce con ciò la possibilità, già esistente attualmente, di segnalare persone e veicoli nel sistema di ricerca informatizzato di polizia (RIPOL) per consentire al SIC di accertare il luogo in cui trovano determinati soggetti (per es. membri di gruppi sospettati di attività terroristiche) e i loro spostamenti. La legislazione in materia di polizia utilizza per questa misura l'espressione «segnalazione per sorveglianza discreta». Aggiuntivamente, in avvenire la segnalazione potrà essere effettuata anche nella parte nazionale del Sistema d'informazione Schengen (N-SIS). Se le persone segnalate dal SIC entrano nello spazio Schengen o lo abbandonano, oppure sono oggetto di un controllo di polizia all'interno dello spazio Schengen o di un controllo della polizia di frontiera, la Svizzera, ossia il SIC, riceverà in avvenire la relativa comunicazione da parte delle competenti autorità estere. L'informazione sarà trasmessa per il tramite dell'ufficio svizzero di SIRENE (servizio di collegamento tra le autorità competenti degli Stati Schengen per la collaborazione nell'ambito del Sistema d'informazione di Schengen; cfr. art. 8 e 9 dell'ordinanza N-SIS dell'8 marzo 2013[19]). Va da sé che la necessità o utilità di una segnalazione dovrà essere valutata caso per caso. In particolare, non è previsto alcun nesso automatico tra la segnalazione a livello nazionale e la segnalazione nello spazio Schengen.

L'eccezione prevista nel *capoverso 3* per la segnalazione nel RIPOL o nel N-SIS riguarda soltanto i veicoli di terzi che soggiacciono a segreti professionali e corrisponde anch'essa alla vigente prassi. Si tratta dei gruppi di persone alle quali è riconosciuta la facoltà di non deporre (per es. ecclesiastici, avvocati, detentori di segreti professionali e giornalisti).

Nei rispettivi ambiti d'interesse anche i Cantoni possono procedere a simili segnalazioni nel quadro della legislazione in materia di polizia.

Capitolo 3, sezione 2

Dal 1997 il Servizio informazioni strategico (SIS) aveva la facoltà, in virtù dell'articolo 99 della legge militare, di fornire identità fittizie ai membri dei suoi organi di ricerca (cfr. il rapporto annuale 2002/2003 delle Commissioni della gestione e della Delegazione delle Commissioni della gestione delle Camere federali del 23 gennaio 2004[20]). Dalla fusione del SAP e del SIS nella nuova unità organizzativa SIC, l'articolo 16 capoverso 1 lettera e O-SIC prevede ora espressamente l'impiego di «documenti fittizi e identità fittizie» in relazione con l'acquisizione di informazioni all'estero. Le identità fittizie e le relative coperture sono impiegate dal 1997 come misura di protezione permanente dai collaboratori che si occupano dell'acquisizione di informazioni all'estero. Tali identità sono approvate internamente dal SIC e la vigilanza è esercitata dal capo del DDPS, dalla Delegazione Sicurezza del Consiglio federale e dalla Delegazione delle Commissioni della gestione.

Grazie alla revisione della LMSI approvata dal Parlamento il 23 dicembre 2011, con l'articolo 14*c* è stata altresì introdotta quale principale novità la possibilità di utilizzare le identità fittizie e le relative coperture nell'ambito dell'acquisizione di informazioni in Svizzera. A differenza della procedura di approvazione interna al SIC applicabile alle identità fittizie per l'acquisizione di informazioni all'estero, l'assegnazione di un'identità fittizia a persone incaricate di compiti previsti dalla

19 RS **362.0**
20 FF **2004** 1504

LMSI deve essere richiesta al capo del DDPS. Inoltre, con l'articolo 14*c* capoverso 1 lettera c LMSI è stata introdotta la possibilità di dotare di un'identità fittizia anche le fonti umane del SIC nell'ambito di una determinata attività di acquisizione di informazioni.

Gli articoli 17 e 18 introducono la distinzione tra le nozioni di «copertura» e «identità fittizia», poiché si tratta di misure diverse che possono essere adottate l'una indipendentemente dall'altra. Per questo motivo la terminologia impiegata differisce da quella del CPP.

Nel presente disegno le varie norme sinora applicabili all'autorizzazione delle identità fittizie vengono raggruppate ed estese tanto all'acquisizione di informazioni all'estero quanto all'acquisizione in Svizzera. Le nuove norme tengono ora conto del carattere di protezione permanente di queste identità. In considerazione delle nuove norme introdotte nella LMSI, il Consiglio federale propone di attribuire al capo del DDPS la competenza per l'autorizzazione di identità fittizie tanto per gli impieghi all'estero quanto per quelli in Svizzera.

L'autorizzazione di mere coperture, tuttavia, dovrebbe rimanere di competenza del direttore del SIC, dal momento che questo tipo di misura non comporta la necessità di produrre documenti d'identità fittizi con nomi falsi e non consente nemmeno di concludere negozi giuridici sotto falso nome.

Art. 17 Coperture

La copertura serve a celare l'appartenenza di una persona al SIC. Ad esempio, si può fingere che l'interessato dipenda da un altro datore di lavoro e non dal SIC e che svolga un'attività professionale diversa da quella di collaboratore del servizio informazioni. Le persone che vengono dotate di una copertura mantengono però il loro vero nome e gli altri dati anagrafici (data di nascita, luogo di nascita ecc.). Disporre di una copertura può essere indispensabile già solo per permettere un'attività di intelligence altrimenti impossibile, ad esempio se le persone sulle quali occorre acquisire informazioni o l'ambiente di cui fanno parte non vorrebbero mai avere a che fare con il SIC o se un legame evidente tra l'agente incaricato di acquisire informazioni e il SIC comporterebbe dei rischi (per es. se in un determinato Stato l'attività è considerata spionaggio e sarebbe severamente perseguita).

È impossibile per un collaboratore del servizio informazioni recarsi all'estero per un'operazione di acquisizione segreta e al tempo stesso essere chiaramente identificabile come agente di un servizio informazioni. In tal caso, i collaboratori e le fonti con le quali sono in contatto potrebbero essere smascherati e quindi essere esposti a rischi. I collaboratori del SIC e le loro fonti, in particolare nell'ambito del terrorismo o dello spionaggio, possono essere in pericolo anche in Svizzera se viene scoperto un nesso con il SIC.

In seguito ai progressi della biometria diventa sempre più difficile recarsi all'estero sotto una falsa identità. Pertanto, per continuare a garantire lo svolgimento di attività informative all'estero è necessario fare in modo che sia possibile il ricorso a una copertura della vera identità.

L'allestimento di coperture è spesso una misura di protezione a lungo termine e in genere non è connessa a singole operazioni. In funzione del bisogno di protezione, la copertura può essere necessaria per un periodo breve (per es. tessere telefoniche prepagate e biglietti da visita fittizi) o più prolungato (per es. invenzione/creazione

di un datore di lavoro fittizio, assegnazione di un recapito verificabile con telefono, e-mail ecc.). Per documenti s'intendono scritti destinati e atti a provare un fatto di portata giuridica nonché supporti d'immagini o di dati equiparati a detti scritti (cfr. art. 110 cpv. 4 CP). L'impiego di coperture corrisponde alla prassi sinora adottata nell'ambito dell'acquisizione di informazioni all'estero, fondata sull'articolo 16 capoverso 1 lettera e O-SIC. Con il presente articolo questa prassi poggerà su una base legale chiara. Se l'allestimento di coperture richiede il concorso delle autorità svizzere, deve essere imposto loro l'obbligo di collaborare. Il loro concorso può ad esempio rivelarsi necessario quando per rendere credibile una copertura occorrono documenti ufficiali (per es. per rendere credibile un'attività commerciale).

Conformemente a quanto auspicato dai Cantoni durante la procedura di consultazione, il nuovo *capoverso 2* precisa che il SIC non è autorizzato a dotare di una copertura collaboratori di autorità d'esecuzione cantonali senza previa intesa con gli organi cantonali preposti.

Si considera che non vi è ricorso a documenti se l'appartenenza al SIC è semplicemente taciuta o dissimulata mediante indicazioni generiche, ma veritiere (per es. «impiegato della Confederazione», «collaboratore del DDPS», «giurista»). Il *capoverso 5* precisa che a tal fine non è necessaria un'autorizzazione del direttore del SIC.

L'obbligo di rendere conto annualmente alla direzione del Dipartimento garantisce una vigilanza costante.

Art. 18 Identità fittizie

Un'identità fittizia conferisce a una persona un'altra identità, vale a dire un altro nome ed eventualmente altri dati anagrafici (data di nascita, luogo di nascita ecc.). Perciò soggiace a condizioni notevolmente più severe rispetto alla semplice copertura. Come la copertura, l'identità fittizia può comportare il mascheramento del nesso con il SIC, rispettivamente l'indicazione di un datore di lavoro diverso dal SIC. Se si tratta invece unicamente di proteggere il collaboratore come persona, e non della sua attività a favore del SIC, gli può essere conferita anche un'identità fittizia senza una differente storia di copertura.

Per adempiere i propri compiti e in particolare proteggere i propri collaboratori quando acquisiscono informazioni all'estero e in determinati ambienti in Svizzera, i servizi informazioni sono costretti a servirsi di identità fittizie e delle relative coperture. Indizi sulla vera identità del collaboratore che si occupa dell'acquisizione di informazioni, per esempio nell'ambito del terrorismo o dello spionaggio all'estero o in Svizzera, possono esporre tale collaboratore e i suoi familiari a tentativi di pressione, a intimidazioni e persino a minacce concrete per l'incolumità fisica. Pertanto, le identità fittizie costituiscono in primo luogo una misura di protezione permanente per i collaboratori incaricati dell'acquisizione di informazioni.

Oltre a servire da protezione, a seconda dei casi le identità fittizie possono essere necessarie segnatamente per poter instaurare e mantenere contatti con determinate persone o strutture ai fini dell'acquisizione di informazioni. Nell'ambito del terrorismo o dello spionaggio o di un'acquisizione di informazioni all'estero, per esempio, qualunque nesso tra un collaboratore e il SIC può rendere impossibile ogni tentativo di acquisizione di informazioni.

Per predisporre un'identità fittizia occorre una lunga preparazione, per cui raramente una simile identità può essere assunta soltanto con l'avvio di un caso specifico. Anzi, a dipendenza del grado di intensità del mascheramento, per fare in modo che un'identità fittizia raggiunga il necessario livello di credibilità possono occorrere anni di preparativi e di perfezionamenti.

Il *capoverso 1* pone le basi per dotare le persone di un'identità fittizia a garanzia della loro sicurezza e allo scopo di acquisire informazioni. Esso elenca in modo esaustivo la cerchia di persone a cui possono essere fornite identità fittizie.

Poiché l'allestimento di identità fittizie richiede tempi lunghi e rappresenta una misura di protezione permanente, il loro conferimento ai collaboratori incaricati dell'acquisizione di informazioni costituisce un compito fondamentale del servizio; siccome comporta il ricorso a documenti d'identità fittizi, sottostà inoltre all'autorizzazione del capo del DDPS. La vigilanza in materia è garantita mediante l'approvazione a livello di Dipartimento. Anche in questo ambito la Delegazione delle Commissioni della gestione ha accesso a tutte le informazioni e a tutti gli atti di cui necessita (cfr. art. 77).

L'utilizzazione delle identità fittizie è limitata nel tempo e, se necessario, può essere prorogata (cfr. cpv. 2). Essa soggiace a criteri precisi che, in virtù del capoverso 3, devono essere rispettati in ogni caso.

La creazione di un'identità fittizia è connessa al diritto di servirsene per concludere negozi giuridici e, in particolare, per costituire strutture fittizie, che occultano il legame esistente con il SIC. A differenza della creazione di coperture della reale identità (art. 17), le esigenze riguardanti le identità fittizie e il loro allestimento sono spesso più complesse, poiché si tratta di creare e rendere credibile un'altra identità (fittizia), l'esistenza di un datore di lavoro, di un domicilio ecc. Le persone provviste di un'identità fittizia hanno piena personalità giuridica e possono stipulare contratti (per es. affittare locali e noleggiare veicoli o collegamenti di telecomunicazione, costituire strutture fittizie quali ditte o altre persone giuridiche come base per un'identità fittizia e la relativa storia).

Secondo il *capoverso 2*, l'utilizzazione di identità fittizie è limitata nel tempo e deve essere riesaminata dopo un determinato periodo. In tal modo si può garantire che le identità fittizie siano utilizzate soltanto fintanto che sono necessarie alla protezione dei collaboratori e delle loro fonti. Non è invece ragionevole fissare una scadenza in termini assoluti. Un gestore (case officer), ad esempio, deve presentarsi alle sue fonti sempre con la medesima identità. Perciò questa non deve venir meno allo scadere di una durata massima: la sua durata deve al contrario poter essere adeguata in funzione delle esigenze di servizio.

Per garantire la necessaria flessibilità e migliorare il controllo sui rischi inerenti alla loro utilizzazione da parte delle fonti umane, le identità fittizie loro attribuite sono limitate a dodici mesi.

Il *capoverso 3* fissa i criteri per l'utilizzazione di identità fittizie per l'acquisizione di informazioni facendo riferimento ai principi di proporzionalità e sussidiarietà.

Il *capoverso 4* consente l'allestimento dei documenti d'identità e di ulteriori documenti: al riguardo il SIC deve poter contare sul concorso delle competenti autorità, le quali sono tenute a collaborare. Lo scopo principale di un'identità fittizia è la protezione di persone esposte a particolare pericolo conferendo loro un'altra identità per la durata di tale pericolo. In questo contesto, soltanto a titolo eccezionale e con

estrema prudenza documenti d'identità svizzeri saranno messi a disposizione di cittadini stranieri. In simili casi, il rilascio temporaneo di documenti svizzeri non implica evidentemente alcuna concessione permanente della cittadinanza svizzera.

Art. 19 Obbligo d'informazione in caso di minaccia concreta

Dati i compiti che gli sono assegnati, il SIC deve potersi basare su informazioni che gli possono essere fornite da altre autorità (autorità della Confederazione e dei Cantoni, organizzazioni incaricate di compiti pubblici). Tali organizzazioni e servizi possono comunicare informazioni sulla base di una richiesta del SIC, oppure spontaneamente, quando constatano una minaccia concreta.

In caso di gravi minacce per la sicurezza interna o esterna, gli interessi della comunità statale alla comunicazione delle informazioni prevale di principio sul diritto dei cittadini interessati alla tutela della sfera privata. L'idea di fondo è che, di fronte a una concreta minaccia per la sicurezza della Svizzera e dei suoi cittadini, gli enti pubblici (Confederazione, Cantoni, Comuni) hanno l'obbligo di contribuire solidalmente alla difesa.

I *capoversi 1 e 2* stabiliscono obblighi d'informazione per determinate forme di minaccia che rischiano di ledere beni giuridici importanti. Le varie fonti di minaccia sono enumerate esaustivamente nel capoverso 2. Si tratta di attività terroristiche, di attività di spionaggio politico, economico o militare, della proliferazione, di attacchi a infrastrutture critiche e dell'estremismo violento. Questa disposizione impone di norma un obbligo d'informazione basato sui principi dell'assistenza amministrativa per tutte le autorità e le unità amministrative della Confederazione e dei Cantoni. In tale contesto, come prevede il diritto vigente, la motivazione nei confronti degli organi consultati non deve essere particolarmente dettagliata né avere alcun carattere di prova. L'organo consultato dev'essere informato unicamente del campo d'attività del SIC al quale si riferisce l'informazione richiesta.

Il *capoverso 2* precisa in certo qual modo gli ambiti di compiti del SIC menzionati nell'articolo 6; non dà una definizione legale di termini quali «terrorismo», ma descrive le minacce in modo analogo al vigente articolo 13*a* LMSI.

Se l'obbligo d'informazione è motivato dalla salvaguardia di interessi essenziali della Svizzera secondo l'articolo 3, esso necessita di una corrispondente decisione del Consiglio federale (cfr. al riguardo il commento agli art. 3 e 70).

L'articolo corrisponde ampiamente al nuovo articolo 13*a* LMSI introdotto nel quadro della LMSI II. Le relative formulazioni sono state trasposte nella prassi in materia di politica di sicurezza del servizio informazioni, motivo per il quale non è stato fatto ricorso ad altre descrizioni, come ad esempio quella di cui all'articolo 260^{quinquies} CP per il perseguimento penale in caso di finanziamento del terrorismo.

Le autorità fiscali, che nella LMSI sono ancora elencate specificamente tra le autorità soggette all'obbligo d'informazione, nel presente disegno non sono più menzionate esplicitamente. Infatti esse sottostanno a detto obbligo, poiché sono comprese tra le autorità di cui al capoverso 1. Una menzione specifica susciterebbe l'errata impressione che le autorità fiscali forniscono particolarmente spesso informazioni al SIC, ciò che non corrisponde al vero. Per rispondere alle incertezze emerse in occasione della consultazione, si conferma che, in relazione alla presente disposizione, le banche cantonali non possono essere considerate organi del Cantone. Le banche

cantonali potranno quindi continuare a far valere il segreto bancario nei confronti del SIC.

Le autorità cantonali tenute a informare comprendono anche le autorità comunali; esse sono incluse nel termine «Cantone».

Le organizzazioni che esercitano funzioni pubbliche sono, a loro volta, tenute a fornire informazioni. Si tratta delle organizzazioni e delle persone di diritto pubblico o privato, esterne all'Amministrazione federale, cui sono attribuiti compiti amministrativi ai sensi all'articolo 2 capoverso 4 LOGA.

L'espressione «nel singolo caso» serve a chiarire che le autorità e organizzazioni cui l'obbligo si riferisce, pur essendo costantemente assoggettate all'obbligo d'informazione, sono tenute a informare soltanto in riferimento a determinati casi concreti e soltanto sulla base di una domanda da parte del SIC (o delle autorità d'esecuzione cantonali che agissero per incarico del SIC). Il fatto che l'obbligo d'informazione sussista soltanto per il singolo caso e in riferimento a minacce concrete giustifica la relativa estensione della cerchia dei destinatari.

Secondo l'articolo 81 capoverso 1, le autorità di sicurezza cantonali, invocando il presente articolo, possono acquisire anche autonomamente informazioni per l'esecuzione della LAIn. Dopo la trasmissione delle relative informazioni alla Confederazione, i dati acquisiti in tal modo diventano dati federali.

Il *capoverso 4* disciplina i casi in cui altre autorità constatano autonomamente l'esistenza di una minaccia per la sicurezza interna o esterna. Queste devono avere in tal caso la possibilità di segnalare i fatti al SIC. A questa disposizione corrisponde, qualora si sospettino fatti penalmente rilevanti, l'articolo 22*a* della legge federale del 24 marzo 2000[21] sul personale federale, in virtù del quale gli impiegati della Confederazione sono tenuti a denunciare qualsiasi sospetto di reato perseguibile d'ufficio.

Art. 20 Obbligo speciale d'informazione e di comunicazione

Il *capoverso 1* elenca le autorità e i servizi le cui attribuzioni si trovano in un rapporto particolarmente stretto con l'esecuzione di compiti in materia di sicurezza e sono quindi tenute a fornire informazioni. L'obbligo d'informazione ai sensi del capoverso 1 è più esteso rispetto all'obbligo previsto dall'articolo 19 (obbligo d'informazione generale): non è limitato a singoli ambiti tematici né è vincolato a particolari condizioni e serve all'esecuzione della legge in quanto tale. Per questa ragione, contrariamente all'obbligo previsto dall'articolo 19, è circoscritto a determinate autorità. Il nostro Collegio considera inutile e sproporzionata un'estensione ai servizi sociali e alle autorità fiscali, come proposto da taluni partecipanti alla procedura di consultazione.

L'obbligo secondo la disposizione del capoverso 1 non è inteso come obbligo integrale d'informazione, bensì come obbligo riferito a casi e organizzazioni concreti.

Gli obblighi d'informazione si riferiscono di volta in volta ai compiti specifici delle autorità menzionate. Segnatamente in relazione alla lettera i, questo significa che le autorità competenti per l'esercizio di sistemi informatici sono tenute soltanto a informare in merito all'esercizio tecnico dei sistemi, ma non ai contenuti, per esem-

21 RS **172.220.1**

pio ai contenuti delle banche dati gestite. Questa lettera intende coprire anche il settore della cyber-sicurezza e della protezione delle infrastrutture critiche.

Il *capoverso 3* disciplina nuovamente i casi in cui altre autorità constatano autonomamente l'esistenza di una minaccia per la sicurezza interna o esterna.

Il *capoverso 4* corrisponde alla vigente normativa prevista dall'articolo 11 capoverso 2 lettera a LMSI. Gli obblighi di comunicazione sono in gran parte elencati nell'allegato 1 dell'O-SIC. Fatti e constatazioni che devono essere comunicati spontaneamente al SIC, ma che per motivi inerenti alla tutela del segreto non possono essere pubblicati, saranno come sinora stabiliti in un elenco confidenziale. Gli organi ufficiali interessati sono informati individualmente in merito agli obblighi di comunicazione cui soggiacciono e la Delegazione delle Commissioni della gestione ha accesso a tutte le informazioni necessarie alla vigilanza in materia.

Art. 21 Procedura in caso di divergenze d'opinione in merito agli obblighi d'informazione e di comunicazione

Il *capoverso 1* disciplina la procedura per il trattamento di divergenze d'opinione all'interno dell'Amministrazione federale. In caso di divergenze la decisione spetta all'autorità di vigilanza comune, ossia al capo del DDPS in caso di divergenze all'interno del DDPS e al Consiglio federale in caso di divergenze con uffici di altri dipartimenti. Ciò corrisponde al disciplinamento generale previsto per l'organizzazione dell'amministrazione.

Il *capoverso 2* disciplina la procedura per il trattamento di divergenze d'opinione tra Confederazione e Cantoni. In tal caso la decisione spetta al Tribunale amministrativo federale.

Art. 22 Comunicazioni e informazioni fornite da terzi

L'assunzione di informazioni da parte del SIC o delle autorità d'esecuzione cantonali presso i privati interessati avviene su base volontaria. Tuttavia, se è stata autorizzata l'utilizzazione di una copertura per celare l'appartenenza al servizio informazioni non è possibile rendere attenta la persona interrogata in merito al fatto che è libera di fornire informazioni o di rifiutare di farlo, poiché altrimenti occorrerebbe svelare la copertura. Se soggiace al segreto professionale o a un altro obbligo di riservatezza previsto dalla legge, la persona che invia una comunicazione o fornisce informazioni deve rispettare tale obbligo anche nei confronti del SIC o delle autorità d'esecuzione cantonali così come nei confronti di qualsiasi altra persona o altro organo ufficiale.

Il *capoverso 3* si applica soltanto se è impiegata una copertura, poiché l'impiego di identità fittizie non è necessariamente connesso a un occultamento dell'appartenenza al SIC, in special modo in caso di acquisizione di informazioni in Svizzera.

Art. 23 Identificazione e audizione di persone

Il presente articolo è stato introdotto soltanto dopo la procedura di consultazione allo scopo di eliminare una discrepanza rispetto alla LMSI vigente, che consente al SIC di accertare l'identità e il luogo di soggiorno di persone. La nuova regolamentazione è stata formulata rifacendosi all'articolo 215 CPP, che disciplina il fermo di polizia nell'interesse del chiarimento di un reato. Le leggi di polizia dei Cantoni contem-

plano di regola disposizioni comparabili per l'adempimento di compiti in materia di sicurezza.

Nel caso disciplinato nel presente articolo, il fermo e l'identificazione servono per adempiere in Svizzera compiti in materia di servizio informazioni nei classici ambiti di compiti dell'antiterrorismo, dello spionaggio, dell'estremismo violento, della proliferazione e degli attacchi alle infrastrutture critiche. Il fermo e l'audizione possono durare soltanto il tempo necessario per raggiungere l'obiettivo prefissato.

Come nel Codice di procedura penale, non è opportuno stabilire una durata massima, poiché la durata varia fortemente in funzione delle circostanze concrete e deve essere proporzionale a queste ultime. Un semplice controllo di persone può durare soltanto qualche minuto, mentre un'audizione, a dipendenza delle circostanze, può durare fino a qualche ora se occorre ad esempio reperire un luogo protetto per il suo svolgimento. La durata complessiva, per analogia alla distinzione tra fermo e arresto di polizia secondo il CPP (art. 215 segg.) deve essere inferiore alle tre ore.

L'audizione ha luogo secondo l'articolo 22. La persona interrogata è di conseguenza libera di rispondere alle domande o di rifiutarsi.

Art. 24 Obbligo speciale d'informazione dei privati

Il *capoverso 1* riprende l'obbligo d'informazione dei trasportatori commerciali introdotto nel 2012 nella LMSI con il nuovo articolo 13*c* e lo estende ai gestori privati di infrastrutture di sicurezza, in particolare di sistemi di videosorveglianza. Analoghe importanti informazioni possono essere fornite anche da sistemi elettronici di controllo degli accessi. Come già previsto per la disposizione introdotta nella LMSI, questa disposizione non obbliga nessuno a registrare o a conservare determinati dati. Essa è unicamente intesa a garantire, in presenza di una minaccia concreta, l'accesso a dati comunque disponibili.

Questo tipo di informazioni potrebbe assumere importanza ad esempio per accertare gli spostamenti di soggetti coinvolti negli ambiti del terrorismo, dell'estremismo violento, dello spionaggio e della proliferazione. L'obbligo d'informazione potrebbe ad esempio riguardare compagnie aeree, agenzie di viaggi e imprese di autonoleggio. Per quanto concerne i «gestori privati di infrastrutture di sicurezza», si tratterà soprattutto di aziende che proteggono infrastrutture proprie o di terzi, ad esempio nell'ambito della circolazione e dei trasporti, nel settore energetico o in campo commerciale.

Il *capoverso 2* richiama la possibilità, già prevista in virtù della LSCPT, di procurarsi, per il tramite del Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni del DFGP, informazioni sui collegamenti di telecomunicazione di una persona e su altri elementi d'indirizzo ad essa assegnati, rispettivamente sull'identità della persona alla quale sono assegnati determinati elementi d'indirizzo (per es. numeri di telefono). Anche l'articolo 14 capoverso 2bis LSCPT sarà adeguato di conseguenza[22]. Si tratta di informazioni che non sottostanno al segreto delle telecomunicazioni.

22 Nel disegno di revisione totale della LSCPT (FF **2013** 2383; messaggio: FF **2013** 2283), la corrispondente disposizione si trova nell'art. 15.

In caso di necessità, l'obbligo d'informazione dei privati è imposto per mezzo della procedura amministrativa federale mediante una decisione impugnabile, se del caso con la comminatoria dell'articolo 292 CP (Disobbedienza a decisioni dell'autorità). Sottoporre la domanda d'informazione a un'autorizzazione giudiziaria preliminare sarebbe pertanto sproporzionato.

Le decisioni del SIC possono essere impugnate mediante ricorso in virtù dell'articolo 79. L'acquisizione di informazioni, ad esempio su persone sospettate di svolgere attività terroristiche ai danni della Svizzera, avviene spesso nell'urgenza. Se si dovesse attendere l'esito di una procedura di ricorso, l'informazione fornita retroattivamente da un'impresa di trasporto, ad esempio, potrebbe rivelarsi inutile. Di conseguenza, la legge stabilisce che il ricorso non ha effetto sospensivo (art. 79 cpv. 3).

Capitolo 3, sezione 4

Per poter svolgere i propri compiti, in particolare per poter identificare e valutare tempestivamente minacce e pericoli che rischiano di limitare la capacità di decidere e di agire delle autorità svizzere o di pregiudicare i fondamenti democratici e le strutture dello Stato, il SIC deve poter ricorrere a mezzi efficaci per l'acquisizione delle necessarie informazioni.

Gli organi informativi della Confederazione e dei Cantoni si trovano confrontati con avversari sempre più brutali e spietati, specialmente nel campo del terrorismo. Ad esempio, tra l'11 e il 19 marzo 2012, a Tolosa e Montauban, città del sud della Francia, sette persone sono state uccise a colpi di pistola sulla pubblica via; tra le vittime vi erano anche bambini. L'autore è un Francese di origine algerina che ha affermato di appartenere al movimento terroristico Al-Qaida. Egli era già noto alle autorità francesi per aver intrapreso viaggi in Afghanistan e in Pakistan e intratteneva contatti con un movimento radicale salafita attivo in Francia.

Al SIC sono note diverse persone che hanno legami con la Svizzera e che presentano paralleli per quanto riguarda la radicalizzazione così come descritta nel caso di Tolosa e Montauban. La radicalizzazione di queste persone è avvenuta tramite Internet ed esse hanno soggiornato in campi di addestramento terroristici all'estero. Proprio gli individui radicalizzati come l'autore degli omicidi di Tolosa e Montauban conducono una vita apparentemente ordinaria e sembrano ben integrati nella società. Spesso non rivelano le loro reali intenzioni nemmeno alle persone a loro più vicine. Di conseguenza, le autorità non ricevono in pratica alcuna segnalazione dalla popolazione. Per poter acquisire con il debito anticipo informazioni su queste persone, le autorità dipendono sempre più dall'impiego di misure di acquisizione particolari, come quelle proposte nella presente legge. Benché la Svizzera non sia attualmente un bersaglio del terrorismo internazionale, nessuno può escludere che possa divenirlo in avvenire.

Anche negli altri settori di compiti del SIC, la controparte opera spesso in modo cospirativo, sia nell'ambito dello spionaggio sia nell'ambito della proliferazione o degli attacchi a infrastrutture critiche. Acquisendo informazioni principalmente in luoghi pubblici risulta molto difficile raccogliere indicazioni su attività e intenzioni.

Secondo il nostro giudizio, con i mezzi di acquisizione attualmente a disposizione, che si riducono sostanzialmente all'acquisizione di informazioni da fonti accessibili al pubblico, alla richiesta e ricezione di informazioni e all'osservazione di fatti in

luoghi pubblici (art. 14 LMSI), il SIC può adempiere il proprio compito soltanto in misura oltremodo limitata. Molti fatti rilevanti per la valutazione delle minacce non avvengono in luoghi pubblici. Rilevare atteggiamenti cospirativi in Internet, che è pubblicamente accessibile, è praticamente impossibile. Se si vuole che il SIC possa adempiere in modo efficiente il proprio ruolo di organo di sicurezza preventivo della Confederazione e svolgere i compiti previsti dalla legge, deve avere la possibilità di impiegare in casi particolari mezzi di acquisizione supplementari e più efficaci.

Nell'attuale situazione di minaccia, stimiamo che possano entrare in considerazione misure di acquisizione soggette ad autorizzazione in una decina di casi l'anno, benché si possa ipotizzare anche l'adozione di più misure per un singolo caso (per es. sorveglianza di vari collegamenti di telecomunicazione, localizzazione di un veicolo e perquisizione della camera d'albergo di una medesima persona). Si tratta di casi che presentano un potenziale di minaccia particolarmente elevato nei campi del terrorismo, dello spionaggio, della proliferazione e degli attacchi a infrastrutture critiche oppure della tutela di interessi nazionali essenziali secondo l'articolo 3: in simili casi le altre misure d'acquisizione non sarebbero sufficienti per ottenere informazioni di base per la salvaguardia della sicurezza della Svizzera.

Le misure soggette ad autorizzazione comprendono in particolare (art. 25):

- la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni secondo la LSCPT[23];
- l'individuazione del luogo in cui si trovano persone o oggetti mediante localizzazione dei telefoni cellulari utilizzati dagli interessati (conformemente alla LSCPT) o per mezzo di particolari dispositivi di localizzazione (in genere ricevitori GPS con o senza trasmettitore);
- l'impiego di apparecchi di sorveglianza per captare conversazioni e osservare fatti in luoghi privati;
- l'introduzione in sistemi e reti informatici per acquisire informazioni ivi disponibili o trasmesse da questi sistemi o reti , oppure per perturbare, impedire o rallentare l'accesso a informazioni, se da questi sistemi vengono sferrati attacchi a infrastrutture critiche;
- le perquisizioni di locali, veicoli o contenitori portati con sé da persone per acquisire gli oggetti ivi disponibili o le informazioni trasmesse da questi luoghi. La perquisizione può essere eseguita in segreto e all'insaputa delle persone aventi diritto per quanto riguarda i locali, i veicoli o i contenitori.

Prima che possano essere applicate dal SIC, queste misure devono essere autorizzate dal Tribunale amministrativo federale, mentre il capo del DDPS, dopo aver consultato la Delegazione Sicurezza, deve aver rilasciato il nullaosta. Se vi è pericolo nel ritardo, il direttore del SIC può ordinare in via eccezionale l'impiego immediato di una misura. La domanda di autorizzazione deve essere inoltrata al Tribunale amministrativo federale entro 24 ore (art. 30 cpv. 2).

Occorre sottolineare che queste misure di acquisizione riguardano soltanto casi che comportano una minaccia rilevante in materia di politica di sicurezza e che non sono oggetto di indagini penali. Se la minaccia è connessa a sospetti di reato, le autorità di perseguimento penale devono esserne informate (cfr. art. 59). Un eventuale proce-

23 Un disegno di revisione totale della LSCPT è attualmente in discussione in Parlamento; cfr. anche i commenti al n. 14 della modifica di altri atti normativi.

dimento penale e le misure di sorveglianza ordinate nell'ambito di tale procedimento hanno la precedenza sulle misure di acquisizione ai sensi della LAIn. Tuttavia, non tutte le minacce rilevanti in materia politica di sicurezza hanno anche una rilevanza penale e i sospetti esistenti spesso non bastano ancora per avviare indagini penali.

La legge intende autorizzare queste misure incisive soltanto in casi importanti nei quali la sicurezza della Svizzera è minacciata. Al riguardo, definisce condizioni rigorose e una procedura di autorizzazione a più livelli.

Come per tutti i settori d'esecuzione della LAIn, la Delegazione delle Commissioni della gestione delle Camere federali ha accesso integrale a tutti i dati e i documenti necessari per la sua attività di vigilanza.

Art. 25 Generi di misure di acquisizione soggette ad autorizzazione

Il *capoverso 1 lettera a* consente al SIC di ordinare la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni secondo le disposizioni della LSCPT. A differenza delle autorità di perseguimento penale, che impiegano queste misure di sorveglianza nell'ambito di un procedimento penale per smascherare gli autori di reati (funzione repressiva), il SIC ordinerà la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni esclusivamente a scopo preventivo. L'obiettivo consiste nell'individuare tempestivamente le minacce per la sicurezza interna o esterna della Svizzera. Se nell'ambito dei propri accertamenti ha il sospetto di essere in presenza di atti penalmente perseguibili, il SIC ne informa le autorità di perseguimento penale.

Contrariamente all'avamprogetto, nel quale le misure di sorveglianza nell'ambito della corrispondenza postale e del traffico delle telecomunicazioni sono state elencate singolarmente per una migliore comprensibilità in occasione della consultazione, nel disegno di legge ora si rinvia in generale ai tipi di sorveglianza secondo la LSCPT. In tal modo è facilitato il coordinamento con la revisione totale di questa legge[24] attualmente in corso e sono evitati i malintesi sorti in occasione della consultazione, ossia che con la LAIn sarebbero stati introdotti altri tipi di sorveglianza e nuovi obblighi per i fornitori di servizi di telecomunicazione. Lo svolgimento della sorveglianza avviene poi per mezzo del Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT) del DFGP.

Durante la consultazione diversi fornitori di servizi di telecomunicazione (di seguito fornitori) hanno fatto valere che le indennità per la sorveglianza secondo la LSCPT non coprirebbero i costi; inoltre è stato fatto valere che l'obbligo legale dei fornitori di eseguire determinate misure, in particolare quelle nuove, non sarebbe sempre chiaro. Tali temi tuttavia non devono essere trattati nel quadro della LAIn ma in occasione della revisione totale della LSCPT. Gli oneri legali per i fornitori di garantire le capacità di sorveglianza sotto il profilo tecnico sono una conseguenza dell'autorizzazione statale a operare in un ambito commerciale importante e lucrativo del service public.

Le presumibili prestazioni di sorveglianza richieste in più dal SIC comporteranno per il Servizio SCPT un aumento piuttosto modesto dell'onere rispetto alle prestazioni già fornite attualmente a favore delle autorità di perseguimento penale (2011:

24 FF **2013** 2283

2699 misure di sorveglianza in tempo reale, 5758 misure di sorveglianza retroattive/dati marginali e 3918 informazioni tecniche e amministrative[25]).

La *lettera b* disciplina l'impiego di mezzi tecnici, come ad esempio gli apparecchi GPS, che consentono di localizzare persone, veicoli o altri oggetti mobili. Questi strumenti forniscono la registrazione di uno schema degli spostamenti oppure trasmettono un segnale che consente di determinare l'ubicazione dell'emittente e quindi di localizzare la persona, il veicolo o l'oggetto mobile e di registrare i corrispondenti dati. Questi mezzi tecnici vengono utilizzati in particolare a sostegno di misure di osservazione (come per gli impieghi di polizia, nell'ambito dei quali tali strumenti sono correntemente impiegati ormai da anni). Possono facilitare tali misure (per es. in caso di perdita del contatto con il soggetto osservato) e in certi casi addirittura sostituirli parzialmente (se non è necessaria un'osservazione diretta) oppure servono per prepararli (studio delle abitudini del soggetto per consentire un impiego più mirato di squadre di osservazione).

Allo scopo di non escludere futuri progressi della tecnica in questo campo, la definizione degli apparecchi da impiegare è stata volontariamente formulata in maniera aperta.

Se la localizzazione di un telefono mobile avviene per mezzo di dati del fornitore, si tratta di una sorveglianza del traffico delle telecomunicazioni secondo la LSCPT disciplinata nella lettera a.

La *lettera c* consente in particolare di registrare le conversazioni delle persone sorvegliate in locali privati e di sottoporle a videosorveglianza (videotecnica). Il diritto vigente non consente questo tipo di sorveglianza al di fuori di un procedimento penale. In presenza di indizi concreti di gravi atti che minacciano la sicurezza da parte di determinati individui, il SIC deve essere in grado di estendere i propri accertamenti anche a spazi privati. Pure in questo caso si applicano i principi sanciti dall'articolo 26.

L'esempio di seguito illustra il possibile impiego di misure tecniche di sorveglianza: nei casi di piccole cellule terroristiche (come per es. in Germania il trio del «nationalsozialistischer Untergrund» [Clandestinità nazionalsocialista]), i contatti assumono carattere cospirativo e avvengono soltanto nella clandestinità. In pubblico queste persone non manifestano le loro reali intenzioni. Non hanno quindi contatti con persone esterne alle quali confidano le loro intenzioni e le loro opinioni. In simili ambienti, di conseguenza non è neppure possibile impiegare fonti umane, poiché queste cellule non consentono agli estranei di accedervi. Per acquisire le informazioni di cui necessita e sventare possibili minacce per la sicurezza, ad esempio attentati terroristici, il SIC non può fare a meno di mezzi tecnici di sorveglianza. Non appena viene superata la soglia del sospetto di reato, il SIC fa intervenire le autorità di perseguimento penale (art. 59).

La *lettera d* tiene conto del progressivo trasferimento in aree Internet ad accesso protetto di attività e dichiarazioni che minacciano la sicurezza. Considerate le crescenti minacce per la sicurezza della Svizzera provenienti da Internet, il SIC necessita di nuovi mezzi adeguati che gli consentano, nel quadro del proprio compito preventivo, di esplorare le reti per poter valutare la minaccia. Può trattarsi di acquisire

25 La statistica del Servizio SCPT può essere consultata in Internet all'indirizzo https://www.li.admin.ch/ > Temi > Statistica

informazioni (n. 1), ma anche di perturbare, impedire o rallentare l'accesso a informazioni (n. 2) in occasione di attacchi a infrastrutture critiche.

Per scoprire e valutare importanti sviluppi che minacciano la sicurezza, il SIC deve poter penetrare se necessario anche in reti particolarmente protette. Le informazioni così ottenute possono ad esempio contribuire a scoprire e sventare piani di matrice terroristica.

Gli attacchi volti a perturbare le infrastrutture critiche possono minacciare gravemente la sicurezza interna o esterna della Svizzera e comportare danni considerevoli. Si pensi per esempio ad attacchi elettronici all'approvvigionamento energetico (per es. centrali nucleari), ai trasporti e al traffico (per es. aviazione, traffico ferroviario e stradale), all'industria chimica (per es. rifiuti speciali), alle telecomunicazioni (per es. radio e televisione), alla sanità pubblica (per es. assistenza sanitaria) o al settore finanziario e assicurativo (per es. borse). Il numero 2 è inteso a consentire di lottare contro danni imminenti oppure contro danni parzialmente o totalmente già avvenuti durante un attacco in corso. È fatto salvo il principio di sussidiarietà, in quanto il SIC si attiva soltanto come una sorta di «ultima ratio», vale a dire che la precedenza dev'essere data a eventuali procedimenti penali e il SIC potrebbe attivarsi soltanto quando le condizioni per un procedimento penale non sono (ancora) date oppure un simile procedimento sarebbe vano per sventare un attacco effettivo. In questo contesto, la precedenza deve essere data alla protezione preventiva del Paese (per es. dalla contaminazione nucleare). Occorre sottolineare che le misure di difesa nei confronti di sistemi in Svizzera secondo il numero 2 sottostanno sempre ad autorizzazione, sia da parte dell'autorità giudiziaria (autorizzazione del Tribunale amministrativo federale), sia da parte dell'autorità politica (nullaosta del capo del DDPS).

In seno al DFGP, il Servizio nazionale di coordinazione per la lotta contro la criminalità in Internet (SCOCI) si occupa dell'aspetto penale delle attività svolte in Internet.

La *lettera e* concedere una nuova competenza al SIC, ossia la possibilità, in casi importanti e sotto il controllo del potere giudiziario e politico, di perquisire locali, veicoli e contenitori per acquisire informazioni o oggetti (per es. documenti) in rapporto con una minaccia per la sicurezza. Può trattarsi di borse, valige, container, supporti di dati o apparecchi di registrazione quali videocamere e dittafoni. Come sinora, il SIC non potrà procedere a perquisizioni fisiche. Questa prerogativa rimarrà riservata agli organi di polizia.

Si veda anche il commento concernente l'articolo 25 capoverso 1 lettere a e a^{bis} (LSIC) sotto «Coordinamento con la revisione totale della (LSCPT)» (modifica di altri atti normativi).

Il *capoverso 2* dispone che le misure previste siano eseguite segretamente e all'insaputa delle persone interessate. Questo è necessario per non pregiudicare il risultato auspicato con la misura. In contropartita, il controllo costituzionale delle misure è garantito da una duplice procedura di autorizzazione, giudiziaria e politica. È inoltre prevista la comunicazione a posteriori (art. 32) con possibilità di impugnare le misure ordinate (art. 79).

Oggi i membri di servizi informazioni esteri o di reti terroristiche in Svizzera possono sentirsi al riparo da un rilevamento precoce nelle loro comunicazioni. Questa situazione è peraltro sfruttata di conseguenza. In futuro il fatto che il SIC disporrà di maggiori competenze in materia dovrebbe già indurre questi attori ad agire con

maggiore cautela e a frenare i progetti dei servizi esteri di intervenire di propria iniziativa nel nostro Paese.

Art. 26 Principio

Il *capoverso 1* stabilisce due condizioni per l'impiego di misure di acquisizione soggette ad autorizzazione, ossia che esista una concreta minaccia per la sicurezza interna o esterna (ad eccezione dell'estremismo violento), o che sulla base di una decisione del Consiglio federale debbano essere salvaguardati interessi nazionali essenziali secondo l'articolo 3. Nella propria decisione il Consiglio federale stabilisce anche a quali condizioni possono essere impiegate misure di acquisizione soggette ad autorizzazione. La procedura di autorizzazione si fonda in ogni caso sugli articoli 28 segg.; ciò significa che la decisione del Consiglio federale non sostituisce la procedura ma è semplicemente un presupposto formale per l'adozione delle misure in questione se non sussiste una minaccia concreta nel senso definito restrittivamente dalla legge.

Tanto in presenza di interessi nazionali essenziali quanto in caso di concreta minaccia per la sicurezza interna o esterna ai sensi dell'articolo 19 capoverso 2 lettere a–d, per poter impiegare misure soggette ad autorizzazione devono essere adempiute (cumulativamente) le seguenti condizioni aggiuntive:

- la gravità della minaccia per la sicurezza della Svizzera deve giustificare la misura;
- gli accertamenti informativi effettuati fino a quel momento non hanno avuto successo oppure senza la misura di acquisizione speciale sarebbero comunque vani o sproporzionatamente difficili.

Queste condizioni aggiuntive descritte restrittivamente discendono dal principio costituzionale di proporzionalità e ricalcano quelle previste dal Codice di procedura penale (cfr. art. 269 cpv. 1 CPP). Non è sufficiente neppure che un'organizzazione o un gruppo figuri sulla lista d'osservazione secondo l'articolo 71. Questo può essere un indizio della gravità della minaccia per la sicurezza interna, tuttavia occorre fornirne la prova nel caso concreto prima di poter disporre la misura, come la necessità secondo la lettera c.

L'estremismo violento sarà escluso da queste misure di acquisizione. Il nostro Collegio ritiene che questo sia giustificato, poiché l'estremismo violento è più vicino a movimenti politico-ideologici, ciò che impone particolare precauzione. Quando per contro l'estremismo violento si trasforma in terrorismo, una sorveglianza sotto questo aspetto diventa possibile. La designazione annuale dei gruppi estremisti violenti da parte del Consiglio federale secondo l'articolo 69 del presente disegno garantisce la direzione politica e impedisce che il SIC possa attribuire autonomamente gruppi di estremisti violenti al terrorismo.

Quanto ai servizi terzi partecipanti all'esecuzione della misura ai sensi del *capoverso 3*, nella prassi si tratterà soprattutto del Servizio SCPT del DFGP per la sorveglianza del traffico delle telecomunicazioni, ma anche degli organi di sicurezza cantonali per l'impiego di apparecchi tecnici di sorveglianza o per le perquisizioni.

Art. 27 Misure di acquisizione soggette ad autorizzazione ordinate nei confronti di terzi

Può accadere che una persona per la quale sono date le condizioni previste dall'articolo 26 capoverso 1 per l'adozione di una misura soggetta ad autorizzazione utilizzi il telefono, l'indirizzo postale, l'ordinatore, il veicolo o altre installazioni di terzi per la trasmissione e la ricezione di informazioni. Il terzo interessato può esserne consapevole oppure ignaro. In questi casi, per accedere alle informazioni sul vero e proprio oggetto della sorveglianza, il SIC deve avere la possibilità di far sorvegliare la corrispondenza postale e il traffico telefonico del terzo in questione, di accedere al suo ordinatore o di far perquisire i suoi locali e veicoli. La sfera privata della terza persona dev'essere tutelata per quanto possibile ed essa dev'essere informata riguardo alla misura dopo la sua conclusione (art. 32).

Non è ammessa la sorveglianza di terzi che beneficiano della facoltà di non deporre a norma degli articoli 171–173 CPP, ossia di ecclesiastici, avvocati, medici e loro ausiliari o giornalisti. Anche da questo punto di vista la LSIC segue le regole del CPP. Un'estensione ad altri gruppi professionali, come richiesto in singoli casi durante la consultazione (per es. fornitori di prestazioni finanziarie) costituirebbe una considerevole novità dal profilo giuridico che il nostro Collegio non considera attualmente necessaria. Questa possibile novità dovrebbe essere discussa in maniera più approfondita di quanto consentito nel quadro della LAIn.

Art. 28 Procedura di autorizzazione

La procedura di autorizzazione proposta si articola in due livelli. In un primo tempo, il SIC deve chiedere l'autorizzazione a un organo giudiziario, vale a dire al Tribunale amministrativo federale. Soltanto dopo aver ottenuto l'autorizzazione giudiziaria, la misura sarà valutata in un secondo tempo dal punto di vista politico dal capo del Dipartimento, il quale deciderà in merito al rilascio del nullaosta (art. 29), dopo aver consultato la Delegazione Sicurezza del Consiglio federale.

Nei particolari, la procedura si svolge come segue:

1. il SIC presenta al Tribunale amministrativo federale una domanda per l'impiego di una misura di acquisizione soggetta ad autorizzazione;
2. il presidente della corte competente del Tribunale amministrativo federale esamina la domanda e decide se autorizzare o rifiutare la misura proposta o se chiedere il completamento degli atti;
3. se la misura è autorizzata, il capo del DDPS decide in seguito se concedere il nullaosta per l'esecuzione;
4. dopodiché, il SIC può eseguire la misura o ordinarne l'esecuzione da parte di terzi (per es. il Servizio SCPT).

La domanda contiene tutte le indicazioni necessarie per valutare se la misura è conforme alle esigenze di legge, ossia la descrizione degli indizi di fatto dell'esistenza di una minaccia concreta per la sicurezza interna o esterna della Svizzera, l'illustrazione della proporzionalità della misura, la designazione dei soggetti da sorvegliare nella misura in cui siano già stati identificati, i mezzi da impiegare ed eventuali misure di protezione a tutela dei diritti della personalità della persona sorvegliata o di terzi. Analogamente al CPP il presidente della corte competente deve motivare succintamente la decisione. La legge sul Tribunale amministrativo

federale prevede nell'articolo 23 decisioni da parte del giudice unico (cfr. anche «Modifica di altri atti normativi», n. 5).

Il Tribunale amministrativo federale è l'autorità giusta perché già oggi è incaricato dell'esame giuridico di misure connesse alla politica di sicurezza, per esempio in occasione della valutazione di ricorsi concernenti divieti d'entrata contro stranieri per motivi di sicurezza interna o esterna. Il Tribunale penale federale, proposto da alcuni partecipanti alla consultazione, nell'applicazione dei criteri di diritto penale nelle corrispondenti situazioni di sospetto ha un approccio totalmente diverso dal Tribunale amministrativo federale. Il nostro Collegio intende perciò rispettare anche nella procedura di autorizzazione la separazione tra servizio informazioni e perseguimento penale.

Analogamente a quanto previsto dall'articolo 274 capoverso 5 CPP, l'autorizzazione è concessa per tre mesi al massimo e può essere prorogata più volte, di volta in volta per altri tre mesi al massimo. Se è necessaria una proroga, il SIC presenta una domanda di proroga corredata delle stesse indicazioni necessarie per l'autorizzazione (cpv. 5). In occasione dell'autorizzazione di proroghe, nel quadro della verifica della proporzionalità la durata totale della misura dovrà essere ponderata rispetto ad altri fattori quali la gravità e la concretezza della minaccia.

Questa procedura intende tener conto del fatto che il ricorso a misure di acquisizione soggette ad autorizzazione può comportare ingerenze nei diritti fondamentali all'insaputa della persona sorvegliata e senza che questa possa opporvisi fintanto che perdura la misura.

I riscontri ottenuti con le misure di acquisizione soggette ad autorizzazione devono essere messi a disposizione delle autorità di perseguimento penale rispettando particolari cautele; in tal modo si eviterà che le misure di sorveglianza vengano utilizzate per casi penali nell'ambito dei quali la procedura penale non consentirebbe di ordinare una misura investigativa comparabile (cfr. art. 59 cpv. 3 e 4).

In occasione della consultazione, alcuni partecipanti hanno proposto che l'ottenimento dell'autorizzazione giudiziaria abbia luogo dopo quella politica, affinché il giudice non debba occuparsi di disposizioni senza alcuna speranza di successo a livello politico e i decisori politici non si fondino esclusivamente sulla valutazione giuridica. Il nostro Collegio è tuttavia dell'opinione che occorra mantenere la proposta originaria. In caso di inversione della procedura, prima del giudice unico tre consiglieri federali dovrebbero occuparsi di una proposta eventualmente contraria alla legge. Inoltre si potrebbe argomentare che un giudice unico potrebbe non sentirsi più libero di adottare una decisione di rifiuto contraria alla raccomandazione della Delegazione Sicurezza e alla decisione del capo del DDPS. La procedura di autorizzazione proposta in occasione della consultazione è stata comunque approvata dalla grande maggioranza dei partecipanti.

Art. 29 Nullaosta

Questo articolo disciplina il rilascio del nullaosta che il capo del DDPS deve concedere alle misure di acquisizione autorizzate dall'autorità giudiziaria, , dopo aver preliminarmente consultato la Delegazione Sicurezza del Consiglio federale. Questa procedura a due livelli garantisce una valutazione politica oltre che giuridica di misure che comportano una forte ingerenza nei diritti fondamentali. Gli organi di condotta in materia di politica di sicurezza beneficiano, a livello politico, di un

ampio margine discrezionale per quanto riguarda l'eventuale rinuncia a rilasciare il nullaosta.

Occorre comunque sottolineare che il capo del DDPS può concedere il nullaosta soltanto per misure già autorizzate dall'autorità giudiziaria. Non può concedere il nullaosta per alcuna misura che non sia già stata autorizzata.

Conformemente all'articolo 22 LOGA, la supplenza del capo del DDPS è assunta da un altro membro del Consiglio federale. Una delega all'interno del Dipartimento non è possibile.

Art. 30 Procedura in caso d'urgenza

Contrariamente alle autorità di perseguimento penale, che sono abilitate a disporre immediatamente ad esempio la sorveglianza della corrispondenza postale e delle comunicazioni telefoniche richiedendone l'approvazione soltanto a posteriori (art. 274 cpv. 1 CPP), per ordinare le misure previste dagli articoli 25 e seguenti il SIC deve di principio attendere l'autorizzazione del Tribunale amministrativo federale e il nullaosta del capo del DDPS, il quale preliminarmente ha consultato la Delegazione Sicurezza.

L'articolo 30 concede dunque al SIC la possibilità, in caso di pericolo incombente, di ricorrere immediatamente a misure secondo gli articoli 25 e seguenti (ordinare l'impiego immediato di una misura). Un pericolo incombente è sempre dato quando unicamente un'azione immediata permette di accertare fatti oppure osservare attività in modo tempestivo.

Se il SIC ad esempio è informato che un importante soggetto sorvegliato appartenente agli ambienti del terrorismo o dell'intelligence si trova su un volo a destinazione di Zurigo che atterrerà tra tre ore, a dipendenza delle circostanze l'unica possibilità per acquisire le informazioni necessarie a valutare l'attuale minaccia può consistere nell'eseguire immediatamente misure di acquisizione soggette ad autorizzazione (per es. la sorveglianza del telefono cellulare, la perquisizione segreta dei bagagli, l'applicazione di un apparecchio di localizzazione). Più tardi, non sarà in pratica più possibile acquisire le informazioni sfuggite.

Se intende interrompere l'impiego di una misura ordinata d'urgenza, il capo del DDPS dispone delle seguenti possibilità:

- ordinare l'interruzione della misura già dopo essere stato informato dal SIC;
- rifiutare il nullaosta dopo che il Tribunale amministrativo federale ha concesso l'autorizzazione (cfr. art. 32). Una simile eventualità è ipotizzabile nei casi in cui il capo del DDPS abbia preso atto dell'insieme delle circostanze relative all'impiego soltanto con la domanda scritta, mentre le prime informazioni erano sommarie.

Art. 31 Fine della misura di acquisizione

Le regole applicabili alla cessazione di misure di acquisizione soggette ad autorizzazione corrispondono alle norme ordinarie (cfr. art. 275 CPP). Il *capoverso 1 lettera b* esplicita il principio di proporzionalità disponendo che una misura non deve essere applicata più a lungo di quanto effettivamente necessario.

La comunicazione secondo il *capoverso 4* alle autorità che hanno rilasciato l'autorizzazione e il nullaosta è intesa a garantire che anch'esse siano tenute sempre al corrente sulle misure ancora in corso.

Art. 32 Obbligo di comunicazione nei confronti delle persone sorvegliate

L'obbligo di informare retroattivamente le persone interessate in merito alle misure informative adottate è desunto dal diritto alla protezione della vita privata e al rispetto della sfera privata. Si tratta di un diritto garantito dall'articolo 8 della Convenzione del 4 novembre 1950[26] per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dall'articolo 13 della Costituzione federale (Cost.).

Dopo la conclusione di un'operazione, rispettivamente di un complesso correlato di più misure di acquisizione riguardanti una determinata fattispecie, di principio entro un mese il SIC deve informare in merito alla misura di acquisizione le persone che ne sono state oggetto e i terzi di cui ha eventualmente sorvegliato i collegamenti (*cpv. 1*). In questo contesto la legge non fa riferimento alla singola misura, poiché ad esempio possono ancora essere simultaneamente in corso altre misure di acquisizione autorizzate che potrebbero essere compromesse dalla comunicazione di una misura già conclusa (tipico esempio: l'acquisizione dei dati marginali di passati collegamenti di telecomunicazione secondo l'art. 25 cpv. 1 lett. c termina con la trasmissione dei dati, ma nel contempo è ancora in corso una sorveglianza del traffico corrente delle telecomunicazioni). Spesso, inoltre, per valutare se una comunicazione può essere effettuata o se invece è necessario ricorrere a un'eccezione ai sensi del capoverso 2 bisogna attendere la conclusione di tutte le misure (per es. poiché il caso è stato trasmesso alle autorità di perseguimento penale e quindi è avviato un procedimento giudiziario). Alla comunicazione è aggiunta l'indicazione della possibilità di ricorso secondo l'articolo 79.

L'obbligo di comunicazione non si applica all'esplorazione radio e all'esplorazione dei segnali via cavo (art. 36–42), poiché esse non sono incentrate sui collegamenti di telecomunicazione di persone, ma sull'esplorazione di emissioni radio o di trasmissioni via cavo dall'estero allo scopo di raccogliere informazioni importanti in materia di politica di sicurezza. In tal caso l'obiettivo delle misure di acquisizione non sono né le persone né il loro esteso traffico di telecomunicazioni.

Il *capoverso 2 lettera a* fa riferimento alla giurisprudenza della Corte europea dei diritti dell'uomo, la quale nella sentenza Klass contro Repubblica federale di Germania del 6 settembre 1978 ha stabilito che una comunicazione a posteriori può pregiudicare lo scopo ultimo di una sorveglianza, e che pertanto a determinate condizioni può essere omessa. Nella citata sentenza la Corte espone in particolare quanto segue:

«… L'informazione a posteriori di chiunque sia stato a un dato momento oggetto di una misura frattanto soppressa potrebbe benissimo compromettere lo scopo ultimo perseguito a suo tempo con l'adozione della misura. Come giustamente ritenuto dalla Corte costituzionale federale [tedesca], questo tipo di comunicazione rischierebbe inoltre di svelare le modalità operative e i campi d'osservazione dei servizi segreti e di condurre anche all'identificazione dei loro agenti. Nella misura in cui l'«ingerenza» risultante dalle prescrizioni contestate appare giustificata alla luce dell'articolo 8 capoverso 2 [CEDU] […], la Corte europea dei diritti dell'uomo

26 RS **0.101**

ritiene che non sia incompatibile con quest'ultima disposizione che una volta conclusa l'operazione di sorveglianza l'interessato non venga informato, poiché è esattamente questa circostanza a garantire l'efficacia dell'«ingerenza».»

La *lettera b* fa riferimento a interessi pubblici preponderanti in materia di salvaguardia della sicurezza interna o esterna, rispettati anche dalla CEDU. Considera anche la necessità di non dare ad ambienti pericolosi per la sicurezza informazioni sulle attività difensive della Svizzera. Ad esempio il cittadino somalo che, dalla Svizzera, recluta nel Paese volontari per i viaggi della Jihad non viene informato a posteriori, e per ovvi motivi, in merito all'intercettazione.

La *lettera c* riprende il principio della tutela dei legittimi interessi di terzi. Si può ad esempio prescindere dal comunicare una sorveglianza a una terza persona se la comunicazione comprometterebbe il vero e proprio oggetto della misura.

La *lettera d* fa riferimento a casi in cui il luogo di dimora della persona interessata o della terza persona in questione può essere determinato soltanto con un impegno eccessivo, oppure a casi in cui, pur essendo noto il luogo di dimora, la persona interessata potrebbe essere raggiunta soltanto con un onere eccessivo (specialmente all'estero) o potrebbe addirittura essere messa in pericolo da una comunicazione formale da parte delle autorità svizzere.

Conformemente al *capoverso 3*, per il differimento o la rinuncia alla comunicazione a posteriori si applica la stessa procedura prevista per le misure di acquisizione soggette ad autorizzazione: autorizzazione da parte del Tribunale amministrativo federale e successivo nullaosta da parte del capo del DDPS (art. 29).

Art. 33 Collaborazione e mandati nell'ambito dell'acquisizione

Oggigiorno, gli attori statali e non statali negli ambiti del terrorismo, dello spionaggio, dell'estremismo violento, del commercio vietato di armi, delle armi di distruzione di massa chimiche, biologiche e nucleari oppure dei trasferimenti vietati di tecnologia, operano a livello globale e non si fermano nemmeno di fronte a confini o convenzioni interstatali. Questi attori sfruttano ad esempio l'assenza di obbligo del visto all'interno dello spazio Schengen per incontrarsi segretamente in altri Paesi e aggirare così le misure di sorveglianza applicate nei propri Stati. I servizi informazioni di molti Paesi si trovano confrontati agli stessi problemi transfrontalieri e spesso non sono più in grado di acquisire le informazioni necessarie senza il concorso di altri.

Perciò, la collaborazione con autorità svizzere ed estere, prevista nel *capoverso 1*, assume un'importanza crescente, soprattutto nel campo della comunicazione di informazioni, dell'osservazione transfrontaliera, delle operazioni di acquisizione congiunte e delle misure tecniche di sorveglianza. Queste ultime vengono eseguite conformemente al vigente diritto svizzero. In particolare, il SIC non è legittimato a servirsi della collaborazione con autorità estere per eludere le prescrizioni che prevedono l'obbligo di autorizzazione per determinate misure di acquisizione.

Il *capoverso 2* si applica all'assegnazione, in via eccezionale, di mandati a privati che hanno la possibilità di acquisire informazioni, anche avvalendosi di registrazioni audiovisive. Tali mandati possono essere assegnati soltanto a condizione che senza il concorso di questi privati l'acquisizione di informazioni da parte del SIC risulti molto più difficile o addirittura impossibile. Per accedere a un determinato gruppo di persone a fini informativi, ad esempio, l'impiego di una fonte (piuttosto che di un

collaboratore del SIC) per collocare un dispositivo tecnico può essere l'unica soluzione promettente. Più una persona passa inosservata in una determinata cerchia, maggiori saranno le probabilità che l'acquisizione di informazioni sia coronata dal successo.

Le misure d'acquisizione di cui al *capoverso 2* comprendono ad esempio complessi apparecchi tecnici di sorveglianza che possono essere gestiti soltanto da una ditta privata specializzata. È ipotizzabile anche l'impiego di specialisti privati in informatica quando si tratta di reti di dati particolarmente protette.

Il SIC è tenuto ad assicurarsi che tutti gli incaricati di cui ai capoversi 1 e 2 garantiscano di eseguire l'acquisizione conformemente alle disposizioni di legge e deve anche vigilare strettamente sull'adempimento del mandato da parte di tali persone come se fossero suoi propri collaboratori. In occasione dell'assegnazione del mandato esso disciplinerà pertanto per scritto aspetti quali la tutela del segreto, il diritto di controllo del SIC e dell'IFPDT per quanto riguarda l'utilizzazione dei dati, il divieto dell'utilizzazione dei dati per altri scopi o misure relative alla sicurezza delle informazioni. Gli aspetti che è necessario disciplinare dipendono di volta in volta dal genere di mandato.

Il SIC non assegna formalmente incarichi a servizi ufficiali esteri, ma trasmette loro delle domande nel quadro della collaborazione instaurata con tali servizi. In questo contesto, secondo l'articolo 69 capoverso 1 lettera f il Consiglio federale stabilisce annualmente la collaborazione con autorità estere.

Alle eventuali pretese si applica il diritto federale generale in materia di responsabilità secondo la legge del 14 marzo 1958[27] sulla responsabilità.

Art. 34 Protezione delle fonti

Per i servizi informazioni, la protezione delle fonti è fondamentale. L'identità di una fonte deve poter essere rivelata soltanto in via eccezionale, in presenza di interessi pubblici preponderanti. L'identità di certe fonti deve essere protetta addirittura con assoluto rigore. In caso contrario, la fiducia nella discrezione del SIC ne sarebbe compromessa e l'acquisizione di informazioni ne risulterebbe gravemente pregiudicata.

Nel diritto vigente è previsto soltanto un disciplinamento rudimentale della protezione delle fonti, nell'articolo 7 LSIC, il quale si limita peraltro a delegarne il disciplinamento al Consiglio federale. Il nostro Collegio ritiene che la regolamentazione completa in materia di servizio informazioni debba comprendere anche un esauriente disciplinamento della protezione delle fonti. Si eviteranno così anche eventuali contraddizioni tra disposizioni speciali a livello di ordinanza e le disposizioni legali di altri atti normativi.

Il *capoverso 1* sancisce il principio della protezione delle fonti e della necessità particolare di proteggere le persone che svolgono un'attività informativa concernente l'estero, come sinora previsto dall'articolo 7 LSIC. In questo ambito rientrano però anche le relazioni con servizi informazioni e autorità di sicurezza esteri; senza la piena protezione di tali relazioni, la Svizzera sarebbe infatti considerata un partner non sicuro. Questo potrebbe avere gravi ripercussioni sull'affidabilità del SIC come partner nell'ambito di una cooperazione. Tuttavia non meritano alcuna protezione le

27 RS **170.32**

persone imputate di crimini contro l'umanità (art. 264 e 264*a* CP) o di crimini di guerra (art. 264*b*–264*j*). In questo caso non si applica la protezione delle fonti se contro la persona è stato aperto un procedimento da parte di un tribunale svizzero o di un tribunale internazionale riconosciuto dalla Svizzera. La protezione delle fonti non si applica neppure quando la Svizzera è tenuta a prestare assistenza giudiziaria.

Il *capoverso 2* limita la protezione delle fonti umane (art. 15) in Svizzera nei confronti delle autorità di perseguimento penale. Le persone in questione non ricevono protezione in quanto fonti umane se viene loro imputato un reato perseguito d'ufficio o se la rivelazione della loro identità è indispensabile per far luce su un reato grave. Per quanto riguarda la nozione di reato grave, il diritto penale materiale e processuale non fornisce una definizione di validità generale a livello di legge formale. Non esistono neppure criteri di validità generale per stabilire se un reato sia grave. Per qualificare un reato come reato grave ha un influsso il contesto. Come spunto si può comunque fare riferimento alla definizione contenuta nell'articolo 11 capoverso 3 dell'ordinanza del 12 novembre 2008[28] sulla coercizione di polizia e le misure di polizia negli ambiti di competenza della Confederazione:

[3] Sono considerati gravi i reati contro la vita, l'integrità della persona, la libertà, l'integrità sessuale o la sicurezza pubblica.

Il *capoverso 3* enuncia i criteri applicabili alla protezione delle fonti. Tra questi spicca il mantenimento della fonte ai fini di un'ulteriore utilizzazione per l'acquisizione di informazioni. Conformemente alle regole generali sull'emanazione delle disposizioni d'esecuzione, il Consiglio federale disciplina i dettagli per via di ordinanza.

Il nostro Collegio ritiene opportuno che la legge, per giudicare le controversie nell'ambito delle attività del SIC, preveda un'unica autorità che possa sviluppare le opportune competenze specialistiche in ambito informativo. Propone pertanto, nel *capoverso 4*, che il Tribunale amministrativo federale sia designato come autorità decisionale in materia di protezione delle fonti. Il rinvio all'assistenza giudiziaria concerne soltanto l'assistenza giudiziaria nazionale. L'assistenza giudiziaria internazionale avviene per il tramite delle autorità di giustizia competenti e non per il tramite del servizio informazioni.

Art. 35 Disposizioni generali

Nota introduttiva

L'acquisizione di informazioni su fatti che avvengono all'estero si basa attualmente sulle regole generali previste dall'articolo 1 lettera a LSIC:

«Il Consiglio federale designa le unità della Confederazione chiamate ad assolvere i compiti del servizio informazioni civile. Tali unità:

a. raccolgono le informazioni concernenti l'estero rilevanti sotto il profilo della politica di sicurezza e le valutano all'attenzione dei Dipartimenti e del Consiglio federale; …».

Questa soluzione normativa risale al previgente articolo 99 capoverso 1 della legge militare (LM). Nella LSIC è stata formulata in modo alquanto generico, poiché ci si voleva limitare a riunire le vigenti basi legali in materia di servizio informazioni

28 RS **364.3**

civile senza introdurre nuovi limiti materiali. Nella LSIC è stata pertanto ripresa la soluzione prevista dalla LM, poiché si intendeva concedere al servizio informazioni un ampio margine per l'acquisizione di informazioni all'estero ed evitare inoltre di rivelare all'estero i metodi e le possibilità di cui disponeva il servizio informazioni concernente l'estero (allora il Servizio informazioni strategico, SIS) per acquisire informazioni.

L'articolo 16 O-SIC descrive oggi in modo più dettagliato i metodi ammessi per l'acquisizione di informazioni all'estero da parte del servizio informazioni.

Se le informazioni riguardanti fatti all'estero vengono acquisite in Svizzera, si applicano, di principio, le regole previste per l'acquisizione di informazioni in Svizzera (cpv. 2).

L'acquisizione di informazioni all'estero segue altre regole rispetto a quelle per l'acquisizione in Svizzera. Il SIC adotta le misure di acquisizione all'estero sotto la propria responsabilità, comprese le misure che in Svizzera sarebbero soggette ad autorizzazione (art. 25 segg.).

La diversa regolamentazione applicabile all'acquisizione di informazioni in Svizzera o all'estero corrisponde alla prassi seguita dalla maggior parte dei servizi informazioni e risulta sostanzialmente dal fatto che le attività informative che uno Stato svolge per acquisire informazioni in altri Stati sono generalmente da questi considerate attività di spionaggio e in quanto tali perseguite penalmente. A livello internazionale non è per contro prevista l'assistenza giudiziaria per i reati di spionaggio. Pertanto, il nostro Collegio non ritiene sensato assoggettare l'acquisizione di informazioni all'estero a una procedura di autorizzazione giudiziaria o politica. All'estero l'autorizzazione non esplicherebbe comunque alcun effetto giuridico o politico, bensì potrebbe essere considerata dallo Stato che ne è oggetto un'illecita ingerenza nella sua sovranità da parte delle autorità giudiziarie e politiche svizzere. Per il resto occorre considerare che:

- i diritti fondamentali devono essere rispettati nella loro essenza anche nell'acquisizione di informazioni all'estero e l'ingerenza nei diritti fondamentali delle persone deve essere limitata al minimo indispensabile (art. 3);
- le attività volte all'acquisizione di informazioni su fatti all'estero devono essere rigorosamente documentate all'indirizzo degli organi di vigilanza e di controllo (cpv. 4);
- l'acquisizione di informazioni all'estero sottostà al controllo del DDPS e del Consiglio federale e, in ultima istanza, della Delegazione delle Commissioni della gestione delle Camere federali (cfr. art. 74 segg.).

A queste condizioni, le attività del SIC previste nel disegno di legge sono conformi agli obblighi della Svizzera in materia di diritto internazionale pubblico.

Il *capoverso 1* statuisce il principio secondo cui le attività di acquisizione all'estero sono svolte in segreto. La ragione di questo principio risiede nel fatto che altrimenti le attività in questione potrebbero essere impedite dagli Stati o attori interessati e sia i collaboratori del SIC sia le sue fonti umane potrebbero essere esposte a pericoli.

Il *capoverso 2* consente di acquisire informazioni riguardanti fatti che avvengono all'estero anche in Svizzera (per es. organizzandovi incontri con fonti umane), ma garantisce al tempo stesso che il SIC debba rispettare le stesse regole applicabili all'acquisizione in Svizzera. Ciò riguarda in particolare l'eventuale applicazione di

misure di acquisizione soggette ad autorizzazione (sezione 4). È fatta eccezione per attività particolari secondo l'articolo 36 (Introduzione in sistemi e reti informatici all'estero).

Il SIC impiega misure di acquisizione segreta di informazioni all'estero sotto la propria responsabilità, comprese le misure che sarebbero soggette ad autorizzazione secondo gli articoli 25 e seguenti se fossero applicate in Svizzera. Oltre che dalle suddette ragioni, la diversa regolamentazione rispetto alle misure di acquisizione in Svizzera è motivata anche dal fatto che, per poter adempiere i mandati loro assegnati, i collaboratori del SIC incaricati dell'acquisizione di informazioni concernenti l'estero necessitano di una maggiore libertà d'azione e di un maggior margine discrezionale nella scelta dei mezzi a cui ricorrere in funzione della situazione.

Pertanto, il Consiglio federale propone di disciplinare le misure di acquisizione segreta di informazioni all'estero ammesse dalla legge senza particolari necessità di autorizzazione. Tale proposta è giustificata dal fatto che i tribunali svizzeri di regola non possono conoscere le condizioni sul posto né acquisire in tempo utile le informazioni necessarie per un processo decisionale pienamente responsabile. Di conseguenza, in simili situazioni non è possibile alcuna procedura ordinaria di autorizzazione (che per altro costituirebbe un unicum a livello internazionale). A ciò si aggiunge il problema risultante dal fatto che uno dei massimi tribunali svizzeri dichiarerebbe preliminarmente conformi al diritto atti che nei Paesi nei quali dovrebbero essere eseguiti sarebbero considerati per lo più punibili. Tuttavia, anche nell'acquisizione di informazioni all'estero dev'essere rispettato il principio della proporzionalità, come stabilisce espressamente il *capoverso 3*. Anche all'estero, le ingerenze nei diritti fondamentali non devono essere sproporzionate rispetto agli attesi benefici a livello informativo. Conformemente alla Costituzione federale, l'essenza dei diritti fondamentali dev'essere tutelata da tutte le autorità, anche dal servizio informazioni in occasione dell'acquisizione di informazioni all'estero.

Il fatto che il SIC possa agire in gran parte sotto la propria responsabilità in materia di acquisizione di informazioni all'estero non implica tuttavia la scomparsa di un controllo efficace. Al contrario, il *capoverso 4* impone al SIC di documentare l'acquisizione di tutte le informazioni riguardanti fatti all'estero affinché il Consiglio federale, il Parlamento (Commissione della gestione o Delegazione delle Commissioni della gestione) e il DDPS (Vigilanza sulle attività informative) possano esercitare una vigilanza politica sul SIC.

I dati acquisiti all'estero con l'ausilio di metodi comparabili alle misure di acquisizione soggette ad autorizzazione (per es. mediante l'impiego di apparecchi di localizzazione GPS) sono comparabili ai dati risultanti da misure di acquisizione soggette ad autorizzazione in Svizzera per quanto riguarda l'entità, le necessità in materia di tutela del segreto e i rischi in materia di sicurezza (per es. per quanto riguarda il malware nei dati informatici). Secondo il *capoverso 5,* tali dati possono essere memorizzati in sistemi d'informazione separati analogamente ai dati comparabili provenienti dall'acquisizione in Svizzera (cfr. art. 57). Da tali sistemi possono essere trasferiti in forma elaborata in altri sistemi, se le premesse per la loro registrazione sono date. Questo trasferimento riguarderà principalmente il sistema di analisi integrata IASA SIC (art. 48).

I collaboratori del SIC impiegati all'estero sono esposti a un rischio accresciuto e agiscono anche in zone di guerra e in regioni di crisi, in parte sotto copertura o utilizzando un'identità fittizia. Nel *capoverso 6* il Consiglio federale propone pertanto di assoggettarli all'assicurazione militare.

Le misure di protezione previste nel *capoverso 7* possono consistere in equipaggiamenti tecnici, ma anche in coperture e identità fittizie o nel supporto operativo, ad esempio con l'impiego di misure di contro-osservazione per il riconoscimento tempestivo di pericoli nel contesto di un impiego.

Art. 36 Introduzione in sistemi e reti informatici

L'*articolo 36* disciplina alcuni casi particolari dell'acquisizione di informazioni concernenti l'estero rilevanti in materia di politica di sicurezza. Il *capoverso 1* disciplina l'introduzione a partire dalla Svizzera in sistemi e reti informatici ubicati all'estero allo scopo di perturbare, impedire o ritardare l'accesso a informazioni (cfr. art. 25 cpv. 1 lett. d n. 2). L'esercizio di condotta strategica svolto nel 2013 ha indicato che simili operazioni possono essere sensibili sotto il profilo della politica estera e pertanto non possono essere di sola competenza del SIC. Devono di conseguenza essere eseguite soltanto su decisione del Consiglio federale e unicamente quando i sistemi esteri sono utilizzati per attacchi alle infrastrutture critiche. Per i motivi già indicati nell'articolo 35, secondo il nostro Collegio un'autorizzazione giudiziaria non è necessaria.

Il *capoverso 2* disciplina per contro l'introduzione a partire dalla Svizzera in sistemi e reti informatici con l'unico scopo di acquisire informazioni (cfr. art. 25 cpv. 1 lett. d n. 1), sempre che tali sistemi e reti siano ubicati all'estero. In tale contesto l'oggetto di interesse per l'esplorazione deve situarsi all'estero (per es. programma di proliferazione di uno Stato estero). Poiché in questo caso nessun sistema è perturbato o limitato nel suo funzionamento, il rischio di implicazioni in materia di politica estera è molto minore rispetto al caso di misure secondo il capoverso 1. Il SIC sarà pertanto autorizzato, a partire dalla Svizzera e sotto la propria responsabilità, ad applicare questa modalità di acquisizione praticata in modo intensivo anche da servizi informazioni esteri. Tuttavia, qualora si dovessero temere rischi politici particolari, il direttore del SIC dovrà ottenere preliminarmente l'approvazione del capo del DDPS.

Art. 37 Esplorazione radio

Nel quadro del progetto di revisione LMSI II, le Camere federali hanno introdotto nella LSIC un nuovo articolo 4*a* che per la prima volta disciplina l'esplorazione radio a livello di legge. La nuova disposizione è entrata in vigore soltanto il 1° novembre 2012, dopo l'adeguamento dell'ordinanza del 17 ottobre 2012[29] sulla condotta della guerra elettronica e sull'esplorazione radio. Perciò, il Consiglio federale l'ha ampiamente ripresa nella LAIn, limitandosi a qualche adeguamento alla terminologia e al campo d'applicazione della LAIn. Nel capoverso 2, ad esempio, è stata inserita, tra i possibili presupposti del ricorso all'esplorazione radio, la salvaguardia di interessi essenziali della Svizzera su mandato diretto del Consiglio federale (cfr. art. 3 e art. 70).

29 RS **510.292**

L'esplorazione radio è orientata all'estero, vale a dire che può rilevare soltanto sistemi radio che si trovano all'estero. In pratica si tratta soprattutto di satelliti di telecomunicazioni e di emittenti a onde corte. Il «servizio preposto all'esecuzione» è il Centro operazioni elettroniche dell'Esercito svizzero (COE). Il COE è l'unico servizio che dispone dei necessari impianti tecnici. Il capoverso 4 garantisce che le trasmissioni radio possano essere analizzate soltanto in base a contenuti in rapporto con l'estero. Tuttavia, l'esplorazione può portare anche all'intercettazione di informazioni su persone in Svizzera, segnatamente quando il partner di comunicazione di una persona o installazione estera oggetto dell'esplorazione utilizza un collegamento di telecomunicazione svizzero. Il COE può trasmettere al SIC questo tipo di informazioni soltanto in forma anonimizzata, sempre che non ne emergano indizi relativi a una minaccia concreta per la sicurezza interna (cpv. 5). La LSIC rinvia in questo contesto all'ulteriore trattamento conformemente alle disposizioni della LMSI. Nel regime della LAIn le minacce in questione sono quelle di cui all'articolo 6 capoverso 1 lettera a.

Oggi l'esplorazione radio è già sottoposta alla verifica di un'autorità di controllo indipendente (ACI). Anche in questo caso, nell'articolo 75 LAIn il Consiglio federale riprende, con minime modifiche, la corrispondente disposizione della LSIC (art. 4*b*). Secondo il capoverso 3 il Consiglio federale disciplina gli altri dettagli relativi all'esplorazione radio. Tale capoverso stabilisce soltanto il contenuto minimo delle regolamentazioni a livello di ordinanza. Come finora, il Consiglio federale dovrà integrare nell'ordinanza anche altre disposizioni, quali le normative sul trattamento dei dati in seno al servizio preposto all'esecuzione oppure disposizioni in materia di sicurezza dei dati.

La LAIn riprende dunque le nuove normative e la prassi della LSIC e della LMSI. Nel quadro dei lavori legislativi svolti a suo tempo, su mandato delle Camere federali, all'elaborazione della LMSI aveva partecipato in misura determinante il professor Giovanni Biaggini, ordinario di diritto pubblico, amministrativo ed europeo all'Università di Zurigo. La presente disposizione della LAIn, come pure la successiva sezione sull'esplorazione dei segnali via cavo, sono state pertanto elaborate nuovamente con la partecipazione del professor Biaggini.

Art. 38 Disposizioni generali

Accanto all'esplorazione radio, già praticata anche in Svizzera, sul piano internazionale sta assumendo crescente importanza anche l'esplorazione dei segnali via cavo. Quest'ultima, che a causa dell'elevato fabbisogno di regolamentazione è disciplinata in un'apposita sezione, appartiene però anche all'ambito dell'acquisizione di informazioni su fatti che avvengono all'estero. L'esplorazione dei segnali via cavo riguardante eventi in Svizzera anche in futuro non sarà autorizzata.

Negli ultimi anni, in seguito allo sviluppo delle efficientissime reti a fibre ottiche, lo spostamento delle telecomunicazioni da dispositivi senza filo (radio) verso reti filari (per semplicità qui è utilizzato il termine «cavo») si è intensificato. Al tempo stesso, le possibilità di ottenere informazioni per mezzo dell'esplorazione radio si riducono. L'avamprogetto si ispirava pertanto in parte a una legge adottata nel 2008 dal Regno di Svezia (Legge 2008:717 sull'esplorazione dei segnali nell'ambito del Servizio informazioni militare [in Svezia questo servizio svolge le funzioni di servizio informazioni concernente l'estero]) che disciplina anche l'esplorazione dei segnali via cavo. In Svizzera si potranno effettuare più approfonditi accertamenti tecnici e test

di esplorazione di segnali via cavo soltanto una volta che si disporrà delle necessarie basi legali. Dal profilo puramente tecnico, l'esplorazione di segnali via cavo è fattibile come dimostrano i casi all'estero. Tuttavia, soltanto l'analisi dei flussi di dati che attraversano la Svizzera consentirà di stabilire se con l'esplorazione di segnali via cavo anche in Svizzera può essere raccolta una quantità sufficiente di informazioni utili. Tuttavia, per procedere a una simile esplorazione è imperativamente necessaria una base legale formale.

Come l'esplorazione radio, l'esplorazione dei segnali via cavo serve ad acquisire informazioni su fatti concernenti l'estero e quindi non è concepita come misura di acquisizione soggetta ad autorizzazione per la Svizzera. Per perseguire scopi di esplorazione analoghi in rapporto con la Svizzera sarebbe necessario richiedere una misura di acquisizione soggetta ad autorizzazione. L'esplorazione di segnali via cavo può però essere effettuata soltanto con il concorso dei fornitori svizzeri di servizi di telecomunicazione, ai quali deve essere impartito un ordine di trasmissione dei relativi flussi di dati al COE. Poiché in questi casi non è possibile una procedura di ricorso da parte delle persone interessate dalla misura di esplorazione, la legge prevede una procedura di autorizzazione analoga a quella istituita per le misure di acquisizione in Svizzera soggette ad autorizzazione (art. 28). A differenza di quanto previsto per le misure di acquisizione soggette ad autorizzazione, tuttavia, il trattamento dei dati non avviene in sistemi separati, bensì, come per i riscontri ottenuti dall'esplorazione radio, nell'Archivio dei dati residui e in IASA SIC (art. 46 segg.).

Nell'ambito dell'esplorazione di segnali via cavo vengono rilevati determinati flussi di dati nei cavi delle telecomunicazioni internazionali e come nel caso dell'esplorazione radio questi dati vengono vagliati in base ai contenuti, selezionati e convogliati verso l'analisi. A differenza di quanto previsto per la sorveglianza del traffico delle telecomunicazioni in Svizzera, per la quale è necessaria una misura di acquisizione soggetta ad autorizzazione, l'esplorazione di segnali via cavo è uno strumento dell'esplorazione concernente l'estero e non mira al rilevamento di tutto il traffico delle telecomunicazioni che avviene tra determinati collegamenti. Tecnicamente un simile rilevamento non può essere effettuato con le stesse modalità della sorveglianza delle telecomunicazioni in Svizzera, poiché nel caso dell'esplorazione di segnali via cavo, gli oggetti sorvegliati si trovano all'estero.

Per questo mezzo d'esplorazione, in Svizzera mancano ancora le basi legali. Per il nostro Paese si tratta di una nuova forma di esplorazione orientata all'estero che non è comparabile con le forme di sorveglianza previste dalla LSCPT. Di conseguenza, le terminologie non devono né possono essere identiche e non devono nemmeno ispirarsi troppo strettamente a nozioni tecniche attuali per non escludere ulteriori sviluppi tecnologici.

Come nel caso dell'esplorazione radio, per l'esecuzione dell'esplorazione dei segnali via cavo il servizio preposto all'esecuzione secondo il *capoverso 1* è il COE. Esso possiede le competenze tecniche e gli impianti necessari all'esecuzione dell'esplorazione. Per tutelare i diritti fondamentali delle persone di cui vengono rilevate le comunicazioni nell'ambito dell'esplorazione dei segnali via cavo, ma che non corrispondono ai criteri di ricerca definiti nel mandato del SIC, è necessario che la selezione dei dati sia effettuata non dal SIC ma da un altro servizio. Come nel caso dell'esplorazione radio, il COE trasmette al SIC soltanto i dati che corrispondono a un mandato di ricerca, oppure che contengono indizi diretti relativi a una minaccia per la sicurezza interna o esterna della Svizzera. I criteri e le procedure corrispondono ampiamente a quelli definiti per l'esplorazione radio. In tale contesto, una parte-

cipazione del Servizio SCPT non è necessaria né opportuna poiché nel caso dell'esplorazione dei segnali via cavo non si tratta di uno dei tipi di sorveglianza offerti da tale servizio secondo la LSCPT. Di conseguenza il COE, in quanto servizio preposto all'esecuzione, contatta direttamente i gestori di reti filari e i fornitori di servizi di telecomunicazione allo scopo di pianificare ed eseguire l'esplorazione dei segnali via cavo nel caso concreto.

Il *capoverso 2* garantisce che non vengano rilevate comunicazioni esclusivamente svizzere. Se tecnicamente non è possibile escludere queste comunicazioni (per es. il canale di pacchetti di dati IP non può essere previsto in anticipo, nonostante mittente e destinatario si trovino in Svizzera), i relativi dati devono essere immediatamente distrutti non appena sia stato constatato che provengono dalla Svizzera e sia stato identificato l'indirizzo destinatario. Quest'obbligo riguarda tanto il COE quanto il SIC.

Il *capoverso 3* stabilisce condizioni per le chiavi di ricerca che il SIC definisce nell'ambito del mandato di esplorazione. Le chiavi di ricerca devono essere formulate con la massima precisione possibile, affinché sia registrato il minor numero possibile di dati e siano minimizzate le ingerenze nella sfera privata delle persone. In altri termini, la ricerca ad esempio sulla base di dati anagrafici concreti di persone straniere sospettate di attività terroristiche o dei collegamenti di telecomunicazione che queste utilizzano è più efficace e più rispettosa dell'impiego di chiavi di ricerca grossolane quali «Al-Qaida» o «attentato esplosivo». In proposito l'esplorazione radio conosce già una prassi ben collaudata, giuridicamente corretta e controllata.

Il *capoverso 4* incarica il Consiglio federale, come il capoverso 3 della disposizione sull'esplorazione radio, di emanare le disposizioni d'esecuzione per via di ordinanza.

Art. 39 e 40 Obbligo dell'autorizzazione e procedura di autorizzazione

Questi articoli disciplinano l'autorizzazione dei mandati di esplorazione di segnali via cavo in modo analogo a quanto previsto per le misure di acquisizione soggette ad autorizzazione. Nel caso dell'esplorazione di segnali via cavo è necessaria una verifica giudiziaria, poiché deve essere impartito l'ordine ai provider di servizi di telecomunicazione di trasmettere determinati flussi di dati e non può essere prevista una procedura in contraddittorio per le persone interessate. Per tale motivo, l'ACI non opererà in questo ambito. In caso contrario ne deriverebbe una concorrenza e una commistione tra differenti autorità di approvazione, di controllo e di vigilanza.

La domanda di cui all'*articolo 40 capoverso 1* comprende anche le categorie di chiavi di ricerca in base alle quali devono essere selezionati i dati da trasmettere al SIC. L'esperienza maturata nella pratica dell'esplorazione radio insegna che queste chiavi di ricerca devono essere gestite in modo dinamico e poter essere continuamente perfezionate. Perciò, anche per l'esplorazione di segnali via cavo si prevede di operare con categorie di chiavi di ricerca, per non dover richiedere una nuova autorizzazione a ogni perfezionamento di dette chiavi. Può costituire una categoria di chiavi di ricerca ad esempio un gruppo di membri di una determinata organizzazione terroristica e le persone che con questi intrattengono contatti operativi. Tali persone possono infatti essere identificate soltanto nel corso dell'esplorazione. Chiavi di ricerca precise che vengono definite soltanto durante l'esecuzione della misura possono essere ad esempio indicazioni su elementi di indirizzo utilizzati nella

tecnica di telecomunicazione (per es. numeri telefonici), indirizzi o designazioni commerciali o di progetti.

A differenza delle misure di acquisizione soggette ad autorizzazione, che possono essere autorizzate di volta in volta soltanto per tre mesi al massimo, secondo il *capoverso 3* il mandato iniziale di esplorazione di segnali via cavo può essere autorizzato per sei mesi. La maggior durata è giustificata dal fatto che l'avvio del rilevamento nonché la formazione e l'introduzione degli addetti alla selezione, nell'ambito di un mandato, richiede più tempo rispetto ad esempio di una misura di sorveglianza del traffico delle telecomunicazioni secondo l'articolo 25 capoverso 1 lettera a (per la quale tutte le comunicazioni sono trasmesse al SIC). In seguito, per le proroghe è previsto un termine di tre mesi come per le misure di acquisizione soggette ad autorizzazione.

Art. 41 Esecuzione

L'esecuzione segue la stessa procedura prevista per l'esplorazione radio, eccettuato il fatto che nel caso dell'esplorazione di segnali via cavo il servizio preposto all'esecuzione non rileva direttamente (per mezzo di antenne) i segnali degli impianti di telecomunicazione, bensì li riceve da provider e fornitori di servizi di telecomunicazione. I provider interessati saranno determinati nel singolo caso in base al tracciato seguito dalle linee lungo le quali le comunicazioni attraversano la Svizzera.

L'ulteriore procedura e i criteri applicabili alla selezione dei dati da trasmettere al SIC si ispirano peraltro largamente alle regole previste per l'esplorazione radio (cpv. 2–5).

L'analisi informativa dei dati spetta al SIC. Esso decide inoltre, conformemente alle basi legali, quali dati archiviare e trattare ulteriormente nei propri sistemi d'informazione (cfr. cap. 4). Come sinora, il COE può però anche completare i dati trasmessi con spiegazioni tecniche o commenti sul contenuto, sintesi o traduzioni destinati al SIC.

Art. 42 Obblighi dei gestori di reti filari e dei fornitori di servizi di telecomunicazione

Dato che, come illustrato in precedenza, l'esplorazione di segnali via cavo può essere praticata soltanto con il concorso dei fornitori di servizi di telecomunicazione e dei gestori di reti filari, l'articolo 42 ne definisce gli obblighi. Sono soggetti ai corrispondenti obblighi previsti soltanto i gestori che offrono servizi pubblici ai sensi della legge del 30 aprile 1997[30] sulle telecomunicazioni (LTC) nel traffico transfrontaliero. La comunicazione di dati tecnici è necessaria in particolare anche per poter formulare i singoli mandati e le domande da sottoporre alle autorità competenti per l'autorizzazione. Pertanto la loro comunicazione non si limita alla concreta esecuzione di un mandato autorizzato e che ha ricevuto il nullaosta. Di norma le questioni tecniche devono essere chiarite tra il servizio preposto all'esecuzione (COE) e i provider. Per motivare e documentare i propri mandati, tuttavia, anche il SIC necessita di informazioni dirette da parte dei fornitori di servizi di telecomunicazione e dei gestori di reti filari.

30 RS **784.10**

In questo contesto, il concorso del Servizio SCPT del DFGP come già menzionato non è necessario, poiché l'esplorazione di segnali via cavo non è una forma di sorveglianza offerta da questo servizio secondo la LSCPT. Le modalità tecniche devono invece essere definite direttamente nel singolo caso d'intesa tra il SIC, il COE e i gestori.

Mancando ogni esperienza, l'onere connesso all'esecuzione dell'esplorazione di segnali via cavo non può al momento essere stimato. In particolare non si sa quali flussi di dati di rilevanza informativa attraversino oggi o attraverseranno in futuro la Svizzera. Queste informazioni potranno essere raccolte, come illustrato sopra, soltanto una volta che saranno disponibili opportune basi legali.

Nell'ambito della consultazione i provider hanno richiesto un indennizzo integrale dei loro costi. In occasione dell'attuale revisione della LSCPT è stata però mantenuta la vigente regolamentazione (indennizzo adeguato per l'utilizzazione dell'infrastruttura di sorveglianza dei provider in caso di utilizzazione effettiva); tale principio è ripreso anche in questa sede. In caso contrario non vi sarebbe, in particolare, alcun incentivo per i provider a cercare soluzioni economiche. La strutturazione concreta delle indennità a livello di ordinanza sarà discussa con i provider.

Stimiamo che l'avvio dei preparativi concreti in vista dell'esplorazione di segnali via cavo e l'esercizio a titolo sperimentale da parte del SIC e del COE richiederanno inizialmente due posti supplementari. Questi saranno sollecitati nell'ambito della pianificazione ordinaria del personale.

Capitolo 4, Sezione 1

Per adempiere i compiti conformemente alla presente legge e per poter individuare e valutare tempestivamente le minacce che incombono sulla sicurezza interna o esterna della Svizzera, il SIC, come del resto ogni servizio informazioni, deve poter disporre di un ampio ventaglio di informazioni provenienti da molteplici fonti.

Gli attentati terroristici, le attività di spionaggio e gli atti di estremismo violento vengono generalmente preparati nella clandestinità e tali preparativi vengono tenuti nascosti il più a lungo possibile. Possono però provocare danni considerevoli e per questa ragione è essenziale poterli individuare tempestivamente e combatterli. Perciò, il trattamento delle informazioni deve essere già effettuato in una fase in cui non è ancora dato alcun sospetto giuridicamente sufficiente relativo alla preparazione o all'esistenza di un reato. Il SIC deve appunto individuare attivamente questo tipo di minacce e combatterle congiuntamente con le altre autorità.

Il presente disegno di legge rinuncia logicamente alla separazione, ormai obsoleta, tra sicurezza interna ed esterna, sicché tale distinzione non svolge più un ruolo determinante neppure nell'ambito del trattamento dei dati da parte del SIC.

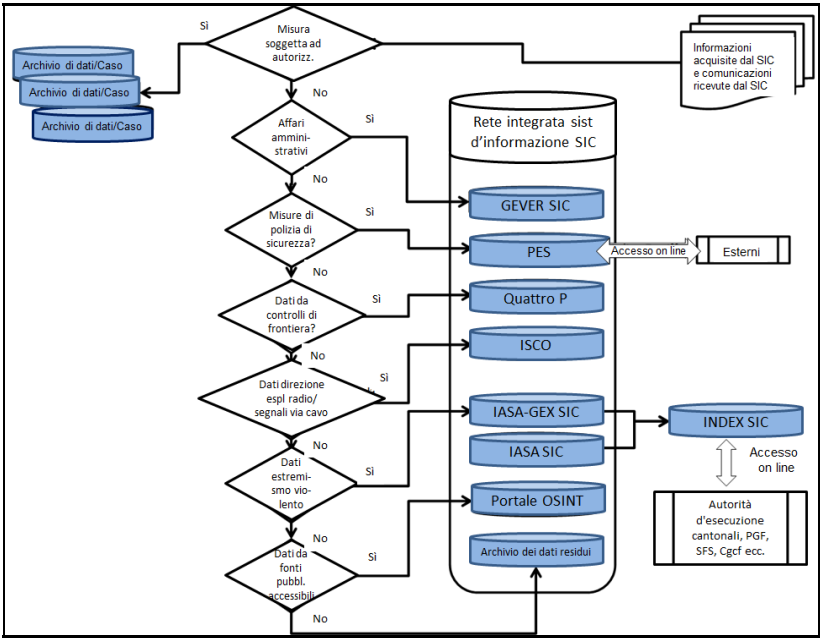
Per poter realizzare l'incremento di efficienza cui mirava la fusione del SIS e del SAP e l'auspicata valutazione globale dei dati di intelligence, il SIC necessita piuttosto di una regolamentazione unitaria negli ambiti della registrazione, della conservazione e della gestione dei dati. Per elaborare tale regolamentazione occorre tener adeguatamente conto degli elementi la cui validità è comprovata da una prassi pluriennale maturata nell'applicazione delle basi legali vigenti secondo la LMSI e la LSIC.

Il presente disegno prevede che le informazioni acquisite o le comunicazioni ricevute dal SIC siano archiviate in una rete integrata di sistemi d'informazione in funzione del tema, della fonte e della sensibilità dei dati. Il SIC non può raccogliere e

conservare dati indiscriminatamente. Deve sempre esistere un nesso sufficiente con i compiti secondo la LAIn. Inoltre devono essere rispettati i limiti posti al trattamento dei dati in relazione all'esercizio dei diritti politici (art. 5 cpv. 5–8). Infine, deve garantire che la rilevanza e l'esattezza dei dati vengano verificate prima dell'archiviazione. Questa verifica è inoltre effettuata prima che i dati personali abbiano effetti all'esterno, ossia quando vengono impiegati in un prodotto del SIC (per es. un rapporto d'analisi, una segnalazione a un servizio informazioni estero, una valutazione della situazione).

I dati che il SIC ottiene in virtù di una misura di acquisizione soggetta ad autorizzazione o di controlli alla frontiera vengono trattati separatamente e sono esclusivamente a disposizione degli specialisti all'interno del servizio.

I vari sistemi d'informazione del SIC consentono di disciplinare la conservazione dei dati in modo differenziato. Mentre il trattamento dei dati ad esempio nel campo del controspionaggio, della non proliferazione o della protezione di infrastrutture critiche non ha quasi mai dato adito a critiche, quello riguardante l'estremismo violento si è regolarmente rivelato particolarmente delicato, sia politicamente sia dal profilo della protezione dei dati. Come già la LMSI, anche il disegno di legge prevede pertanto condizioni severissime per l'elaborazione dei dati in quest'ambito delicato (sistematica applicazione dei controlli di qualità a brevi intervalli). Le condizioni applicabili alle informazioni ottenute da fonti pubblicamente accessibili sono invece meno severe (verifiche a intervalli più lunghi, periodo di conservazione più lungo, cerchia più ampia delle persone autorizzate ad accedervi), poiché in genere questi dati potrebbero essere ancora ottenuti dalle fonti originarie, quantunque strutturati diversamente e con minori garanzie riguardo alla loro disponibilità.



Art. 43 Principi

I principi stabiliti nell'articolo 43 si applicano a tutti i sistemi d'informazione del SIC. La loro applicazione generalizzata garantisce, a prescindere dal sistema nel quale vengono memorizzati dati personali, un elevato grado di uniformità alla qualità del trattamento dei dati. I vari sistemi possono contenere i dati in forma di testi, suoni o immagini o anche in altri formati appropriati.

Per adempiere i propri compiti, il SIC è regolarmente tenuto a elaborare dati personali degni di particolare protezione, ad esempio dati riguardanti l'appartenenza a una religione nel caso dei terroristi motivati da idee fondamentaliste, l'espiazione di pene detentive da parte di condannati o lo stato di salute di personaggi simbolo o politici stranieri. Il servizio allestisce ed elabora profili della personalità, ad esempio per valutare la minaccia proveniente da individui o gruppi di estremisti violenti. Il *capoverso 1* istituisce la necessaria base legale per queste forme di trattamento dei dati.

In deroga ai vincoli ordinari in materia di protezione dei dati, il SIC deve avere la facoltà, conferitagli nel *capoverso 2*, di conservare anche dati riconosciuti inesatti e valutati di conseguenza. Nel quadro della valutazione di informazioni di intelligence occorre individuare anche la disinformazione e la falsa informazione. Da informazioni di questo genere si possono dedurre le intenzioni dei rispettivi produttori e fornitori. Per scongiurare errori di valutazione, una volta individuata la disinformazione o la falsa informazione deve essere identificata in quanto tale e in quanto tale resa disponibile anche per il futuro, onde evitare il ripetersi di tali errori in futuro. Anche nell'ambito della collaborazione internazionale deve essere possibile accedere a informazioni riconosciute come false, per poterle valutare correttamente ed essere in grado di reagire a un'eventuale successiva propagazione di false informazioni (per es. identificazione erronea di un individuo come membro di un gruppo terroristico). Questi dati inesatti possono rivelarsi preziosi per la valutazione dell'attendibilità o delle intenzioni di una determinata fonte umana o di un servizio informazioni estero. La designazione chiara di tali dati impedisce che siano erroneamente trattati come dati corretti.

I sistemi d'informazione del SIC formano una rete integrata; tutti sono destinati a facilitare l'adempimento dei compiti che la legge assegna al SIC. Nel quadro dell'adempimento di questi compiti, i dati devono spesso essere trasferiti da un sistema all'altro. L'analista chiamato a redigere un rapporto su un gruppo di terroristi, ad esempio, deve disporre di comunicazioni di servizi di sicurezza esteri, notizie giornalistiche, segnalazioni di entrate in Svizzera ecc. Potrà effettuare e documentare il suo lavoro di analisi nel sistema d'informazione IASA SIC, previsto a tale scopo, soltanto se avrà potuto riunire i dati necessari in detto sistema. Tuttavia, poiché nel sistema d'origine gli stessi dati possono ancora essere utili per altri scopi o che in un dato caso può essere necessaria soltanto parte di una comunicazione più completa, le comunicazioni in questione devono rimanere nel sistema d'origine, nel quale sono a disposizione di altri utenti. Nel sistema d'origine, la rilevanza e l'esattezza delle comunicazioni vengono verificate a scadenza regolare (cfr. art. 44, Controllo della qualità). I dati possono quindi essere copiati da un sistema all'altro e soggiacciono alle direttive previste per ciascuno dei sistemi d'informazione in cui sono trattati.

La correlazione dei dati nei sistemi, già oggi praticata per i sistemi ISIS e ISAS, migliora la qualità dell'archiviazione e le possibilità di analisi rispetto alla semplice

registrazione di singoli oggetti. Ad esempio, consente di cogliere e illustrare in modo efficiente le relazioni esistenti tra persone o eventi. Per questo motivo il *capoverso 4* istituisce una base legale esplicita per simili correlazioni e per l'impiego di programmi di ricerca e di analisi automatizzati.

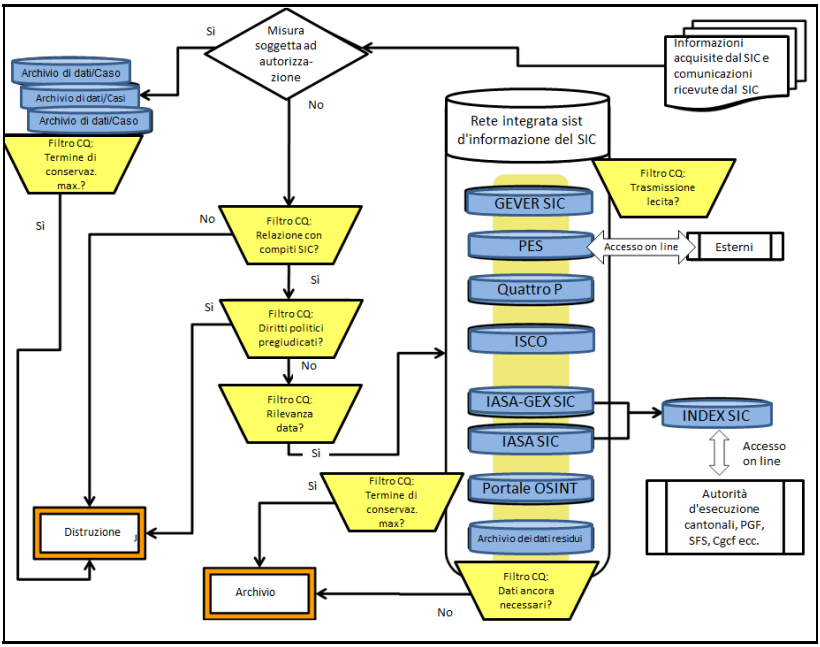
Art. 44 Controllo della qualità

I vari rapporti degli organi di vigilanza hanno regolarmente evidenziato quanto sia importante, per la qualità dei dati, poter contare su un controllo della qualità affidabile e di facile applicazione. L'istituzione di un organo interno incaricato del controllo della qualità in seno al SIC si è dimostrata una valida soluzione e viene ora sancita anche nella legge. Gli strumenti destinati al controllo della qualità vengono impiegati in modo mirato in analogia al modello differenziato previsto per il trattamento dei dati:

- un controllo diretto e capillare da parte dell'organo interno di controllo della qualità è previsto al momento del trattamento dei dati nel settore dell'estremismo violento (cpv. 5 lett. a) e al momento della registrazione dei rapporti cantonali nell'INDEX SIC (art. 5 lett. b). Mentre negli ambiti dello spionaggio, della proliferazione e del terrorismo si osservano perlopiù tendenze di durata pluriennale, per quanto riguarda la qualità dei dati sull'estremismo violento occorre invece aspettarsi fasi di emivita dei dati molto più brevi. In quest'ultimo ambito, il rischio che un sistema sia sommerso di dati ormai inutili è da considerarsi molto più elevato e questo giustifica pertanto cicli di verifica più brevi. Le condizioni severe in materia di trattamento dei dati per le banche dati cantonali nel campo d'applicazione della LMSI impongono un'altrettanto rigorosa verifica e cancellazione periodica dei rapporti cantonali e dei relativi lavori preparatori. La centralizzazione a livello federale della titolarità dei dati non deve coincidere con un allentamento di tali condizioni;
- per tutti gli altri sistemi d'informazione del SIC, la responsabilità della periodica esecuzione dei controlli di qualità spetta in primo luogo agli utenti (cpv. 4). L'organo interno incaricato del controllo della qualità provvede per mezzo di corsi di formazione, direttive e controlli alla corretta applicazione dei filtri prescritti per il trattamento dei dati. È previsto che sarà dato accesso ai sistemi d'informazione soltanto ai collaboratori che hanno superato con successo il relativo esame;
- l'organo interno incaricato del controllo della qualità verifica per campionamento la legalità, l'adeguatezza e l'efficacia del trattamento dei dati in tutti i sistemi. Questi criteri corrispondono a quelli definiti per gli organi di vigilanza (art. 73 segg.). I riscontri che se ne traggono saranno a loro volta integrati nella formazione degli utenti;
- per quanto riguarda l'Archivio dei dati residui, sarà effettuato periodicamente un controllo delle comunicazioni affinché rimangano memorizzate soltanto quelle che soddisferebbero i requisiti previsti per la registrazione iniziale. Il controllo non consisterà in una verifica capillare di tutti i dati personali, bensì in una verifica della rilevanza e dell'esattezza dell'entrata di informazioni nel suo insieme (cfr. art. 56 cpv. 2).

Concretamente, le fasi di selezione intese a garantire un'elevata qualità dei dati in seno al SIC sono le seguenti:

- selezione d'entrata: limitazione ai dati personali che possono essere trattati in base al mandato legale, rispetto dei diritti politici, verifica dell'esattezza e della rilevanza di tutti i dati;
- verifica periodica: periodicamente si verifica che i dati personali memorizzati nei sistemi d'informazione del SIC siano ancora necessari all'adempimento dei compiti previsti dalla presente legge (verifica della rilevanza). La verifica comprende di volta in volta l'intero record di dati personali. Conseguentemente, tutti i dati registrati relativi una determinata persona o organizzazione vengono confermati oppure cancellati. Questo corrisponde alla collaudata prassi in ISIS come pure alla procedura applicata da servizi partner del SIC nella misura in cui essi provvedono a una verifica periodica dei dati;
- selezione d'uscita: i dati personali possono avere effetti all'esterno soltanto se il trattamento è lecito (cfr. art. 58);
- termini di conservazione massimi: il Consiglio federale stabilisce per ciascun sistema d'informazione il termine di conservazione massimo dei dati.



I *capoversi 1 e 2* definiscono la valutazione iniziale alla quale il SIC procede prima di registrare qualsiasi dato in un sistema d'informazione.

Determinante secondo il *capoverso 1* è la rilevanza ed esattezza dei dati personali. Per il sistema Archivio dei dati residui, nel quale i dati non sono ordinati con riferi-

mento a persone o oggetti, tale valutazione non viene effettuata per i singoli dati personali di una comunicazione, bensì per la comunicazione nel suo insieme.

Secondo il *capoverso 2*, il SIC può trattare solo i dati che presentano un nesso con l'adempimento dei compiti assegnatigli dalla legge (art. 6 cpv. 1). Concretamente, procedendo a un controllo al momento dell'entrata dei dati, il SIC deve garantire già prima della registrazione dei dati in uno dei suoi sistemi d'informazione che il contenuto delle comunicazioni e informazioni ricevute abbia un nesso con l'estremismo violento, il terrorismo, lo spionaggio, la proliferazione, gli attacchi a infrastrutture critiche o con fatti rilevanti per la politica di sicurezza. Devono inoltre essere rispettati i limiti posti al trattamento dei dati, a tutela dei diritti politici (art. 5 cpv. 5–8).

Soprattutto le comunicazioni delle autorità d'esecuzione cantonali possono essere rinviate loro affinché procedano a completare gli accertamenti, se tali comunicazioni non sono ancora sufficienti per un trattamento da parte del SIC. Se il SIC non è competente per il trattamento, il mittente può avere un interesse o una competenza propri per trattare ulteriormente un affare annunciato. Anche in simili casi ha luogo un rinvio al mittente.

Secondo il *capoverso 4,* il SIC verifica periodicamente i dati personali memorizzati in tutti i suoi sistemi d'informazione. Cancella dai suoi sistemi i dati che non gli servono più per l'adempimento dei suoi compiti e provvede alla loro archiviazione conformemente alle prescrizioni dell'Archivio federale (art. 67). Durante la procedura di consultazione, in singoli casi è stato chiesto di rinunciare a registrazioni multiple (ossia alla registrazione della medesima persona in più sistemi) oppure di verificare regolarmente simili registrazioni. Il nostro Collegio non ritiene tuttavia appropriate simili restrizioni, poiché una registrazione multipla è ad esempio obbligatoria nei sistemi riservati esclusivamente al SIC e nel sistema INDEX SIC. Le registrazioni multiple sono necessarie e opportune soprattutto a causa dell'architettura comprendente numerosi sistemi con differenti contenuti e scopi. I dati si trovano pertanto sempre là dove devono essere in funzione del nesso materiale e soggiacciono alle regolamentazioni in materia di verifica e di controllo della qualità valevoli per il rispettivo sistema. Se tali regolamentazioni sono rispettate, non è possibile aspettarsi che una verifica supplementare delle registrazioni multiple giunga ad altre valutazioni.

Art. 45 Trattamento dei dati nei Cantoni

Il *capoverso 1* si fonda sulla seguente concezione: nella misura in cui operano nel campo d'applicazione della presente legge, le autorità d'esecuzione cantonali si avvalgono esclusivamente dei sistemi d'informazione che la Confederazione mette loro a disposizione. Nel sistema INDEX SIC, ad esempio, i Cantoni possono registrare gli accertamenti preliminari condotti in vista della redazione di rapporti destinati alla Confederazione, gestire i propri mandati e archiviare i propri rapporti (art. 50). I dati sono amministrati esclusivamente dalla Confederazione, ossia dal SIC, e sottostanno al diritto federale in materia di protezione dei dati. Nel campo d'applicazione della presente legge, la Confederazione sarà l'unico detentore dei dati.

Il *capoverso 2* concerne i dati trattati dai Cantoni nell'ambito dei compiti di intelligence cantonali di loro competenza (ossia che non rientrano nella competenza della Confederazione rispettivamente del SIC) oppure nell'adempimento di altri

compiti in materia di polizia di sicurezza o di polizia giudiziaria. Tra le competenze proprie dei Cantoni rientra ad esempio il trattamento dei dati relativi alle domande di autorizzazione per le manifestazioni. Se si temono scontri di matrice estremista violenta, il SIC tratta i relativi dati anche da questo punto di vista. Se la manifestazione degenera effettivamente nella violenza, il SIC tratta queste informazioni dal profilo dell'estremismo violento ai sensi della presente legge, mentre la competenza propria delle autorità cantonali riguarda il perseguimento dei reati, ad esempio danneggiamento, sommossa o lesioni. Considerate le diverse regole applicabili all'informazione degli interessati in merito al trattamento di questi dati («diritto d'accesso» secondo la LPD), occorre evitare che una banca dati contenga rimandi all'altra. Le disposizioni d'esecuzione possono prevedere eccezioni in particolare per le comunicazioni che non contengono alcun dato personale o nel caso in cui le persone interessate siano a conoscenza del duplice trattamento, ad esempio perché ne sono state informate durante un interrogatorio.

In seguito alla consultazione, l'articolo è stato completato con il *capoverso 3* che consente l'utilizzazione dei risultati delle valutazioni della situazione all'interno dei Cantoni; questo è possibile già oggi nel quadro delle regolamentazioni della LMSI. Sono state completate e precisate anche le disposizioni concernenti la conservazione dei dati nei Cantoni (art. 50) e il controllo e la vigilanza cantonali (art. 78).

Art. 46 Sistemi d'informazione del SIC

L'articolo 46 definisce la rete integrata di sistemi d'informazione che il SIC gestisce per l'adempimento dei propri compiti. Questa rete è comparabile alla rete dei sistemi d'informazione di polizia prevista dalla legge federale del 13 giugno 2008[31] sui sistemi d'informazione di polizia della Confederazione (LSIP; cfr. art. 2 LSIP).

Questo articolo offre una panoramica di tutti i sistemi d'informazione del SIC, per i quali il presente disegno di legge fornisce le basi legali formali. Ciascun sistema d'informazione è in seguito trattato in un articolo specifico.

Il *capoverso 2* delega al Consiglio federale il compito di disciplinare i dettagli del trattamento dei dati per ogni sistema d'informazione. Tra i dettagli da disciplinare figurano in particolare anche i termini applicabili alle verifiche periodiche e la durata massima di conservazione. La delega al Consiglio federale del disciplinamento di dettaglio corrisponde alla vigente normativa e alla procedura comunemente utilizzata in materia di sistemi d'informazione. Nel sistema vigente, ad esempio, la durata massima di conservazione dei dati è stabilita nell'ordinanza del 4 dicembre 2009[32] sui sistemi d'informazione del Servizio delle attività informative della Confederazione (OSI-SIC). Per i dati provenienti dall'attività informativa all'estero, tale termine è di 30 anni dall'ultimo trattamento, ma al massimo di 45 anni. Per i dati acquisiti in Svizzera il termine varia, a dipendenza della provenienza dei dati, da cinque anni (dati dei controlli di sicurezza relativi alle persone) a 45 anni (dati provenienti da fonti pubblicamente accessibili). L'OSI-SIC stabilisce anche i termini per le verifiche dei dati dell'attività informativa in Svizzera, che sono di cinque anni dalla prima registrazione; in seguito i dati sono sottoposti a una valutazione periodica ogni tre anni, fino al raggiungimento della durata massima di conservazione. La LAIn dispone a questo riguardo che nel definire i termini il Consiglio federale deve

31 RS **361**
32 RS **121.2**

tener conto delle peculiarità dei dati, rispettivamente delle esigenze specifiche dei settori di compiti. Come sinora, occorrerà dunque prevedere soluzioni differenziate per i singoli sistemi e per le singole categorie di dati.

Le disposizioni d'esecuzione conterranno regolamentazioni dettagliate che preciseranno quali persone sono autorizzate a effettuare i differenti trattamenti dei dati (come leggere, scrivere, modificare, cancellare), quali persone sono autorizzate a eseguire le consultazioni di dati in più sistemi e le relative modalità, nonché quali autorità dei Cantoni e della Confederazione degli ambiti della polizia, della giustizia e del perseguimento penale al di fuori del SIC possono accedere all'INDEX SIC.

Per il resto, il SIC emanerà per tutti i sistemi d'informazione regolamenti sul trattamento dei dati conformi alle norme generali in materia di protezione dei dati e delle informazioni, che definiranno in particolare l'organizzazione interna, la procedura di trattamento e controllo e la documentazione a livello di progettazione, realizzazione e gestione della collezione di dati e dei mezzi informatici.

Art. 47 Assegnazione dei dati ai sistemi d'informazione

Quando riceve nuovi dati, il SIC ne valuta dapprima sia la rilevanza per l'adempimento dei propri compiti sia l'esattezza. Dopodiché il competente servizio del SIC li assegna al sistema previsto per il rispettivo genere di dati. Ai sistemi IASA SIC e INDEX SIC non vengono assegnati direttamente dati. IASA SIC serve agli analisti del SIC per riunire, analizzare e documentare i dati e i riscontri necessari per la produzione. Nell'INDEX SIC il SIC immette soprattutto i dati relativi all'identificazione di persone, organizzazioni, oggetti ed eventi che vengono copiati nell'INDEX SIC dai sistemi IASA SIC e IASA-GEX SIC.

Art. 48 IASA SIC

L'articolo 48 fornisce la base legale formale per il sistema di analisi integrale del SIC (IASA SIC), utilizzato per l'analisi informativa in tutti i settori di compiti del SIC eccettuato quello dell'estremismo violento. Secondo il nuovo disciplinamento, i dati relativi all'estremismo violento possono essere trattati esclusivamente nel sistema IASA-GEX SIC (art. 49). IASA SIC sostituisce dunque ampiamente gli attuali Sistema d'informazione Sicurezza interna (ISIS) e Sistema d'informazione Sicurezza esterna (ISAS).

Gli ambiti specialistici responsabili della registrazione eseguono nel loro ambito specifico le verifiche periodiche dei dati memorizzati in IASA SIC. L'organo interno incaricato del controllo della qualità effettua inoltre controlli periodici per campionamento allo scopo di verificare la conformità legale del trattamento (cfr. art. 44).

Art. 49 IASA-GEX SIC

I dati riguardanti l'estremismo violento sono frequentemente caratterizzati da un nesso più esclusivo con la Svizzera rispetto ai dati di altri ambiti di attività del SIC. Spesso sono anche più delicati, poiché presentano una maggiore contiguità con l'attività politica, sottratta all'acquisizione e al trattamento di informazioni in virtù dell'articolo 5 capoverso 5 LAIn, e tutelata dalla Cost. Perciò, il SIC registra questi dati in un sistema d'informazione distinto, il sistema di analisi integrale dell'estremismo violento (IASA-GEX SIC) riservato alla registrazione, al trattamento e all'analisi centralizzati di tutti i dati che rientrano in questo settore. I dati immessi in

questo sistema soggiacciono inoltre a controlli più severi e frequenti da parte dell'organo interno del SIC incaricato del controllo della qualità (art. 44 cpv. 5 lett. a).

In virtù dell'articolo 69 capoverso 1 lettera c, il Consiglio federale determina ogni anno i gruppi da considerare di matrice estremista violenta.

Art. 50 INDEX SIC

INDEX SIC serve ad accertare se il SIC tratta dati concernenti una determinata persona, un'organizzazione, un oggetto o un evento. In questo sistema sono consultabili tutte le persone registrate in IASA SIC e IASA-GEX SIC. In pratica, nell'INDEX SIC vengono inseriti i principali dati di identificazione, per le persone ad esempio il nome, la data di nascita, la nazionalità ecc. A questo indice hanno accesso anche i servizi autorizzati che non sono allacciati alla rete particolarmente protetta del SIC.

INDEX SIC serve dunque a coordinare le attività di intelligence di Confederazione e Cantoni, ma garantisce anche il coordinamento tra attività in ambito di intelligence e attività in materia di polizia di sicurezza e giudiziaria. Questo coordinamento è attualmente assicurato consentendo a servizi esterni al SIC un accesso diretto a ISIS limitato ai dati di identificazione. I servizi esterni al SIC e le autorità d'esecuzione cantonali sono autorizzati ad accedere soltanto ai dati di identificazione e non al resto delle informazioni. Per ottenere eventualmente ulteriori dati devono rivolgersi al SIC seguendo le vie formali previste per la collaborazione e la trasmissione di dati (art. 58 segg.).

INDEX SIC è necessario per questo scopo, poiché per ragioni di sicurezza IASA SIC e IASA-GEX SIC devono essere gestiti nella rete particolarmente protetta del SIC, alla quale non è possibile accedere dall'esterno del SIC. INDEX SIC consente ai servizi terzi autorizzati di ricercare rapidamente i dati di identificazione mentre i dati completi del SIC rimangono protetti dagli accessi esterni.

INDEX SIC serve pure da piattaforma per il trattamento dei dati da parte delle autorità cantonali. In tale sistema queste ultime trattano i dati prima di redigere i rapporti destinati al SIC. Il sistema consente loro anche di avere una panoramica dei mandati della Confederazione e di archiviare i loro dati. Questa centralizzazione di tutti i trattamenti di dati previsti dal presente disegno di legge garantisce un disciplinamento e un controllo unitari a livello federale.

In occasione della consultazione qualche Cantone ha espresso il desiderio che i Cantoni possano avere reciprocamente accesso ai loro dati cantonali. Dagli accertamenti è risultato che vi era piuttosto la necessità di una trasmissione sicura dei dati tra Cantoni. Questa richiesta è stata di conseguenza considerata nel capoverso 2.

Art. 51 GEVER SIC

Il sistema d'informazione per la gestione degli affari del SIC (GEVER SIC) è un sistema standard di gestione degli affari analogo a quello in uso in altri settori dell'Amministrazione federale. Per le sue caratteristiche, tuttavia, il SIC tratta soprattutto affari di intelligence quali rapporti d'analisi, valutazioni della situazione scritte o orali o risposte a singole richieste. In questo sistema centrale vengono gestiti tali affari e gli affari prettamente amministrativi (per es. pareri nell'ambito di consultazioni degli uffici, processi finanziari, affari del personale ecc.), in modo da

disporre di una panoramica e di un controllo di tutti gli affari in corso e conclusi. L'archiviazione dei prodotti del SIC è assicurata grazie a GEVER SIC mediante il sistema di ordinamento definito in collaborazione con l'Archivio federale.

Per garantire la protezione dei dati di intelligence, il SIC gestisce anche il GEVER SIC nella propria rete particolarmente protetta, alla quale nessun servizio terzo è autorizzato ad accedere.

Art. 52 PES

L'articolo 52 riprende dall'articolo 10*a* LMSI la base legale formale del sistema d'informazione del SIC per la presentazione elettronica della situazione (PES). Il disciplinamento previsto corrisponde ampiamente a quello introdotto nella LMSI con la modifica del 23 dicembre 2011, entrata in vigore il 16 luglio 2012.

Nella PES vengono registrati dati personali soltanto se sono assolutamente necessari per la presentazione e la valutazione della situazione.

Nell'ambito del progetto LMSI II l'accesso concesso a privati o autorità estere ha sollevato intense discussioni. La prassi attuale ha confermato l'applicazione restrittiva di questa disposizione da parte del SIC. Tuttavia, il nostro Collegio rimane del parere che la Svizzera, in quanto Paese ospite di eventi internazionali, debba garantire la sicurezza delle manifestazioni che accoglie in collaborazione con privati e partner esteri. Le esperienze maturate ad esempio nel contesto di EURO 08 mostrano che per le manifestazioni importanti caratterizzate da un potenziale di rischio accresciuto può essere necessario consentire anche a organizzazioni private o ad autorità estere di accedere senza indugio a determinati dati della PES SIC. In tale contesto occorre sempre garantire il rispetto del principio di proporzionalità; in altri termini, il SIC concede l'accesso soltanto ai dati necessari per affrontare le minacce specifiche.

Art. 53 Portale OSINT

L'articolo 53 fornisce la base legale formale per il Portale «Open Source Intelligence» (Portale OSINT), sistema del SIC per lo sfruttamento dei dati accessibili al pubblico. La memorizzazione di dati disponibili in Internet è ad esempio indispensabile per un'analisi mirata, poiché altrimenti occorrerebbe ogni volta ripetere le ricerche in tutta la rete Internet e inoltre dati precedentemente reperibili in Internet potrebbero non essere più disponibili.

Trattandosi di dati che di principio sono accessibili a chiunque, anche all'interno del SIC devono essere trattati meno restrittivamente rispetto a dati da altre fonti. Pertanto, nel *capoverso 3* non è opportuno limitarne l'accesso all'interno del SIC.

Come auspicato dai Cantoni in occasione della consultazione, il *capoverso 4* è stato completato in modo da consentire alle autorità d'esecuzione cantonali l'accesso a parti del Portale OSINT. Un accesso integrale non sarebbe possibile, tra l'altro per motivi inerenti ai diritti d'autore.

Art. 54 Quattro P

Attualmente gli organi incaricati dei controlli di frontiera presso gli aeroporti svizzeri registrano già per il SIC i dati relativi all'entrata di determinate persone provenienti da certi Paesi ai fini dell'individuazione tempestiva di attività di spionaggio e

proliferazione. Il SIC tratterà questi dati in un sistema d'informazione distinto denominato Quattro P («Programme préventif de contrôle des passeports», sinora compreso nel «Modulo informatico P4» di cui all'art. 25 cpv. 1 lett. h OSI-SIC). Le formulazioni di questo articolo nell'avamprogetto sono state all'origine di alcuni malintesi, motivo per cui è stato riformulato in modo più preciso.

Secondo il *capoverso 3*, l'accesso a questo sistema è consentito soltanto a una ristretta cerchia di persone all'interno del SIC (attualmente meno di dieci) incaricate della registrazione, della consultazione e dell'analisi di questi dati. Per questo motivo anche in futuro non è previsto alcun accesso per i Cantoni.

Secondo il *capoverso 4*, il Consiglio federale stabilisce annualmente l'estensione delle categorie di persone da registrare, ossia i Paesi di provenienza determinanti ed eventuali restrizioni a determinate categorie di persone (per es. soltanto gli uomini adulti o i titolari di determinati tipi di passaporto). La procedura è analoga a quella in virtù dell'articolo 20 capoverso 4 secondo il quale il Consiglio federale stabilisce fatti e constatazioni che devono essere comunicati spontaneamente al SIC. Per i dati inseriti nel sistema Quattro P oggi è prevista una durata massima di conservazione di cinque anni (art. 33 cpv. 1 lett. i OSI-SIC).

Art. 55 ISCO

Il sistema d'informazione COMINT (ISCO) serve al SIC per amministrare e gestire i propri mandati che affida al COE. La direzione delle attività di esplorazione radio e di esplorazione dei segnali via cavo avviene mediante mandati scritti del SIC (cfr. art. 37 segg.). Essi precisano il mandato di esplorazione, le informazioni sugli oggetti concreti dell'esplorazione, i risultati attesi e altre condizioni quadro per lo svolgimento del mandato. Nel sistema ISCO sono registrati anche i risultati delle verifiche periodiche interne della legalità, dell'adeguatezza e dell'efficacia delle misure di esplorazione. I dati contenuti nel sistema servono come base per le attività degli organi di vigilanza (in particolare l'Autorità di controllo indipendente, cfr. art. 75).

Al sistema ISCO hanno accesso soltanto pochissimi collaboratori del SIC (attualmente meno di dieci persone) che si occupano direttamente della direzione dei mandati.

I risultati dell'esplorazione radio e dei segnali via cavo destinati all'analisi e all'utilizzazione in prodotti, esposizioni della situazione ecc. vengono registrati nell'Archivio dei dati residui (art. 56).

Art. 56 Archivio dei dati residui

Nell'Archivio dei dati residui il SIC memorizza tutte le informazioni che non ha potuto assegnare a un altro sistema nell'ambito della selezione che segue la verifica in entrata. Si tratta soprattutto delle comunicazioni pervenute da autorità di sicurezza estere, di dati ottenuti con l'esplorazione radio e di segnali via cavo, di fonti umane e di informazioni che non sono state attivamente acquisite dal SIC. L'Archivio dei dati residui non contiene dati sull'estremismo violento, poiché questi dati vengono tutti registrati e trattati nel sistema IASA-GEX SIC.

Le informazioni tratte dall'Archivio dei dati residui vengono trasferite nel sistema IASA SIC soprattutto per fini di analisi, nel caso in cui servano per allestire prodotti di intelligence o per l'aggiornamento della situazione, per studi o simili.

Il SIC effettua controlli periodici per assicurare che l'Archivio dei dati residui contenga soltanto informazioni che soddisfano i criteri attuali di rilevanza (nesso con un settore di compiti del SIC, rispetto dell'art. 5 cpv. 5–8 LAIn) ed esattezza definiti per il loro trattamento. I dati che non soddisfano più questi criteri vengono distrutti e le informazioni inesatte ma ancora necessarie vengono designate come tali. Come nel caso della verifica in entrata, la valutazione periodica viene effettuata per la comunicazione nel suo insieme, ossia non si procede alla verifica dei singoli elementi contenuti in un ampio documento, per esempio una lista di persone.

Art. 57 Dati provenienti da misure di acquisizione soggette ad autorizzazione

I dati acquisiti ricorrendo a misure di acquisizione soggette ad autorizzazione che impiegano mezzi tecnologici (come per es. nei casi di sorveglianza delle comunicazioni) possono essere molto voluminosi, ma possono anche contenere molte informazioni che non hanno niente a che fare con l'obiettivo dell'esplorazione, ad esempio perché sono di natura strettamente privata. Inoltre occorre considerare la protezione della personalità di terzi che utilizzano ad esempio il collegamento di telecomunicazione della persona sorvegliata. Spesso non è nemmeno possibile constatare di primo acchito se una determinata comunicazione sia rilevante o meno, ad esempio perché la rete di contatti della persona sorvegliata deve ancora essere individuata, oppure perché nella comunicazione la persona in questione utilizza elementi cospirativi per proteggere tali contatti. Perciò non è possibile determinare subito se queste comunicazioni siano o non siano necessarie.

La memorizzazione in un sistema distinto serve non da ultimo anche a proteggere l'infrastruttura informatica del SIC, poiché nell'ambito della sorveglianza di comunicazioni via Internet o dell'introduzione in sistemi informatici si possono incontrare anche malware (virus, cavalli di Troia). I sistemi del SIC devono essere imperativamente protetti da questo tipo di contagio.

Per questa ragione l'articolo 57 dispone che i dati provenienti da questo genere di misure di acquisizione soggette ad autorizzazione devono essere memorizzati in sistemi d'informazione separati dalla rete integrata ed essere consultati in questi sistemi separati. Secondo il *capoverso 2*, il SIC può archiviare per ulteriore analisi negli appositi sistemi d'informazione della rete integrata, ossia in genere nel IASA SIC, soltanto i dati necessari all'adempimento del mandato.

Per i dati acquisiti all'estero con misure comparabili, l'articolo 35 capoverso 5 prevede un'analoga possibilità di memorizzazione separata.

Il *capoverso 3* limita pertanto la cerchia delle persone autorizzate ad accedere a questi dati ai soli collaboratori del SIC direttamente incaricati dell'esecuzione della misura di acquisizione e dell'analisi dei risultati. Si tratterà di norma dei collaboratori competenti per l'acquisizione e l'analisi incaricati di elaborare il caso in questione.

I sistemi di memorizzazione che entrano in considerazione saranno di regola sistemi informatici non collegati alle rete protetta del SIC. Anche in questo caso il Consiglio federale disciplinerà in un'ordinanza gli usuali dettagli (record di dati, diritti di trattamento e autorizzazioni d'accesso ecc.).

Art. 58 Verifica prima della trasmissione

Oltre ai servizi del SIC incaricati specificamente del controllo della qualità, anche ogni persona che partecipa alla comunicazione di informazioni del SIC è tenuta a controllare la qualità dei dati prima di procedere alla trasmissione. Queste persone sono tenute ad assicurarsi che le condizioni cui la legge subordina la trasmissione siano adempiute e che i dati personali siano trattati in modo corretto.

Art. 59 Trasmissione di dati personali ad autorità svizzere

Per adempiere il proprio compito di allarme precoce e di prevenzione, il SIC deve poter trasmettere dati personali ad autorità politiche, autorità di perseguimento penale, autorità giudiziarie e di sicurezza. La regolamentazione prevista corrisponde ampiamente a quella vigente (art. 17 LMSI), ma nella LAIn è stata ulteriormente sviluppata e differenziata.

L'introduzione di ulteriori meccanismi di protezione è necessaria segnatamente per quanto riguarda la trasmissione di dati provenienti da misure di acquisizione soggette ad autorizzazione. Tali meccanismi devono impedire che reati di minima importanza, scoperti ad esempio nell'ambito della sorveglianza delle telecomunicazioni, vengano comunicati alle autorità di perseguimento penale. Il Codice di procedura penale contiene una disposizione comparabile per questi casi, denominati reperti casuali (art. 278 CPP). Di conseguenza, nel *capoverso 3* la LAIn riprende il principio che limita l'utilizzazione di dati relativi a reati ai soli casi per il cui perseguimento anche in virtù delle norme di procedura penale avrebbe potuto essere ordinata una misura di sorveglianza comparabile. Un'ulteriore armonizzazione con il diritto processuale penale non è tuttavia opportuna poiché la LAIn ha in primo luogo scopi diversi dal perseguimento penale e anche altri settori dell'amministrazione sono tenuti a trasmettere alle autorità di perseguimento penale le informazioni di cui dispongono in merito a eventuali reati.

Durante la consultazione sono state formulate richieste in parte contraddittorie che chiedevano una trasmissione più ampia o più ridotta di dati alle autorità di perseguimento penale. Il nostro Collegio ritiene che il disegno di legge discusso in questa sede rappresenti una soluzione equilibrata.

Art. 60 Trasmissione di dati personali ad autorità estere

Questo articolo riprende ampiamente le disposizioni dell'articolo 17 LMSI. La legislazione in materia di protezione dei dati stabilisce che di norma i dati personali possono essere trasmessi soltanto agli Stati la cui legislazione garantisce un livello di protezione dei dati comparabile a quello svizzero (cfr. art. 6 cpv. 1 LPD). Con questa disposizione sarebbero esclusi dalla collaborazione con il SIC la maggior parte dei Paesi extraeuropei, salvo qualora nella fattispecie trovassero applicazione le restrittive eccezioni di cui all'articolo 6 capoverso 1 LPD. Questa esclusione costringerebbe il SIC a rinunciare a importanti fonti d'informazione proprio nelle regioni di crisi.

La vigente LMSI contempla già regole speciali per la collaborazione in ambito informativo con l'estero e la trasmissione di dati personali; queste regole vengono riprese nel presente articolo della LAIn. Al riguardo esiste una prassi di lunga data, seguita e controllata dagli organi di vigilanza (vigilanza sui servizi informazioni da

parte del DDPS [in precedenza da parte del DFGP] e della Delegazione delle Commissioni della gestione delle Camere federali).

La collaborazione e lo scambio di dati con autorità di sicurezza estere che non sono servizi informazioni in senso stretto si limita alle rispettive funzioni comparabili con i compiti del SIC. La collaborazione di altri servizi svizzeri con autorità di sicurezza estere nelle rispettive sfere di competenza non ne risulta limitata ed essi sono competenti per la trasmissione dei loro dati secondo le rispettive basi legali.

Il *capoverso 2 lettera d* concerne le richieste di nullaosta (richieste clearing) di cui tratta anche l'articolo 12 capoverso 1 lettera d, a favore di persone (di norma cittadini svizzeri) che dovrebbero avere accesso all'estero a progetti, informazioni, impianti ecc. classificati. Queste informazioni sono in genere nell'interesse della persona in questione, la quale altrimenti non potrebbe assumere un posto di lavoro o svolgere un'attività commerciale.

Art. 61 Trasmissione di dati personali a terzi

Le attività informative esigono talvolta che vengano trasmessi dati anche a terzi privati. Il caso d'applicazione più frequente è rappresentato dalla necessità di motivare una propria richiesta di informazioni. Nel raccogliere informazioni su una persona fisica o giuridica il SIC deve evidentemente poter indicare alla persona interrogata qual è la persona sulla quale chiede informazioni e in quale contesto. La disposizione corrisponde al vigente articolo 17 capoverso 3 LMSI.

Art. 62–65 Diritto d'accesso

Per quanto riguarda il diritto d'accesso, il disegno riprende ampiamente, sotto il profilo dei contenuti, la soluzione adottata dal Parlamento nel quadro della «LMSI II ridotta», la quale si ispira a sua volta alla LSIP. Contrariamente all'articolo 18 LMSI in vigore dal 16 giugno 2012, in questa sede la regolamentazione è suddivisa in più articoli, ciò che ne migliora la leggibilità e la comprensibilità.

Il vecchio diritto d'accesso indiretto secondo la LMSI era stato giudicato conforme alla Costituzione federale qualora fosse dotato di una possibilità di ricorso efficace. Il progetto iniziale della LMSI II conteneva pertanto una simile soluzione che tuttavia è stata respinta. Il Consiglio federale aveva successivamente proposto l'applicazione integrale della LPD anche nella LMSI. Il Parlamento ha però deciso consapevolmente a favore di una soluzione analoga a quella della LSIP. Anche oggi il nostro Collegio continua a ritenere che vi siano altre soluzioni realizzabili, ma non considera opportuno presentare nuovamente al Parlamento, nella LAIn, un altro disciplinamento in materia di diritto d'accesso.

La procedura prevede che il SIC esamini dapprima una domanda di informazioni ma differisca l'informazione in presenza di interessi al mantenimento del segreto o qualora si tratti di una persona non registrata. Dopo aver ricevuto comunicazione del differimento, la persona interessata può rivolgersi all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), che applica per analogia la procedura dell'informazione indiretta.

Derogando alla vigente regolamentazione prevista dalla LMSI, nell'articolo 63 capoverso 5 proponiamo di tornare alla formulazione originaria prevista dalla LSIP. La LSIP prevede su questo punto che se la comunicazione è stata differita (in virtù di interessi al mantenimento del segreto o perché la persona non è registrata), le

informazioni possono eccezionalmente essere fornite se l'IFPDT lo raccomanda e se e nella misura in cui ciò non pregiudichi la sicurezza interna o esterna, a condizione che la persona interessata renda verosimile che il differimento dell'informazione le arrecherebbe un danno rilevante e irreparabile.

Su questo elemento la LMSI inverte l'onere della prova rispetto alla LSIP, stabilendo che il SIC può fornire informazioni su raccomandazione dell'IFPDT se e nella misura in cui ciò non pregiudichi la sicurezza interna o esterna. Per le persone non registrate, tuttavia, il SIC non è in grado di fornire questa dimostrazione, poiché non dispone appunto di informazioni sulla persona in questione. Questa soluzione vanificherebbe la regola prevista nell'articolo 62 capoverso 2 lettera c, la quale dispone di differire l'informazione se il richiedente non è registrato. Si ritiene pertanto che nel caso del progetto di legge discusso in questa sede la procedura secondo la LSIP sia oggettivamente corretta.

Art. 66 Deroga al principio di trasparenza

Le esperienze maturate dal SIC dalla sua istituzione per quanto riguarda le domande di consultazione fondate sulla legge del 17 dicembre 2004[33] sulla trasparenza (LTras) hanno evidenziato che il bisogno di protezione particolare delle informazioni di intelligence è difficilmente compatibile con lo spirito di trasparenza preconizzato dalla LTras.

Le domande di accesso presentate finora riguardavano prevalentemente documenti e dossier concernenti l'acquisizione di informazioni da parte del SIC oppure operazioni eseguite dal SIC (o dalle organizzazioni che l'hanno preceduto). Puntualmente è stata chiesta espressamente la consultazione di altri documenti, per esempio riguardanti i contatti con servizi informazioni e autorità di sicurezza esteri. In considerazione delle persone o dei servizi esteri implicati e in sintonia con le regolamentazioni eccezionali della LTras, il SIC, dopo un esame approfondito e la redazione una motivazione interna, deve ogni volta rifiutare l'accesso ai dossier riguardanti l'acquisizione e la collaborazione. Di conseguenza non è opportuno mantenere il principio secondo il quale debba essere concessa la consultazione di documenti sull'acquisizione informativa quando è evidente sin dall'inizio che essi sottostanno alle disposizioni derogatorie della LTras.

È stata esaminata la questione della necessità di escludere integralmente il SIC dal campo d'applicazione della LTras. Tuttavia, poiché esso gestisce anche pratiche puramente amministrative per le quali è senz'altro possibile dare informazioni sulla base della LTras, proponiamo soltanto un'eccezione materiale per i documenti concernenti l'acquisizione di informazioni di intelligence.

Art. 67 Archiviazione

I dati e i documenti del SIC soggiacciono di principio alla legge federale del 26 giugno 1998[34] sull'archiviazione, che prevede un'archiviazione integrale di tutti i documenti che l'Archivio federale considera degni di essere archiviati. Tuttavia, tra i documenti del servizio informazioni vi sono anche documenti provenienti da servizi partner esteri che sono stati trasmessi soltanto con la riserva della protezione delle

33 RS **152.3**
34 RS **152.1**

fonti. Se una tale protezione non è più garantita, le informazioni si esaurirebbero e la Svizzera si troverebbe isolata nella lotta contro minacce globali quali il terrorismo, la non proliferazione, l'estremismo violento e lo spionaggio.

Nei *capoversi 1 e 2* l'articolo considera l'interesse dell'Archivio federale a un'archiviazione per quanto possibile integrale ma anche l'interesse legittimo delle autorità di sicurezza a una protezione delle fonti efficace. I dati e i documenti del SIC sono archiviati integralmente dall'Archivio federale in locali particolarmente protetti. In occasione di una domanda concreta di consultazione, già le disposizioni della legge sull'archiviazione prevedono la possibilità di limitare o vietare la consultazione nel singolo caso quando interessi pubblici o privati preponderanti e degni di particolare protezione vi si oppongono. Il capoverso 2 chiarisce che un simile interesse pubblico è dato quando il servizio estero interessato rifiuta in maniera motivata la consultazione. In occasione della consegna, il SIC designerà adeguatamente i documenti interessati affinché l'Archivio federale possa facilmente identificare in quali casi è necessario consultare il SIC. Altri Paesi procedono nello stesso modo per quanto riguarda la Svizzera.

In alcuni casi il SIC deve avere la possibilità di consultare dati personali archiviati (*cpv. 3*). Regolamentazioni analoghe si applicano già oggi alle autorità di perseguimento penale. Esempio: il SIC riceve da un servizio informazioni estero una domanda in relazione con la ripresa di accertamenti relativi a un attentato terroristico. Il SIC ha tuttavia già cancellato e consegnato all'Archivio federale i dati relativi agli accertamenti effettuati a suo tempo in Svizzera.

Art. 68 Prestazioni

Il SIC ha di principio il diritto e l'obbligo, al pari di qualsiasi altro servizio, di fornire assistenza amministrativa negli ambiti di sua competenza nei quali è in grado di farlo anche dal profilo delle risorse di personale e delle conoscenze specialistiche. In questo caso può mettere a disposizione mezzi e metodi operativi, tra cui ad esempio prestazioni nel campo delle trasmissioni, dei trasporti e della consulenza, che mancano agli altri servizi.

I mezzi del SIC per comunicazioni sicure, ad esempio, vengono regolarmente impiegati nell'ambito della gestione internazionale delle crisi (per es. in casi di rapimento), segnatamente cellulari criptati. Gli organi di sicurezza della Confederazione e le organizzazioni internazionali fanno capo alle competenze del SIC nel settore dei sistemi protetti dalle intercettazioni e della protezione delle informazioni, per esempio nella bonifica di locali da dispositivi d'intercettazione. Il SIC consiglia gli organi della Confederazione competenti negli acquisti di casseforti e nelle speciali tecnologie di chiusura dei locali. Inoltre, assiste servizi informazioni e autorità di sicurezza esteri effettuando, tra l'altro, trasporti speciali.

In un caso di rapimento conclusosi positivamente, il SIC ha partecipato alla gestione della crisi fornendo le prestazioni seguenti:

- ha messo a disposizione mezzi per effettuare comunicazioni sicure nei collegamenti tra il Centro di gestione delle crisi del DFAE e la rappresentanza locale del DFAE e ha fornito il supporto tecnico;
- ha fornito i suoi mezzi per effettuare comunicazioni sicure nello scambio quotidiano di informazioni;

– ha installato nella rappresentanza locale un ambiente di lavoro protetto e sicuro, adeguato all'attività sensibile;
– ha messo in permanenza a disposizione dell'ambasciatore svizzero un collaboratore per assicurare il collegamento con il servizio informazioni locale e i rappresentanti di altri servizi informazioni, nonché per analizzare costantemente le informazioni;
– ha appoggiato il Centro di gestione delle crisi con una cellula interna per la valutazione della situazione, l'avvio di contatti con altri servizi informazioni esteri e la collaborazione con altri servizi svizzeri;
– ha garantito le basi per le trattative e le comunicazioni con il servizio informazioni estero competente.

Per contro, ai privati l'appoggio è fornito soltanto a titolo eccezionale e nei casi nei quali sussiste un interesse informativo, e quindi anche pubblico, a fornire tale appoggio. Nel caso di un rapimento può ad esempio rivelarsi necessario equipaggiare anche un familiare della persona rapita con mezzi di comunicazione criptati. In casi particolari l'interesse informativo può anche consistere nella bonifica di locali di aziende private, con la loro autorizzazione, da dispositivi d'intercettazione illegali («cimici», microspie). In questo caso, tuttavia, determinante è l'interesse statale, non i desideri dei privati. Il SIC, in particolare, non deve entrare in concorrenza con offerenti privati di prestazioni comparabili. Se si tratta di tutelare interessi essenziali della Svizzera secondo l'articolo 3, anche il Consiglio federale può incaricare il SIC di fornire simili prestazioni.

Sembra pertanto opportuno istituire una base legale esplicita per queste prestazioni di supporto e le limitazioni alle quali sottostanno.

Art. 69 Direzione politica da parte del Consiglio federale

Il SIC è uno strumento destinato in modo particolare a tutelare gli interessi nazionali e a operare per il Governo federale. Perciò, nella LAIn il ruolo del Consiglio federale nell'ambito della direzione politica e della definizione dell'orientamento delle attività del SIC non deve essere semplicemente ripreso dalle vigenti basi legali, ma va esplicitato e ulteriormente rafforzato. L'articolo 69 riprende dunque vari elementi della vigente legislazione e li riunisce in una disposizione centrale sulla direzione politica. Come per tutti gli altri documenti del SIC, la Delegazione delle Commissioni della gestione avrà naturalmente pieno accesso ai menzionati strumenti della direzione politica.

La *lettera a* riprende il sistema già in uso, che impone al Consiglio federale di assegnare al SIC un mandato strategico fondamentale. Questo mandato si attiene al quadro stabilito dalla legge ma definisce temi e regioni prioritari. A causa delle sue ridotte dimensioni, il SIC non è in grado, soprattutto all'estero, di coprire nella stessa misura tutte le regioni e tutti gli sviluppi in materia di politica di sicurezza. Il mandato strategico fondamentale assegnato dal Consiglio federale gli indica pertanto la direzione da seguire. Per di più, eventi e sviluppi improvvisi possono naturalmente influenzare l'attività del SIC nei limiti previsti dalla legge. Se sviluppi di questo genere hanno ripercussioni a lungo termine, è possibile che sia necessario adeguare il mandato fondamentale prima che trascorra il periodo di verifica ordinario di quattro anni. Tuttavia, la direzione politica deve di principio aspirare alla continuità. L'autorizzazione di un giudice, proposta in maniera puntuale in occasione della

consultazione, non è opportuna per questo strumento di direzione politica. Inoltre, essa sposterebbe la responsabilità dal Consiglio federale al tribunale.

Attualmente il mandato fondamentale è disciplinato a livello di ordinanza (art. 2 cpv. 2 O-SIC). In considerazione della sua importanza e del suo contenuto, è classificato «segreto».

La *lettera b* rimanda alla lista d'osservazione esaurientemente disciplinata nell'articolo 71 e già prevista dal vigente diritto (art. 11 cpv. 3–7 LMSI).

La *lettera c* si riallaccia alla nuova concezione in materia di trattamento dei dati, separando e sottoponendo a un più severo regime il trattamento dei dati sull'estremismo violento. Affinché il SIC applichi in modo univoco questa distinzione, il Consiglio federale designa ogni anno i gruppi di matrice estremista violenta. Nei confronti di tali gruppi, ad esempio, non possono essere adottate misure soggette ad autorizzazione ai sensi degli articoli 25 e seguenti. Inoltre, nell'ambito del trattamento dei dati il SIC inserisce i dati relativi ai gruppi di matrice estremista violenta nell'apposito sistema d'informazione IASA-GEX SIC (art. 49). Nel contempo il Consiglio federale prende atto del numero di persone legate alla galassia dell'estremismo violento ma non ancora attribuibili a un determinato gruppo. Questo gli consente di disporre di una panoramica dell'estremismo violento in Svizzera.

Come già previsto dal diritto vigente, secondo la *lettera f* il Consiglio federale autorizza inoltre la collaborazione del SIC con organi di sicurezza di altri Stati. In questa disposizione ci si riferisce in primo luogo a quei servizi informazioni con cui il SIC intrattiene contatti istituzionalizzati. Questi contatti sono riassunti in un elenco speciale che il DDPS sottopone al Consiglio federale per approvazione.

La collaborazione con autorità estere in ambito di intelligence, soggetta all'autorizzazione del Consiglio federale, normalmente non è disciplinata mediante accordi formali, ad esempio trattati internazionali. In genere si fonda piuttosto su «agreement» o intese non vincolanti e informali conclusi a livello amministrativo.

Il *capoverso 3* prevede che il collegamento del SIC a una banca dati comune gestita insieme a servizi informazioni esteri debba invece essere disciplinato mediante una convenzione internazionale conclusa dal Consiglio federale. Al momento non esistono né banche dati di questo tipo né convenzioni in tal senso, ma sul piano internazionale ritornano periodicamente riflessioni intese a migliorare la collaborazione introducendo questo tipo di strumenti. In relazione con le attuali questioni in materia di pratiche d'intercettazione internazionali da parte di grandi servizi informazioni esteri, si discute tra l'altro di disciplinare in futuro in trattati internazionali le reciproche attività di intelligence (per es. «Trattato di non spionaggio»). Attualmente è troppo presto per dire se a livello internazionale si stia sviluppando effettivamente una nuova prassi che comporterà anche regole vincolanti e imponibili. Il nostro Collegio considera opportuno che nell'ambito del rinnovamento della codificazione della legislazione applicabile in materia di servizio informazioni si predispongano le basi per consentire in futuro alla Svizzera di partecipare eventualmente a questo genere di sviluppi. Riteniamo che fino a nuovo avviso saranno soltanto le questioni tecniche di secondaria importanza a essere parte integrante di trattati nell'ambito del servizio informazioni.

Art. 70 Salvaguardia di interessi nazionali essenziali

Questo articolo, che si ricollega all'articolo 3, definisce la procedura da seguire per incaricare il SIC, in situazioni particolari, di adottare misure intese a salvaguardare interessi nazionali essenziali. Questa procedura non conferisce al SIC poteri supplementari e nemmeno sopprime le disposizioni concernenti l'obbligo di autorizzazione previsto per determinate misure di acquisizione. Il mandato formale è semplicemente una condizione necessaria affinché il SIC possa agire in un ambito che esula dal normale settore di compiti definito dalla legge e dal mandato fondamentale.

Art. 71 Lista d'osservazione

La lista d'osservazione, già prevista dalla LMSI, è uno strumento di condotta del Consiglio federale. È allestita dal DDPS e deve essere approvata annualmente dal Consiglio federale (art. 69 cpv. 1 lett. b). Dopo l'11 settembre 2001, la comunità internazionale ha intensificato la lotta contro il terrorismo. In seguito all'integrazione delle liste internazionali nel quadro della revisione «LMSI II ridotta», il nesso con le liste internazionali di terroristi è definito come il criterio di riferimento per la lista d'osservazione. A differenza di quanto previsto dalla LMSI, la quale incarica il Consiglio federale di designare le organizzazioni e comunità internazionali le cui liste sono da considerarsi rilevanti, nel *capoverso 2* la LAIn si limita a citare le Nazioni Unite (ONU) e l'UE. È poco probabile che altre organizzazioni internazionali emanino liste di importanza comparabile a quelle di queste due istituzioni.

L'inserimento di un'organizzazione o di un gruppo di persone nella lista d'osservazione non comporta sanzioni (per es. divieto di determinate organizzazioni) come quelle connesse al sistema di liste istituito dalla risoluzione 1267 del Consiglio di sicurezza delle Nazioni Unite[35]. Contrariamente a quanto previsto per la lista del Consiglio di sicurezza delle Nazioni Unite, nella lista d'osservazione non vengono neppure iscritti singoli individui. L'inserimento di un'organizzazione o di un gruppo (o una persona) in una lista internazionale non comporta automaticamente il suo inserimento nella lista d'osservazione svizzera. Quando è manifesto che una determinata organizzazione o un determinato gruppo sono irrilevanti per la Svizzera, si può rinunciare alla loro iscrizione nella lista. Altre organizzazioni o altri gruppi che figurano su liste internazionali possono tuttavia essere iscritti nella lista d'osservazione svizzera senza ulteriori motivazioni.

Grazie alla procedura di autorizzazione regolare da parte del Consiglio federale, vi è inoltre il margine di manovra per radiare un gruppo dalla lista quando è comprovato che non minaccia più la sicurezza interna o esterna della Svizzera (cosiddetto *delisting*).

Il limite posto al trattamento dall'articolo 5 capoverso 5 (attività politica ed esercizio di diritti fondamentali) non si applica alla lista d'osservazione (cfr. art. 5 cpv. 8). Il SIC può acquisire e trattare tutte le informazioni disponibili riguardo alle organizzazioni e ai gruppi figuranti nella lista, purché siano utili per valutare la minaccia che da essi deriva. Per le organizzazioni o i gruppi interessati non vi sono tuttavia altre ripercussioni immediate quali sanzioni, divieti o simili. Se necessario, tali misure devono continuare a essere adottate nel quadro di decisioni particolari o ordinanze, che non sono di competenza del servizio informazioni.

35 La risoluzione 1267 (1999) sulla situazione in Afghanistan può essere consultata, in francese, al seguente indirizzo: www.un.org/fr > Conseil de sécurité > Documents >

Questa disposizione corrisponde nei contenuti all'articolo 9 LMSI nella versione secondo la modifica del 23 dicembre 2011 («LMSI II ridotta»).

La disposizione disciplina la competenza legale del Consiglio federale nei casi previsti dalla LAIn, ma non ne restringe la competenza generale a emanare ordinanze e decisioni fondate sull'articolo 185 capoverso 3 Cost. per far fronte a gravi turbamenti, attuali o imminenti, dell'ordine pubblico o della sicurezza interna o esterna della Svizzera. Questa competenza del Governo continua a sussistere parallelamente nei casi non disciplinati dalla legge.

La disposizione proposta offre al Consiglio federale la possibilità, in materia di sicurezza interna o esterna, di vietare determinate attività per cinque anni al massimo e di prorogare il divieto di volta in volta per ulteriori cinque anni se le necessarie condizioni continuano a essere adempiute. Avvalendosi di questa nuova disposizione sarebbe ad esempio possibile, in futuro, disporre un divieto di attività per i seguaci di organizzazioni terroristiche. Attualmente è in vigore un'ordinanza dell'Assemblea federale che vieta il gruppo Al-Qaida e le organizzazioni associate (l'ordinanza è in vigore fino al dicembre 2014). Occorrerà valutare se in avvenire convenga piuttosto vietare determinate attività in virtù dell'articolo 9 LMSI o della LAIn o se non sia più opportuno che sia il Parlamento a decretare o a prolungare, applicando la propria competenza normativa, il divieto di determinate organizzazioni.

In base alle esperienze maturate in passato, si può ipotizzare che si verificheranno al massimo alcuni casi l'anno. Per tale motivo l'onere connesso a tali divieti non può essere indicato separatamente, ma rientra piuttosto nei limiti degli affari politici ordinari.

Si tratta di una misura preventiva volta a neutralizzare gravi minacce alla sicurezza o a impedire reati. Se sussiste già il sospetto di reato, occorre avviare un procedimento penale ordinario e coordinare strettamente eventuali divieti preventivi con l'autorità di perseguimento penale competente per non pregiudicare un procedimento penale in corso. Anche in simili casi può tuttavia essere opportuno ordinare misure preventive d'accompagnamento per garantire la sicurezza interna o esterna.

Il *capoverso 1* attribuisce al Consiglio federale la competenza di pronunciare un divieto di diritto amministrativo contro attività che comportano una concreta minaccia per la sicurezza interna o esterna della Svizzera. Tutti i dipartimenti avranno la possibilità di presentare pertinenti domande.

L'estensione e il contenuto delle attività vietate devono essere descritti con la massima precisione possibile nella decisione affinché il divieto possa essere efficacemente attuato e controllato. Estensione e contenuto dipendono però dalle attività degli interessati nella singola fattispecie e quindi non è possibile descriverli in modo esaustivo nella legge.

I divieti ai sensi del *capoverso 1* possono impedire agli interessati di esercitare i loro diritti fondamentali e pertanto, secondo il *capoverso 2*, devono essere limitati nel tempo. La limitazione obbliga le autorità a riesaminare il divieto dopo la sua scadenza, per verificare se i presupposti validi al momento dell'emanazione sono ancora adempiuti o sono venuti meno.

Se le condizioni sono ancora adempiute, la durata di un divieto può essere prorogata di volta in volta per ulteriori cinque anni, fintantoché le circostanze lo esigono. Se non è necessaria una proroga, il divieto decade automaticamente.

I divieti pronunciati in virtù del presente articolo possono essere impugnati conformemente all'articolo 79, dapprima dinanzi al Tribunale amministrativo federale secondo la procedura prevista dalla legge federale del 20 dicembre 1968[36] sulla procedura amministrativa e successivamente dinanzi al Tribunale federale.

Capitolo 6, Sezione 2

Gli articoli 73–77 contengono la sequenza in ordine ascendente delle prescrizioni di vigilanza e di controllo:

1. controllo autonomo da parte del SIC,
2. vigilanza e controllo da parte del DDPS,
3. autorità di controllo indipendente,
4. vigilanza e controllo da parte del Consiglio federale,
5. alta vigilanza parlamentare.

I singoli livelli ed elementi di controllo corrispondono sostanzialmente al diritto vigente (art. 4*b* LSIC, art. 25 segg. LMSI e art. 31 segg. O-SIC).

L'autorità di controllo indipendente (ACI) garantisce la legalità dell'esplorazione radio concernente l'estero conformemente all'articolo 37.

Viene ora proposto anche un disciplinamento della vigilanza parlamentare cantonale che istituisce competenze chiaramente distinte per la vigilanza della Confederazione e dei Cantoni (art. 78 cpv. 2). In tal modo saranno evitati doppioni per quanto riguarda le responsabilità e anche lacune nella vigilanza.

Il nostro Collegio non ha specificamente preso in considerazione la richiesta formulata in qualche caso durante la consultazione di verificare anche l'economicità delle attività informative. Ciò è già garantito dalle disposizioni generali sulla vigilanza finanziaria delle autorità federali e ulteriormente rafforzato dalla nuova menzione della Delegazione delle finanze nell'articolo 77. Inoltre, la garanzia della sicurezza interna o esterna può orientarsi soltanto in misura limitata ad aspetti inerenti all'economicità. In considerazione delle finalità della presente legge – per esempio la garanzia dei fondamenti della democrazia e dello Stato di diritto della Svizzera, la sicurezza della sua popolazione e degli Svizzeri all'estero o la tutela della capacità di agire degli organi statali – una valutazione monetaria passa spesso in secondo piano.

Art. 74 Vigilanza da parte del Dipartimento

Come finora, il DDPS disporrà di un organo interno di vigilanza, la Vigilanza sulle attività informative, per esercitare la vigilanza tecnica sui servizi informazioni. Tale organo è ora menzionato a livello di legge (cpv. 2) poiché gli saranno assegnate competenze più ampie.

La struttura degli organi di vigilanza deve assolutamente prevedere un organo di controllo in seno al Dipartimento. In caso contrario, il Consiglio federale non potrebbe esercitare la sua vigilanza in modo autonomo rispetto all'alta vigilanza parlamentare. L'organo di vigilanza interno dispone di ampi diritti in materia di consultazione e di informazione.

36 RS **172.021**

Per quanto riguarda la sua subordinazione, sono ipotizzabili un'attribuzione alla Delegazione delle Commissioni della gestione delle Camere federali (analoga al Controllo federale delle finanze nei confronti delle Commissioni della gestione), un'aggregazione amministrativa alla Cancelleria federale in quanto organo di Stato maggiore del Consiglio federale oppure, come finora, una subordinazione (puramente amministrativa) alla Segreteria generale del DDPS; conformemente a quest'ultima variante, l'organo di vigilanza riferiva direttamente al capo del DDPS trasmettendogli le proprie raccomandazioni. Il nostro Collegio ritiene che la soluzione in cui l'organo di vigilanza risponde direttamente e senza influenza esterna al capo del DDPS, tenga conto nel modo migliore della responsabilità in materia di condotta politica, dato che il capo del DDPS assume personalmente e direttamente la responsabilità suprema del Dipartimento.

In seno all'Amministrazione federale non vi è alcun ufficio federale che sia autorizzato in maniera analoga al servizio informazioni a ingerire nei diritti fondamentali delle persone interessate, prevalentemente a loro insaputa,, toccando in particolare la sfera privata e l'autodeterminazione in materia d'informazione. Istituendo l'organo di vigilanza interno parallelamente alla costituzione, il 1° gennaio 2010, del Servizio delle attività informative della Confederazione, il Consiglio federale ha concretizzato un'istanza del Parlamento che auspicava un ampio controllo permanente dei servizi informazioni. Da questo punto di vista, l'organo di vigilanza interno rappresenta un unicum nel diritto inerente all'Amministrazione federale.

Almeno una volta l'anno, l'organo di vigilanza interno definisce un piano di controllo confidenziale che dev'essere armonizzato con la Delegazione delle Commissioni della gestione delle Camere federali e sottoposto al capo del DDPS per approvazione. Quest'ultimo può assegnare all'organo di controllo interno ulteriori mandati di controllo in funzione della situazione. Allo scopo di rafforzare l'indipendenza e l'efficacia della vigilanza nonché per concretizzare una raccomandazione della Commissione della gestione delle Camere federali, la regolamentazione necessaria figurerà ora a livello di legge formale. Nella norma concernente l'organo di vigilanza interno sono di conseguenza stabiliti il suo statuto, le sue competenze e il suo svincolo da istruzioni. Rimangono applicabili le disposizioni della LOGA.

Anche l'attività di controllo dell'organo di vigilanza interno presso le autorità d'esecuzione cantonali sarà disciplinato a livello di legge (cpv. 3). Gli ambiti interessati sono quelli in cui i Cantoni acquisiscono informazioni in virtù di mandati della Confederazione (cfr. art. 81). In questo modo viene completato il compito di controllo e di gestione assegnato al DDPS secondo il capoverso 1.

Alcuni partecipanti alla consultazione hanno proposto di sostituire l'organo di vigilanza dipartimentale con un organo esterno totalmente indipendente. Il nostro Collegio non considera appropriata una simile vigilanza, completamente nuova. Essa pregiudicherebbe l'obbligo legale di vigilanza e la responsabilità del capo del DDPS e porrebbe altre questioni relative alla condotta politica da parte del Consiglio federale e del Parlamento. Il sistema di vigilanza proposto corrisponde per contro alle basi legali vigenti della LOGA e della legge sulla responsabilità ed è idoneo a garantire una vigilanza efficace.

Art. 75 Autorità di controllo indipendente per l'esplorazione radio

Come quello applicabile all'esplorazione radio (art. 37), il disciplinamento previsto per l'autorità di controllo indipendente (ACI) corrisponde pienamente alla normativa entrata in vigore il 1° novembre 2012 che il Parlamento ha direttamente sancito nella LSIC (art. 4*b* LSIC; cfr. anche le considerazioni relative all'art. 37). Oggi questa funzione è svolta da una commissione interna all'amministrazione. La LSIC non esclude tuttavia la presenza di membri esterni all'amministrazione, ciò che può per esempio rivelarsi opportuno per un determinato periodo di tempo quando uno specialista membro dell'ACI lascia l'Amministrazione federale.

L'attività di controllo dell'ACI era già disciplinata in modo analogo nell'ordinanza del 15 ottobre 2003 sulla condotta della guerra elettronica e negli scorsi anni tale disciplinamento si è dimostrato valido. Esso corrisponde a una necessità in un ambito sensibile dell'intelligence concernente l'estero. I compiti dell'ACI per quanto riguarda le verifiche dei mandati e il loro trattamento sono disciplinati nel capoverso 2. Come finora essa non può né deve verificare globalmente il trattamento, ma garantire, mediante verifiche adeguate, che sia il servizio esecutivo sia il SIC, che riceve i risultati, rispettino le prescrizioni legali.

Per quanto concerne l'esplorazione dei segnali via cavo vigono disposizioni comparabili, ma in quest'ultimo ambito è prevista un'autorizzazione da parte degli organi giudiziari e politici simile a quella in vigore per le misure di acquisizione soggette ad autorizzazione, poiché per eseguire l'acquisizione è indispensabile far capo a fornitori privati di servizi di telecomunicazione in Svizzera. Questa necessità non sussiste nel caso dell'esplorazione radio, che le autorità federali (COE e SIC) possono eseguire autonomamente.

Per quanto riguarda l'esplorazione dei segnali via cavo un controllo ulteriore da parte dell'ACI non è invece indicato, poiché creerebbe confusione tra gli ambiti di responsabilità delle autorità coinvolte (Tribunale amministrativo federale e capo del DDPS da un lato, ACI dall'altro).

Art. 76 Vigilanza e controllo da parte del Consiglio federale

Questo articolo sancisce nella LAIn la verifica della legalità, dell'adeguatezza e dell'efficacia delle attività, già prevista dall'articolo 26 LMSI ed estesa a tutte le attività informative dall'articolo 8 LSIC. In questa disposizione, la LAIn mantiene lo standard vigente in materia di vigilanza e controllo. Tale standard comprende anche l'informazione regolare del Consiglio federale in merito ai risultati delle attività degli organi di vigilanza del DDPS e della Delegazione delle Commissioni della gestione delle Camere federali.

Art. 77 Alta vigilanza parlamentare

La vigente regolamentazione, definita nell'articolo 25 LMSI, viene ripresa nel principio e al tempo stesso precisata: l'alta vigilanza parlamentare sull'esecuzione della presente legge compete esclusivamente alla Delegazione delle Commissioni della gestione e alla Delegazione delle finanze delle Camere federali, nei rispettivi ambiti di competenza. Tale vigilanza non si limita alle attività del SIC ma comprende anche quelle delle autorità d'esecuzione cantonali, purché quest'ultime operino su mandato diretto della Confederazione, vale a dire sulla base di un mandato concreto del SIC. Le attività dei Cantoni risultanti dalla lista d'osservazione (art. 71) sono

pure comprese nei mandati diretti, poiché la lista d'osservazione è inviata ogni anno ai Cantoni con la richiesta di acquisire tutte le informazioni disponibili sulle organizzazioni e i gruppi che vi figurano e di trasmetterle al SIC.

Le attività delle autorità d'esecuzione cantonali svolte nel quadro dell'applicazione diretta della LAIn, invece, potranno ora essere sottoposte all'alta vigilanza dei parlamenti cantonali. In tal modo saranno evitati doppioni in materia di competenze o lacune nella vigilanza. Il sistema d'informazione INDEX SIC (art. 50) comprenderà rubriche speciali per i Cantoni nelle quali essi potranno archiviare le loro informazioni e che consentiranno una chiara distinzione dei due ambiti di vigilanza.

Per quanto riguarda le attività delle autorità d'esecuzione cantonali su mandato diretto della Confederazione, il nostro Collegio ritiene che il legislatore federale ha disciplinato in maniera definitiva l'alta vigilanza parlamentare istituendo la Delegazione delle Commissioni della gestione e la Delegazione delle finanze per la vigilanza delle attività informative e assegnando particolari competenze a tali delegazioni negli articoli 51 e 53 della legge del 13 dicembre 2002[37] sul Parlamento. Non sarebbe coerente se il legislatore federale riservasse ai Cantoni competenze parallele a livello cantonale.

Art. 78 Vigilanza cantonale

È prevista una suddivisione della vigilanza sulle autorità d'esecuzione cantonali tra Confederazione e Cantoni.

Vigilanza da parte della Confederazione

L'alta vigilanza sull'esecuzione dei mandati federali impartiti secondo la presente legge, e quindi anche sulle corrispondenti attività delle autorità d'esecuzione cantonali, spetta alla Delegazione delle Commissioni della gestione delle Camere federali. Controlli presso le autorità d'esecuzione cantonali possono essere effettuati anche dall'organo di vigilanza interno del DDPS (art. 74 cpv. 3).

Vigilanza da parte dei Cantoni

La vigilanza da parte dei Cantoni consiste in sostanza nella vigilanza sulla funzione di servizio da parte dei superiori delle autorità d'esecuzione cantonali. L'autorità cantonale di vigilanza verifica:

- se le procedure amministrative cantonali sono conformi alle pertinenti prescrizioni legali;
- se le autorità d'esecuzione cantonali trattano i dati federali separatamente dai dati cantonali;
- il modo in cui l'autorità d'esecuzione esegue i mandati impartiti dalla Confederazione;
- le fonti e le modalità utilizzate dall'autorità d'esecuzione per acquisire informazioni, e
- se l'autorità d'esecuzione rispetta le esigenze della normativa in materia di protezione dei dati (sicurezza dei dati, protezione della personalità).

37 RS **171.10**

Questa ripartizione dei compiti corrisponde a quella prevista dal diritto vigente (art. 6 cpv. 3 LMSI e art. 35 O-SIC) e si è dimostrata valida nella pratica. Essa va pertanto mantenuta.

Le disposizioni applicabili alla vigilanza cantonale prevedono inoltre che gli organi di controllo federali forniscano il loro sostegno alle autorità cantonali di vigilanza sulla funzione di servizio (per es. da parte di un organo di controllo analogo all'attuale Vigilanza sulle attività informative) e che i servizi cantonali che esercitano tale vigilanza abbiano accesso alle informazioni utili al riguardo (*cpv. 3*).

Nell'ambito della valutazione di una soluzione adeguata per la vigilanza sulle autorità d'esecuzione cantonali sono state vagliate le seguenti varianti:

a. una *soluzione integralmente federale*: scegliere questa alternativa significherebbe affidare alla Confederazione, rispettivamente al SIC, tutti i compiti di vigilanza sulle autorità d'esecuzione cantonali. Questa soluzione unitaria ingloberebbe tutti gli aspetti della vigilanza, in particolare la vigilanza sulla funzione di servizio e sulla protezione dei dati. Secondo questo modello, la competenza per emanare la relativa normativa spetterebbe esclusivamente alla Confederazione. Gli impiegati pubblici incaricati dell'esecuzione della LMSI, sinora subordinati ai Cantoni, sarebbero integrati nell'Amministrazione federale;

b. una *soluzione integralmente cantonale*: rispetto alla soluzione odierna, questo modello toglierebbe alla Confederazione ogni competenza in materia di vigilanza sulle autorità d'esecuzione cantonali, compresa l'alta vigilanza sulle medesime da parte della Delegazione delle Commissioni della gestione delle Camere federali. In materia di protezione dei dati, la vigilanza cantonale dovrebbe disporre di estesi poteri di consultazione per quanto riguarda i dati trattati dalle autorità d'esecuzione cantonali.

La *soluzione federale* presenterebbe il vantaggio di un disciplinamento unitario della vigilanza sulle autorità d'esecuzione cantonali. Sarebbe tuttavia in contraddizione con la concezione federalistica della sicurezza interna, secondo la quale la Confederazione e i Cantoni provvedono, ciascuno nell'ambito delle proprie competenze, alla sicurezza del Paese e alla protezione della popolazione (art. 57 cpv. 1 Cost.). L'introduzione di una soluzione integralmente federale sarebbe in contrasto con la struttura federalistica del nostro ordinamento statale e non sarebbe profondamente radicata a livello locale presso le autorità di sicurezza. Pertanto deve essere scartata.

Una *soluzione integralmente cantonale* per la vigilanza sulle autorità d'esecuzione cantonali avrebbe anch'essa il vantaggio di garantire un disciplinamento unitario della vigilanza per tutti i Cantoni. Tale soluzione eliminerebbe la dicotomia Confederazione/Cantoni in materia di vigilanza. La vigilanza spetterebbe esclusivamente al Cantone. Questo modello presenta comunque uno svantaggio: i Parlamenti cantonali, che sarebbero chiamati in avvenire a esercitare l'alta vigilanza sull'attività delle autorità d'esecuzione cantonali, potrebbero sviluppare prassi differenti. Inoltre, in caso di soluzione puramente cantonale, gli organi cantonali di vigilanza dovrebbero avere completo accesso ai dati della Confederazione elaborati dalle autorità d'esecuzione cantonali, altrimenti non potrebbero esercitare integralmente la loro funzione di vigilanza. Tuttavia, in tal modo si intrometterebbero forzatamente nella sfera di vigilanza degli organi di vigilanza federali ed eventualmente entrerebbero in conflitto con tali organi. Si porrebbero inoltre ardue questioni di delimitazione per quanto riguarda la vigilanza sul mandato impartito dall'autorità federale. Il SIC

sarebbe tenuto per certi ambiti a rendere conto anche alle autorità di vigilanza cantonali, altro aspetto che risulterebbe contrario al sistema. Pertanto, nel complesso anche la soluzione cantonale non è convincente.

Per queste ragioni occorre attenersi alla soluzione attuale, ossia alla vigilanza ripartita tra Confederazione e Cantoni.

Del resto, il principio della vigilanza ripartita non rappresenta nulla di insolito. Non lo si ritrova solo nell'ambito del servizio informazioni: infatti, nella maggioranza dei Cantoni la polizia giudiziaria è subordinata dal profilo organizzativo e della funzione di servizio al comando della polizia cantonale. Tuttavia, quando svolge compiti investigativi per incarico delle autorità giudiziarie, è subordinata alla vigilanza tecnica di queste ultime.

Il *capoverso 2* definisce e delimita ora l'ambito di vigilanza che può essere affidato alla responsabilità degli organi parlamentari cantonali. Si tratta delle attività delle autorità d'esecuzione cantonali che esse svolgono in esecuzione diretta della LAIn sul loro territorio, senza aver ricevuto nel singolo caso un mandato esplicito del SIC. Al riguardo, l'articolo 81 capoverso 1 contiene il rinvio alle competenze dei Cantoni di adottare autonomamente misure di acquisizione. Questo nuovo ordinamento è opportuno perché gli organi federali di regola non hanno conoscenza di tali attività dei Cantoni ed è perciò difficile integrare queste ultime nelle attività di vigilanza. Con un'attribuzione al livello cantonale vengono così evitate eventuali lacune senza tuttavia generare doppioni. Il sistema d'informazione INDEX SIC conterrà apposite rubriche per il trattamento dei dati corrispondenti e il loro controllo.

I parlamenti cantonali mantengono evidentemente la loro autonomia in quei settori nei quali le autorità d'esecuzione cantonali operano per la sicurezza del rispettivo territorio al di fuori del campo d'applicazione della LAIn, la quale non prescrive che esse siano impiegate esclusivamente per l'esecuzione di tale legge. Di regola, nell'esecuzione della LAIn e della legislazione cantonale in materia di polizia vi sono utili sinergie che la Confederazione non vuole ostacolare.

Art. 79 Tutela giurisdizionale

La LAIn consente in certi casi misure e decisioni incisive per le quali va garantita un'adeguata tutela giurisdizionale. Il presente articolo prevede nel *capoverso 1* la via ordinaria del ricorso al Tribunale amministrativo federale e quindi al Tribunale federale. È pertanto chiaro che le misure adottate in virtù della LAIn non rientrano tra le eccezioni all'ammissibilità del ricorso previste dall'articolo 83 lettera a della legge federale del 17 giugno 2005[38] sul Tribunale federale, che in materia di diritto pubblico dichiara inammissibile il ricorso contro le decisioni relative alla sicurezza interna o esterna del Paese.

Il *capoverso 2* stabilisce che i ricorsi contro decisioni del SIC concernenti l'obbligo speciale d'informazione dei privati (art. 24) non hanno alcun effetto sospensivo. Secondo l'articolo 55 capoverso 1 della legge federale sulla procedura amministrativa, i ricorsi hanno effetto sospensivo salvo esso non venga espressamente revocato. Se per ottenere le informazioni necessarie occorresse ogni volta attendere l'esito di una procedura di ricorso, nella maggior parte dei casi le minacce per la sicurezza

38 RS **173.110**

interna o esterna non potrebbero essere valutate tempestivamente. La LAIn, in quanto *lex specialis*, non prevede pertanto l'effetto sospensivo.

Il *capoverso 3* impedisce che un ricorso possa differire la comunicazione al SIC di informazioni necessarie per la sicurezza del Paese fino a quando sarà troppo tardi per sventare la minaccia.

Poiché, a dipendenza delle circostanze, la comunicazione di una misura d'acquisizione soggetta ad autorizzazione può avvenire soltanto molto tempo dopo la sua fine (per es. per non compromettere ulteriori misure d'acquisizione ancora in corso), il *capoverso 4* stabilisce che il termine di ricorso decorre soltanto dal momento del ricevimento della comunicazione.

In occasione della consultazione il Tribunale amministrativo federale aveva espresso qualche preoccupazione riguardo al fatto di concentrare nel medesimo tribunale le funzioni di autorità di approvazione di determinate misure e più tardi di autorità di ricorso nella procedura di ricorso. Esso ha proposto di prevedere come autorità di ricorso il Tribunale penale federale. Tuttavia, il nostro Collegio intende mantenere una netta separazione tra autorità di diritto amministrativo e autorità di diritto processuale penale nonché di concentrare la competenza giuridica e materiale per la valutazione di fatti inerenti al servizio informazioni in seno al Tribunale amministrativo federale. Eventuali conflitti d'interesse tra il presidente di una corte che autorizza le misure in quanto autorità di approvazione e e quello della corte chiamata ad assumere la funzione di autorità di ricorso possono essere evitati mediante un'adeguata organizzazione delle competenze all'interno del Tribunale amministrativo federale. I vantaggi della concentrazione della procedura nell'ambito del diritto amministrativo sono chiaramente prevalenti.

Art. 80 Disposizioni d'esecuzione

Secondo l'articolo 7 LOGA, il Consiglio federale emana le ordinanze, purché ne sia autorizzato dalla Costituzione federale o dalla legge (cfr. anche l'art. 182 cpv. 1 Cost.). L'articolo 80 incarica il Consiglio federale, oltre che delle deleghe speciali previste nella legge, di emanare disposizioni d'esecuzione di carattere generale.

Art. 81 Esecuzione da parte dei Cantoni

Innanzitutto nel *capoverso 1* è stabilito il principio secondo cui i Cantoni sono competenti per l'esecuzione della presente legge sui rispettivi territori, congiuntamente con la Confederazione. Riguardo al principio della suddivisione dei compiti tra Confederazione e Cantoni in materia di sicurezza interna occorre precisare alcuni aspetti.

L'articolo 57 Cost. sottende la competenza implicita della Confederazione a provvedere alla propria sicurezza interna e a emanare disposizioni di legge laddove si tratta di esercitare effettive competenze federali (misure a protezione della Confederazione stessa o delle sue istituzioni e dei suoi organi). Tuttavia, la Confederazione è competente a legiferare soltanto settorialmente, e non ha una competenza legislativa generale in materia di sicurezza interna (cfr. rapporto del Consiglio federale del 2 marzo 2012[39] in adempimento del postulato Malama del 3 marzo 2010 «Sicurezza interna: chiarire le competenze»). I Cantoni sono dunque liberi di svolgere attività proprie in

39 FF **2012** 3973

materia di servizio informazioni e di emanare disposizioni di legge, purché non intervengano in ambiti che rientrano nella competenza normativa della Confederazione (competenza originaria o implicita). Per quanto riguarda la salvaguardia della sicurezza interna, la competenza normativa della Confederazione è concretizzata nel presente disegno di legge.

Nel rapporto in questione, il Consiglio federale afferma quanto segue in merito alla questione delle competenze dei Cantoni in materia di sicurezza interna (cfr. pag. 3993/3994):

«… La competenza dei Cantoni di provvedere alla tutela della sicurezza e dell'ordine pubblico nei rispettivi territori va considerata una loro competenza originaria. I Cantoni esercitano sul loro territorio la sovranità in materia di polizia e sono di conseguenza competenti a legiferare in adempimento del loro mandato generale concernente la prevenzione delle minacce. Il principio della responsabilità primaria dei Cantoni in materia di sicurezza sul loro territorio non è messo in discussione dalla dottrina né dalla giurisprudenza. Il Consiglio federale ha reiteratamente stabilito nella prassi che il potere legislativo in materia di polizia spetta fondamentalmente ai Cantoni. Il fatto che la Confederazione non disponga di un mandato generale in materia di prevenzione delle minacce trova riscontro anche sul piano istituzionale: mentre ciascuno dei 26 Cantoni dispone di un proprio corpo di polizia, non esiste un'autorità di polizia operante globalmente a livello federale.

Se, riguardo a uno specifico settore, la Costituzione federale non attribuisce competenze alla Confederazione, queste spettano ai Cantoni, in conformità alle regole generali in materia. Questo significa che i Cantoni possono assumere tutte le competenze che non sono state espressamente attribuite alla Confederazione. Di conseguenza le competenze in materia di sicurezza non specificamente attribuite alla Confederazione incombono sostanzialmente ai Cantoni. L'articolo 43 Cost. precisa che i Cantoni stabiliscono quali compiti svolgere e come adempiervi nei limiti delle rispettive competenze. Questo principio non si applica però in modo incondizionato: non sempre i Cantoni sono liberi, pur nell'ambito delle loro competenze, di stabilire quali compiti svolgere e in che modo portarli a termine, soprattutto quando la Costituzione attribuisce loro compiti specifici o impone modalità d'adempimento. In tali casi l'autonomia cantonale è limitata nella misura in cui la Costituzione federale pone determinate esigenze in relazione all'adempimento dei compiti. Un esempio in questo senso è riportato nell'articolo 57 capoverso 1 Cost.; anche i diritti fondamentali garantiti dalla Costituzione federale (art. 35 Cost.) limitano il margine d'azione dei Cantoni».

I principi contemplati nei *capoversi 1 e 2* di questa disposizione (acquisizione di informazioni, di propria iniziativa o sulla base di un mandato del SIC, rispettivamente comunicazione spontanea al SIC) sono stati ripresi dal diritto vigente (art. 12 LMSI). Si tratta di principi che nella prassi si sono dimostrati validi e che pertanto vanno mantenuti. Sulla base della proposta formulata da numerosi Cantoni in occasione della consultazione, il capoverso 1 è stato completato con un secondo periodo che contiene un elenco delle misure di acquisizione non soggette ad autorizzazione che le autorità d'esecuzione cantonali possono impiegare per l'esecuzione autonoma della LAIn. Si tratta della valutazione di fonti pubblicamente accessibili (art. 13), delle osservazioni in luoghi pubblici e liberamente accessibili (art. 14), della gestione di fonti umane (art. 15), dell'acquisizione di informazioni o del ricevimento di comunicazioni di altre autorità (art. 19 e 20), del ricevimento di comunicazioni e dell'audizione di terzi (art. 22 e 24). Le altre misure di acquisizione, in particolare

quelle soggette ad autorizzazione, sono eseguite dagli organi d'esecuzione cantonali soltanto su mandato del SIC. Al riguardo, essi possono sottoporgli domande. Continuano a essere possibili anche attività delle autorità d'esecuzione cantonali nel quadro della legislazione cantonale in materia di polizia. Secondo l'articolo 20 capoverso 1, i relativi risultati possono essere trasferiti anche nell'ambito della LAIn, se sono necessari per l'esecuzione di quest'ultima.

La reciproca assistenza tecnica e operativa secondo i *capoversi 3 e 4* è già da anni una realtà e consente di impiegare in modo efficiente le risorse di personale e i mezzi tecnici di cui dispongono Confederazione e Cantoni.

Le indennità concesse ai Cantoni in virtù del *capoverso 5* per le prestazioni che forniscono nell'ambito dell'esecuzione della presente legge sono anch'esse già previste dal diritto vigente (cfr. art. 28 cpv. 1 LMSI). Considerata la situazione particolare sul piano dell'esecuzione, il nostro Collegio intende mantenere questa indennità speciale, che del resto copre solo in parte i costi sostenuti dai Cantoni; le prestazioni connesse con l'esecuzione della LAIn non devono essere considerate già pareggiate nell'ambito della perequazione finanziaria generale tra Confederazione e Cantoni.

Del rimanente, il rispetto dei principi della legislazione sui sussidi risulta, da un lato, dal fatto che i Cantoni sono tenuti per legge a designare un'autorità incaricata di collaborare con il SIC per l'esecuzione della presente legge e incaricata, di principio, di operare su mandato della Confederazione e del SIC (strutturazione e gestione materiale; cfr. soprattutto l'art. 9 del disegno di legge e il relativo commento). I lavori interessati sottostanno a un rigido controllo da parte degli organi di controllo e di vigilanza della Confederazione e dei Cantoni (cfr. sezione 2 del disegno di legge). D'altro lato, l'indennità (che non copre i costi dei Cantoni) è forfettaria, tuttavia la chiave di ripartizione si fonda sul numero di persone attive prevalentemente per compiti federali nel rispettivo Cantone e il relativo pagamento avviene esclusivamente nel quadro dei crediti stanziati (sono pertanto garantite la trasparenza e le possibilità di gestione finanziaria). Come precisato sopra, in tal modo si intende mantenere una prassi collaudata ed efficiente, dalla quale non conviene scostarsi.

Abrogazione di altri atti normativi

Il presente disegno riprende i contenuti in materia di intelligence della LMSI, ma non le sue disposizioni in materia di polizia (protezione di persone ed edifici, misure contro la violenza in occasione di manifestazioni sportive, sequestro di materiale di propaganda con contenuti che incitano alla violenza). Poiché sono stati sospesi i lavori relativi a una legge sui compiti di polizia, la LMSI deve continuare a essere mantenuta per le questioni inerenti al diritto di polizia. Inoltre, sarà integrata da nuove disposizioni riprese dall'avamprogetto di legge sui compiti di polizia e che sono necessarie per l'ulteriore esecuzione della rimanente LMSI. La LMSI non può perciò essere abrogata integralmente; sono soppresse soltanto le parti inerenti all'intelligence.

Per i controlli di sicurezza relativi alle persone è in preparazione una nuova base legale: la futura legge sulla sicurezza delle informazioni riprenderà questo ambito della LMSI.

La LSIC viene invece ripresa integralmente dalla LAIn e di conseguenza può essere abrogata.

Legge federale del 21 marzo 1997[40] sulle misure per la salvaguardia della sicurezza interna

Osservazioni preliminari

Originariamente era stato previsto di disciplinare le disposizioni di polizia della LMSI nella nuova legge sui compiti di polizia (LCPol). Con l'introduzione della LAIn, si sarebbe così potuto semplicemente abrogare la LMSI. La procedura di consultazione relativa all'avamprogetto di LCPol (AP-LCPol) si è svolta presso i Cantoni, i partiti e altre organizzazioni dal novembre 2009 al marzo 2010[41]. Il 26 giugno 2013 il nostro Collegio ha deciso di sospendere i lavori relativi a questo progetto di legge e di modificare puntualmente, in caso di bisogno, le basi legali esistenti. Diversamente da quanto previsto ancora nell'avamprogetto della LAIn (cfr. l'allegato, modifica del diritto vigente, I, n. 1), la LMSI viene così mantenuta parallelamente alla nuova LAIn ma, con l'entrata in vigore di quest'ultima, il suo contenuto si limiterà a disciplinare i compiti di polizia assegnati all'Ufficio federale di polizia (fedpol). Si tratta in particolare dei provvedimenti contro il materiale di propaganda con contenuti che incitano alla violenza e contro la violenza in occasione di manifestazioni sportive, dei compiti di polizia di sicurezza a protezione di persone ed edifici della Confederazione e dell'adempimento degli obblighi sanciti dal diritto internazionale nei confronti di persone ed edifici. Le rimanenti disposizioni della LMSI saranno adeguate dal profilo redazionale in seguito all'avvento della LAIn.

Inoltre, nella LMSI vanno incluse tre nuove normative già contenute nell'AP-LCPol; si tratta di integrazioni direttamente connesse con i compiti di polizia di sicurezza del fedpol in virtù della LMSI e che ne garantiscono l'adempimento: si tratta degli articoli 13*f* (Sequestro di oggetti pericolosi; art. 32 AP-LCPol), 23 capoverso 3bis (Contatto con gli autori delle minacce, art. 31 AP-LCPol) e 23*a*–*c* (Sistema d'informazione e documentazione del Servizio federale di sicurezza; art. 75 segg. AP-LCPol). In quanto contenute nell'AP-LCPol, queste disposizioni sono già state sottoposte all'esame nell'ambito della summenzionata procedura di consultazione, il cui risultato non ha richiesto alcun adeguamento delle disposizioni citate[42], motivo per cui esse vengono riprese per lo più invariate dall'AP-LCPol nella presente revisione della LMSI.

Il principio dell'unità materiale di un progetto esige che esso presenti una compattezza oggettiva, che quindi i suoi singoli capitoli tematici abbiano un chiaro nesso materiale tra loro. Tale requisito è soddisfatto. Pur se con il suo nuovo campo d'applicazione la LMSI non è in correlazione diretta con l'oggetto della legge sulle attività informative, sussiste un nesso materiale in senso più ampio: entrambi – i compiti e le competenze in materia di *intelligence* della Confederazione e i suoi

40 RS **120**

41 Questo documento è consultabile all'indirizzo: www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione concluse > 2009 > Dipartimento federale di giustizia e polizia

42 Cfr. il rapporto sui risultati della procedura di consultazione sull'avamprogetto di legge federale sui compiti della Confederazione in materia di polizia, Ufficio federale di polizia, ottobre 2010, pag. 24 (sugli art. 31 e 32 AP-LCPol) e pag. 28 (sull'art. 75 segg. AP-LCPol).

compiti limitati in materia di polizia di sicurezza nella LMSI rimanente – servono a raggiungere l'obiettivo superiore della salvaguardia della sicurezza interna nell'ambito di competenze della Confederazione. D'altronde, funzioni in materia di polizia di sicurezza vengono assunte dal fedpol anche al di fuori del summenzionato ambito di competenze (protezione di persone ed edifici della Confederazione e di persone protette in virtù del diritto internazionale). Così, nell'ambito dell'adempimento dei suoi compiti, ad esempio in occasione dell'arresto di persone inclini a commettere atti di violenza, la Polizia giudiziaria federale (PGF) può vedersi indotta a proteggere dai pericoli i propri inquirenti e i procuratori federali competenti, ma anche terzi non coinvolti (passanti, vicini di casa ecc.). In relazione diretta con l'esecuzione di una misura coercitiva di diritto processuale penale, la PGF opera quindi, in via complementare, a livello di polizia di sicurezza (prevenzione delle minacce). All'interno dell'ambito di competenze della PGF, questa sua funzione di polizia di sicurezza non ha tuttavia alcuna importanza autonoma, vale a dire un'importanza indipendente da un mandato di polizia giudiziaria concreto. Tale funzione è altresì al di fuori della materia normativa «sicurezza interna» e, di conseguenza, non è oggetto delle presente revisione parziale della LMSI.

Art. 2 Compiti

La riformulazione di questa disposizione rispecchia il fatto che ora la LMSI si limita a disciplinare i compiti del fedpol:

Cpv. 1: ora l'attività informativa nei settori delle attività terroristiche e di spionaggio, nonché del commercio illecito di armi e materiali radioattivi è disciplinata nella LAIn (cfr. art. 6 cpv. 1 D-LAIn). Di conseguenza, le «misure [preventive] ai sensi della presente legge», ossia della LMSI, sono ora qualificate «di polizia». Il capoverso 2 specifica di quali ambiti di misure da adottare si tratta.

I *capoversi 2 e 3* della vigente LMSI possono venire abrogati completamente, poiché riguardano materie che ora sono disciplinate nella LAIn. Il vigente capoverso 4 diventa così il capoverso 2.

Cpv. 2: la valutazione periodica della situazione di minaccia e il trattamento di informazioni sulla sicurezza interna ed esterna (art. 2 cpv. 4 lett. a e b della vigente LMSI) non sono più contenuti nell'enumerazione dei compiti di polizia preventivi, poiché ora tali compiti sono disciplinati nella LAIn. I quattro ambiti di competenze rimanenti vengono ripresi invariati e vengono integrati da una nuova lettera d (Sequestro di oggetti pericolosi).

Art. 3 Limiti

La normativa generale riguardante i limiti materiali del trattamento di informazioni in relazione con l'acquisizione e l'analisi di informazioni da parte dei servizi di intelligence ora si trova nella LAIn (cfr. art. 5 cpv. 5 e 6 D-LAIn). I settori del trattamento di informazioni che rimangono nella LMSI non necessitano di una normativa generale concernente i limiti materiali, disponendo essi al riguardo di disciplinamenti speciali (cfr. art. 20 cpv. 1 ultimo periodo per il settore dei controlli di sicurezza relativi alle persone e il nuovo art. 23*b* cpv. 3 per il sistema d'informazione del Servizio federale di sicurezza [SFS]). La disposizione può quindi venire abrogata.

Art. 5 Adempimento dei compiti da parte della Confederazione

La base sulla quale si fonda il fedpol per stabilire il livello di protezione per le rappresentanze diplomatiche e consolari straniere è il Concetto direttivo del Consiglio federale in materia. In virtù della ripartizione delle competenze tra Confederazione e Cantoni nell'ambito della sicurezza interna sancita dalla Costituzione federale, questo mandato di protezione compete in primo luogo ai Cantoni, mentre la Confederazione esercita una funzione consultiva e di coordinamento (rapporto del Consiglio federale del 2 marzo 2012[43] in adempimento del postulato Malama 10.3045 del 3 marzo 2010 «Sicurezza interna: chiarire le competenze »).

I capoversi 2 e 3 nell'articolo 5 della vigente LMSI disciplinano i contenuti che ora lo sono disciplinati nella LAIn (cfr. art. 9 e 11 D-LAIn). Non appaiono perciò più nella versione riveduta della LMSI.

Art. 5a

Il contenuto di questa norma viene disciplinato nella LAIn, motivo per cui va abrogata nella LMSI.

Art. 6 cpv. 1

Il tenore della norma va adeguato al nuovo contenuto della LMSI: il fedpol è ora l'unico partner per la collaborazione con i Cantoni.

Art. 7–9

Queste norme disciplinano compiti specifici del SIC, motivo per cui vanno abrogate nella LMSI.

Art. 10 Obbligo d'informazione del fedpol

Il tenore della norma viene adeguato al nuovo contenuto della LMSI: il fedpol è ora l'unica autorità che sottostà all'obbligo d'informazione.

Art. 10a–13d

Queste norme disciplinano compiti specifici del SIC, motivo per cui vanno abrogate nella LMSI.

Art. 13e cpv. 2

L'unica modifica rispetto alla versione vigente di questa norma consiste nel fatto che, poiché nella presente nuova versione della LMSI il SIC qui viene menzionato per la prima volta, viene inserita la sua denominazione per intero e la relativa sigla.

Art. 13f Sequestro di oggetti pericolosi

Ai sensi dell'articolo 28*a* della legge sulle armi del 20 giugno 1997[44] (LArm), è vietato il porto di oggetti pericolosi in luoghi accessibili al pubblico e portarli seco

43 FF **2012** 3973, qui 4018, n. 2.3.2.2.1.2
44 RS **514.54**

in un veicolo se non si può rendere verosimile che il porto di tali oggetti è giustificato da un impiego o da una manutenzione conformi allo scopo e gli oggetti suscitano l'impressione che possano essere usati abusivamente, in particolare per intimidire, minacciare o ferire persone. Ai sensi dell'articolo 4 capoverso 6 LArm, per simili oggetti pericolosi s'intendono oggetti come arnesi, utensili domestici e attrezzi sportivi che sono adatti a minacciare o a ferire persone. Coltelli da tasca, come ad esempio il coltello tascabile dell'esercito svizzero e prodotti analoghi, non sono per contro considerati oggetti pericolosi. Secondo l'articolo 31 capoverso 1 lettera c LArm, l'autorità competente procede al sequestro degli oggetti pericolosi portati abusivamente; se le condizioni dell'articolo 31 capoverso 3 LArm sono adempiute, può sequestrarli definitivamente. A tenore dell'articolo 38 capoverso 1 LArm, i Cantoni applicano la presente legge, nella misura in cui la Confederazione non venga dichiarata competente.

Con l'*articolo 13f*, il fedpol sarà ora autorizzato, nel suo settore di competenze, a sequestrare siffatti oggetti pericolosi. Nell'ambito della protezione di autorità ed edifici della Confederazione, è essenziale per il fedpol potere autonomamente sequestrare e confiscare in via definitiva questi oggetti pericolosi. Parimenti, nell'adempimento di compiti di polizia giudiziaria, il fedpol deve avere la possibilità di garantire la sicurezza delle persone coinvolte e impedire direttamente intimidazioni o minacce.

Art. 14 cpv. 1

La modifica rispetto al vigente tenore di questa norma consiste nel fatto che – conformemente al nuovo contenuto della LMSI – la disposizione si applica ora unicamente al fedpol e non più, in generale, agli «organi di sicurezza federali».

Art. 14a–18

Queste norme disciplinano compiti specifici del SIC, motivo per cui vanno abrogate nella LMSI.

Art. 21 cpv. 2

Questa modifica è puramente formale.

Art. 23 cpv. 1 lett. a e c e 3bis

Cpv. 1 lett. a e c: la nuova versione di questa norma è precisata sotto due aspetti rispetto al vigente tenore: viene chiarito che, in linea di massima, beneficiano di misure di protezione unicamente le persone della Confederazione che esercitano una funzione di interesse pubblico, quali parlamentari federali, magistrati e determinati impiegati della Confederazione. Al momento, queste persone figurano già nell'ordinanza del 27 giugno 2001[45] sui Servizi di sicurezza di competenza federale (OSF). Al contempo, devono essere esposte a una particolare situazione di minaccia in ragione della funzione che assumono per avere diritto a misure di protezione. Da questo consegue anche la durata delle misure di protezione: di principio, esse vengono accordate soltanto finché la persona ricopre per la Confederazione una carica

45 RS **120.72**

pubblica connessa a rischi particolari. Qualora una di queste persone, al di fuori della sua funzione professionale, dovesse ad esempio trovarsi in una situazione di minaccia o di pericolo per motivi esclusivamente privati, la protezione incombe, come per tutti gli altri cittadini, alle competenti autorità di polizia cantonali che dispongono di ampie competenze di polizia di sicurezza.

Finora, l'articolo 23 capoverso 1 lettera c della vigente LMSI (edifici e manifestazioni per la cui protezione vengono impiegati altri servizi) non è mai stato applicato e va perciò abrogato.

Cpv. 3bis: ora la polizia – il Servizio federale di sicurezza del fedpol (SFS) o la polizia cantonale competente nel caso concreto – sarà autorizzata a entrare direttamente in contatto con una persona della quale deve presumere che rappresenti un serio rischio per le persone o gli edifici da proteggere. La polizia interpellerà questa persona in merito ai concreti indizi di reati, segnalandole le conseguenze penali se dovesse commettere il fatto, allo scopo di dissuaderla dal commetterlo (cosiddetto «contatto con gli autori delle minacce»). La persona contattata può rendersi conto delle misure di polizia o di diritto amministrativo che risulterebbero nei suoi confronti da un eventuale comportamento scorretto. Le esperienze maturate in Germania e nel Cantone di Zurigo nel settore della violenza domestica e della tifoseria violenta nel corso di EURO 2008 hanno dimostrato che il contatto diretto e tempestivo da parte della polizia con i soggetti potenzialmente pericolosi ha un sicuro effetto dissuasivo su di loro. Il contatto con gli autori delle minacce è una misura di natura non formale che viene annotata nel sistema d'informazione e documentazione di cui all'articolo 23*a*. Non ne risultano effetti negativi per la persona in questione e non ha luogo alcuna comunicazione ad altre autorità o altri registri.

Art. 23a Sistema d'informazione e di documentazione

Cpv. 1: poiché il SFS tratta anche dati personali, in conformità con l'articolo 17 capoverso 2 LPD tale trattamento presuppone una base legale formale. Attualmente, il trattamento di informazioni del SFS per adempiere il proprio mandato di protezione ai sensi della sezione 5 della LMSI si fonda sull'articolo 3 capoverso 4 LMSI. L'articolo 13 OSF attua in modo dettagliato la norma di legge. Originariamente, nel progetto di revisione LMSI II era previsto di elaborare una nuova base legale formale. Dopo che il DFGP, nell'agosto del 2005, ha rinviato questo progetto al fedpol per essere rielaborato, è stato deciso di riprendere nella LCPol la nuova normativa prevista. Con la sospensione di quel progetto legislativo, la nuova normativa sarà ora integrata nella LMSI.

Per il trattamento di informazioni del SFS nell'ambito di competenze dell'articolo 22 capoverso 1 LMSI, l'AP-LCPol aveva previsto i due sistemi d'informazione autonomi «documentazione sugli eventi» e «documentazione sulle minacce» (art. 75 e 76 AP-LCPol). Nella consultazione è stato criticato il fatto che i due sistemi non fossero delimitati in maniera del tutto chiara a livello di contenuti. Riprendendo questa critica, i due sistemi che oggi sono gestiti separatamente verranno ora riuniti in *un* sistema completo. Il sistema d'informazione è oggetto del nuovo articolo 23*a* e degli articoli seguenti. Il fatto che il servizio competente del fedpol è autorizzato a raccogliere le necessarie informazioni risulta già dal precedente articolo 14 capoverso 1 formulato in maniera generale. Il presente articolo 23*a* istituisce la richiesta base legale formale speciale per il sistema d'informazione elettronico del SFS.

Cpv. 2: per adempiere il suo mandato di protezione, il fedpol necessita e tratta informazioni, da un lato, su eventi concernenti fatti rilevanti per la sicurezza e, dall'altro, sulle persone connesse con tali fatti. Gli eventi possono consentire deduzioni relative alla minaccia a cui sono esposti persone o edifici. Questi eventi vanno documentati per poterli analizzare al di là dell'attualità quotidiana e posizionare in contesti più vasti. Per il 90 per cento, le informazioni su tali eventi provengono da fonti accessibili al pubblico. La cerchia delle persone connesse con eventi concernenti fatti rilevanti per la sicurezza contempla due categorie fondamentalmente diverse: da una parte, le persone che il fedpol deve proteggere e, dall'altra, i potenziali autori da cui derivano pericoli per persone e installazioni. Per inserire una determinata persona nel sistema d'informazione è necessario che indizi concreti lascino presupporre che tale persona rappresenti un pericolo per talune persone e taluni edifici.

Art. 23b Dati, categorie di dati e limiti del trattamento dei dati

Cpv. 1: nel sistema d'informazione vengono registrati e trattati dati da fonti del tutto differenti. Spesso all'origine della registrazione dei dati vi è una lettera minatoria che nella maggior parte dei casi è in forma anonima. Per valutare la pericolosità di una persona è importante sapere se è violenta, come si è sviluppata in passato la sua inclinazione alla violenza oppure se è già stata condannata per reati violenti. Per scoprire l'identità dell'autore della minaccia e per valutarne la pericolosità occorre raccogliere varie informazioni da diverse fonti. Anche in questi casi la maggioranza dei dati proviene da fonti accessibili al pubblico.

Cpv. 3: questa disposizione stabilisce i limiti materiali del trattamento di informazioni. Il tenore è ripreso dall'articolo 3 capoverso 1 della vigente LMSI (che a sua volta, come illustrato in precedenza, viene abrogato). Per indicazioni più precise in merito alla presente norma si può rinviare al commento all'articolo 5 capoversi 5 e 6 D-LAIn, materialmente conforme.

Art. 23c Diritti d'accesso e comunicazione dei dati

L'accesso ai dati è disciplinato in modo differenziato: soltanto alcune unità organizzative del fedpol, ossia i servizi incaricati della valutazione delle minacce, della protezione delle persone e della protezione dello Stato (*cpv. 1*). I servizi enumerati nel *capoverso 2* sono i servizi ai quali è consentito comunicare, in singoli casi, i dati registrati nel sistema. Così, ad esempio, i collaboratori che controllano l'accesso alle singole sedi dei consiglieri federali, possono venire informati se una certa persona costituisce un pericolo per il consigliere federale che si trova nell'edificio. Solitamente tali informazioni comprendono, oltre ai connotati e a una fotografia per identificare la persona, anche indicazioni sulle caratteristiche essenziali della personalità, ad esempio sulla predisposizione alla violenza. Informazioni di questo tipo possono essere comunicate anche a tutela delle persone protette in Svizzera in virtù del diritto internazionale. Una rappresentanza estera nel nostro Paese deve ad esempio essere informata delle persone che costituiscono un pericolo per la sicurezza degli incaricati d'affari del Paese in questione. Per lo stesso motivo le società di sicurezza private che sorvegliano ad esempio un edificio per conto del fedpol devono ricevere informazioni di questo tipo per adempiere i loro compiti di protezione.

Art. 25–27

Le norme contenute in questa disposizione si trovano ora nella LAIn, motivo per cui vanno abrogate nella LMSI.

Art. 28 cpv. 1

Il disciplinamento dell'indennità per le prestazioni fornite dai Cantoni nell'ambito dell'acquisizione informativa ora si trova nell'articolo 81 capoverso 5, motivo per cui la pertinente norma può essere abrogata nella LMSI.

Legge federale del 20 giugno 2003[46] sul sistema d'informazione per il settore degli stranieri e dell'asilo

Art. 9 cpv. 1 lett. c e l, nonché cpv. 2 lett. c e k

L'articolo 9 capoverso 1 lettera c (Accesso tramite procedura di richiamo) menziona oggi le autorità federali competenti per la sicurezza interna. L'accesso online al sistema d'informazione dell'Ufficio federale della migrazione (UFM) per il SIC è tuttavia limitato alla verifica delle misure di respingimento, ciò che non corrisponde all'intera gamma di compiti del SIC. Esso partecipa per esempio a numerose procedure del settore degli stranieri e dell'asilo per valutare possibili pericoli per la sicurezza interna o esterna. Si propone pertanto di definire le condizioni per l'accesso online conformemente ai compiti legali del SIC e contemporaneamente di disciplinarle in una lettera separata dell'articolo 9 capoverso 1. Le riserve riguardanti i pericoli per la sicurezza interna o esterna sono contenute in numerose disposizioni della legge federale del 16 dicembre 2005[47] sugli stranieri e della legge del 26 giugno 1998[48] sull'asilo, motivo per cui nel testo della presente legge si rinuncia a menzionarle singolarmente.

Lo stesso vale, per analogia, per il capoverso 2 lettera c e k.

Legge del 17 giugno 2005[49] sul Tribunale amministrativo federale

Art. 23 cpv. 2 e 36b

Nell'articolo 23 capoverso 2 lettera b è introdotta la competenza del presidente della corte competente del Tribunale amministrativo federale per la procedura di autorizzazione concernente le misure di acquisizione soggette ad autorizzazione e l'esplorazione dei segnali via cavo.

L'articolo 36*b* prevede la competenza di principio del Tribunale amministrativo federale per l'autorizzazione di misure di acquisizione del SIC.

46 RS **142.51**
47 RS **142.20**
48 RS **142.31**
49 RS **173.32**

Art. 33 lett. b n. 4

Il ricorso contro le decisioni del Consiglio federale intese a vietare determinate attività (art. 72) deve essere prevista esplicitamente poiché finora non figurava nell'elenco esaustivo di cui all'articolo 33 lettera b della legge sul Tribunale amministrativo federale.

Codice civile[50]

Art. 43a cpv. 4 n. 5

Con l'integrazione dell'articolo 43*a* capoverso 4 CC, al SIC sarà concesso l'accesso al sistema Infostar (registro dello stato civile) allo scopo di identificare persone e accertare la loro dimora attuale ed eventualmente quelle precedenti. Il Consiglio federale dovrà tuttavia disciplinare più dettagliatamente l'accesso on line del SIC a Infostar nell'ordinanza (per es. l'estensione dell'accesso). La numerazione tiene conto della revisione di questo articolo attualmente in corso, la quale introdurrà ulteriori accessi da parte di altri servizi. Gli accessi del SIC avverranno attraverso interfacce analoghe a quelle già utilizzate da altri servizi della Confederazione e dei Cantoni.

Codice penale[51]

Art. 317bis cpv. 1 e 2

Il rinvio alla LMSI è sostituito dal rinvio alla legge sulle attività informative.

Art. 365 cpv. 2 lett. r–u

La novità di questa disposizione consiste nella menzione dei compiti per la cui esecuzione al SIC occorre l'accesso al casellario giudiziale informatizzato (VOSTRA). Questi accessi sono disponibili già oggi in applicazione della disposizione d'eccezione dell'articolo 367 capoverso 3 CP in combinato disposto con l'articolo 21 capoverso 4 dell'ordinanza VOSTRA del 29 settembre 2006[52]. Ciò vale però soltanto fino all'entrata in vigore di una base legale formale, che sarà istituita nella nuova legislazione sulle attività informative. Gli scopi per i quali il SIC deve avere accesso al sistema vengono precisati e provvisti dei pertinenti rinvii alla LAIn.

Art. 367 cpv. 2 lett. m e 4

Il SIC deve essere menzionato formalmente anche nell'articolo 367 CP che enumera le autorità che ottengono l'accesso online al VOSTRA. Per adempiere i suoi compiti legali, il SIC non soltanto dev'essere informato in merito alle condanne già pronunciate (cfr. art. 367 cpv. 2 lett. m; compresi i condoni con provvedimenti giudiziari), bensì anche in merito a eventuali procedimenti penali pendenti (cfr. art. 367 cpv. 4).

50 RS **210**
51 RS **311.0**
52 RS **331**

Ciò serve non soltanto a evitare l'intersecarsi di attività di intelligence con attività di organi di perseguimento penale, ma anche alla corretta trasmissione di informazioni ad autorità di sicurezza estere in occasione di accertamenti dell'affidabilità secondo l'articolo 12 capoverso 1 lettera d LAIn. Per accordarsi in merito alla trasmissione di comunicazioni concernenti procedimenti penali pendenti, come finora il SIC contatterà l'autorità di perseguimento penale competente allo scopo di evitare ripercussioni negative sulle indagini in corso.

Codice di procedura penale[53]

La modifica del Codice di procedura penale concerne soltanto il testo francese

Legge federale del 13 giugno 2008[54] sui sistemi d'informazione di polizia della Confederazione

Art. 15 cpv. 3 lett. k e 4 lett. i

Nell'ambito degli accessi ai sistemi d'informazione di polizia, la LAIn aggiorna semplicemente le basi legali per gli accessi oggi già esistenti (art. 15 LSIP, sistema di ricerca informatizzato di polizia) e sancisce la possibilità della segnalazione ai fini della ricerca di persone e oggetti secondo l'articolo 16 LAIn. Non tutti i collaboratori del SIC avranno accesso ai dati, ma unicamente quelli che ne hanno bisogno per l'adempimento dei compiti previsti dalla legge. Come d'uso, il Consiglio federale disciplinerà nelle ordinanze esecutive la cerchia dei collaboratori del SIC autorizzati ad accedere ai sistemi e l'estensione del loro diritto d'accesso. I rimandi alla LMSI sono sostituiti da quelli alle norme determinanti della LAIn.

Art. 16 cpv. 9

Il rimando alla LMSI è sostituito da quello alle norme determinanti della LAIn.

Legge militare del 3 febbraio 1995[55]

Art. 99 cpv. 1bis, 1^{quater} e 3bis

Nell'articolo 99 capoverso 1bis viene inserita la nuova base legale per l'esplorazione radio da parte del Servizio informazioni dell'esercito. Finora il corrispondente rinvio nell'articolo 99 capoverso 1bis si riferiva all'articolo 4*a* LSIC.

Il capoverso 1^{quater} mette a disposizione del Servizio informazioni dell'esercito gli stessi mezzi di cui dispone il SIC per l'osservazione aerea e satellitare (art. 14 LAIn) e riprende anche i medesimi provvedimenti per proteggere la sfera privata.

Il capoverso 3bis corrisponde alla disposizione dell'articolo 68 capoverso 2 LAIn.

53 RS **312.0**
54 RS **361**
55 RS **510.10**

Legge federale del 3 ottobre 2008[56] sui sistemi d'informazione militari

Art. 16 cpv. 1 lett. h

Ora è previsto che il SIC abbia l'accesso online alla banca dati PISA affinché possa individuare possibili minacce per la sicurezza dell'esercito da parte di persone incorporate nell'esercito e appartenenti per esempio a gruppi estremisti violenti. Si eviterà così che persone con propensione alla violenza pregiudichino la sicurezza dell'esercito, ma anche che esse siano istruite dall'esercito al maneggio di armi ed esplosivi nonché all'applicazione di procedure di combattimento.

Legge federale del 21 marzo 2003[57] sull'energia nucleare

Art. 101 cpv. 3

Il servizio centrale ATOM, di cui si tratta in questo articolo, è subordinato al SIC. Il compito del servizio centrale consiste nell'acquisire e trattare i dati necessari per l'esecuzione della legge federale sull'energia nucleare, la prevenzione dei reati e il loro perseguimento. La prassi ha evidenziato la necessità di estendere il campo di attività del servizio centrale anche all'ambito della legge del 22 marzo 1991[58] sulla radioprotezione, che presenta affinità con la legge federale sull'energia nucleare. Possono così essere evitate questioni di delimitazione del campo d'applicazione per quanto concerne il genere di sostanze radioattive (materiale fissile o non fissile), certamente determinanti per stabilire a quale delle due leggi sottostanno dette sostanze, ma che tuttavia nella prassi informativa sono irrilevanti o che, in occasione dell'avvio dell'elaborazione di un caso di contrabbando nucleare, non possono ancora essere valutate.

Legge federale del 19 dicembre 1958[59] sulla circolazione stradale

Art. 104c cpv. 5 lett. c

Con l'adeguamento dell'articolo 104*c* capoverso 5, il SIC disporrà dell'accesso on line al registro delle autorizzazioni a condurre. Tale accesso è necessario per avere informazioni sull'autorizzazione a condurre di determinate persone, informazioni in assenza delle quali l'esecuzione di misure informative come le osservazioni potrebbe essere preparata soltanto in misura insufficiente.

56 RS **510.91**
57 RS **732.1**
58 RS **814.50**
59 RS **741.01**

Legge federale del 6 ottobre 2000[60] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni

Al momento questa legge è sottoposta a una revisione totale che adeguerà le normative della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) ai nuovi bisogni[61]. In questo ambito continuano a essere previste soltanto la sorveglianza in funzione del perseguimento penale e scopi di polizia definiti in modo troppo restrittivo. Con la LAIn lo scopo della sorveglianza verrà esteso al settore dell'intelligence, il che deve essere integrato di conseguenza nella LSCPT.

Tuttavia, secondo i principi dell'attività legislativa, un messaggio può solamente modificare un testo di legge esistente. Perciò, nella modifica di altri atti normativi, il messaggio della LAIn fa riferimento all'attuale LSCPT, mentre il coordinamento con la revisione totale deve avvenire sulla scia delle deliberazioni parlamentari di LAIn e LSCPT e, se del caso, della messa in vigore da parte del Consiglio federale.

Seguono perciò i commenti alle modifiche che sarebbero necessarie per aggiungere all'attuale LSCPT disposizioni sulla sorveglianza a scopi informativi.

Art. 1 cpv. 1 lett. d

In futuro il SIC potrà ordinare la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (art. 22 cpv. 1 lett. a–d). L'esecuzione di queste misure avverrà, conformemente alla procedura secondo la LSCPT, per il tramite del servizio competente, il Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, in seno al DFGP. A tale scopo, il SIC deve essere aggiunto nella LSCPT quale ulteriore autorità ordinante.

Art. 11 cpv. 1 lett. a e 13 cpv. 1 lett. a

In queste due disposizioni anche il SIC è ora citato in quanto organo autorizzato ad assegnare incarichi di sorveglianza. Ciò è la conseguenza della facoltà del SIC di far sorvegliare la corrispondenza postale e il traffico delle telecomunicazioni di una persona secondo l'articolo 25 capoverso 1 lettere a–d LAIn.

Art. 14 cpv. 2bis

Nella fattispecie il rinvio alla LMSI è stato semplicemente sostituito dal rinvio alla nuova LAIn.

Coordinamento con la revisione totale della LSCPT

Segue una panoramica sulle necessarie modifiche nella LSCPT sottoposta a revisione totale, conformemente al messaggio del 27 febbraio 2013[62], con riserva delle deliberazioni e delle decisioni delle Camere federali. Le disposizioni corrispondono nelle formulazioni, nel contenuto e nel grado di precisione al disegno della LSCPT.

60 RS **780.1**
61 FF **2013** 2283
62 FF **2013** 2283

Ingresso

visti gli articoli 57 capoverso 2, 92 capoverso 1 e 123 capoverso 1 della Costituzione federale[63];
visto il messaggio del Consiglio federale del 27 febbraio 2013[64],

Art. 1 cpv. 1 lett. e

La presente legge si applica alla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni ordinata e attuata nell'ambito:

e. dell'esecuzione della legge del …[65] sulle attività informative (LAIn).

Art. 5 cpv. 1

1 Il DFGP può istituire un organo consultivo composto da rappresentanti del DFGP, del Servizio, dei Cantoni, delle autorità di perseguimento penale, del Servizio delle attività informative della Confederazione (SIC) e dei fornitori di servizi postali e di telecomunicazione.

Art. 10 cpv. 2bis

2bis Il diritto d'accesso ai dati raccolti nell'ambito dell'esecuzione della LAIn è retto dalla LAIn.

Art. 11 cpv. 3bis

3bis I dati raccolti nell'ambito dell'esecuzione della LAIn sono conservati nel sistema di trattamento finché necessario per lo scopo perseguito ma al massimo per 30 anni dalla fine della sorveglianza.

Art. 14a Interfaccia con il sistema d'informazione del SIC

1 Una copia dei dati contenuti nel sistema di trattamento può essere trasferita online nel sistema d'informazione di cui all'articolo 57 LAIn, sempre che:

a. il diritto applicabile consenta il trattamento dei dati in questo sistema; e

b. sia garantito che soltanto le persone incaricate della misura di sorveglianza in questione vi abbiano accesso.

2 Il trasferimento può essere eseguito soltanto da una persona che ha diritto di accedere al sistema di trattamento secondo la presente legge e di accedere al sistema d'informazione in questione ai sensi della LAIn.

Art. 15 cpv. 1 lett. d e cpv. 2 lett. a

1 Il Servizio fornisce informazioni sui dati di cui agli articoli 21 e 22 esclusivamente alle autorità seguenti che ne fanno richiesta e solo ai fini indicati:

d. al SIC, al fine di adempiere compiti ai sensi della LAIn.

63 RS **101**
64 FF **2013** 2283
65 RS …; FF **2014** 2015

2 Il Servizio fornisce informazioni sui dati di cui all'articolo 21 alle autorità seguenti che ne fanno richiesta e solo ai fini indicati:

a. al SIC, al fine di eseguire la LAIn;

Art. 22a Informazioni per identificare persone in caso di minacce alla sicurezza interna o esterna

Se vi sono indizi sufficienti che verrà o è stata compiuta via Internet una minaccia alla sicurezza interna o esterna, i fornitori di servizi di telecomunicazione consegnano tutte le indicazioni che consentono di identificarne l'autore o l'origine.

L'articolo 24 LAIn dovrebbe poi rinviare all'articolo 15 LSCPT (con la data della revisione totale) per le informazioni concernenti i collegamenti di comunicazione.

Nella LSCPT totalmente riveduta le misure di sorveglianza non sono più elencate nella stessa maniera che nell'attuale legge. Per recepire una suddivisione normativa analoga a quella prevista tra LSCPT e Codice di procedura penale, la LAIn dovrebbe perciò essere formulata come segue (i commenti sui dettagli corrispondono a quelli nel messaggio sulla revisione totale della LSCPT):

Art. 25 cpv. 1 lett. a e a^{bis} (LAIn)

1 Le seguenti misure di acquisizione sono soggette ad autorizzazione:

a. la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni e la richiesta di dati marginali della corrispondenza postale e del traffico delle telecomunicazioni conformemente alla legge federale del …[66] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni;

a^{bis}. l'impiego di dispositivi tecnici speciali per sorvegliare il traffico delle telecomunicazioni, registrare trasmissioni o identificare una persona o un oggetto oppure determinarne la posizione, se la sorveglianza di cui alla lettera a è stata infruttuosa, sarebbe comunque vana o sproporzionatamente difficile e sono disponibili le autorizzazioni in materia di diritto delle telecomunicazioni per i dispositivi tecnici speciali;

Legge del 30 aprile 1997[67] sulle telecomunicazioni

Art. 34 cpv. 1ter e 1^{quater}

Nel capoverso 1ter viene ora menzionato anche il SIC. In tal modo, nella legge sulle telecomunicazioni è integrato il corrispettivo, sotto il profilo legale formale, dell'articolo 7 capoverso 1 lettera d LAIn.

Nota riassuntiva concernente le leggi federali modificate nei numeri 14–20:

Per quanto riguarda le leggi federali nei numeri 14–20, negli articoli concernenti la comunicazione di informazioni vi sono stati esclusivamente adeguamenti formali. Il

66 RS …; FF **2013** 2283
67 RS **784.10**

rinvio alla LMSI è sostituito ogni volta dal rinvio alla LAIn. Dal profilo materiale non risulta alcun cambiamento.

Inoltre, in alcune leggi è stralciata l'indicazione, introdotta con la LMSI II, relativa alla comunicazione dei dati al SIC quando si tratta di una comunicazione di dati «in singoli casi e su richiesta scritta e motivata». Tale indicazione è risultata inutile poiché la comunicazione di informazioni al SIC è già compresa in un'altra disposizione delle leggi interessate. Si tratta pertanto di una semplice correzione di una svista e non di una modifica della situazione giuridica.

Legge federale del 19 giugno 1992[68] sull'assicurazione militare

Art. 1a cpv. 1 lett. q

Questa disposizione rappresenta il corrispettivo dell'articolo 35 capoverso 6 LAIn, in virtù del quale i collaboratori del SIC impiegati all'estero sono assoggettati all'assicurazione militare. Questa disposizione deve essere sancita anche nella LAM in quanto legge che disciplina la materia.

Art. 95a cpv. 1 lett. h^{bis} e i n. 8

Si tratta dell'adeguamento formale menzionato in precedenza (sostituzione del rinvio alla LMSI con un rinvio alla LAIn).

3 Ripercussioni

3.1 Ripercussioni per la Confederazione

3.1.1 Ripercussioni finanziarie

Le ripercussioni finanziarie dipendono fortemente dalle modalità di attuazione delle singole misure e dalla frequenza della loro applicazione. Ipotizziamo che, nell'attuale situazione di minaccia, simili misure saranno applicate in una decina di casi l'anno, tenuto conto del fatto che per ogni caso sono possibili più misure.

I mezzi e i sistemi impiegati per la localizzazione tecnica all'estero nonché per l'osservazione tramite mezzi aerei e spaziali sono noti e affermati, ragion per cui le loro ripercussioni finanziarie sono ben valutabili. I costi per gli acquisti e gli investimenti sono compresi tra cinque e sette milioni di franchi e i costi annui ricorrenti per la manutenzione e l'adeguamento dei sistemi nonché le licenze ammontano a circa 800 000 franchi. L'acquisto e il finanziamento dei sistemi avviene di regola nel quadro della procedura d'armamento.

In Svizzera, per le misure di acquisizione soggette ad autorizzazione come per esempio le localizzazioni, la sorveglianza dell'utilizzazione e del traffico delle telecomunicazioni di telefoni mobili e fissi, nonché per la sorveglianza di accessi Internet, il SIC ricorrerà al competente Servizio SCPT. In questo caso, considerando il numero stimato di casi si calcolano emolumenti annui per un ammontare di circa 500 000 franchi.

68 RS **833.1**

Per i lavori di traduzione delle comunicazioni registrate occorre preventivare annualmente circa 800 000 franchi.

Anche i costi per l'indennizzo dei fornitori nel caso dell'esplorazione di segnali via cavo (art. 38 segg.) sono stimati, per analogia con l'indennizzo della sorveglianza delle telecomunicazioni eseguita mediante il Servizio SCPT, a circa 500 000 franchi.

Determinate tecnologie, per esempio per la penetrazione in sistemi di ordinatori particolarmente protetti, sono ancora poco sviluppate. Considerando anche il fatto che il mercato per questi sistemi è relativamente piccolo e volatile e, inoltre, che in questo campo lo sviluppo tecnico è molto rapido, attualmente i costi di questi sistemi possono essere stimati soltanto approssimativamente.

Per l'equipaggiamento dei posti supplementari e la formazione delle persone interessate sono previsti costi per circa 720 000 franchi (35 000 franchi per posto a tempo pieno).

3.1.2 Ripercussioni sull'effettivo del personale

Per l'attuazione delle nuove misure proposte per l'acquisizione di informazioni, si farà ricorso per quanto possibile alle strutture esistenti (SIC, Base d'aiuto alla condotta dell'esercito [BAC], Servizio SCPT del DFGP). Complessivamente occorre comunque prevedere circa 20,5 posti supplementari, ripartiti tra le seguenti nuove funzioni: nel SIC tecnici operativi per la gestione tecnica delle misure di acquisizione soggette ad autorizzazione, analisti per l'analisi operativa di informazioni acquisite con misure soggette ad autorizzazione, giuristi per la preparazione delle domande, il controllo dell'esecuzione e i resoconti in relazione con le misure di acquisizione soggetti ad autorizzazione nonché altri posti per il controllo della qualità dei nuovi sistemi e la direzione dell'esplorazione dei segnali via cavo. Altri posti saranno necessari in seno al Tribunale amministrativo federale per la procedura di autorizzazione delle misure di acquisizione, presso l'Archivio federale per l'archiviazione e presso il Centro operazioni elettroniche (COE) della BAC per l'esercizio a titolo sperimentale dell'esplorazione di segnali via cavo. Per questi 20,5 posti è prevista un'occupazione scaglionata (il primo anno [prima priorità] 12 posti, il secondo anno [seconda priorità] 8,5 posti).

Le esigenze in materia di conservazione dei dati, più elevate rispetto a quelle attuali, saranno in gran parte soddisfatte ricorrendo alle risorse disponibili.

3.1.3 Altre ripercussioni

Per loro natura, le prestazioni di supporto a favore di terzi non sono pianificabili. L'approntamento delle risorse finanziarie e di personale necessarie deve essere regolato caso per caso con i destinatari e il mandante. Dipende, tra l'altro, dalle possibilità del SIC.

Non sono pianificabili neanche gli impieghi svolti dal SIC in situazioni particolari per tutelare interessi nazionali essenziali secondo l'articolo 3. In quest'ambito non vengono inoltre richiesti né posti supplementari né risorse materiali a titolo di riserva. Nel caso in cui, per l'adempimento di un simile compito, il SIC non possa ricor-

rere a risorse, conoscenze specialistiche e mezzi già disponibili, è necessario farne richiesta.

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

Secondo la concezione del disegno di legge, il SIC assume i compiti di intelligence in collaborazione con le autorità d'esecuzione cantonali.

L'attuale organizzazione decentrata e la stretta collaborazione con i Cantoni hanno dato buone prove e sono mantenute. Come sinora, i Cantoni sono in primo luogo responsabili della sicurezza interna nei rispettivi territori. Nella misura in cui, secondo la Costituzione federale (Cost.) e le leggi, la Confederazione è responsabile della sicurezza interna, i Cantoni prestano a quest'ultima assistenza amministrativa e giudiziaria. Il SIC collabora strettamente con la Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS) e con la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP).

In linea di principio, nel caso di determinate minacce tutte le autorità e unità amministrative dei Cantoni sono tenute a fornire informazioni in virtù del principio dell'assistenza amministrativa. Le informazioni possono essere richieste dal SIC o dalle autorità d'esecuzione cantonali.

Quale novità, le autorità d'esecuzione cantonali non gestiscono più alcuna collezione di dati propria nel campo di applicazione del presente disegno di legge. In contropartita hanno accesso alle informazioni del SIC necessarie per l'adempimento dei loro compiti. Per le autorità d'esecuzione cantonali il disegno prevede un accesso al sistema INDEX SIC mediante procedura di richiamo. Grazie a questo accesso, i Cantoni possono richiamare, tra l'altro, i rapporti e gli accertamenti preliminari che essi stessi hanno allestito.

L'organo di controllo del DDPS sulle attività informative può eseguire controlli in quei settori in cui le autorità d'esecuzione cantonali sono chiamate a eseguire la presente legge.

Per quanto riguarda la vigilanza parlamentare, si rimanda al commento all'articolo 77.

Come sinora, il SIC continuerà a contribuire al finanziamento delle autorità d'esecuzione cantonali.

3.3 Ripercussioni per l'economia e per la società

Le norme proposte rafforzano la sicurezza interna ed esterna e migliorano pertanto ulteriormente la protezione della popolazione. Inoltre, un contesto sicuro e socialmente stabile favorisce indirettamente condizioni quadro economiche migliori, con il conseguente rafforzamento della piazza economica svizzera.

3.4 Altre ripercussioni

Dal punto di vista formale, il disegno di legge non attua alcun impegno internazionale diretto. Può tuttavia favorire un miglioramento duraturo della reputazione della Svizzera a livello internazionale, soprattutto perché il Paese dimostra la propria volontà di combattere efficacemente il terrorismo. In particolare, l'ampliamento delle misure di acquisizione di informazioni migliorerà presumibilmente la collaborazione internazionale.

4 Programma di legislatura e strategie nazionali del Consiglio federale

4.1 Rapporto con il programma di legislatura

Il disegno di legge è annunciato nel messaggio del 25 gennaio 2012[69] sul programma di legislatura 2011–2015 e nel decreto federale del 15 giugno 2012[70] sul programma di legislatura 2011–2015.

4.2 Rapporto con le strategie nazionali del Consiglio federale

Il 25 marzo 2009 il nostro Collegio ha deciso di raggruppare l'allora Servizio di analisi e prevenzione (servizio informazioni interno) e il Servizio informazioni strategico (servizio informazioni concernente l'estero) in un unico nuovo Ufficio federale. Nel Rapporto del Consiglio federale sulla politica di sicurezza, il SIC è designato quale centro di competenza per tutte le questioni di intelligence relative alla sicurezza interna ed esterna nonché quale strumento della politica di sicurezza. Con il presente disegno di legge si prosegue in maniera coerente su questa strada, riunendo le norme determinanti in un unico atto normativo e adeguandole alle nuove esigenze.

Viene prestata particolare attenzione alle strategie nazionali per la protezione delle infrastrutture critiche[71] e per la protezione della Svizzera contro i cyber-rischi[72]. Entrambe le strategie considerano necessario un ruolo attivo del servizio informazioni per individuare tempestivamente e sventare attacchi a infrastrutture critiche. L'articolo 6 concernente i compiti del SIC è stato esplicitamente integrato in tal senso. Nella misura in cui gli attacchi a infrastrutture critiche sono sferrati con mezzi delle tecnologie dell'informazione e della comunicazione, occorre essere in grado di contrastarli attivamente (cfr. art. 25 cpv. 1 lett. d.).

69 FF **2012** 305, in particolare 380 e 432.
70 FF **2012** 6413, in particolare 6417.
71 www.bevoelkerungsschutz.admin.ch > Temi > Protezione delle infrastrutture critiche > Pubblicazioni PIC > Strategia di base del Consiglio federale per la protezione delle infrastrutture critiche
72 www.isb.admin.ch > Temi > Cyber-rischi SNPC > Strategia nazionale per la protezione della Svizzera contro i cyber-rischi SNPC

5 Aspetti giuridici

5.1 Costituzionalità e legalità

Secondo le norme costituzionali che disciplinano la ripartizione delle competenze tra la Confederazione e i Cantoni, la Confederazione può legiferare là dove la Costituzione federale le assegna la necessaria competenza. Per i compiti non assegnati alla Confederazione sono competenti i Cantoni in virtù delle norme generali (art. 3 e 42 cpv. 1 Cost.).

Nell'ambito della sicurezza interna ed esterna, tuttavia, il testo costituzionale, da solo, non è determinante per stabilire se la Costituzione federale attribuisca o no alla Confederazione una competenza per legiferare. Le competenze che derivano dall'esistenza stessa della Confederazione in quanto Stato ricadono infatti nella sfera di competenza della Confederazione anche se non sono espressamente citate nella Costituzione federale (le cosiddette competenze intrinseche; cfr. DTF *117* Ia 202, consid. 4a). È per esempio intrinseca la competenza della Confederazione ad adottare, a livello interno ed esterno, le misure necessarie per la propria salvaguardia e per quella dei propri organi e delle proprie istituzioni; la Confederazione deve garantire e assicurare la sopravvivenza della comunità svizzera nel suo complesso e provvedere a contrastare gli eventuali pericoli che ne potrebbero minacciare l'esistenza. La competenza intrinseca della Confederazione nell'ambito della sicurezza interna ed esterna comprende anche competenze legislative.

Nell'ambito della sicurezza esterna, la Confederazione dispone inoltre di una competenza generale che include a sua volta ampie competenze legislative. Tra queste figura tra l'altro la competenza di acquisire informazioni concernenti l'estero che possono essere importanti per la valutazione della situazione in materia di politica di sicurezza. Nella misura in cui sussiste una stretta relazione con gli affari esteri, l'articolo 54 della Costituzione federale funge anche da base costituzionale per atti normativi nazionali.

La dottrina costituzionale considera certa l'esistenza di un diritto costituzionale non scritto. In virtù della situazione giuridica vigente, la Confederazione dispone pertanto della competenza per legiferare sia in materia di protezione dello Stato in Svizzera che nell'ambito del servizio informazioni concernente l'estero. Secondo la nuova prassi, per queste competenze della Confederazione, che derivano dall'esistenza e dalla natura stessa di quest'ultima e che non le vengono assegnate in maniera esplicita, si fa riferimento all'articolo 173 capoverso 2 Cost. Nel presente contesto non è pertanto obbligatorio istituire una base costituzionale esplicita per il servizio informazioni. Tale esigenza era stata sollevata da alcuni partecipanti alla procedura di consultazione, che si erano basati tra l'altro su conoscenze risultanti dal rapporto del Consiglio federale in adempimento del postulato Malama. Tuttavia, sebbene nel rapporto in questione si raccomandasse di introdurre, nell'ambito di un ampio aggiornamento normativo a livello di ripartizione costituzionale delle competenze tra la Confederazione e i Cantoni in materia di sicurezza interna, anche una base costituzionale esplicita per l'attività di protezione dello Stato da parte della Confederazione, durante la deliberazione sul rapporto le Camere federali hanno rinunciato a conferire un mandato in tal senso al Consiglio federale. Con il presente disegno di legge, il Collegio governativo non si spinge oltre competenze già assegnate alla Confederazione dalla Costituzione e può pertanto fondarsi su una base costituzionale sufficiente.

Tutela dei diritti fondamentali delle persone in Svizzera

Nell'ambito del presente progetto, ingerenze gravi nei diritti fondamentali possono prodursi in occasione di misure di acquisizione soggette ad autorizzazione (p. es. nel caso di intercettazioni telefoniche o di registrazioni audiovisive in spazi privati). Ciò interessa soprattutto il diritto fondamentale alla protezione della sfera privata (art. 13 Cost.; art. 8 CEDU) nonché, a seconda delle circostanze, altre garanzie quali la libertà personale (art. 10 cpv. 2 Cost.) e la libertà d'opinione e d'informazione (art. 16 Cost.; art. 10 CEDU). Le misure di acquisizione soggette ad autorizzazione secondo il presente disegno di legge sono eseguite soltanto in Svizzera.

Le misure di acquisizione soggette ad autorizzazione che figurano nel disegno tengono conto dell'esigenza di una base legale formale che soddisfi anche il principio di determinatezza. Le regolamentazioni proposte soddisfano inoltre i requisiti della proporzionalità e dell'esistenza di un interesse pubblico sufficiente contemplati dalla Costituzione federale.

Per quanto riguarda la natura della prevista acquisizione di informazioni, il disegno non prevede misure che contemplino lesioni dell'integrità fisica, come ispezioni corporali o l'applicazione della coercizione fisica. Simili misure continuano a essere riservate alle autorità di polizia a cui è consentito impiegare, per l'adempimento dei propri compiti, la coercizione di polizia o misure di polizia (cfr. legge del 20 marzo 2008[73] sulla coercizione).

Infine, il disegno di legge (come già la LMSI) contempla il divieto fondamentale di raccogliere in Svizzera informazioni sull'attività politica e sull'esercizio della libertà d'opinione, della libertà di riunione o della libertà di associazione. Al riguardo, si rinvia al commento relativo all'articolo 5 capoverso 5.

Tutela dei diritti fondamentali delle persone all'estero

L'acquisizione di informazioni concernenti l'estero è un tema delicato, poiché potrebbero essere pregiudicati la sovranità di Stati esteri e i diritti fondamentali di cittadini stranieri (p. es. la tutela della sfera privata).

L'acquisizione di informazioni concernenti l'estero deve pertanto avvenire esclusivamente quando le informazioni necessarie non possono essere acquisite in Svizzera. Essa serve in primo luogo a valutare e sventare minacce per la Svizzera dal punto di vista della politica di sicurezza, per esempio negli ambiti del terrorismo e della proliferazione, e viene impiegata per valutare lo sviluppo di rapporti egemonici e conflitti.

Nel muoversi tra gli interessi svizzeri in materia di sicurezza e la tutela dei diritti fondamentali di persone all'estero occorre sempre tenere in considerazione i diritti fondamentali. La LAIn concretizza tale aspetto stabilendo che un'eventuale ingerenza nei diritti fondamentali non deve essere sproporzionata rispetto al valore atteso delle informazioni.

La tutela dei diritti fondamentali meno ampia, a livello di procedura, rispetto a quanto previsto per la Svizzera riguarda soprattutto le misure di acquisizione ai sensi dell'articolo 22 del disegno di legge. A prescindere dalle riflessioni di principio menzionate in precedenza, contro un obbligo dell'autorizzazione analogo a quello vigente in Svizzera depongono i motivi seguenti:

73 RS **364**

- a causa della distanza, per l'autorità svizzera di autorizzazione sarebbe difficile o addirittura impossibile farsi un'idea della situazione sul posto in tempo utile e, su tale base, adottare una decisione appropriata;
- l'autorizzazione dell'autorità svizzera non modificherebbe minimamente l'illegalità della misura nei confronti del diritto estero.

Se per contro le informazioni concernenti l'estero sono acquisite in Svizzera, si applica la tutela dei diritti fondamentali vigente per la Svizzera, in particolare per quanto riguarda le misure di acquisizione soggette ad autorizzazione. È fatta salva l'introduzione in sistemi e reti di ordinatori ubicati all'estero (art. 36).

Delimitazione rispetto all'attività delle autorità di polizia e di perseguimento penale

Gli accertamenti informativi sono volti a chiarire l'eventuale esistenza di una minaccia per la Svizzera rilevante dal punto di vista della politica di sicurezza. Tale minaccia può essere generata sia da un comportamento che, in ultima analisi, si rivela non punibile, sia da un comportamento perseguibile penalmente. I risultati degli accertamenti informativi vengono in primo luogo comunicati ai decisori politici, ossia agli organi esecutivi di Confederazione e Cantoni, affinché essi possano intervenire in tempo utile secondo il rispettivo diritto determinante. Se il servizio informazioni, nell'ambito dei propri accertamenti, scopre l'esistenza di reati concreti, ne informa anche le autorità di perseguimento penale.

Le indagini nell'ambito del perseguimento penale servono invece a chiarire un eventuale sospetto di reato o la colpevolezza di un individuo e si concentrano sugli elementi dei reati in questione e non primariamente sugli aspetti legati alla politica di sicurezza. Gli organi di perseguimento penale includono i risultati delle loro indagini nei procedimenti giudiziari, ma non li presentano alle autorità politiche. Tali organi non hanno infatti interessi diretti in materia di politica di sicurezza, sebbene il buon esito del perseguimento penale sia utile anche a tutelare gli interessi in materia di sicurezza.

L'accertamento di situazioni di minaccia in ambito informativo si distingue dalle indagini in caso di reati perseguibili secondo il Codice penale. Cambiano infatti gli eventi scatenanti (a livello informativo: sospetto di minaccia per la sicurezza della Svizzera; a livello penale: sospetto che sia stato commesso un reato concreto), l'oggetto stesso degli accertamenti (a livello informativo: smascherare intenzioni, strutture e reti; a livello penale: provare l'esistenza di un comportamento perseguibile penalmente) e l'obiettivo primario perseguito (a livello informativo: fornire all'Esecutivo una base decisionale per adottare le necessarie misure; a livello penale: chiarire un sospetto di reato o la colpevolezza di un individuo).

Punti di contatto si riscontrano quando, in un singolo caso concreto, gli accertamenti informativi finalizzati alla sicurezza della Svizzera coincidono con le indagini condotte dalle autorità di perseguimento penale in merito a comportamenti rilevanti dal punto di vista penale in quanto la persona sospettata di reato o lo stesso presunto reato sono contemporaneamente oggetto di interessi legati alla prevenzione. La stessa persona o lo stesso reato possono pertanto essere all'origine di accertamenti simultanei, seppure da punti di vista fondamentalmente diversi. Di conseguenza, le rispettive procedure possono in parte completarsi, ma non sostituirsi l'una all'altra. La legge sulle attività informative consente di coordinare queste attività disciplinando i flussi di informazioni e gli accordi in tale ambito.

5.2 Compatibilità con gli impegni internazionali della Svizzera

Nel diritto internazionale pubblico non esiste un disciplinamento contrattuale esaustivo in materia di spionaggio internazionale. Secondo il diritto consuetudinario internazionale, le attività di spionaggio sono in certa misura tollerate nell'ambito delle relazioni internazionali. Di regola, gli Stati oggetto di spionaggio non considerano quest'ultimo una violazione del diritto internazionale pubblico, bensì un atto non amichevole. Nel contempo, la maggior parte degli Stati si riserva esplicitamente il diritto di condurre attività di spionaggio all'estero. L'assenza di un divieto generale di spionaggio internazionale nel diritto internazionale pubblico non impedisce tuttavia agli Stati di prevedere, nel proprio diritto nazionale, conseguenze penali per chi svolge attività di spionaggio. La maggioranza degli Stati, tra cui la Svizzera, contempla simili disposizioni penali nel proprio diritto nazionale, che spesso prevede anche misure di controspionaggio per contrastare le attività di spionaggio condotte da altri Paesi.

Sebbene lo spionaggio in sé non sia vietato dal diritto internazionale pubblico, quest'ultimo prevede, in determinati ambiti parziali, norme in grado di limitare le attività di spionaggio condotte all'estero. Simili norme sono per esempio contemplate da diversi strumenti volti alla protezione dei diritti fondamentali e dei diritti dell'uomo, come pure dalla Convenzione di Vienna del 18 aprile 1961[74] sulle relazioni diplomatiche. In linea di principio, la protezione dei diritti fondamentali e dei diritti dell'uomo deve essere accettata anche nell'ambito di operazioni condotte all'estero da organi statali. Spesso, invece, è proprio la Convenzione di Vienna a non essere rispettata nella prassi, per esempio abusando delle prerogative diplomatiche per svolgere attività di spionaggio o ignorando la protezione diplomatica di determinate persone e installazioni per procedere ad accertamenti informativi nei loro confronti.

Ciò riguarda in particolare, tra l'altro, il diritto fondamentale alla protezione della sfera privata (art. 13 Cost.; art. 8 CEDU; art. 17 del Patto II dell'ONU[75]) come pure, a seconda delle circostanze, altre garanzie quali i diritti fondamentali rappresentati dalla libertà d'opinione e d'informazione (art. 16 Cost.; art. 10 CEDU; art. 19 del Patto II dell'ONU), dalla libertà dei media (art. 17 Cost.; art. 10 CEDU), dalla libertà di riunione (art. 22 Cost.; art. 11 CEDU; art. 21 del Patto II dell'ONU) e dalla libertà d'associazione (art. 23 Cost.; art. 11 CEDU; art. 22 del Patto II dell'ONU), nonché la libertà personale (art. 10 cpv. 2 Cost.), la libertà di credo e di coscienza (art. 15 Cost.; art. 9 CEDU; art. 18 del Patto II dell'ONU), la libertà economica (art. 27 Cost.) o l'uguaglianza giuridica (art. 8 Cost.; art. 2 e 26 del Patto II dell'ONU). Nel presente contesto, la protezione della sfera privata (art. 13 Cost.; art. 8 CEDU; art. 17 del Patto II dell'ONU) può essere considerata un «diritto fondamentale guida».

In quest'ambito va inoltre ricordato che, a partire da una certa gravità, le ingerenze nei diritti fondamentali devono previamente essere sottoposte a una procedura di autorizzazione da parte dell'organo giudiziario (Tribunale amministrativo federale) e degli organi politici competenti. Al termine di un'operazione, il SIC deve altresì informare della misura di acquisizione le persone che ne sono state oggetto e la

74 RS **0.191.01**
75 RS **0.103.2**; Patto internazionale del 16 dicembre 1966 relativo ai diritti civili e politici

misura stessa può essere sottoposta a un ulteriore controllo giudiziario a posteriori (Tribunale amministrativo federale con possibilità di interporre ricorso presso il Tribunale federale). Pertanto, considerati anche i vigenti diritti d'accesso (conformemente alla legge sulla protezione dei dati [LPD] o in virtù della possibilità di presentare una domanda in tal senso, tramite l'IFPDT o il Tribunale amministrativo federale, per tutta la durata di un interesse motivato al mantenimento del segreto), si dispone di misure efficaci ai sensi della CEDU contro eventuali abusi.

Le attività del SIC previste nel disegno di legge sono quindi conformi al diritto internazionale pubblico.

In materia di diritto internazionale pubblico si pongono alcune questioni particolari quando, all'estero, non ci si limita ad acquisire attivamente informazioni di intelligence ma, come reazione a un cyber-attacco sferrato dall'estero, si adottano misure volte a introdursi in reti e sistemi informatici per disturbare, impedire o rallentare l'accesso a informazioni. Se decide di adottare simili misure, il Consiglio federale valuterà caso per caso tutti gli aspetti legati al diritto internazionale pubblico.

5.3 Forma dell'atto

Secondo l'articolo 164 capoverso 1 Cost., tutte le disposizioni importanti che contengono norme di diritto sono emanate sotto forma di legge federale, in particolare quelle che concernono diritti costituzionali. Ciò viene garantito con il presente disegno di legge.

5.4 Subordinazione al freno alle spese

Secondo l'articolo 159 Cost., le disposizioni in materia di sussidi nonché i crediti d'impegno e le dotazioni finanziarie implicanti nuove spese uniche di oltre 20 milioni di franchi o nuove spese ricorrenti di oltre 2 milioni di franchi richiedono il consenso della maggioranza dei membri di ciascuna Camera. Il presente disegno di legge contiene una disposizione in materia di sussidi che esiste già e di cui è previsto il mantenimento entro il limite attuale (8,4 mio. di fr.). Al momento della sua emanazione, tale disposizione non era stata subordinata al freno alle spese. Ciò avverrà nell'ambito dell'adozione del presente disegno di legge. L'articolo 81 capoverso 5 è pertanto subordinato al freno alle spese.

5.5 Conformità alla legge sui sussidi

Nell'ambito della procedura di consultazione, i Cantoni hanno chiesto all'unanimità un indennizzo per le spese derivanti dall'adempimento del mandato ricevuto dalla Confederazione e, pertanto, una deroga al principio secondo cui i Cantoni si fanno carico delle spese di esecuzione del diritto federale. Per questo il disegno di legge stabilisce, all'articolo 81 capoverso 5, che la Confederazione, nei limiti dei crediti stanziati, indennizzi i Cantoni per le prestazioni che forniscono nell'ambito dell'esecuzione della presente legge. Il Consiglio federale stabilisce forfettariamente l'indennizzo sulla base del numero di persone attive prevalentemente per compiti della Confederazione. Tale disposizione, che copre soltanto in parte le spese dei

Cantoni, corrisponde interamente alla legislazione attualmente in vigore (cfr. art. 28 cpv. 1 LMSI). È opportuno mantenere tale prassi, che continua a essere giustificata dalla particolare situazione a livello di esecuzione:

«… La non assunzione delle spese di collaborazione al trattamento delle informazioni potrebbe avere implicazioni fatali: il mandato di ricercare un luogo di soggiorno o di osservare una persona può avere ripercussioni finanziarie totalmente diverse. Se la Confederazione non partecipa alle spese, vi potrebbero essere numerose risposte negative alle domande di collaborazione, poiché certi Cantoni rinuncerebbero a mettere a disposizione personale specialmente formato per interventi adeguati alla minaccia. […] È quindi nell'interesse della Confederazione che i Cantoni dispongano di specialisti capaci che, sulla base di un'ottima conoscenza delle contingenze locali, siano in grado di conseguire i risultati sperati grazie all'impiego di mezzi ragionevoli. Il personale assunto della Confederazione costerebbe certo più caro: questa alternativa è d'altro canto da respingere per considerazioni d'ordine federalista. Un rimborso adeguato delle spese dipende quindi dal numero di persone che, in un Cantone determinato, lavorano per la Confederazione».[76]

Queste riflessioni sono tuttora valide, tanto più che, presumibilmente, con l'entrata in vigore della legge sulle attività informative non si ridurranno le spese d'esecuzione per i Cantoni. Gli attuali indennizzi ammontano complessivamente a 8,4 milioni di franchi e si prevede di mantenerli entro tale limite anche dopo l'entrata in vigore della presente legge.

5.6 Delega di competenze legislative

La legge contiene norme di delega per l'emanazione di prescrizioni a livello di ordinanza nella misura in cui il Consiglio federale, in qualità di autorità competente per il diritto regolamentare, può emanare ordinanze entro i limiti stabiliti dalla legge. Questa delega è necessaria poiché riguarda disposizioni troppo concrete per essere iscritte nella legge. La competenza a legiferare per via di ordinanza è definita in misura sufficientemente concreta dalle disposizioni della legge.

Oltre alle competenze di cui già dispone, il Collegio governativo potrà emanare caso per caso disposizioni nei seguenti ambiti:

- categorie di collaboratori del SIC che portano armi e relativa istruzione (art. 8 cpv. 3);
- collaborazione e scambio di informazioni tra il SIC e gli organi competenti del Servizio informazioni dell'esercito, nonché 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. 11 cpv. 3);
- fatti e constatazioni che devono essere comunicati spontaneamente al SIC da determinate autorità ed estensione dell'obbligo di comunicazione e procedura per fornire le informazioni (art. 20 cpv. 4);

76 Commento all'articolo 26 nel messaggio del 7 marzo 1994 concernente la legge federale sulle misure per la salvaguardia della sicurezza interna e sull'iniziativa popolare «S.o.S. – per una Svizzera senza polizia ficcanaso», FF **1994** II 1004, in particolare 1075 seg.

- ambiti di esplorazione, organizzazione e procedura in materia di esplorazione radio, nonché durata massima di conservazione presso il servizio preposto all'esecuzione (art. 37 cpv. 3);
- ambiti di esplorazione ammessi, organizzazione e procedura in materia di esplorazione dei segnali via cavo nonché durata massima di conservazione presso il servizio preposto all'esecuzione (art. 38 cpv. 4);
- indennizzo dei gestori di reti filari e dei fornitori di servizi di telecomunicazione (art. 42 cpv. 4);
- comunicazione, da parte delle autorità d'esecuzione, di valutazioni della situazione e di dati ricevuti dal SIC (art. 45 cpv. 3);
- dettagli del trattamento dei dati per ogni sistema d'informazione (art. 46 cpv. 2);
- categorie di persone da registrare nel sistema d'informazione Quattro P (art. 54 cpv. 4);
- diritti d'accesso, durata di conservazione e sicurezza dei dati provenienti da misure di acquisizione soggette ad autorizzazione (art. 57 cpv. 4);
- direzione del servizio informazioni sul piano politico, assegnazione del mandato fondamentale, approvazione della lista d'osservazione, determinazione dei gruppi da considerare di matrice estremista violenta, valutazione della situazione di minaccia ecc. (art. 69);
- in situazioni particolari, conferimento al SIC del mandato di salvaguardare interessi essenziali della Svizzera secondo l'articolo 3, nonché durata, scopo, genere ed estensione delle misure necessarie (art.70);
- allestimento della lista d'osservazione (art. 71 cpv. 3);
- composizione e organizzazione dell'autorità di controllo indipendente che verifica la legalità dell'esplorazione radio (art. 75 cpv. 4);
- vigilanza finanziaria dei settori d'attività del SIC che richiedono una particolare tutela del segreto, nonché requisiti minimi per quanto riguarda i controlli nei Cantoni e le competenze degli organi di vigilanza della Confederazione e dei Cantoni (art. 76 cpv. 3);
- vigilanza cantonale: ricorso a organi di vigilanza per assistere l'autorità cantonale di vigilanza, accesso a informazioni sull'esistenza e sul contenuto dei mandati eseguiti per la Confederazione nonché sulle modalità con le quali le autorità d'esecuzione cantonali li eseguono e separazione fra i dati trattati in modo autonomo dalle autorità d'esecuzione cantonali e i dati che esse trattano su mandato del SIC o sulla base della lista d'osservazione (art. 78 cpv. 3);
- indennizzo dei Cantoni per le prestazioni che forniscono per l'ambito dell'esecuzione della presente legge (art. 81 cpv. 5).

5.7 Protezione dei dati

La legge deve consentire al SIC di allestire un'ampia base di informazioni attingendo a molteplici fonti al fine di garantire un'individuazione tempestiva e una valutazione completa delle minacce per la sicurezza interna ed esterna della Svizzera. D'altro canto, tuttavia, occorre garantire per quanto possibile il rispetto dei diritti fondamentali delle persone su cui si acquisiscono informazioni. Questa tensione tra sicurezza e libertà rende necessaria una regolamentazione differenziata dell'acquisizione e della gestione dei dati. In funzione della tematica, della fonte e del grado di sensibilità, i dati del SIC vengono archiviati in diversi sistemi d'informazione che, a loro volta, sottostanno a varie regolamentazioni. Le condizioni più severe in materia di trattamento dei dati sono previste per il sistema d'informazione che contiene le informazioni sull'estremismo violento (IASA-GEX). Ciò tiene conto del fatto che, in base alle esperienze raccolte, il trattamento dei dati nell'ambito dell'estremismo violento si è sempre rivelato una questione particolarmente delicata, sia politicamente sia sotto il profilo della protezione dei dati. Non ha invece praticamente mai dato adito a critiche il trattamento dei dati in altri ambiti quali il controspionaggio, la proliferazione o la protezione di infrastrutture critiche.

Per ogni sistema d'informazione, la legge disciplina lo scopo, il contenuto e la cerchia di utenti. Se è previsto un accesso online esterno, quest'ultimo viene specificamente indicato.

Le prescrizioni per la gestione e il controllo della qualità dei dati vengono ulteriormente inasprite rispetto al diritto vigente. In particolare, le nuove disposizioni esigono una rigorosa selezione d'entrata e uno smistamento dei dati. La condizione necessaria per memorizzare qualsiasi informazione è che vi sia sempre un sufficiente nesso contenutistico con i compiti del SIC. Occorre altresì garantire che i dati vengano esaminati per quanto riguarda l'esattezza e la rilevanza. Un esame analogo va inoltre effettuato nel caso in cui il SIC intenda comunicare dati personali a terzi (p. es. in un rapporto di analisi, una comunicazione a un'autorità o una valutazione della situazione). Il SIC deve ora verificare periodicamente che tutti i dati memorizzati nei suoi sistemi d'informazione siano ancora necessari all'adempimento dei compiti previsti dalla legge. I dati che non servono più o che hanno raggiunto la durata massima di conservazione vengono cancellati.

Un'ulteriore novità è rappresentata dal fatto che la legge prevede un'ampia centralizzazione a livello federale delle prescrizioni concernenti la protezione dei dati. La Confederazione mette a disposizione delle autorità d'esecuzione cantonali i sistemi d'informazione necessari e gestisce i dati, che ora sottostanno completamente alle disposizioni della Confederazione.

La legge conferma il divieto fondamentale, contemplato dalla LMSI, di raccogliere in Svizzera informazioni sull'attività politica e sull'esercizio della libertà d'opinione, della libertà di riunione o della libertà di associazione.

In conclusione, va ricordato che, salvo disposizioni derogatorie speciali, i principi e le prescrizioni della LPD si applicano anche al servizio informazioni.