Legge sul servizio informazioni (LSI)

Rapporto esplicativo relativo all'avamprogetto

8 marzo 2013

Compendio

Il presente avamprogetto intende creare una base legale formale unitaria per il servizio informazioni civile svizzero (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.

Il SIC fa parte, come l'esercito, la politica estera e la polizia, degli strumenti di politica di sicurezza della Confederazione.

L'obiettivo principale dell'avamprogetto 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:

Quasi contemporaneamente all'approvazione della legge federale del 3 ottobre 2008 sul servizio informazioni civile (LSIC), il Consiglio federale aveva deciso, in una prima fase, di trasferire al 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, il Governo federale 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 creerà una base legale per i compiti, i diritti, gli obblighi e i sistemi d'informazione del servizio informazioni civile. L'avamprogetto di legge non rappresenterà un ulteriore sviluppo delle basi legali vigenti, 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 (in particolare per quanto riguarda la raccolta di dati personali) e prende meglio in considerazione i mutamenti sul fronte dei rischi e delle minacce.

Il presente avamprogetto di legge comprende essenzialmente le seguenti novità:

- *base legale unitaria per il SIC: l'attuale suddivisione delle basi legali tra legge federale del 3 ottobre 2008[1] sul servizio informazioni civile (LSIC) e legge federale del 21 marzo 1997[2] sulla 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 dalla Svizzera e minacce provenienti*

[1] RS **121**
[2] RS **120**

dall'estero, bensì tra, da un lato, l'estremismo violento con riferimento alla Svizzera e, dall'altro, i rimanenti ambiti di minacce e compiti.

- *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, l'impiego di apparecchi tecnici di sorveglianza nel settore privato ecc. presentati 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 ed 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 (Tribunale amministrativo federale) e una politica (capo del DDPS) decideranno nel singolo caso in merito all'autorizzazione di queste misure;*
- *conservazione e rilevamento differenziati dei dati: l'avamprogetto 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 di sistemi d'informazione. 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 partner, valutazione della situazione), 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/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 nuove misure di acquisizione soggette ad autorizzazione e l'esplorazione dei segnali via cavo sono dal canto loro applicabili solo se il Tribunale amministrativo federale ha autorizzato l'impiego di tali misure e il capo del DDPS ha concesso il relativo nullaosta. Con questi meccanismi si intende garantire la legalità e la proporzionalità delle attività del SIC.*

Indice

Rapporto esplicativo relativo all'avamprogetto

1 Parte generale

1.1 Introduzione

Il presente avamprogetto intende creare 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.

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 della Svizzera.

Il rapporto del Consiglio federale all'Assemblea federale del 23 giugno 2010[3] sulla politica di sicurezza della Svizzera (RAPOLSIC 2010) 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 il Consiglio federale ha contemporaneamente definito i limiti che la Costituzione prevede per i compiti del SIC.

L'obiettivo principale dell'avamprogetto 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.

1.2 Antefatti e mandato del Consiglio federale

Nel rapporto del 29 febbraio 2008[4] sull'iniziativa parlamentare «Trasferimento dei compiti dei servizi informazioni civili a un dipartimento», la Commissione della gestione del Consiglio degli Stati si era, tra l'altro, espressa come segue in merito all'attività dei servizi informazioni:

«Le attività dei due servizi (nota: si intendono il SIS e il SAP) 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

[3] FF **2010** 4511
[4] FF **2008** 3439

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 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 e del DDPS. 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 sul servizio informazioni civile (LSIC)[5], elaborata in seguito all'iniziativa parlamentare, è stata approvata il 3 ottobre 2008 dalle Camere federali ed è entrata in vigore il 1° gennaio 2010.

Dopo l'approvazione della LSIC il Consiglio federale 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, il Governo federale ha deciso nel marzo del 2009 di riunire il SIS e il SAP nel SIC, con effetto dal 1° gennaio 2010.

[5] RS **121**

Quale terza fase, il Consiglio federale ha 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):

«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) 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 Consiglio federale, ai fini di una rielaborazione, il progetto legislativo LMSI II del 15 giugno 2007 (Mezzi speciali per la ricerca di informazioni: «LMSI II»). In quell'occasione non si era giunti all'esame dei contenuti dei singoli articoli. Il dibattito parlamentare si era limitato alla questione dell'entrata in materia. Non sono pertanto possibili deduzioni precise sul consenso politico di allora riguardo a singoli elementi del progetto legislativo.

Successivamente, il Consiglio federale aveva deciso di scaglionare i lavori legislativi (decisione del Consiglio federale del 27 novembre 2009): nell'ambito di un primo progetto legislativo occorreva concretizzare 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 «LMSI II ridotta» e approvata dal Parlamento in data 23 dicembre 2011. La LMSI riveduta è entrata in vigore il 16 luglio 2012.

Il secondo progetto legislativo doveva essere focalizzato sulla citata legge sul servizio informazioni.

1.3 Genesi del presente avamprogetto di legge

Per preparare la nuova legge il SIC ha istituito un gruppo di lavoro interdipartimentale (GLID) composto di rappresentanti del DDPS, del DFAE, dell'UFG, di fedpol, dell'Incaricato della protezione dei dati e della trasparenza (IFPDT), del Ministero pubblico della Confederazione, dei Cantoni e del SIC.

Il GLID ha iniziato i suoi lavori alla fine del mese di ottobre 2010 e fino al 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 presente avamprogetto di legge. Nel corso dei lavori, gli avamprogetti di legge sono stati di volta in volta sottoposti al GLID per parere.

Laddove si è ritenuto opportuno, nell'avamprogetto di legge sono state integrate le regolamentazioni affermate della LMSI e della LSIC nonché le nuove regolamenta-

zioni della «LMSI II ridotta»[6]. Pertanto, ad esempio l'obbligo d'informazione e l'obbligo di comunicazione speciali e il divieto di determinate attività corrispondono di principio alle pertinenti disposizioni nel messaggio «LMSI II ridotta».

La nuova legge sul servizio informazioni 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 civili svizzeri e prende meglio in considerazione i mutamenti sul fronte dei rischi e delle minacce.

Punti controversi

Sia nella procedura di consultazione concernente l'avamprogetto di legge del 2007, sia nei dibattiti politici pubblici sinora condotti 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 suo messaggio aggiuntivo del 27 ottobre 2010 concernente la modifica della LMSI («LMSI II ridotta») il Consiglio federale aveva rinunciato essenzialmente ai seguenti mezzi per l'acquisizione di informazioni soggetti ad autorizzazione:

- sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni;
- osservazioni in luoghi non liberamente accessibili anche mediante apparecchi tecnici di sorveglianza;
- accesso segreto a un sistema per l'elaborazione di dati.

Questi punti sono stati reintegrati nel presente avamprogetto di legge sul servizio informazioni.

1.4 Obiettivi della nuova legge sul servizio informazioni

Fornire un contributo sostanziale alla sicurezza della Svizzera

Per tutelare i propri interessi e proteggere le cittadine e i cittadini, la Svizzera dipende da 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), elaborarle, 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 accessi-

[6] Messaggio aggiuntivo del 27 ottobre 2010 concernente la modifica della legge sulle misure per la salvaguardia della sicurezza interna («LMSI II ridotta»; FF **2010** 6923).

bili 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. L'avamprogetto di legge completa pertanto le misure di acquisizione attuali nel settore della sicurezza interna introducendo misure di acquisizione soggette ad autorizzazione. Esso disciplina altresì l'acquisizione di informazioni da parte dei Cantoni, ossia da parte delle autorità d'esecuzione cantonali, che raccolgono tali informazioni nel quadro della presente legge.

Il SIC nel suo insieme provvede a rifornire 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 condotta 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 della NATO e/o dell'Unione europea (UE). La costituzione di nuovi organismi come il G20, in seno al quale vengono adottate decisioni di vasta portata che interessano anche la Svizzera, ma per le quali il nostro Paese non viene praticamente consultato, completa questo quadro. Proprio i membri dell'UE e della NATO sono strettamente interconnessi anche sul piano informativo. 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 partner e alle informazioni ottenute per loro tramite, il SIC sostiene la politica estera della Svizzera.

Emanazione di un disciplinamento globale

Il presente avamprogetto attua la decisione del Consiglio federale del 27 novembre 2009 e costituisce un disciplinamento 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 legislativo.

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

L'avamprogetto 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, il Consiglio federale definisce nel dettaglio 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 nonché 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 alla concezione della LMSI. Quest'ultima è stata influenzata dal cosiddetto «affare delle schedature», 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 l'elaborazione delle informazioni preliminarmente al perseguimento penale è 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, l'elaborazione 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[7] sulla protezione dei dati. 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 dei mezzi e degli strumenti a loro disposizione. Essi richiedevano inoltre rapporti circostanziati sulla situazione in materia di sicurezza. Nel mese di novembre 2001, il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia (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 ha approvato il rapporto «Analisi della situazione attuale e dei rischi per la Svizzera dopo gli attacchi terroristici dell'11 settembre 2001» e ha nel contempo 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 Consiglio federale 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 Consiglio federale, per rielaborazione, 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 d'informazioni, le autorità di intelligence devono cercare di ottenere informazioni, con un onere incomparabilmente 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 precoce e nella cooperazione internazionale.

[7] RS **235.1**

Qualora dovessero essere raccolte informazioni sullo 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 esteri di procurarsi armi di distruzione di massa avvengono attraverso reti internazionali di estrema complessità. Al riguardo, la Svizzera ottiene da terzi ad esempio 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.

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 elettronici di esplorazione (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); e
- nel settore della protezione della piazza finanziaria svizzera (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).

1.5 Punti principali dell'avamprogetto di legge

Nuovo orientamento dell'acquisizione di informazioni

Per quanto riguarda l'acquisizione di informazioni, l'avamprogetto 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 tal modo si intende lasciare definitivamente dietro le spalle il cosiddetto «affare delle schedature», in quanto sarà tracciata una linea di separazione tra terrorismo vero e proprio ed estremismo violento. Come nel caso della conservazione dei dati, anche l'acquisizione 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 61 capoverso 1 lettera c, il Consiglio federale stabilisce annualmente in un elenco quali gruppi devono essere considerati di matrice estremista violenta.

Introduzione di nuove misure di acquisizione negli ambiti del terrorismo, dello spionaggio, della proliferazione e degli attacchi alle infrastrutture critiche oppure per la tutela di altri interessi nazionali essenziali

I mezzi speciali di acquisizione di informazioni menzionati nel progetto legislativo originario LMSI II[8], 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[9]). Nel presente avamprogetto, il catalogo dei mezzi speciali di acquisizione di informazioni contenuto nella LMSI II è stato rielaborato e nel contempo completato. Il Consiglio federale 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;
- informazioni in merito alle comunicazioni per mezzo della corrispondenza postale o del traffico delle telecomunicazioni delle persone sorvegliate;
- 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 cose;
- impiego di apparecchi tecnici di sorveglianza per captare o registrare conversazioni private e osservare o registrare fatti in luoghi non pubblici;
- intrusione in sistemi e reti di ordinatori per acquisire informazioni o 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.

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 22 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. 11 segg.) vengono ampliate. Occorre rendere sfruttabili le possibilità tecniche disponibili

[8] Messaggio del 15 giugno 2007 concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI; FF **2007** 4613)
[9] GAAC 4/2009 (pag. 238-330)

(ad es. impiego di droni). Sinora questi mezzi non hanno potuto essere utilizzati in Svizzera per mancanza di basi legali formali.

Elaborazione differenziata dei dati

L'avamprogetto prevede che le informazioni acquisite dal SIC o le comunicazioni da esso ricevute siano archiviate in una rete 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 partner, 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 autorizzazione oppure sulla base di controlli di frontiera sono trattati separatamente e sono a disposizione soltanto degli specialisti in seno al SIC.

1.6 Diritto comparato e diritto internazionale pubblico

Nel compendio tabellare dell'*allegato II* vengono messi a confronto aspetti scelti di diversi sistemi di intelligence di alcuni Paesi europei. 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, i servizi informazioni spagnolo e olandese sono anch'essi nati da una fusione di precedenti servizi di intelligence;
- Austria e Belgio sono Paesi di dimensioni comparabili a quelle della Svizzera.

1.7 Ripercussioni finanziarie, sul personale ed economiche dell'avamprogetto di legge

Ripercussioni finanziarie

Le ripercussioni finanziarie dipendono fortemente dalle modalità di attuazione delle singole misure e dalla frequenza della loro applicazione. Il Consiglio federale ipotizza 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 ammontano da 5 a 7 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 ad 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 Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. In questo caso, considerando il numero stimato di casi si calcolano emolumenti annui per un ammontare di 500 000 franchi.

Per i lavori di traduzione delle comunicazioni registrate occorre preventivare annualmente circa 800 000 franchi.

I costi per l'indennizzo degli operatori nel caso dell'esplorazione di segnali via cavo (art. 34 segg.) sono stimati, per analogia all'indennizzo della sorveglianza delle telecomunicazioni eseguita mediante il Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, pure a 500 000 franchi.

Determinate tecnologie, ad esempio per l'intrusione in sistemi di ordinatori particolarmente protetti, sono ancora poco sviluppate. Considerando anche il fatto che il mercato per questi sistemi è comparativamente piccolo e volatile e inoltre che in questo campo lo sviluppo tecnico è molto rapido, i costi di questi sistemi possono essere attualmente stimati soltanto approssimativamente.

Ripercussioni sul 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 Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni del DFGP). Complessivamente occorre comunque prevedere circa 16 posti di lavoro supplementari, ripartiti tra le seguenti nuove funzioni: nel SIC tecnici operativi per la gestione tecnica dei mezzi per l'acquisizione soggetta 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 i metodi di acquisizione soggetti ad autorizzazione nonché altri posti di lavoro per il controllo della qualità dei nuovi sistemi e la direzione dell'esplorazione dei segnali via cavo. Altri posti di lavoro saranno necessari in seno al Tribunale amministrativo federale per la procedura di autorizzazione delle misure di acquisizione, presso l'Archivio federale per l'archiviazione decentralizzata nei locali del SIC e presso il Centro operazioni elettroniche COE della BAC per l'esercizio a titolo sperimentale dell'esplorazione di segnali via cavo.

Le esigenze in materia di conservazione dei dati, più elevate rispetto a quelle attuali, saranno in gran parte soddisfatte ricorrendo alle risorse disponibili.

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.

1.8 Ripercussioni dell'avamprogetto di legge sulla collaborazione con i Cantoni

Secondo la concezione dell'avamprogetto 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).

Nel caso di determinate minacce, tutte le autorità e unità amministrative dei Cantoni sono tenute a fornire informazioni conformemente al principio dell'assistenza amministrativa e giudiziaria. 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 avamprogetto di legge. In contropartita hanno accesso alle informazioni automatizzate del SIC necessarie per l'adempimento dei loro compiti. Per le autorità d'esecuzione cantonali l'avamprogetto prevede un accesso al sistema INDEX SIC mediante procedura di richiamo. I Cantoni possono quindi richiamare, tra l'altro, i rapporti e gli accertamenti preliminari che essi stessi hanno allestito.

L'autorità di controllo del DDPS sulle attività informative potrà eseguire controlli anche in quei settori in cui le autorità d'esecuzione cantonali sono chiamati a eseguire la presente legge.

Per quanto riguarda la vigilanza parlamentare, si rimanda al commento all'articolo 69.

Come sinora, il SIC continuerà a contribuire al finanziamento delle autorità d'esecuzione cantonali.

1.9 Aspetti giuridici

Base costituzionale

La base costituzionale per l'acquisizione di informazioni concernenti l'estero rilevanti sotto il profilo della politica di sicurezza e per la competenza della Confederazione a legiferare in questo settore è essenzialmente disciplinata nell'articolo 54 della Costituzione federale (Cost.)[10] (Affari esteri):

l'articolo 54 capoverso 1 Cost. conferisce alla Confederazione la competenza per gli affari esteri. In questo ambito rientra anche la competenza di acquisire informazioni che possono essere importanti per la valutazione della situazione in materia di politica di sicurezza.

In base alla concezione e alla dottrina correnti la competenza di legiferare in materia di sicurezza interna da parte della Confederazione deriva dell'articolo 57 Cost. (Sicurezza). Sebbene tale articolo costituzionale non contenga alcuna competenza esplicita della Confederazione di agire e legiferare nell'ambito della sicurezza interna, ne contempla una implicita. Al riguardo, si rimanda al commento all'articolo 73.

[10] RS **101**

Tutela dei diritti fondamentali delle persone in Svizzera

Nell'ambito del presente avamprogetto, ingerenze gravi nei diritti fondamentali possono prodursi in occasione di misure di acquisizione soggette ad autorizzazione (art. 22 segg.) (per es. nel caso di intercettazioni telefoniche o di registrazioni audio e video 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 avamprogetto di legge sono eseguite soltanto in Svizzera. La tutela dei diritti fondamentali contemplata negli articoli 22 segg. dell'avamprogetto si riferisce pertanto esclusivamente a persone in Svizzera.

Le misure di acquisizione soggette ad autorizzazione che figurano nell'avamprogetto tengono conto dell'esigenza di una base legale formale che soddisfi anche il principio di determinatezza. La concezione proposta considera inoltre il principio della proporzionalità e l'esistenza di un interesse pubblico sufficiente.

Per quanto riguarda la natura della prevista acquisizione di informazioni, l'avamprogetto non prevede misure che contemplino lesioni dell'integrità fisica (come ispezioni corporali o l'applicazione della coercizione fisica). Tali misure sono riservate alle autorità di polizia alle quali è consentito impiegare, per l'adempimento dei propri compiti, la coercizione di polizia o misure di polizia (cfr. legge del 20 marzo 2008[11] sulla coercizione).

Infine, l'avamprogetto di legge (come già la LMSI) contempla il divieto fondamentale di raccogliere in Svizzera informazioni sulle attività politiche e l'esercizio della libertà d'opinione, della libertà sindacale e della libertà di riunione. Al riguardo, si rinvia al commento all'articolo 3 capoverso 5.

Tutela dei diritti fondamentali delle persone all'estero

L'acquisizione di informazioni all'estero è un tema delicato, poiché potrebbero essere pregiudicati la sovranità di Stati esteri e i diritti fondamentali di cittadini stranieri (per es. la tutela della sfera privata).

L'acquisizione di informazioni all'estero deve pertanto avvenire soltanto quando le informazioni necessarie per sventare i pericoli non possono essere acquisite in Svizzera. Essa serve a sventare pericoli per la Svizzera che possono risultare da fatti all'estero rilevanti sotto il profilo della politica di sicurezza, per esempio negli ambiti del terrorismo, della proliferazione e dello sviluppo di rapporti egemonici.

Nel campo di tensioni tra gli interessi svizzeri in materia di sicurezza e la tutela dei diritti fondamentali di cittadini stranieri o persone all'estero, secondo la concezione del presente avamprogetto prevale di principio l'interesse in materia di sicurezza. La tutela dei diritti fondamentali di persone all'estero va considerata in maniera meno ampia rispetto alla tutela dei diritti fondamentali di persone in Svizzera.

In ogni caso occorre tuttavia considerare il principio della proporzionalità: le lesioni dei diritti fondamentali e il valore previsto delle informazioni non devono essere tra loro sproporzionati.

[11] RS **364**

La tutela dei diritti fondamentali meno ampia rispetto a quanto previsto per la Svizzera riguarda soprattutto le misure di acquisizione ai sensi dell'articolo 22 dell'avamprogetto. A prescindere dalle riflessioni di principio menzionate in precedenza, depongono contro un obbligo dell'autorizzazione analogo a quello vigente in Svizzera i motivi seguenti:

– 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 sull'*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'intrusione in sistemi e reti di ordinatori ubicati all'estero (art. 32 cpv. 2).

Delimitazione rispetto all'attività delle autorità di perseguimento penale

Contrariamente alle autorità di perseguimento penale, la cui attività in definitiva è orientata a smascherare gli autori di reati (obiettivo repressivo), il SIC ha un compito preventivo. Nell'articolo concernente lo scopo, l'avamprogetto di legge sottolinea il carattere preventivo della misure adottate (acquisizione di informazioni, valutazione della situazione di minaccia). Gli obiettivi sono l'individuazione tempestiva di minacce nei confronti della sicurezza interna o esterna della Svizzera e la tutela delle sue basi democratiche e costituzionali.

Se in occasione dei suoi accertamenti il SIC si imbatte in reati o sospetti di reato, ne informa le autorità di perseguimento penale.

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)[12].

Nel presente avamprogetto 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 costituire un'opportunità per impedire o allontanare una minaccia.

[12] FF **2010** 4523

Articoli di senso manifesto:

Per evitare di appesantire il testo, gli articoli e i capoversi il cui senso è già manifesto e che svolgono un ruolo accessorio nel testo di legge non vengono trattati nel commento dell'avamprogetto posto in consultazione. Qualora l'esito della consultazione dovesse evidenziare malintesi, i commenti potranno essere integrati più tardi nel messaggio.

Ingresso:

Conformemente alla recente prassi in materia di legiferazione, l'ingresso della legge non fa più menzione della competenza costituzionale implicita della Confederazione di legiferare sulla salvaguardia della sicurezza interna ed esterna. Secondo la recente interpretazione, la competenza normativa in materia è contemplata all'articolo 173 capoverso 2 della Costituzione federale (trattamento da parte dell'Assemblea federale di questioni rientranti nella competenza della Confederazione e non attribuite ad altre autorità).

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 7 (Autorità d'esecuzione cantonali) e 73 (Esecuzione da parte dei Cantoni).

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

Art. 1 Oggetto e scopo

L'importanza del presente avamprogetto di legge in quanto disciplinamento globale del servizio informazioni svizzero giustifica l'introduzione di una disposizione sullo scopo.

Il *capoverso 1* riassume il contenuto della legge, mentre il *capoverso 2* riprende elementi della LMSI e assume un carattere programmatico. Esso definisce gli scopi a cui si orientano in ultima analisi le attività informative. Il *capoverso 2* non fonda quindi alcuna competenza, ma serve da linea guida per l'esecuzione della legge.

Il *capoverso 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 ordinario del Servizio. A tal fine è necessaria una decisione specifica del Consiglio federale ai sensi dell'articolo 62. Il SIC non può dunque agire di sua iniziativa. La decisione del Consiglio federale non conferisce al SIC competenze particolari più estese di quelle definite dalla LSI. 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. 22 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 esplorative oppure escludendo determinate misure di acquisizione (per es. quelle soggette ad autorizzazione).

Di norma quando saranno invocati questi altri interessi nazionali, non ancora contemplati nel mandato generale che la legge assegna al SIC, si tratterà di attività esplorative all'estero.

Questo capoverso 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 sull'organizzazione del Governo e dell'Amministrazione, RS 172.010).

Art. 3 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 oppure nel concretizzare i riscontri acquisiti in prestazioni operative di carattere preventivo atte a ridurre le minacce nei confronti della sicurezza. L'articolo 3 dell'avamprogetto 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 LSI o per mandato speciale del SIC.

Gli oggetti dei singoli capoversi sono disciplinati e in parte precisati da altre disposizioni della legge.

Il *capoverso 1* rammenta che il SIC acquisisce informazioni sia da fonti pubblicamente accessibili sia da fonti non pubblicamente accessibili. La conoscenza delle fonti pubblicamente accessibili (cfr. art. 11) 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 non soggette e soggette ad autorizzazione impostato in modo dettagliato nel capitolo 3. L'applicazione di queste misure è disciplinata in detto capitolo. Le misure non soggette ad autorizzazione (art. 11 segg.) vengono applicate dal SIC sotto la propria responsabilità e non necessitano di autorizzazione (per es. osservazioni in luoghi pubblici). Esse corrispondono grossomodo al catalogo di misure già contemplato nel vigente articolo 14 capoverso 2 LMSI.

Le misure di acquisizione soggette ad autorizzazione (art. 22 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 comporta presumibilmente la minor ingerenza nei diritti fondamentali della persona interessata. Se un'informazione necessaria può essere acquisita 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 corri-

sponde agli attuali articoli 5 capoverso 1 LSIC e 14 capoverso 1 LMSI. Se l'acquisizione e l'elaborazione di dati personali fossero riconoscibili da parte delle persone interessate, lo scopo dell'elaborazione ne sarebbe in genere compromesso. È riconosciuto invece un diritto d'accesso, disciplinato all'articolo 58.

I *capoversi 5 a 8* riprendono in sostanza collaudati principi già previsti dalla LMSI per proteggere le attività politiche dalle osservazioni di intelligence, con le relative eccezioni. La LSI garantisce in tal modo piena protezione per quanto riguarda fatti in Svizzera, alla stessa stregua della LMSI. Per l'estero una simile riserva non avrebbe senso, poiché renderebbe praticamente impossibile l'osservazione e la valutazione di sviluppi di tipo egemonico.

Per concretizzare la nozione di esercizio abusivo di diritti fondamentali ai sensi del capoverso 5 ai fini dello svolgimento di attività che minacciano la sicurezza si possono citare i seguenti esempi:

– 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. L'esplorazione informativa e l'elaborazione 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. Per i dati cancellati è previsto l'obbligo di offerta all'Archivio federale. I dati privi di valore archivistico devono essere definitivamente distrutti.

Il *capoverso 8* chiarisce che riguardo a organizzazioni e gruppi della lista d'osservazione secondo l'articolo 63 possono essere elaborate tutte le informazioni rilevanti per la valutazione della minaccia (che tali organizzazioni e gruppi rappresentano). Nella LMSI questa disposizione era sinora integrata nelle norme sulla lista d'osservazione, dove ha dato adito a determinate incertezze circa la sua applicazione. Con la nuova collocazione sistematica queste incertezze saranno evitate.

Capitolo 2: Compiti e collaborazione del SIC

Sezione 1: Compiti, misure di protezione e di sicurezza, armamento

Nota introduttiva:

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. 60).

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'attenzione 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.). Servizio informazioni e perseguimento penale sono quindi due ambiti complementari. Tuttavia, l'uno non è preliminare all'altro. Essi sottostanno pertanto anche in materia di vigilanza a due regimi separati (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. 4 Compiti del SIC

Al *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. 73). 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 di spionaggio o terroristiche, gli attacchi di questo genere rientrano come sinora anche tra i compiti definiti al numero 1 o al numero 2. Ma poiché spesso questi retroscena non sono riconoscibili, o lo diventano semmai dopo approfonditi accertamenti, è indispensabile assicurare sin dall'inizio la partecipazione del SIC al trattamento di questo genere di eventi, onde consentire al Servizio di poter svolgere il ruolo assegnatogli nell'ambito della Strategia nazionale per la protezione della Svizzera contro i rischi informatici. Le reti delle infrastrutture critiche devono essere protette contro gli attacchi degli hacker. In questo campo il SIC continuerà ad acquisire all'attenzione dei servizi che si occupano degli attacchi cibernetici le informazioni necessarie sugli attacchi incombenti o già avvenuti, e a contribuire alla difesa da questi attacchi. A questo scopo il SIC può anche contare su contatti internazionali esclusivi.

Alla lettera b, l'espressione «fatti all'estero rilevanti in materia di politica di sicurezza» sta a designare fatti e sviluppi che avvengono all'estero suscettibili di compromettere l'autodeterminazione della Svizzera e i suoi fondamenti democratici e costituzionali, di arrecarle gravi danni nel campo della politica di sicurezza o danni di altra natura o pregiudicare la capacità di agire delle sue autorità.

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 «tutelare altri interessi nazionali essenziali». (cfr. commento all'art. 1 cpv. 3).

L'acquisizione ed elaborazione di dati ai fini della valutazione della 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 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 WEF 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 interessati e legittimati di seguire costantemente l'evoluzione della situazione mediante il sistema PES (Presentazione elettronica della situazione, cfr. art. 48).

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 i servizi partner esteri. Il compito di servizio responsabile assunto dal SIC è ulteriormente precisato all'articolo 10.

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. Attualmente MELANI gestisce già un sistema di allerta precoce all'interno di una cerchia ristretta di gestori di infrastrutture critiche. Questa importante funzione va oltre la mera elaborazione di informazioni ai sensi del capoverso 1 lettera a numero 5 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 5 disciplina la questione in modo più particolareggiato. Contemporaneamente alla LSI, 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 LSI deve garantire autonomamente al SIC una protezione sufficiente.

Il SIC può inoltre 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 all'articolo 60.

Art. 5 Misure di protezione e di sicurezza

Le misure di protezione e di sicurezza enumerate completano la normativa federale generale in materia di sicurezza integrale segnatamente negli ambiti della protezione di persone, informazioni e opere. Tali misure mirano a imporre l'applicazione di prescrizioni per la tutela dei segreti 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 applica-

bile nei confronti dei collaboratori del SIC, ma anche del personale impiegato a tempo determinato, per esempio praticanti o militari. Possono essere controllati anche collaboratori di ditte che forniscono prestazioni all'interno dei locali del SIC. 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 e/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.

Art. 6 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, segnatamente 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 di acquisire informazioni in Svizzera può essere paragonata a quella di un responsabile delle persone di fiducia nel settore di polizia.

L'arma deve essere impiegata soltanto in casi di legittima difesa (art. 15 seg. del Codice penale[13]) o di stato di necessità (art. 17 seg. Codice penale). 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 in particolare le

13 RS **311.0**

prescrizioni sull'attestazione di un addestramento sufficiente e sull'abilitazione al porto di armi da fuoco, l'allenamento obbligatorio al tiro).

Sezione 2: Collaborazione

Art. 7 Autorità d'esecuzione cantonali

Secondo il presente avamprogetto, la Confederazione e i Cantoni assumono congiuntamente l'esecuzione dei compiti di intelligence (cfr. art. 73). Le autorità d'esecuzione cantonali acquisiscono nel territorio sottoposto alla loro giurisdizione le informazioni che sono tenute ad acquisire in virtù della LSI 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 (per quanto concerne l'elaborazione dei dati) e 6 (per quanto concerne il controllo e la vigilanza).

Art. 8 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 servizio informazioni 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). Il SIC è inoltre in contatto permanente con le autorità d'esecuzione cantonali. A queste ultime è così garantita la possibilità di adempiere i propri compiti sul territorio cantonale in sintonia con le esigenze della Confederazione.

Art. 9 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 9 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 agli articoli 17 e 18 (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 partner 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. Non si tratta dunque di persone a cui è attribuito un ruolo di «spie in uniforme», bensì di

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».

Art. 10 Collaborazione con l'estero

A titolo introduttivo va detto che il Consiglio federale rinuncia a evocare espressamente 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 già in forza di quanto disposto all'articolo 56 capoverso 3 della Costituzione federale. Per quanto riguarda l'esecuzione da parte dei Cantoni non vi sono dunque cambiamenti rispetto all'attuale situazione.

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 «agreement» o eventualmente di «memorandum of understanding» (MoU), senza effetto vincolante. Questa realtà 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 partner 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. E questo è anche il caso della Svizzera.

In avvenire potrebbe costituire un'eccezione soprattutto la 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 LSI 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 a concludere simili accordi nel singolo caso spetta non al SIC ma al Consiglio federale (art. 61 cpv. 3).

Il *capoverso 2* introduce la possibilità di stazionare in futuro 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 sarebbe impiegato soltanto d'intesa con il DFAE. I collaboratori del SIC in questione operano in missione ufficiale. Vengono regolarmente annunciati ai competenti servizi dello Stato ospite e di eventuali Stati terzi in caso di accreditamento collaterale e operano esclusivamente come persone di collegamento ufficiali con i competenti servizi. Pertanto non sono incaricati dell'acquisizione segreta di informazioni di intelligence e non violano il diritto degli Stati ospiti.

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 LSI. Lo stesso principio è già oggi applicabile in forma analoga in virtù dell'articolo 8

LMSI ed è precisato nella vigente ordinanza sul Servizio delle attività informative della Confederazione (art. 11 cpv. 1 e 2 dell'ordinanza del 4 dicembre 2009[14] 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 che concernono 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.

Capitolo 3: Acquisizione di informazioni

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 elaborazione 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 7 e 73.

Sezione 1: Misure di acquisizione non soggette ad autorizzazione

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. Queste misure corrispondono sostanzialmente alle possibilità di acquisizione contemplate all'articolo 14 capoverso 2 LMSI. Il capitolo menziona tutti i mezzi classici di intelligence per l'acquisizione di informazioni, dall'«open source intelligence» (OSINT, art. 12) all'«imagery intelligence» (IMINT, art. 12 cpv. 2) e dalla «human intelligence» (HUMINT, art. 13) alla «communication intelligence» (COMINT, art. 24 e 33 segg). Per l'applicazione di queste misure la LSI prevede norme specifiche in funzione dell'intensità dell'ingerenza nei diritti fondamentali.

Art. 11 Fonti d'informazione pubblicamente accessibili

I servizi informazioni reperiscono molte informazioni nella sfera pubblica. Procedendo in questo modo, possono limitarsi a ricorrere a specifici strumenti di intelligence soltanto per chiarire 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, poiché sfrutta informazioni pubblicamente accessibili, vale a dire praticamente a disposizione di chiunque. Il carattere pubblico di queste informazioni non cambia neppure se si tratta di informazioni offerte soltanto a pagamento. In questo contesto, le collezioni di dati elettroniche non devono essere considerate diversamente dai media tradizionali, quali i giornali o le pubblicazioni specializzate, che di norma vengono pure offerti a pagamento.

14 RS **121.1**

La qualità di queste informazioni può essere molto variabile e di conseguenza è importante valutarle al momento della loro utilizzazione. L'avamprogetto prevede pertanto che le informazioni provenienti da fonti pubbliche siano messe a disposizione all'interno del SIC in un apposito sistema d'informazione (art. 49). Da questo sistema possono, se necessario, essere valutate e trasferite in ulteriori sistemi in vista di una loro utilizzazione per prodotti di intelligence.

Art. 12 Osservazioni in luoghi pubblici e liberamente accessibili

Il *capoverso 1* corrisponde sostanzialmente alla vigente normativa prevista all'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 sotto le false spoglie 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 video e audio.

Il *capoverso 2* rappresenta una novità e disciplina il ristretto ambito dell'elaborazione di immagini a fini di intelligence (Imagery Intelligence, IMINT). L'adempimento dei compiti di legge può comportare occasionalmente la necessità di impiegare adeguati mezzi aerei, quali droni, aerei o elicotteri. Anche mezzi spaziali quali i satelliti possono rappresentare mezzi adeguati per l'IMINT (per es. in caso di rapimento di cittadini svizzeri all'estero). L'osservazione mediante immagini satellitari consente di sorvegliare adeguatamente anche il progresso 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 offerenti 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 basi 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. Per osservare questi fatti in modo mirato è necessaria una misura di acquisizione soggetta ad autorizzazione ai sensi degli articoli 22 e seguenti. Negli altri casi, se gli spazi privati non hanno potuto essere preservati al momento dell'osservazione, i dati dovranno 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 fatti al suolo in aree private. Tuttavia, l'utilizzazione di simili riprese sarebbe legalmente impugnabile.

Nella legge militare del 3 febbraio 1995[15] (LM) occorrerà integrare una disposizione analoga per l'ambito militare (art. 99 cpv. 1^{quater}, cfr. modifica del diritto vigente).

Art. 13 Fonti umane

La descrizione del termine «fonti umane» di cui al capoverso 1 si ispira alla definizione di «informatore» data all'articolo 14*a* LMSI. Quest'ultima, tuttavia, si riferisce piuttosto al settore della polizia. L'espressione scelta nell'avamprogetto è pertanto più adatta al gergo del servizio informazioni unificato.

Il termine «fonti umane», 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 ad 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 e/o nel pagamento di informazioni di grande utilità per l'adempimento dei compiti del SIC. Le fonti all'estero in particolare richiedono facilmente denaro per la comunicazione delle informazioni in loro possesso. Se viene scoperto, il pagamento di fonti umane può costituire un grosso 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 contributi sociali, altrimenti la sicurezza di molte fonti non potrebbe essere garantita e una collaborazione sarebbe impossibile. Questo tipo di introiti può essere ufficializzato soltanto in casi particolari, talvolta attraverso strutture di copertura.

15 RS **510.10**

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 vita e la propria integrità fisica. 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:

- uno scienziato nucleare di un Paese asiatico che fornisce informazioni a un servizio informazioni estero, nel suo Paese può essere condannato 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 e 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 un'identità fittizia o di una copertura. Mentre è impiegata attivamente, una fonte umana può ottenere dal SIC una copertura o un'identità fittizia ai sensi dell'articolo 15 o dell'articolo 16, se tale misura risulta necessaria per proteggerla.

Una fonte umana che abbia operato per il SIC può continuare a rischiare la vita o l'integrità fisica 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, l'avamprogetto 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.

Art. 14 Segnalazioni ai fini dell'accertamento della dimora di persone e dell'ubicazione di veicoli

I *capoversi 1 e 2* introducono una regolamentazione analoga a quella prevista dalla nuova 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 avamprogetto 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 la tutela di altri interessi nazionali essenziali. Perciò, la segnalazione di persone e veicoli da parte del SIC presuppone l'esistenza di una minaccia nei confronti della sicurezza interna o esterna (cfr. cpv. 2 lett. a) oppure una decisione del Consiglio federale riguardante la

tutela di altri interessi nazionali essenziali (cfr. art. 1 cpv. 3 in combinato disposto con l'art. 62).

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», che però non viene utilizzata nella LSI onde evitare malintesi. 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, RS 362.0). 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 al *capoverso 3* per la segnalazione nel RIPOL o nel N-SIS riguarda soltanto i veicoli di terze persone 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).

Sezione 2: Coperture e identità fittizie

Nota introduttiva

Il Servizio informazioni strategico (SIS) aveva dal 1998 la facoltà, in virtù dell'articolo 99 della legge militare, di assegnare identità fittizie ai collaboratori dei suoi organi incaricati dell'acquisizione di informazioni (cfr. Rapporto annuale 2002/2003 delle Commissioni della gestione e della Delegazione delle Commissioni della gestione delle Camere federali del 23 gennaio 2004; FF *2004* 1504). 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 il controllo è esercitato 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 che svolgono compiti previsti dalla 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 15 e 16 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.

Nel presente avamprogetto 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. 15 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 dato 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 tra i collaboratori in questione e 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 necessaria una copertura della vera identità.

L'allestimento di coperture è 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, mail ecc.).

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 OSIC. Con il presente articolo questa prassi poggerà su una base legale chiara.

Nella misura in cui 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).

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

Art. 16 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 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 all'estero o in Svizzera nell'ambito del terrorismo o dello spionaggio, possono esporre direttamente tale collaboratore nonché i suoi familiari a tentativi di pressione diretti, 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 risultare 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 qualsiasi tentativo di acquisizione di informazioni.

Tali identità fittizie sono predisposte a lunga scadenza e raramente possono essere assunte soltanto all'inizio di un determinato caso. 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 ai fini dell'acquisizione di informazioni. Esso elenca in modo esaustivo la cerchia di persone cui possono essere conferite 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 e siccome comporta il ricorso a documenti d'identità fittizi, deve sottostare

all'approvazione del capo del DDPS. 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. 15), le esigenze riguardanti le identità fittizie e la loro creazione 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 fissata arbitrariamente: 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 all'utilizzazione di identità fittizie da parte di fonti umane, l'utilizzazione da parte di queste ultime è limitata 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 collaborazione 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 in quanto, per il tempo in cui sussiste tale pericolo, a dette persone è conferita un'altra identità. In questo contesto, a cittadini stranieri saranno messi a disposizione documenti d'identità svizzeri soltanto a titolo eccezionale e con estrema prudenza. In simili casi, il rilascio temporaneo di documenti svizzeri non implica evidentemente alcuna concessione permanente della cittadinanza svizzera.

Sezione 3: Diritti e obblighi d'informazione

Art. 17 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 (servizi 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 ha di principio la precedenza 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* istituiscono obblighi d'informazione per determinate forme di minaccia che rischiano di violare beni giuridici importanti. Le varie fonti di minaccia sono enumerate esaustivamente al capoverso 2. Si tratta di attività terroristiche, di attività di spionaggio politico, economico o militare, della proliferazione, di attacchi a infrastrutture critiche e di estremismo violento. Questa disposizione impone di principio un obbligo d'informazione basato sui principi dell'assistenza amministrativa per tutte le autorità e unità amministrative della Confederazione e dei Cantoni.

Se è giustificato dalla tutela di altri interessi nazionali essenziali, l'obbligo di informazione deve fondarsi su una pertinente decisione del Consiglio federale (cfr. in proposito anche il commento all'art. 1 cpv. 3 e all'art. 62).

L'articolo corrisponde in larga parte al nuovo articolo 13*a* LMSI, introdotto con il progetto LMSI II. Tuttavia, non viene più fatta distinta menzione delle autorità fiscali, come è invece il caso nella LMSI. Secondo il presente avamprogetto soggiacciono anch'esse all'obbligo d'informazione, giacché rientrano nel novero dei servizi menzionati al capoverso 1. Una menzione distinta delle autorità fiscali darebbe l'erronea impressione che esse forniscano informazioni al SIC con particolare frequenza, ciò che invece in realtà non accade.

I servizi cantonali tenuti a informare inglobano anche le autorità comunali; esse sono incluse nel termine di «Cantone».

L'obbligo d'informazione si estende anche alle organizzazioni che adempiono compiti pubblici. Si tratta delle organizzazioni e persone di diritto pubblico o privato, esterne all'Amministrazione federale, cui sono attribuiti compiti amministrativi ai sensi all'articolo 2 capoverso 4 della legge federale del 21 marzo 1997[16] sull'organizzazione del Governo e dell'Amministrazione (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 vastità della cerchia dei destinatari.

Le informazioni fornite da autorità e organizzazioni sono destinate al SIC. Le autorità d'esecuzione dei Cantoni possono agire per incarico della Confederazione e acquisire informazioni presso le autorità e organizzazioni tenute a informare per mettere tali informazioni a disposizione del SIC. Il detentore dei dati è in ogni caso la Confederazione.

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

[16] RS **172.010**

del 24 marzo 2000[17] sul personale federale, in virtù del quale gli impiegati federali sono tenuti a denunciare qualsiasi sospetto di reato perseguibile d'ufficio.

Art. 18 Obbligo d'informazione e obbligo di comunicazione speciali

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 all'articolo 17 (obbligo d'informazione generale), dal momento che non si limita a singoli ambiti tematici e non è nemmeno vincolato a particolari condizioni. Esso serve all'esecuzione della legge in quanto tale. Per questa ragione, contrariamente all'obbligo previsto all'articolo 17, è circoscritto a determinate autorità.

L'obbligo non è inteso come obbligo integrale d'informazione, bensì come obbligo riferito a casi e organizzazioni concreti.

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.

Art. 19 Procedura in caso di divergenze d'opinione in merito agli obblighi d'informazione e di comunicazione

Il *capoverso 1* disciplina il trattamento delle 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 il trattamento delle divergenze d'opinione tra Confederazione e Cantoni. La decisione spetta al Tribunale amministrativo federale. Quale corrispettivo di questa disposizione, nella legge federale del 17 giugno 2005[18] sul Tribunale amministrativo federale (LTAF) viene istituita un'apposita competenza per le relative controversie (cfr. modifiche del diritto vigente).

Art. 20 Comunicazioni e informazioni di 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 ai servizi informazioni, non è possibile rendere attenta la persona interrogata in merito al fatto che essa

[17] RS **172.220.1**
[15] RS **173.32**

risponde a titolo volontario, 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 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. 21 Obbligo d'informazione speciale dei privati

Il *capoverso 1* riprende l'obbligo d'informazione dei trasportatori commerciali introdotto nel 2012 nella LMSI con il nuovo articolo 13*c* ed estende tale obbligo anche ai gestori privati di infrastrutture di sicurezza, in particolare di sistemi di videosorveglianza. Analoghe importanti informazioni potrebbero 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 rilevare o conservare determinati dati. Essa è unicamente intesa a garantire, in presenza di una concreta minaccia, 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 compagne aeree, agenzie di viaggi e imprese di autonoleggio.

Il *capoverso 2* richiama la possibilità, già prevista in virtù della legge federale del 6 ottobre 2000[19] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (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 elementi d'indirizzo emersi (per es. numeri di telefono). Anche l'articolo 14 capoverso 2bis LSCPT sarà adeguato di conseguenza.

Se necessario, l'obbligo d'informazione dei privati è imposto per mezzo della procedura amministrativa federale mediante emanazione di una decisione impugnabile, se del caso con la comminatoria dell'articolo 292 CP (disobbedienza a decisioni dell'autorità).

Le decisioni del SIC possono essere impugnate mediante ricorso in virtù dell'articolo 71. 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. 71 cpv. 3).

19 RS **780.1**

Sezione 4: Misure di acquisizione soggette ad autorizzazione

Nota introduttiva

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 a fini dell'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:

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-Qaïda. Egli era già noto alle autorità francesi per aver intrapreso viaggi in Afghanistan e Pakistan. Intratteneva contatti con un movimento radicale salafita attivo in Francia.

Al SIC sono note diverse persone che hanno legami con la Svizzera e che per quanto riguarda la radicalizzazione presentano paralleli con il 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 giudizio del Consiglio federale, 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 limitata. Molti fatti rilevanti per la valutazione delle minacce non avvengono in luoghi pubblici. Rilevare atteggiamenti cospirativi in Internet 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, il Consiglio federale stima 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 altri interessi nazionali essenziali, in cui le altre misure d'acquisizione non sono sufficienti per ottenere informazioni di base per la salvaguardia della sicurezza della Svizzera.

Le misure soggette ad autorizzazione comprendono in particolare (art. 22):

- la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni di una persona o di un collegamento;
- l'individuazione del luogo in cui si trovano persone o cose mediante localizzazione dei telefoni cellulari utilizzati dagli interessati 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'intrusione in sistemi e reti di ordinatori per acquisire informazioni ivi disponibili o trasmesse, oppure per disturbare, impedire o rallentare l'accesso a informazioni, se da questi sistemi vengono sferrati attacchi a infrastrutture critiche; e
- le perquisizioni di locali, veicoli o contenitori portati con sé da persone per acquisire informazioni ivi disponibili o trasmesse oppure oggetti. 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 e 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 l'impiego immediato di una misura. La domanda di autorizzazione deve essere inoltrata al Tribunale amministrativo federale entro 24 ore (art. 27 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. 55). Un eventuale procedimento penale e le misure di sorveglianza ordinate nell'ambito di tale procedimento hanno la precedenza sulle misure di acquisizione ai sensi della LSI. 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.

Art. 22 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. 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 con il necessario anticipo le minacce per la sicurezza interna o esterna della Svizzera. Se nell'ambito dei propri accertamenti scopre atti penalmente perseguibili o indizi di reato, il SIC ne informa le autorità di perseguimento penale.

Contrariamente alla misura prevista alla lettera a, la *lettera b* prevede la sorveglianza di un collegamento utilizzato da diverse persone o il cui titolare non è identificato. Può trattarsi di una cabina telefonica oppure di una tessera anonima prepagata. In simili casi la sorveglianza serve spesso anche a identificare la persona che utilizza il collegamento e da cui proviene la minaccia.

Dal punto di vista tecnico, il SIC applicherà la procedura prevista dalla legge federale del 6 ottobre 2000[20] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT), applicata anche da Confederazione e Cantoni nell'ambito di procedimenti penali. La sorveglianza in quanto tale è eseguita dal Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (SCPT). In questo ambito il SIC non effettua autonomamente alcuna sorveglianza.

Per le prestazioni a norma delle lettere a-d, il SIC indennizza il SCPT in base alle tariffe normalmente applicabili. L'articolo 16 LSCPT disciplina le indennità e sarà direttamente applicabile anche al SIC. Le presumibili prestazioni di sorveglianza richieste in più dal SIC comporteranno per il SCPT un aumento piuttosto modesto dell'onere rispetto alle prestazioni già fornite attualmente a favore delle autorità di perseguimento penale (2011: 2699 misure di sorveglianza in tempo reale, 5758 misure di sorveglianza retroattive/dati marginali e 3918 informazioni tecniche e amministrative[21]).

La *lettera c* consente la cosiddetta sorveglianza retroattiva di comunicazioni avute mediante corrispondenza postale o traffico delle telecomunicazioni attraverso il rilevamento dei cosiddetti dati marginali o dati di collegamento. Il rilevamento, effettuato presso il provider per il tramite del SCPT, consente di accertare in quale momento un determinato collegamento di telecomunicazione è stato in comunicazione con altri, e quali erano questi altri collegamenti. Questo tipo di rilevamento non consente invece di ottenere informazioni sul contenuto delle comunicazioni.

Esempio: un agente di un servizio informazioni estero soggiornante in Svizzera e operante sotto copertura cerca di reclutare fonti umane per ottenere da loro illegalmente informazioni da ambiti sensibili. Il SIC è a conoscenza del fatto che l'agente utilizza collegamenti di telefonia mobile per la gestione delle sue fonti umane. In totale ha acquistato quattro abbonamenti prepagati per telefoni cellulari in Svizzera. Per stabilire con quali persone è in contatto attraverso questi numeri di telefono è necessario rilevare i dati di collegamento o i dati marginali relativi a questi collegamenti di telefonia mobile.

La *lettera d* fa riferimento alla possibilità, già prevista per le autorità di perseguimento penale dalla legislazione in materia di sorveglianza del traffico delle telecomunicazioni, di determinare la posizione e la direzione di trasmissione dell'antenna con la quale è momentaneamente collegata l'apparecchiatura terminale della persona sorvegliata (cfr. art. 16 lett. b dell'ordinanza del 31 ottobre 2001[22] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni). Questa misura consente di localizzare approssimativamente il luogo in cui si trova un telefono cellulare e di determinare i suoi spostamenti senza dover accedere fisicamente all'apparecchio o collocare un sensore sulla persona. Poiché a tal fine occorre acce-

[20] RS **780.1**
[21] Fonte: statistica pubblicata in Internet, cfr. https://www.li.admin.ch/de/themes/stats.html
[22] RS **780.11**

dere a dati riguardanti il traffico delle telecomunicazioni ed è quindi necessario il concorso di un operatore di servizi di telecomunicazione, la misura è soggetta alla procedura di autorizzazione.

La *lettera e* disciplina l'impiego di mezzi tecnici, come ad esempio gli apparecchi GPS, che consentono di localizzare persone, veicoli o altri oggetti mobili. Grazie all'emissione di un segnale viene determinata la posizione della persona, del veicolo o dell'oggetto mobile; se necessario, tali movimenti o segnali possono essere registrati. 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 sostituirle (se non è necessaria un'osservazione diretta) oppure servono per prepararle (studio delle abitudini del soggetto per consentire un impiego più mirato di squadre di osservazione).

La definizione degli apparecchi da impiegare non è circoscritta, in modo da non escludere futuri progressi della tecnica.

La *lettera f* consente in particolare di registrare le conversazioni in locali privati delle persone sorvegliate 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 23.

Esempio di 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 contatti con persone esterne alle quali confidano le loro intenzioni e le loro opinioni. In simili ambienti, non è neppure possibile impiegare fonti umane, poiché queste cellule non consentono agli estranei di accedervi. Per acquisire le informazioni di cui necessita per adempiere i propri compiti 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. 55).

La *lettera g* 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 l'entità della minaccia. Può trattarsi di acquisire informazioni (n 1), ma anche di disturbare, impedire o rallentare l'accesso a informazioni (n. 2) in caso di attacco 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.

I disturbi alle infrastrutture critiche possono minacciare gravemente la sicurezza interna e esterna della Svizzera e implicano un enorme potenziale di dannosità. Si pensi per esempio ad attacchi elettronici all'approvvigionamento energetico (p. es.

centrali nucleari), ai trasporti e al traffico (p. es. aviazione, traffico ferroviario e stradale), all'industria chimica (p. es. rifiuti speciali), alle telecomunicazioni (p. es. radio e televisione), alla sanità pubblica (p. es. assistenza sanitaria) o al settore finanziario e assicurativo (p. es. borse). Il numero 2 è inteso a consentire di lottare contro danni imminenti oppure 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». In questo contesto, la precedenza deve essere data alla protezione preventiva del Paese (p es. dalla contaminazione nucleare). Occorre sottolineare che le misure di lotta nei confronti di sistemi in Svizzera sono sempre soggette 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 che si svolgono in Internet.

Alla *lettera h* proponiamo di concedere al SIC, in casi importanti e sotto il controllo del potere giudiziario e politico, la nuova possibilità 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.

Il *capoverso 2* dispone che le misure previste siano eseguite segretamente e all'insaputa delle persone interessate. Questa discrezione è necessaria 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. 29) con possibilità di impugnare le misure ordinate (art. 71).

Art. 23 Principio

Il *capoverso 1* vincola dapprima l'impiego di misure di acquisizione soggette ad autorizzazione alla condizione (alternativa) dell'esistenza di una concreta minaccia per la sicurezza interna o esterna, ad eccezione dell'estremismo violento, o della necessità di tutelare altri interessi nazionali essenziali in virtù di una decisione del Consiglio federale. Nella propria decisione il Consiglio federale stabilisce inoltre se possono essere impiegate misure di acquisizione soggette ad autorizzazione. A queste misure si applica però in ogni caso la procedura di autorizzazione prevista dagli articoli 25 e seguenti; ciò significa che la decisione del Consiglio federale non può sopperire alla 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 17 capoverso 2 lettere a-d, per poter impiegare misure soggette ad autorizzazione ai sensi dell'articolo 30 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.

Si tratta di condizioni aggiuntive descritte restrittivamente, che discendono dal principio costituzionale di proporzionalità e ricalcano quelle previste dal Codice di procedura penale (cfr. art. 269 cpv. 1 del Codice di diritto processuale penale svizzero del 5 ottobre 2007[23] [CPP]).

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

Art. 24 Misure di acquisizione soggette ad autorizzazione ordinate nei confronti di terzi

Può accadere che una persona per la quale sono date le condizioni previste all'articolo 23 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 cointeressata sarà tutelata per quanto possibile ed essa sarà informata riguardo alla misura dopo la sua conclusione (art. 29).

Non è ammessa la sorveglianza di terze persone 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 il SIC segue le regole del CPP.

Art. 25 Procedura di autorizzazione

La procedura di autorizzazione proposta nel presente avamprogetto 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. 26) dopo aver consultato la Delegazione Sicurezza.

Nei particolari, la procedura si svolge come segue:

– il SIC presenta al Tribunale amministrativo federale una domanda per l'impiego di una misura di acquisizione soggetta ad autorizzazione;

– 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;

– se la misura è autorizzata, il capo del DDPS decide in seguito se concedere il nullaosta per l'esecuzione;

23 RS **312.0**

– dopodiché, il SIC può eseguire la misura o ordinarne l'esecuzione da parte di terzi (per es. il 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 concreta minaccia 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 a quanto previsto dall'articolo 274 capoverso 5 CPP, l'autorizzazione è concessa per tre mesi al massimo e può essere prorogata 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).

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 la misura perdura.

I riscontri ottenuti con le misure di acquisizione soggette ad autorizzazione devono essere messi a disposizione delle autorità di perseguimento penale rispettando particolari cautele, per evitare che vengano utilizzati per casi penali nell'ambito dei quali la procedura penale non consentirebbe di ordinare una misura investigativa comparabile (cfr. art. 55 cpv. 3 e 4).

Art. 26 Nullaosta

Questo articolo disciplina, per misure di acquisizione autorizzate dall'autorità giudiziaria, il rilascio del nullaosta da parte del capo del DDPS, che al riguardo consulta preliminarmente la Delegazione Sicurezza. La prevista 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 al rilascio del 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.

Art. 27 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 agli articoli 22 e seguenti il SIC deve di principio attendere l'autorizzazione del Tribunale amministrativo federale e il nullaosta del capo del DDPS, dopo la consultazione preliminare della Delegazione Sicurezza.

L'articolo 27 concede dunque al SIC la possibilità, in caso di incombente pericolo, di ordinare l'impiego immediato di una misura. Un incombente pericolo è sempre

dato quando l'unico modo per accertare fatti oppure osservare attività in modo tempestivo consiste nell'agire immediatamente.

Se ad esempio al SIC giunge comunicazione 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:

- può ordinare l'interruzione della misura già dopo essere stato informato dal SIC;
- oppure può rifiutare il nullaosta dopo che il Tribunale amministrativo federale ha concesso l'autorizzazione (cfr. art. 29). 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. 28 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, quand'anche fosse ancora autorizzata.

La comunicazione 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. 29 Obbligo di comunicazione

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 CEDU e dall'articolo 13 Cost.

In virtù del *capoverso 1*, dopo la conclusione di un'operazione, rispettivamente di un complesso correlato di più misure d'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. 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. 22 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 inizia un procedimento giudiziario).

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[24] (…), la Corte europea dei diritti dell'uomo 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. Un combattente o comandante talebano il cui cellulare sia stato oggetto di intercettazioni nell'ambito di un caso di rapimento, ad esempio, 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 sforzi eccessivi, oppure a casi in cui, pur essendo noto il luogo di dimora, la persona interessata potrebbe essere raggiunta soltanto con sforzi eccessivi (specialmente all'estero) o potrebbe addirittura essere messa in pericolo da una comunicazione formale da parte delle autorità svizzere.

Secondo il *capoverso 3*, per il differimento o la rinuncia alla comunicazione a posteriori è applicabile 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. 26).

[24] CEDU; RS **0.101**

Sezione 5: Collaborazione e protezione delle fonti

Art. 30 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 secondo modalità cospirative in altri Paesi e aggirare così le misure di sorveglianza applicate nei rispettivi 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 al *capoverso 1*, assume un'importanza crescente, soprattutto nel campo della trasmissione 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 audio e video. 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 concepibile 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, ed è tenuto anche a sorvegliare queste persone nell'adempimento del mandato come se fossero suoi propri collaboratori.

Art. 31 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, all'articolo 7 LSIC, il quale si limita peraltro a delegarne il disciplinamento al Consiglio federale. Il Consiglio federale ritiene che la regolamentazione completa in materia di servizio informazioni debba comprendere anche un esauriente disciplinamento della protezione delle fonti. Si eviteranno così anche incertezze tra le disposizioni speciali a livello di ordinanza e un eventuale normativa discrepante a livello di legge formale.

Il *capoverso 1* sancisce il principio della protezione delle fonti e che, come sinora previsto dall'articolo 7 LSIC, le persone che svolgono un'attività informativa concernente l'estero meritano di essere particolarmente protette. In questo ambito rientrano però anche le relazioni con servizi partner esteri; senza la piena protezione di tali relazioni, la Svizzera sarebbe considerata un partner insicuro. Questo potrebbe avere gravi ripercussioni sull'affidabilità del SIC come partner nell'ambito di una cooperazione. La protezione non è comunque concessa alle persone ricercate e condannate per crimini gravi contro l'umanità.

Il *capoverso 2* limita la protezione delle fonti umane (art. 13) 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 all'articolo 11 capoverso 3 dell'ordinanza del 12 novembre 2008[25] 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 ancora 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 Consiglio federale 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, al *capoverso 4*, che il Tribunale amministrativo federale sia designato come autorità decisionale in materia di protezione delle fonti.

[25] RS **364.3**

Sezione 6: Acquisizione di informazioni su fatti all'estero

Art. 32 Disposizioni generali

Nota introduttiva

L'acquisizione di informazioni su fatti 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 federale del 3 febbraio 1995[26] sull'esercito e sull'amministrazione militare (LM). Nella LSIC è stata formulata in modo alquanto generico, poiché ci si voleva limitare a raggruppare le vigenti basi legali in materia di servizio informazioni 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 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 su 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 regole leggermente diverse rispetto all'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. 22 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 risultante 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 invece prevista l'assistenza giudiziaria per i reati di spionaggio. Pertanto, il Consiglio federale 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'acquisire informazioni all'estero (cpv. 3);

[26] RS **510.10**

– le attività volte all'acquisizione di informazioni su fatti all'estero devono essere rigorosamente documentate all'attenzione degli organi di vigilanza e di controllo (cpv. 4); e

– l'acquisizione di informazioni all'estero è assoggettata al controllo del DDPS e del Consiglio federale e, in ultima istanza, della Delegazione delle Commissioni della gestione delle Camere federali (cfr. art. 66 segg.).

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 su fatti all'estero anche in Svizzera (per es. organizzandovi incontri con fonti umane), ma garantisce al tempo stesso che il SIC debba rispettare in tal caso 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 l'intrusione in sistemi e reti di ordinatori (art. 22 cpv. 1 lett. g), sempre che si tratti di sistemi e reti ubicati all'estero. In questo contesto un obbligo di autorizzazione non avrebbe senso, poiché la stessa intrusione non sarebbe soggetta ad autorizzazione se avvenisse da un luogo al di là del confine.

Il SIC ricorre alle misure di acquisizione segreta di informazioni all'estero sotto la propria responsabilità, comprese le misure che sarebbero soggette ad autorizzazione secondo gli articoli 22 e seguenti se fossero applicate in Svizzera. Oltre che dalle suddette ragioni, la diversa soluzione adottata per l'impiego delle misure di acquisizione all'estero 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 riunire in un elenco esaustivo le misure di acquisizione segreta di informazioni all'estero ammesse dalla legge senza particolare 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.

Questo non significa tuttavia la scomparsa di un controllo efficace, al contrario: il *capoverso 4* impone al SIC di documentare l'acquisizione di tutte le informazioni su fatti all'estero all'attenzione della vigilanza politica sul SIC da parte del Consiglio federale, del Parlamento (Commissione della gestione o Delegazione delle Commissioni della gestione) e del DDPS (Vigilanza sulle attività informative).

I collaboratori del SIC impiegati all'estero sono esposti a un rischio accresciuto e agiscono anche in zone in guerra e in regioni di crisi, in parte sotto copertura o con identità fittizie. Al *capoverso 5* il Consiglio federale propone pertanto di assoggettarli all'assicurazione militare.

Le misure di protezione previste al *capoverso 6* 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. 33 Esplorazione radio

Nel quadro del progetto di revisione LMSI II, il Parlamento ha 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[27] sulla condotta della guerra elettronica e sull'esplorazione radio (OCGE). Perciò, il Consiglio federale l'ha ampiamente ripresa nella LSI, limitandosi a qualche adeguamento alla terminologia e al campo d'applicazione della LSI. Nel capoverso 2, ad esempio, è stata inserita, tra i possibili presupposti del ricorso all'esplorazione radio, la tutela di altri interessi nazionali essenziali su mandato diretto del Consiglio federale (cfr. art. 1 cpv. 3 e art. 62).

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 delle telecomunicazioni e di emittenti a onde corte. Il «servizio esecutivo» 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 all'intercettazione anche 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 anonima, 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 elaborazione conformemente alle disposizioni della LMSI. Nel regime della LSI si intendono le minacce secondo l'articolo 4 capoverso 1 lettera a.

Oggi l'esplorazione radio è già sottoposta alla verifica di un'autorità di controllo indipendente. Anche in questo caso , nell'articolo 67 LSI il Consiglio federale riprende, con minime modifiche, la corrispondente disposizione della LSIC (art. 4*b*).

La LSI riprende dunque integralmente la normativa e la prassi della vigente LMSI. Nel quadro dei lavori legislativi svolti a suo tempo, alla creazione di tale legge ha partecipato in misura determinante il prof. dott. iur. Giovanni Biaggini, ordinario di diritto pubblico, amministrativo ed europeo dell'Università di Zurigo. La presente disposizione della LSI, come pure la successiva sezione sull'esplorazione dei segnali via cavo, sono stati pertanto elaborati nuovamente con la partecipazione del prof. Biaggini.

[27] RS **510.292**

Sezione 7: Esplorazione di segnali via cavo

Art. 34 In generale

Accanto all'esplorazione radio, già praticata anche in Svizzera, sul piano internazionale sta assumendo crescente importanza anche l'esplorazione dei segnali via cavo. Negli ultimi anni, in seguito allo sviluppo delle efficientissime reti a fibre ottiche, lo spostamento delle telecomunicazioni da dispositivi senza filo (radio) verso reti collegate per filo (per semplicità qui denominato «cavo») si è intensificato. Al tempo stesso, le possibilità di ottenere informazioni per mezzo dell'esplorazione radio si riducono. L'avamprogetto si ispira pertanto a una corrispondente 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) e 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.

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 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 degli operatori 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 in contraddittorio 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. 25). 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. 42 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, poiché gli oggetti sorvegliati si trovano all'estero.

Oggi la Svizzera non possiede ancora alcuna esperienza nell'impiego di questo mezzo di esplorazione, dal momento che mancano le necessarie basi legali.

Come nel caso dell'esplorazione radio, per l'esecuzione dell'esplorazione dei segnali via cavo il servizio esecutivo 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.

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 il rilevamento dei dati comporti la minima ingerenza possibile 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-Qaïda» 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 (art. 33), di emanare le disposizioni d'esecuzione per via di ordinanza.

Art. 35 / 36 Obbligo dell'autorizzazione/Autorizzazione del mandato per l'esplorazione dei segnali via cavo

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 dato ordine a un provider di servizi di telecomunicazione di trasmettere determinati flussi di dati e non può essere prevista una procedura in contraddittorio per le persone interessate.

La domanda secondo l'*articolo 36 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 possono 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. numero 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, compresi in un unico mandato, richiede più tempo rispetto ad esempio alla trasmissione integrale al SIC di tutte le comunicazioni nell'ambito di una misura di sorveglianza del traffico delle telecomunicazioni secondo l'articolo 22 capoverso 1 lettera a. In seguito, per le proroghe è previsto lo stesso termine di tre mesi stabilito per le misure di acquisizione soggette ad autorizzazione.

Art. 37 Esecuzione dell'esplorazione di segnali via cavo

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 esecutivo non rileva direttamente (per mezzo di antenne) i segnali degli impianti di telecomunicazione, bensì li riceve da provider e operatori 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. Il SIC decide inoltre, conformemente alle basi legali, quali dati archiviare ed elaborare 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. 38 Obblighi dei gestori di reti filari e degli operatori di servizi di telecomunicazione

Dato che, come illustrato in precedenza, l'esplorazione di segnali via cavo può essere praticata soltanto con il concorso degli operatori di servizi di telecomunicazione e dei gestori di reti filari, l'articolo 38 ne definisce gli obblighi in questo contesto. Sono soggetti ai corrispondenti obblighi previsti soltanto i gestori che offrono servizi pubblici ai sensi della 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 COE in quanto servizio esecutivo e i provider. Per motivare e documentare i propri mandati, tuttavia, anche il SIC necessita di informazioni dirette da parte degli operatori di servizi di telecomunicazione e dei gestori di reti filari.

Il concorso del SCPT del DFGP non è necessario in questo contesto, 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 soltanto una volta che saranno disponibili opportune basi legali.

Il Consiglio federale stima 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: Elaborazione dei dati e archiviazione

Sezione 1: Principi e elaborazione dei dati nei Cantoni

Nota introduttiva

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

Attentati terroristici, attività di spionaggio, atti di estremismo violento ecc. vengono tipicamente 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, l'elaborazione delle informazioni deve essere già effettuata 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.

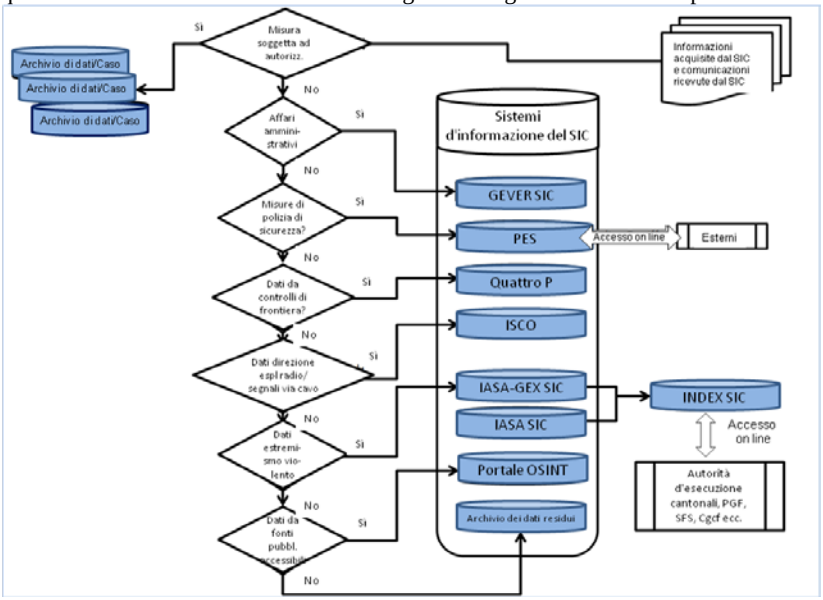
Il presente avamprogetto di legge rinuncia sistematicamente alla separazione, ormai obsoleta, tra sicurezza interna ed esterna, sicché tale distinzione non può più svolgere un ruolo determinante neppure nell'ambito dell'elaborazione dei dati da parte del SIC.

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 del rilevamento, 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, ossia la LMSI e la LSIC.

Il presente avamprogetto prevede che le informazioni acquisite o le comunicazioni ricevute dal SIC siano archiviate in una rete di sistemi d'informazione in funzione del tema, della fonte e della sensibilità dei dati. Il SIC non può raccogliere e conservare dati indiscriminatamente. La precondizione è sempre che esista un nesso sufficiente con i compiti assegnati secondo la presente legge. Inoltre devono essere rispettati i limiti posti all'elaborazione di dati, a tutela dei diritti politici (art. 3 cpv. 5-8). Infine si garantisce che la rilevanza e l'esattezza dei dati vengano verificate prima dell'archiviazione. Questa verifica è inoltre effettuata prima che i dati personali vengano impiegati in un prodotto del SIC (per es. un rapporto d'analisi, una segnalazione a servizi partner, una valutazione della situazione) originando effetti all'esterno.

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 regolare la conservazione dei dati in modo differenziato. Mentre l'elaborazione 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, nel campo dell'estremismo violento si è regolarmente rivelata una questione particolarmente delicata, sia politicamente sia dal profilo della protezione dei dati. Come già la LMSI, anche l'avamprogetto 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. 39 Principi

I principi stabiliti all'articolo 39 si applicano a tutti i sistemi d'informazione del SIC. La loro applicazione generalizzata garantisce un elevato grado di uniformità all'elaborazione dei dati, a prescindere dal sistema nel quale vengono memorizzati dati personali. 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* crea la necessaria base legale per queste forme di elaborazione 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 sempre individuare anche attività di disinformazione e false informazioni. Da informazioni di questo genere si possono dedurre le intenzioni dei rispettivi produttori e fornitori. Una volta individuata, per scongiurare errori di valutazione la disinformazione o la falsa informazione deve essere identificata in quanto tale e in quanto tale resa disponibile anche per il futuro, onde evitare futuri errori di valutazione. Pure 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 partner.

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. 40, 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 si trovano.

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* crea una base legale esplicita per simili correlazioni e per l'impiego di programmi di ricerca e di analisi automatizzati.

Art. 40 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 rilevamento dei dati:

- un controllo diretto e capillare da parte dell'organo interno di controllo della qualità è previsto al momento dell'elaborazione 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, nel settore dell'estremismo violento, per quanto riguarda la qualità occorre invece aspettarsi fasi di emivita dei dati assai più brevi. In quest'ultimo settore, 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 elaborazione 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 l'elaborazione 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 dell'elaborazione dei dati in tutti i sistemi. Questi criteri corrispondono a quelli definiti per gli organi di vigilanza (art. 65 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 della comunicazione nel suo insieme.

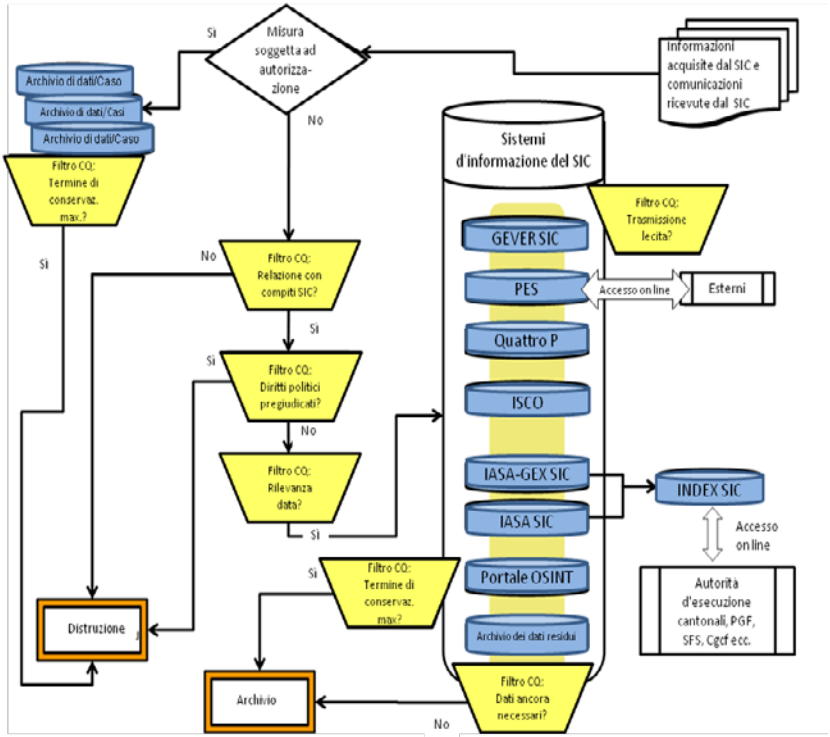
Concretamente, le fasi di selezione intese e a garantire un'elevata qualità dei dati in seno al SIC sono le seguenti:

– selezione d'entrata: limitazione ai dati personali che possono essere elaborati 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 memorizzati nei sistemi d'informazione del SIC siano ancora necessari all'adempimento dei compiti previsti dalla presente legge;

– selezione d'uscita: i dati personali possono avere effetti all'esterno soltanto se l'elaborazione è lecita (cfr. art. 54);

– 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 rilevare qualsiasi dato in un sistema d'informazione.

Determinante secondo il *capoverso 1* è la rilevanza ed esattezza dei dati personali. Nell'Archivio dei dati residui, nel quale i dati non sono ordinati con riferimento alle

persone, tale valutazione non viene effettuata per i singoli dati personali di una comunicazione, bensì sulla comunicazione nel suo insieme.

Secondo il *capoverso 2*, il SIC può elaborare solo i dati che presentano un nesso con l'adempimento dei compiti assegnatigli dalla legge (art. 4 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 all'elaborazione dei dati, a tutela dei diritti politici (art. 3 cpv. 5–8).

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. 59).

Art. 41 Elaborazione dei dati nei Cantoni

Il *capoverso 1* si fonda sulla seguente concezione: nella misura in cui operano nel campo d'applicazione del presente avamprogetto, 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. 46). 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 del presente avamprogetto di legge, la Confederazione sarà l'unico detentore dei dati.

Il *capoverso 2* concerne i dati elaborati dai Cantoni nell'ambito dei compiti di intelligence cantonali di loro competenza (ossia che non rientrano nella competenza della Confederazione, risp. del SIC) oppure nell'adempimento di altri compiti in materia di sicurezza o di polizia giudiziaria. Tra le competenze proprie dei Cantoni rientra ad esempio l'elaborazione dei dati relativi alle domande di autorizzazione per le manifestazioni. Se si temono scontri di matrice estremista violenta, il SIC elabora i relativi dati anche da questo profilo. Se la manifestazione degenera effettivamente nella violenza, il SIC elabora queste informazioni dal profilo dell'estremismo violento ai sensi del presente avamprogetto, 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 all'elaborazione 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 della duplice elaborazione, ad esempio perché ne sono state informate durante un interrogatorio.

Sezione 2: Sistemi d'informazione del SIC

Art. 42 Sistemi d'informazione del SIC

L'articolo 42 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[28] 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 avamprogetto 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 dell'elaborazione 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[29] sui sistemi d'informazione del Servizio delle attività informative della Confederazione (OSI-SIC). Per i dati provenienti dall'esplorazione all'estero, tale termine è di 30 anni dall'ultima elaborazione, 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'esplorazione in Svizzera, che sono di cinque anni dalla prima registrazione e in seguito di tre anni per le valutazioni periodiche, fino alla scadenza della durata massima di conservazione. La LSI dispone a questo riguardo che nel definire i termini il Consiglio federale deve 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.

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

Art. 43 Assegnazione dei dati ai sistemi d'informazione

Quando riceve nuovi dati, il SIC ne valuta per prima cosa sia la rilevanza per l'adempimento dei propri compiti sia l'esattezza. Dopodiché il competente servizio del SIC li assegna al sistema previsto per la categoria di dati alla quale appartengono. 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 riscontri necessari per la produzione. Nell'INDEX SIC il SIC immette soprattutto i

28 RS **361**
29 RS **121.2**

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. 44 IASA SIC

L'articolo 44 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 elaborati esclusivamente nel sistema IASA-GEX SIC (art. 45). IASA SIC sostituisce dunque ampiamente gli attuali sistemi ISIS e ISAS.

Gli analisti del SIC sono responsabili, ciascuno per il proprio ambito specialistico, del rilevamento e della periodica verifica 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 dell'elaborazione (cfr. art. 40).

Art. 45 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 all'elaborazione di informazioni in virtù dell'articolo 3 capoverso 5 LSI, e tutelata dalla Cost. Perciò, il SIC rileva questi dati in un sistema d'informazione distinto, il sistema di analisi integrale dell'estremismo violento (IASA-GEX SIC) riservato al rilevamento, all'elaborazione e all'analisi centralizzati di tutti i dati nel settore dell'estremismo violento. 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. 40 cpv. 5 lett. a).

In virtù dell'articolo 61 capoverso 1 lettera c, il Consiglio federale designa ogni anno i gruppi da considerare di matrice estremista violenta.

Art. 46 INDEX SIC

INDEX SIC serve ad accertare se il SIC elabora dati concernenti una determinata persona, un'organizzazione, un oggetto o un evento. In questo sistema sono registrate tutte le persone rilevate 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 di accedere direttamente ai dati di identificazione nel sistema ISIS. 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. 54 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 essere 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 l'elaborazione dei dati da parte delle autorità cantonali. Queste ultime vi elaborano i dati di cui si servono per la redazione di un rapporto destinato al SIC. Il sistema consente loro anche di avere una panoramica dei mandati della Confederazione e di archiviare i loro dati. Questa centralizzazione a livello federale di tutte le elaborazioni di dati previste dal presente avamprogetto garantisce un disciplinamento e un controllo unitari.

Art. 47 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 elabora 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, iter 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. 48 PES

L'articolo 48 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 nella misura in cui sono assolutamente necessari per l'illustrazione e la valutazione della situazione.

Quanto al *capoverso 3*, nell'ambito del progetto LMSI II l'autorizzazione di accesso concessa in via eccezionale a privati o autorità estere ha sollevato intense discussioni. La prassi sinora seguita ha confermato l'applicazione restrittiva di questa disposizione da parte del SIC: sinora non è stata concessa nemmeno un'autorizzazione di questo genere, poiché non si sono mai presentate corrispondenti situazioni. Tuttavia, il Consiglio federale rimane del parere che la Svizzera, in quanto Paese ospite di eventi internazionali, deve garantire in collaborazione con privati e partner esteri la sicurezza delle manifestazioni che accoglie. 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 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 deve mettere a disposizione soltanto i dati necessari per affrontare le minacce specifiche.

Art. 49 Portale OSINT

L'articolo 49 fornisce la base legale formale per il Portale «Open Source Intelligence» (Portale OSINT), sistema del SIC per lo sfruttamento dei dati pubblicamente accessibili. 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 i 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. Al *capoverso 3* non conviene quindi neppure limitarne l'accesso all'interno del SIC.

Art. 50 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 elaborerà questi dati in un sistema d'informazione distinto denominato Quattro P, sinora compreso nel «Modulo informatico P4» (P4: Programma di informazioni su persone concernenti passaggi del confine da parte di cittadini stranieri di determinati Paesi) di cui all'articolo 25 capoverso 1 lettera h OSI-SIC.

Secondo il *capoverso 3*, l'accesso a questo sistema è consentito soltanto a una ristretta cerchia di persone (attualmente meno di 10) all'interno del SIC incaricate del rilevamento, della consultazione e dell'analisi di questi dati.

Secondo il *capoverso 4*, il Consiglio federale stabilisce annualmente l'estensione dei controlli, 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 prevista per la definizione di fatti e constatazioni che devono essere comunicati spontaneamente al SIC in virtù dell'articolo 18 capoverso 4. Per i dati inseriti nel sistema Quattro P è oggi prevista una durata massima di conservazione di cinque anni (art. 33 cpv. 1 lett. i OSI-SIC).

Art. 51 ISCO

Il sistema d'informazione per l'esplorazione delle comunicazioni ISCO (sistema d'informazione COMINT) serve al SIC per controllare e dirigere i propri mandati al COE. La direzione delle attività di esplorazione radio e di esplorazione dei segnali via cavo avviene mediante mandati scritti del SIC (cfr. art. 33 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 agli organi di vigilanza (in particolare all'Autorità di controllo indipendente, cfr. art. 67) come base delle loro attività.

Al sistema ISCO hanno accesso soltanto pochissimi collaboratori del SIC (attualmente meno di 10 persone) che si occupano direttamente della direzione dei mandati.

I risultati dell'esplorazione radio e dei segnali via cavo destinati all'ulteriore analisi e utilizzazione in prodotti, esposizioni della situazione ecc. vengono registrati nell'Archivio dei dati residui (art. 52).

Art. 52 Archivio dei dati residui

Nell'Archivio dei dati residui il SIC memorizza tutte le informazioni non ha potuto assegnare direttamente 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 rilevati ed elaborati 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 esposizioni della situazione, 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 dei limiti posti all'elaborazione dei dati, a tutela dei diritti politici, dall'art. 3 cpv. 5-8 LSI) ed esattezza definiti per la loro elaborazione. I dati che non soddisfano più questi criteri vengono distrutti, rispettivamente le informazioni inesatte ma ancora necessarie vengono designate come tali. Come nel caso della verifica in entrata, la valutazione periodica viene effettuata sulla comunicazione nel suo insieme, ossia non si procede alla verifica delle singole asserzioni contenute in un documento.

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

Art. 53

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 non solo molto voluminosi, ma contenere anche molte informazioni che non hanno niente a che fare con l'obiettivo dell'esplorazione, ad esempio perché sono di natura puramente 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'intrusione in sistemi di ordinatori si possono ad esempio

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 53 dispone che i dati provenienti da misure di acquisizione soggette ad autorizzazione di questo genere 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.

Analogamente, il *capoverso 3* limita la cerchia delle persone autorizzate ad eccedere 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 incaricati nella fattispecie dell'acquisizione e dell'analisi.

Sezione 4: Disposizioni particolari sulla protezione dei dati

Art. 54 Verifica prima della comunicazione

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 comunicazione. È tenuta ad assicurarsi che le condizioni cui la legge subordina la comunicazione siano adempiute e che i dati personali siano elaborati in modo corretto.

Art. 55 Comunicazione di dati personali ad autorità svizzere

Per adempiere il proprio compito, il SIC deve poter trasmettere dati personali ad autorità politiche, autorità di perseguimento penale, autorità giudiziarie o di sicurezza. La regolamentazione prevista dall'avamprogetto corrisponde ampiamente a quella del vigente articolo 17 LMSI, ma nella LSI è stata sviluppata e differenziata.

L'introduzione di ulteriori meccanismi di protezione è necessaria segnatamente per quanto riguarda la comunicazione 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, la LSI riprende al *capoverso 3* il principio che limita la comunicazione di riscontri su 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.

Art. 56 Comunicazione 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 comunicati soltanto a Stati la cui legislazione garantisce un livello di protezione dei dati comparabile a quello svizzero (cfr. art. 6 cpv. 1 LPD). Questo principio escluderebbe 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. Con ciò, il SIC sarebbe costretto a rinunciare a importanti fonti d'informazione proprio nelle regioni di crisi.

Pertanto, la vigente LMSI contempla già regole speciali per la collaborazione in ambito informativo e la comunicazione di dati personali all'estero; queste regole vengono riprese nella LSI. In quest'ambito 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).

Il *capoverso 2 lettera d* concerne le richieste di nullaosta (richieste clearing) di cui tratta anche l'articolo 10 capoverso 1 lettera d, elaborate 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. 57 Comunicazione di dati personali a terzi

Le attività informative esigono talvolta che vengano comunicati 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 quali sono le persone sulle quali chiede informazioni e in quale contesto. La disposizione corrisponde al vigente articolo 17 capoverso 3 LMSI.

Art. 58 Diritto d'accesso

Per quanto riguarda il diritto d'accesso, l'avamprogetto riprende la soluzione adottata dal Parlamento il 23 dicembre 2011 nel quadro della revisione della LMSI («LMSI II ridotta»), la quale si ispira a sua volta alla LSIP. In pratica la LSI riprende ampiamente l'articolo 18 LMSI nella nuova versione in vigore dal 16 giugno 2012.

Nell'ambito delle deliberazioni relative a LMSI II, nel dibattito sulla reimpostazione del diritto d'accesso il Consiglio federale aveva ancora proposto l'applicazione integrale della LPD. Tuttavia, poiché il Parlamento si è formalmente detto favorevole alla soluzione prevista dalla LSIP, il Consiglio federale non ritiene opportuno presentare un disciplinamento diverso della questione del 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, al *capoverso 9* il Consiglio federale propone 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 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, di regola 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 al capoverso 2 lettera c, la quale detta di differire l'informazione se il richiedente non è registrato. Il Consiglio federale ritiene pertanto che la procedura secondo la LSIP sia oggettivamente corretta.

Sezione 5: Archiviazione

Art. 59

I dati e i documenti del SIC soggiacciono di principio alla legge federale del 26 giugno 1998 sull'archiviazione e di conseguenza, trascorsa la loro durata di conservazione presso il SIC, sono conservati in locali (in parte particolarmente protetti) dell'Archivio federale e amministrati secondo principi archivistici. Un'eccezione è applicata già oggi per quanto riguarda i dati e i documenti provenienti dalle relazioni dirette con servizi di sicurezza esteri. Tali dati e documenti soggiacciono sempre all'usuale riserva internazionale in base alla quale la loro trasmissione e archiviazione sono ammesse soltanto con l'esplicito consenso del proprietario estero dei dati. Pertanto, in un'ordinanza il Consiglio federale disciplinerà la conservazione e la distruzione di questi dati e documenti nel senso dell'attuale base legale (art. 28 cpv. 2 O-SIC).

Capitolo 5: Prestazioni

Art. 60

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. Sotto questo aspetto 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). 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. Il SIC consiglia gli organi della Confederazione incaricati degli acquisti per quanto riguarda le casseforti e le tecniche di chiusura. Appoggia anche servizi partner esteri in particolare effettuando trasporti speciali.

In occasione di un rapimento conclusosi positivamente, nel quadro della gestione della crisi il SIC ha fornito appoggio con le prestazioni seguenti:

- ha messo a disposizione mezzi per comunicazioni sicure per i collegamenti tra il Centro di gestione delle crisi del DFAE e la rappresentanza locale del DFAE e ha fornito il supporto tecnico;
- ha messo a disposizione i suoi mezzi per comunicazioni sicure per lo 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.

Il Consiglio federale reputa corretto creare una base legale esplicita per le prestazioni di questo genere.

Capitolo 6: Direzione politica, controllo e protezione giuridica

Sezione 1: Direzione politica e divieto di determinate attività

Art. 61 Direzione politica da parte del Consiglio federale

Il SIC è uno strumento più di altri destinato a tutelare gli interessi nazionali e a operare per il Governo federale. Perciò, nella LSI 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 61 riprende dunque vari elementi della vigente legislazione e li raggruppa in una disposizione consacrata alla direzione politica.

La *lettera a* riprende il sistema già praticato, che impone al Consiglio federale di assegnare al SIC un mandato strategico fondamentale. Questo man dato 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 esercitano 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.

Attualmente la questione del mandato fondamentale è disciplinata 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 all'articolo 63 e già prevista dal vigente diritto (art. 11 cpv. 3-7 LMSI).

La *lettera c* si riallaccia alla nuova concezione in materia di elaborazione dei dati, separando e sottoponendo a un più severo regime l'elaborazione di 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 22 e seguenti. Inoltre, nell'ambito dell'elaborazione dei dati il SIC inserisce i dati relativi a gruppi di matrice estremista violenta nell'apposito sistema d'informazione IASA-GEX SIC (art. 45). Al tempo stesso, il SIC riferisce al Consiglio federale in merito al numero di persone legate alla galassia dell'estremismo violento ma non ancora attribuibili a un determinato gruppo. Questo consente al Consiglio federale 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 per approvazione al Consiglio federale.

Per sua natura, la collaborazione con autorità estere, soggetta all'autorizzazione del Consiglio federale, in ambito di intelligence 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 di amministrazione.

Per contro, in virtù del *capoverso 2*, il collegamento del SIC a una banca dati comune gestita insieme a servizi partner esteri dovrebbe 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. Il Consiglio federale considera opportuno che nell'ambito del rinnovo 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.

Art. 62 Tutela di altri interessi nazionali essenziali

Questo articolo, che si ricollega all'articolo 1 capoverso 3, definisce la procedura da seguire per incaricare il SIC, in situazioni particolari, di adottare misure intese a tutelare altri 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 intraprendere qualsiasi azione.

Art. 63 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. 61 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 di terroristi nella lista d'osservazione (revisione «LMSI II ridotta» del 23.12.2011), queste sono diventate il criterio di riferimento per il suo allestimento. A differenza di quanto previsto dalla LMSI, la quale incarica il Consiglio federale di designare le organizzazioni e comunità internaziona-

li le cui liste sono da considerarsi rilevanti, al *capoverso 2* la LSI si limita a citare l'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 come quelle connesse al sistema di liste istituito dalla risoluzione 1267 del Consiglio di sicurezza delle Nazioni Unite (per es. divieto di determinate organizzazioni). Contrariamente a quanto previsto per la lista del Consiglio di sicurezza delle Nazioni Unite, nella lista d'osservazione non vengono neppure iscritti singoli individui. Infine, la procedura annuale di approvazione da parte del Consiglio federale garantisce il margine di manovra necessario per stralciare un gruppo dalla lista. L'inserimento di un'organizzazione o di un gruppo (o una persona) in una lista internazionale non comporta dunque automaticamente il suo inserimento nella lista d'osservazione svizzera.

Il limite posto all'elaborazione dall'articolo 3 capoverso 5 (attività politica ed esercizio di diritti fondamentali) non si applica alla lista d'osservazione (cfr. art. 3 cpv. 8). Il SIC può acquisire ed elaborare tutte le informazioni disponibili riguardo alle organizzazioni e ai gruppi figuranti nella lista, purché siano utili per valutare la minaccia che da essi deriva.

Art. 64 Divieto di determinate attività

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

La disposizione disciplina la competenza legale del Consiglio federale nei casi previsti dalla LSI, 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, esistenti o imminenti, dell'ordine pubblico o della sicurezza interna o esterna della Svizzera. Questa competenza 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 seguaci di organizzazioni terroristiche. Attualmente è in vigore un'ordinanza dell'Assemblea federale che vieta il gruppo Al-Qaïda 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 LSI o se non sia più opportuno che sia il Parlamento a decretare o 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.

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. In deroga al disciplinamento

previsto dalla vigente LMSI, tuttavia, il diritto di richiedere un simile provvedimento è riconosciuto a tutti i Dipartimenti.

Nella propria decisione il Consiglio federale deve definire l'estensione e il contenuto del divieto con la massima precisione possibile, affinché 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 giusta l'articolo 71, dapprima dinanzi al Tribunale amministrativo federale e successivamente dinanzi al Tribunale federale.

Sezione 2: Controllo e vigilanza in materia di servizio informazioni

Nota introduttiva

Gli articoli 65 a 69 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. controllo 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 (art. 67) garantisce la legalità dell'esplorazione radio concernente l'estero conformemente all'articolo 33.

Art. 66 Vigilanza da parte del Dipartimento

L'autorità di vigilanza sulle attività informative interna al Dipartimento (attualmente: Vigilanza sulle attività informative) è ora menzionata a livello di legge (cpv. 2), poiché le saranno assegnate competenze più ampie. Anche i controlli che tale autorità esegue presso le autorità d'esecuzione cantonali sono disciplinati a livello di legge (cpv. 3). I settori interessati sono quelli in cui i Cantoni acquisiscono informazioni in virtù del diritto federale (cfr. art. 73). Questa facoltà va a completare il compito di controllo e di gestione assegnato al DDPS secondo il capoverso 1.

Art. 67 Autorità di controllo indipendente per l'esplorazione radio

Il disciplinamento previsto per l'autorità di controllo indipendente (ACI) corrisponde, come quella applicabile all'esplorazione radio (art. 33), alla normativa entrata in vigore il 1° novembre 2012 che il Parlamento ha direttamente iscritto nella LSIC (art. 4*b* LSIC). Oggi questa funzione di controllo è svolta da una commissione interna all'Amministrazione. In precedenza, l'attività di controllo dell'autorità indipendente era già disciplinata per analogia dalla previgente ordinanza del 15 ottobre 2003 sulla condotta della guerra elettronica e negli anni scorsi tale disciplinamento si è dimostrato valido. Esso corrisponde a una necessità in un ambito sensibile dell'esplorazione concernente l'estero. Per quanto concerne l'esplorazione dei segnali via cavo vigono disposizioni comparabili, ma in quest'ultimo ambito è prevista l'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 privati fornitori 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'autorità di controllo indipendente 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, autorità di controllo indipendente dall'altro) e quindi non è indicato.

L'unica differenza rispetto all'articolo 4*b* LSIC riguarda la durata del mandato dell'autorità di controllo indipendente, la quale è definita, essendo un dettaglio relativo all'esecuzione, al capoverso 4 invece che al capoverso 1.

Art. 68 Vigilanza e controllo da parte del Consiglio federale

Questo articolo iscrive nella LSI la verifica della legalità, dell'adeguatezza ed 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 LSI 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. 69 Alta vigilanza parlamentare

La vigente regolamentazione, definita all'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 delle Camere federali. Tale vigilanza non si limita alle attività del SIC, bensì comprende anche quelle delle autorità d'esecuzione cantonali. Il presente progetto legislativo non prevede un'alta vigilanza bipartita tra i Parlamenti cantonali da un canto e l'Assemblea federale dall'altro.

Il Consiglio federale è del parere che istituendo la Delegazione delle Commissioni della gestione per la sorveglianza delle attività informative e assegnando a detta Delegazione competenze particolari (art. 53 della legge federale del 13 dicembre

2002[30] sull'Assemblea federale), il legislatore federale abbia inteso disciplinare in modo esaustivo l'alta vigilanza parlamentare. Non sarebbe coerente che ai Cantoni il legislatore federale riservasse senza particolari condizioni competenze parallele di controllo parlamentare a livello cantonale. Gli organi di sicurezza cantonali si attivano sempre in diretta esecuzione della legge per conto degli organi federali e non per un originario interesse dei Cantoni in merito all'esecuzione.

I Parlamenti cantonali mantengono beninteso la loro autonomia nei settori non disciplinati dalla presente legge in cui le autorità cantonali sono attive per la sicurezza interna del rispettivo territorio.

Art. 70 Vigilanza cantonale

L'avamprogetto propone una suddivisione della vigilanza sulle autorità d'esecuzione cantonali tra Confederazione e Cantoni.

Vigilanza da parte della Confederazione

L'alta vigilanza sulla correttezza materiale dell'esecuzione della presente legge, e quindi anche sull'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'autorità di vigilanza interna del DDPS (art. 66 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 sulla funzione di servizio verifica:

- se le procedure amministrative cantonali sono conformi alle pertinenti prescrizioni legali;
- se le autorità d'esecuzione cantonali elaborano 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).

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 anche l'assistenza da parte di organi di controllo federali a favore delle autorità di vigilanza cantonali (per es. da parte di un organo di controllo analogo all'attuale Vigilanza sulle attività informative) e l'accesso a informazioni utili allo scopo da parte delle autorità cantonali di vigilanza sulla funzione di servizio (cpv. 3).

30 RS **171.10**

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 inglobererebbe 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 elaborati dalle autorità d'esecuzione cantonali.

La *soluzione federale* presenterebbe il vantaggio di un disciplinamento unitario della vigilanza sulle autorità d'esecuzione cantonali. Tuttavia, contraddirebbe 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 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. Si porrebbero inoltre ardue questioni di delimitazione per quanto riguarda la vigilanza sul mandato impartito dall'autorità federale. Il SIC sarebbe tenuto per certi aspetti a rendere conto anche alle autorità di vigilanza cantonali, altro aspetto che risulterebbe contrario al sistema. Pertanto, nel complesso anche il modello cantonale non è convincente.

Per queste ragioni, il Consiglio federale è del parere che occorra attenersi alla soluzione attuale, ossia alla ripartizione dei compiti in materia di vigilanza tra Confederazione e Cantoni.

Del resto, il principio della ripartizione della vigilanza non rappresenta nulla di insolito. Lo si ritrova non solo nell'ambito delle attività informative: infatti, nella maggioranza dei Cantoni, la polizia giudiziaria è subordinata dal profilo organizzativo e della funzione di servizio al comando di polizia. Tuttavia, quando svolge com-

piti investigativi per incarico delle autorità giudiziarie, è subordinata alla vigilanza tecnica di queste ultime.

Il *capoverso 2* chiarisce che l'alta vigilanza parlamentare sull'esecuzione della presente legge spetta alla Delegazione delle Commissioni della gestione delle Camere federali e non contemporaneamente (né nella totalità né in parte) a un organo cantonale.

Sezione 3: Protezione giuridica

Art. 71 Protezione giuridica

Il SIC prevede in certi casi misure e decisioni incisive per le quali va garantita un'adeguata protezione giuridica. Il presente articolo prevede al *capoverso 1* la via ordinaria del ricorso al Tribunale amministrativo federale e quindi al Tribunale federale. È pertanto chiaro che le misure e decisioni adottate in virtù della LSI non rientrano tra le eccezioni all'ammissibilità del ricorso previste dall'articolo 83 lettera a della legge federale del 17 giugno 2005[31] 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 3* impedisce che un ricorso possa differire l'ottenimento 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.

Capitolo 7: Disposizioni finali

Art. 72 Disposizioni esecutive

Secondo l'articolo 7 LOGA, il Consiglio federale emana le ordinanze, purché ne sia autorizzato dalla Costituzione o dalla legge (cfr. anche l'art. 182 cpv. 1 Cost.). L'articolo 72 incarica il Consiglio federale, oltre alle deleghe speciali previste nella legge, di emanare anche disposizioni esecutive di carattere generale.

Art. 73 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 osservare quanto segue:

è vero che l'articolo 57 Cost. sottende la competenza implicita della Confederazione a provvedere alla propria sicurezza interna e a emanare disposizioni di legge nella

31 RS **173.110**

misura in cui 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[32] in adempimento del postulato Malama 10.3045). I Cantoni sono dunque liberi di svolgere attività proprie in materia di attività informative 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 avamprogetto di legge.

Nel «rapporto in adempimento del postulato Malama», 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 ai *capoversi 1 e 2* di questa disposizione (acquisizione di informazioni, di propria iniziativa o sulla base di un mandato del SIC, rispettivamen-

[32] FF **2012** 3973

te 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.

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 Consiglio federale intende mantenere questa indennità speciale, che del resto copre solo in parte i costi sostenuti dai Cantoni, e non considerarla già pareggiata nell'ambito della perequazione finanziaria generale tra Confederazione e Cantoni.

Modifica del diritto vigente

I Abrogazione di atti normativi

Il presente avamprogetto non riprende le disposizioni della LMSI 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). Tali disposizioni saranno oggetto della futura legge sui compiti di polizia, pure in fase di elaborazione.

Qualora la legge sul servizio informazioni dovesse entrare in vigore prima della legge sui compiti di polizia, il Consiglio federale provvederebbe, mediante entrate in vigore e abrogazioni parziali, affinché non sorgano lacune giuridiche.

Considerazioni analoghe si applicano anche all'ambito dei controlli di sicurezza relativi alle persone, per i quali è pure in preparazione una nuova legge (legge sulla sicurezza delle informazioni) destinata a sostituirsi alla LMSI in tale ambito. Per questa ragione le disposizioni sui controlli di sicurezza relativi alle persone non figurano più nel presente avamprogetto.

La LSIC sarà per contro interamente integrata nella LSI e può essere totalmente abrogata.

II Modifica di atti normativi

1. Legge federale del 20 giugno 2003[33] sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA)

Art. 9 cpv. 1 lett. c e l (nuove)

L'articolo 9 capoverso 1 lettera c LSISA menziona oggi le autorità federali competenti per la sicurezza interna. L'accesso on line 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. Proponiamo pertanto di definire le condizioni per l'accesso on line 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[34] sugli stranieri e della legge del 26 giugno 1998[35] sull'asilo, motivo per cui nel testo della presente legge si rinuncia a menzionarle singolarmente.

33 RS **142.51**
34 RS **142.20**
35 RS **142.31**

2. Legge federale del 26 giugno 1998[36] sull'archiviazione

Art. 14 cpv. 1 lett. a^{bis} (nuova)

Questa aggiunta colmerà una lacuna attualmente esistente nel diritto in materia di archiviazione. I terzi hanno parzialmente la possibilità di consultare atti archiviati relativi alla sicurezza interna e esterna, ma non l'ente fornitore, in questo caso il servizio informazioni, quando si tratta di una nuova valutazione delle minacce per le quali i dati archiviati possono fornire chiarimenti. La legge federale sull'archiviazione sarà pertanto completata per quanto riguarda questo aspetto della salvaguardia della sicurezza interna ed esterna.

3. Legge federale del 17 dicembre 2004[37] sul principio di trasparenza dell'Amministrazione (LTras)

Le esperienze relative alle domande di consultazione in virtù della LTrans accumulate dal SIC sin dalla sua istituzione indicano che la necessità particolare di proteggere le informazioni di intelligence è scarsamente compatibile con l'obiettivo di trasparenza della legge sulla trasparenza.

Le domande di accesso ricevute finora riguardavano talvolta anche documenti e dossier relativi all'acquisizione di informazioni da parte del SIC oppure su operazioni eseguite dal SIC (o dagli enti che lo hanno preceduto). In singoli casi è stata chiesta anche la consultazione di altri documenti, per esempio sui contatti con servizi partner esteri. In considerazione delle persone o dei servizi partner interessati, il SIC ha dovuto rifiutare ogni volta la consultazione di dossier relativi all'acquisizione o ai servizi partner. Le domande hanno in parte generato una considerevole mole di lavoro, poiché i documenti desiderati hanno dovuto essere ampiamente raggruppati e valutati. Talvolta si è trattato di documenti particolarmente voluminosi contenenti parecchie centinaia di pagine.

Si è provveduto a esaminare la necessità di escludere totalmente il SIC dal campo d'applicazione della legge sulla trasparenza. Tuttavia, poiché esso gestisce anche pratiche puramente amministrative per le quali è possibile dare informazioni sulla base della LTrans, il Consiglio federale propone soltanto un'eccezione materiale per i documenti concernenti l'acquisizione di informazioni di intelligence.

4. Legge del 17 giugno 2005[38] sul Tribunale amministrativo federale

Art. 23 cpv. 2 e art. 36b Autorizzazione delle misure di acquisizione del servizio informazioni

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.

36 RS **152.1**
37 RS **152.3**
38 RS **173.32**

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

Art. 33 lett. b n. 4

Il ricorso contro le decisioni del Consiglio federale intese a vietare determinate attività (art. 31) deve essere prevista esplicitamente poiché finora non figurava nell'elenco esaustivo di cui all'articolo 33 lettera b della legge sul Tribunale amministrativo federale.

5. Codice civile svizzero[39]

Art. 43a cpv. 4 n. 5 (nuovo)

Con il completamento 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 nonché accertare la loro dimora attuale ed eventualmente quelle precedenti. Poiché il CC nel caso degli altri organi con diritto d'accesso non menziona alcun vincolo riguardo allo scopo, non ne è menzionato alcuno nemmeno per il SIC. 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.

6. Codice penale svizzero[40]

Art. 317bis cpv. 1 e 2

Il rinvio alla LMSI è sostituito dal rinvio alla legge sul servizio informazioni.

Art. 365 cpv. 2 lett. r (nuova), s (nuova), t (nuova) e u (nuova)

La novità di questa disposizione consiste nella menzione dei compiti del SIC per la cui esecuzione al SIC occorre l'accesso al casellario giudiziale informatizzato (VOSTRA). Questi accessi sono disponibili già oggi nel quadro dei compiti attuali secondo l'articolo 365 capoverso 2. Questi coprono tuttavia la gamma di compiti del SIC in parte in maniera molto sommaria. È pertanto giustificato, nel quadro della nuova legislazione sul servizio informazioni, completare tale elencazione. La novità consiste segnatamente nella menzione della verifica dell'affidabilità di persone destinate a collaborare a progetti classificati esteri o ad avere accesso a informazioni, materiali o impianti classificati esteri (cfr. art. 10 cpv. 1 lett. d).

Art. 367 cpv. 2 lett. m (nuova) e cpv. 4

Per l'adempimento dei suoi compiti legali, al SIC non occorre soltanto essere informato in merito alle condanne già pronunciate, ma anche in merito a eventuali procedimenti penali pendenti. 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 accerta-

39 RS **210**
40 RS **311.0**

menti dell'affidabilità secondo l'articolo 10 capoverso 1 lettera d LSI. 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.

7. Legge federale del 13 giugno 2008[41] sui sistemi d'informazione di polizia della Confederazione (LSIP)

Nell'ambito degli accessi ai sistemi d'informazione di polizia, la LSI 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 dell'accertamento della dimora di persone e dell'ubicazione di veicoli secondo l'articolo 14 LSI. 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 delle loro autorizzazioni di accesso.

8. Legge federale del 3 febbraio 1995[42] sull'esercito e sull'amministrazione militare

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

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. 12) e riprende anche le medesime misure per proteggere la sfera privata.

Il capoverso 3bis corrisponde all'analoga disposizione dell'articolo 60 capoverso 2 LSI.

9. Legge federale del 3 ottobre 2008[43] sui sistemi d'informazione militari (LSIM)

Art. 16 cpv. 1 lett. h (nuova)

L'accesso on line del SIC alla banca dati PISA è ora previsto affinché il SIC 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.

41 RS **361**
42 RS **510.10**
43 RS **510.91**

10. Legge federale del 21 marzo 2003[44] 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 ed elaborare dati per l'esecuzione della legge federale sull'energia nucleare e dati relativi alla prevenzione dei reati e al loro perseguimento. La prassi ha evidenziato la necessità di estendere il campo di attività del servizio centrale anche all'ambito della legge 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 oppure, in occasione dell'avvio dell'elaborazione di un caso di contrabbando nucleare, non possono ancora essere valutate.

11. Legge federale del 19 dicembre 1958[45] sulla circolazione stradale

Art. 104c cpv. 5 lett. c (nuova)

Mediante 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 non potrebbero essere preparate in maniera adeguata.

12. Legge federale del 6 ottobre 2000[46] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)

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 SCPT 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 art. 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 22 capoverso 1 lettere a-d LSI.

44 RS **732.1**
45 RS **741.01**
46 RS **780.1**

Art. 14 cpv. 2bis

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

13. Legge del 30 aprile 1997[47] sulle telecomunicazioni

Art. 34 cpv. 1ter e 1quater (nuovo)

In questo capoverso viene ora menzionato anche il SIC. In tal modo, nella legge sulle telecomunicazioni è integrato il corrispettivo, sotto il profilo legale formale, dell'articolo 5 capoverso 1 lettera d LSI. Contemporaneamente è istruito il coordinamento tra entrambe le leggi.

Nota riassuntiva concernente i numeri 14 segg.:

Per quanto riguarda gli atti legislativi seguenti, negli articoli concernenti la comunicazione di informazioni vi sono stati esclusivamente adeguamenti formali. Il rinvio alla LMSI è sostituito ogni volta dal rinvio alla LSI. Dal profilo materiale non risulta alcun cambiamento.

Inoltre, in alcune legge è stralciata l'indicazione relativa alla comunicazione dei dati «in singoli casi e su richiesta scritta e motivata» introdotta con LMSI II. Tale indicazione è risultata inutile poiché ogni comunicazione di informazioni al SIC è già compresa nella disposizione che di volta in volta precede. Si tratta pertanto di una semplice correzione di una svista e non di una modifica della situazione giuridica.

14. Legge federale del 20 dicembre 1946[48] su l'assicurazione per la vecchiaia e per i superstiti

Art. 50a cpv. 1 lett. dbis ed e n. 7

15. Legge federale del 19 giugno 1959[49] su l'assicurazione per l'invalidità

Art. 66a cpv. 1 lett. c

16. Legge federale del 25 giugno 1982[50] sulla previdenza professionale per la vecchiaia, i superstiti e l'invalidità

Art. 86a cpv. 1 lett. g e cpv. 2 lett. g

47 RS **784.10**
48 RS **831.10**
49 RS **831.20**
50 RS **831.40**

17. Legge federale del 18 marzo 1994[51] sull'assicurazione malattie

Art. 84a cpv. 1 lett. g^bis e h n. 6

18. Legge federale del 20 marzo 1981[52] sull'assicurazione contro gli infortuni

Art. 97 cpv. 1 lett. h^bis e i n. 6

19. Legge federale del 19 giugno 1992[53] sull'assicurazione militare (LAM)

Art. 1a cpv. 1 lett. q (nuova)

Questa disposizione rappresenta il corrispettivo dell'articolo 32 capoverso 6 LSI, in virtù del quale i collaboratori del SIC impiegati all'estero sono assoggettati all'assicurazione militare. Questa disposizione deve essere iscritta 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 LSI).

20. Legge federale del 25 giugno 1982[54] sull'assicurazione obbligatoria contro la disoccupazione e l'indennità per insolvenza

Art. 97a cpv. 1 lett. e^bis ed f n. 8

51 RS **832.10**
52 RS **832.20**
53 RS **833.1**
54 RS **837.0**

Misure di acquisizione secondo l'avamprogetto della legge sul servizio informazioni

Acquisizione in Svizzera			**Acquisizione all'estero**
Obiettivi dell'acquisizione	Misure non soggette ad autorizzazione secondo gli art. 11 segg.	Misure soggette ad autorizzazione secondo gli art. 22 segg.	
1. Art. 4 cpv. 1 lett. a n. 1–5: → terrorismo → spionaggio → proliferazione → attacchi a infrastrutture critiche	Applicabile	Applicabile	1. *Misure di acquisizione segrete* Condizione: acquisizione di informazioni sull'estero rilevanti in materia di politica di sicurezza secondo l'art. 4 cpv. 1 lett. b 2. *Esplorazione radio* (art. 33). Condizione: acquisizione di informazioni sull'estero rilevanti in materia di politica di sicurezza. Informazioni su fatti in Svizzera possono essere comunicate soltanto se contengono indizi relativi a una minaccia concreta per la sicurezza interna (art. 33 cpv. 5). 3. *Esplorazione dei segnali via cavo* (art. 34 segg.) Per l'acquisizione di informazioni su fatti all'estero rilevanti in materia di politica di sicurezza e per tute-
2. Art. 4 cpv. 1 lett. a n. 6: → estremismo violento	Applicabile	Non applicabile	

			lare altri interessi nazionali essenziali (art. 62) possono essere rilevati segnali di reti filari.
3. Acquisizione in Svizzera di informazioni su fatti all'estero (art. 32 cpv. 2)	Applicabile	Applicabile. Di principio, autorizzazione analogamente all'acquisizione in Svizzera. Eccezione: intrusione in sistemi di ordinatori se tali sistemi sono ubicati all'estero (art. 35 cpv. 2).	
Tutela di altri interessi nazionali essenziali			
Il Consiglio federale può incaricare il SIC di eseguire misure secondo la presente legge per tutelare altri interessi nazionali essenziali secondo l'articolo 1 capoverso 3 (art. 62).			