

ad 07.057

**Messaggio aggiuntivo
concernente la modifica della legge federale sulle misure
per la salvaguardia della sicurezza interna
(«LMSI II ridotta»)**

del 27 ottobre 2010

Onorevoli presidenti e consiglieri,

a complemento del messaggio del 15 giugno 2007 concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna (Mezzi speciali per la ricerca di informazioni), vi sottoponiamo, per approvazione, un messaggio aggiuntivo e un disegno di modifica della legge federale sulle misure per la salvaguardia della sicurezza interna («LMSI II ridotta»).

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

27 ottobre 2010

In nome del Consiglio federale svizzero:

La presidente della Confederazione, Doris Leuthard
La cancelliera della Confederazione, Corina Casanova

Compendio

Nella primavera del 2009 il Parlamento ha rinviato al Consiglio federale il messaggio del 15 giugno 2007¹ concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna («LMSI II»). Il presente messaggio aggiuntivo si esprime in merito al mandato inerente al rinvio e ripropone le misure che godono di un elevato consenso a livello politico o che si riferiscono ad adeguamenti al mutato quadro organizzativo o giuridico oppure a raccomandazioni delle autorità di vigilanza.

Nel giugno 2009 la perizia commissionata dal Consiglio federale e concernente la questione della costituzionalità, è giunta, sostanzialmente, alla conclusione che il diritto superiore (Costituzione federale [Cost.; RS 101] e Convenzione del 4 novembre 1950 per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali [CEDU; RS 0.101]) non si oppone di principio al progetto di revisione, ma che su alcuni punti sono necessari miglioramenti.

Dal licenziamento del messaggio nel 2007 si sono registrate modifiche con ripercussioni dirette e indirette sul progetto legislativo. Ad esempio, il 1° gennaio 2009, le componenti dell'Ufficio federale di polizia (fedpol) che si occupavano di attività informative sono state trasferite al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) e raggruppate dal 1° gennaio 2010 con il Servizio informazioni strategico (SIS) in un nuovo Ufficio federale (Servizio delle attività informative della Confederazione, SIC). Il 1° gennaio 2010 è entrata in vigore anche la legge federale del 3 ottobre 2008² sul servizio informazioni civile (LSIC). Nell'ambito della sua applicazione occorre segnatamente rispettare in maniera rigorosa le norme più severe della legge federale del 21 marzo 1997³ sulle misure per la salvaguardia della sicurezza interna (LMSI) in materia di trattamento dei dati, evitando di limitare inutilmente l'attività del servizio d'informazione esterno e integrando i sistemi d'informazione Sicurezza esterna (ISAS) e Sicurezza interna (ISIS). Nel rapporto del 28 novembre 2008⁴ sulle circostanze della nomina di Roland Nef a capo dell'esercito la Commissione della gestione del Consiglio nazionale (CdG-N) chiede che siano inserite nella revisione della LMSI in corso due modifiche relative al settore dei controlli di sicurezza delle persone. Anche il rapporto della Delegazione delle Commissioni della gestione delle Camere federali (DelCG) del 21 giugno 2010⁵ concernente il trattamento dei dati nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS), nelle sue raccomandazioni 7 e 11, si riferisce direttamente alla presente revisione.

Nel novembre 2009 il Consiglio federale ha incaricato il DDPS di elaborare un messaggio aggiuntivo limitato alle parti non contestate o poco contestate della revisione originaria della legge («LMSI II ridotta»). Tutte le rimanenti disposizioni

1 FF 2007 4613

2 RS 121

3 RS 120

4 FF 2009 2879

5 FF 2010 6777

dovranno essere integrate in un disciplinamento globale sui servizi informazioni civili («legge sul servizio informazioni») da elaborare entro la fine del 2013 al più tardi.

Pertanto, il messaggio aggiuntivo si limita a colmare le lacune più importanti fino all'elaborazione del disciplinamento globale, sempre che le misure in questione godano di un elevato consenso a livello politico o erano già comprese nel pacchetto legislativo originario o che si tratti di adeguamenti necessari al quadro organizzativo o giuridico nel frattempo mutato oppure di raccomandazioni delle autorità di vigilanza.

Poiché con questo modo di procedere l'oggetto del progetto legislativo originario non subisce alcuna modifica tale da lasciar presagire un risultato in linea di principio differente da quello emerso dalla procedura di consultazione svolta a suo tempo, per il presente messaggio aggiuntivo si è potuto rinunciare a un'ulteriore procedura di consultazione.

Indice

Compendio	6924
1 Situazione iniziale	6928
1.1 Messaggio del 15 giugno 2007 concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna	6928
1.2 Mandato delle due Camere	6928
1.3 Legge federale del 3 ottobre 2008 sul servizio informazioni civile (LSIC)	6929
1.4 Rapporto del 28 novembre 2008 sulle circostanze della nomina di Roland Nef a capo dell'esercito	6930
1.5 Rapporto del 21 giugno 2010 concernente il trattamento dei dati nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS)	6930
1.6 «LMSI II ridotta»	6931
2 Attuazione	6931
2.1 Mandato delle due Camere	6931
2.1.1 Perizia Biaggini	6931
2.1.1.1 Mandato di perizia	6931
2.1.1.2 Risultati degli accertamenti di diritto costituzionale	6931
2.1.2 Mandato 1: definire con esattezza le nozioni di «sicurezza interna e esterna» e «beni giuridici protetti» nonché le caratteristiche di sospettabilità di cui è questione in termini astratti agli articoli 13a e 18a D-LMSI	6933
2.1.3 Mandato 2: precisare la collaborazione degli organi di polizia della Confederazione con le autorità cantonali e il loro obbligo d'informazione come pure, in particolare, la collaborazione con servizi esteri	6934
2.1.4 Mandato 3: disciplinare in modo chiaro le interfacce tra l'amministrazione (organi di polizia della Confederazione) e i tribunali	6937
2.1.5 Mandato 4: strutturare una vigilanza parlamentare più efficace in seno alla Confederazione	6938
2.1.6 Mandato 5: precisare le ripercussioni finanziarie del progetto legislativo per la Confederazione e i Cantoni	6939
2.1.7 Mandato 6: verificare in maniera dettagliata la costituzionalità del progetto, segnatamente per quanto concerne la protezione della sfera privata (art. 13 Cost.), della libertà d'opinione e d'informazione (art. 16 Cost.), della libertà dei media (art. 17 Cost.), della libertà di riunione (art. 22 Cost.) e della libertà d'associazione (art. 23 Cost.)	6940
2.2 Rapporto della CdG-N del 28 novembre 2008 sulle circostanze della nomina di Roland Nef a capo dell'esercito	6940

2.3 Rapporto della DelCG 21 giugno 2010 concernente il trattamento dei dati nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS)	6941
2.4 Messaggio aggiuntivo «LMSI II ridotta»	6941
2.4.1 Disegno di legge precedente	6941
2.4.2 Completamenti	6942
2.4.2.1 Autorità competenti	6942
2.4.2.2 Armamento del Servizio delle attività informative della Confederazione	6942
2.4.2.3 Informazioni sui collegamenti di telecomunicazione	6943
2.4.2.4 Lista d'osservazione («listing»/«delisting»)	6943
2.4.2.5 Registrazione con riferimento alle persone interessate secondo l'articolo 3 capoverso 2 LMSI	6944
3 Commento ai singoli articoli	6944
3.1 Osservazione preliminare	6944
3.2 Commento	6945
Allegato: Modifica del diritto vigente	6973
Legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI) (Disegno)	6977

Messaggio aggiuntivo

1 Situazione iniziale

1.1 Messaggio del 15 giugno 2007⁶ concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna

Dopo anni di lavori preliminari, il 15 giugno 2007 il Consiglio federale ha licenziato il messaggio concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI) (Mezzi speciali per la ricerca di informazioni), il cosiddetto «LMSI II». Successivamente, in data 17 dicembre 2008, il Consiglio nazionale, in qualità di Camera prioritaria, ha deciso di non entrare in materia.⁷ Il 3 marzo 2009 il Consiglio degli Stati, in qualità di seconda Camera, ha deciso l'entrata in materia e, contemporaneamente, il rinvio dell'oggetto al Consiglio federale.⁸ Il 28 aprile 2009 il Consiglio nazionale ha approvato la decisione di rinvio al Consiglio federale.⁹

1.2 Mandato delle due Camere

La decisione parlamentare di rinvio¹⁰ chiede al Consiglio federale di:

1. definire con esattezza le nozioni di «sicurezza interna e esterna» e «beni giuridici protetti» nonché le caratteristiche di sospettabilità di cui è questione in termini astratti agli articoli 13a e 18a del disegno di LMSI (D-LMSI);
2. precisare la collaborazione degli organi di polizia della Confederazione con le autorità cantonali e il loro obbligo d'informazione come pure, in particolare, la collaborazione con servizi esteri;
3. disciplinare in modo chiaro le interfacce tra l'amministrazione (organi di polizia della Confederazione) e i tribunali;
4. strutturare una vigilanza parlamentare più efficace in seno alla Confederazione;
5. precisare le ripercussioni finanziarie del progetto legislativo per la Confederazione e i Cantoni;
6. verificare in maniera dettagliata la costituzionalità del progetto, segnatamente per quanto concerne la protezione della sfera privata (art. 13 Cost.¹¹), della libertà d'opinione e d'informazione (art. 16 Cost.), della libertà dei media (art. 17 Cost.), della libertà di riunione (art. 22 Cost.) e della libertà d'associazione (art. 23 Cost.).

⁶ FF 2007 4613

⁷ Boll. Uff. 2008 N 1886

⁸ Boll. Uff. 2009 S 20

⁹ Boll. Uff. 2009 N 673

¹⁰ Boll. Uff. 2009 S 20

¹¹ RS 101

1.3

Legge federale del 3 ottobre 2008¹² sul servizio informazioni civile (LSIC)

Il 3 ottobre 2008 le Camere federali hanno approvato la legge federale sul servizio informazioni civile (LSIC), entrata in vigore il 1° gennaio 2010.

Considerato il diverso rigore delle norme giuridiche stabilite in materia di trattamento dei dati (tra gli altri: obbligo della valutazione, controllo della qualità, termini di cancellazione) le informazioni del SIC sono trattate in due sistemi d'informazione, ognuno soggetto a un regime (LMSI o LSIC). Si tratta del sistema d'informazione Sicurezza esterna (cfr. art. 17–24 dell'ordinanza del 4 dicembre 2009¹³ sui sistemi d'informazione del Servizio delle attività informative della Confederazione, OSI-SIC), gestito in un primo tempo come un esercizio pilota, e del sistema d'informazione Sicurezza interna (cfr. art. 25-35 OSI-SIC).

Al momento in cui è stata emanata la LSIC, il legislatore presumeva che i compiti nel settore del servizio informazioni civile sarebbero stati adempiuti da due servizi separati sotto il profilo organizzativo, ossia il SIS e il Servizio di analisi e prevenzione (SAP). In tale contesto ogni servizio avrebbe continuato a trattare le sue informazioni nel proprio sistema d'informazione. La LSIC doveva garantire lo scambio d'informazioni tra questi servizi e ha inoltre assegnato loro l'incarico di procedere a una valutazione congiunta e globale della situazione di minaccia (cfr. art. 3 LSIC).

Il Consiglio federale ha tratto le conseguenze risultanti da questo incarico comune e ha deciso di fondere i due servizi nel SIC. La fusione aveva lo scopo di assicurare che la valutazione avvenisse in un'unica unità organizzativa, in base a criteri unitari e considerando tutte le informazioni disponibili. Tali informazioni non sono procurate attivamente, soltanto tramite l'acquisizione operativa in Svizzera e all'estero, ma anche mediante lo sfruttamento di fonti aperte (Internet, media, letteratura specializzata, scienza) oppure giungono al SIC senza particolari misure d'acquisizione, segnatamente dai servizi partner nazionali e internazionali.

Attualmente il SIC si trova nella situazione particolare di dover applicare, per il trattamento delle sue informazioni, due diverse basi legali. Le norme più restrittive della LMSI devono essere rigorosamente osservate, evitando di limitare inutilmente l'attività del servizio informazione concernente l'estero. Abbiamo pertanto deciso di estendere, in linea di principio, le norme più severe della LMSI in materia di trattamento dei dati a tutte le informazioni del SIC aventi una relazione diretta con la Svizzera e i suoi abitanti. Le norme meno severe della LSIC si applicano esclusivamente a informazioni del SIC concernenti l'estero e senza alcuna relazione diretta con la Svizzera. Un'istruzione del SIC precisa la nozione di «relazione del contenuto con la Svizzera» (elenco dei criteri) determinante per la selezione dei dati. Sono escluse dalla selezione le comunicazioni dei servizi cantonali incaricati della protezione dello Stato che, in quanto dati LMSI originali (ossia dati che possono essere rilevati esclusivamente sulla base della LMSI), sono soggetti senza eccezioni al regime della LMSI. Questa gestione dei dati è disciplinata dalla OSI-SIC e si fonda sull'articolo 19 capoverso 4 dell'ordinanza del 4 dicembre 2009¹⁴ sul Servizio delle attività informative della Confederazione (O-SIC).

¹² RS 121

¹³ RS 121.2

¹⁴ RS 121.1

Dal gennaio 2010 i dati del SIC sono trattati in sistemi d'informazione differenti, a seconda che abbiano, a livello di contenuto, una relazione diretta con la Svizzera (cittadino svizzero, fattispecie/evento/soggiorno in Svizzera) o concernano esclusivamente l'estero. Lo sviluppo (ulteriore) dei sistemi d'informazione e in particolare la realizzazione dell'esercizio pilota del «sistema d'informazione Sicurezza esterna (ISAS)» per i dati concernenti l'estero avverrà d'intesa con l'Incaricato federale della protezione dei dati e della trasparenza. È nostra intenzione fondare il trattamento delle informazioni del SIC su una base legale che soddisfi anche le moderne esigenze e sottoporre a breve termine al Parlamento un pertinente complemento alla LSIC.

1.4 Rapporto del 28 novembre 2008¹⁵ sulle circostanze della nomina di Roland Nef a capo dell'esercito

Il 28 novembre 2008 la CdG-N ha presentato un rapporto sulle «Circostanze della nomina di Roland Nef a capo dell'esercito». Due (delle complessive sei) raccomandazioni della CdG-N al Consiglio federale includono la condizione che siano attuate nell'ambito della corrente revisione della LMSI. Tali raccomandazioni concernono il momento dell'esecuzione del controllo di sicurezza relativo alle persone e la consultazione degli incarti concernenti procedimenti penali abbandonati o conclusi.

1.5 Rapporto del 21 giugno 2010¹⁶ concernente il trattamento dei dati nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS)

In due raccomandazioni del summenzionato rapporto, la DelCG si riferisce direttamente alla revisione in corso della LMSI:

- Raccomandazione 7: «La DelCG raccomanda al Consiglio federale di proporre alle Camere federali, nel quadro della corrente revisione della LMSI, una chiara definizione legale dei cosiddetti «terzi». Tale definizione deve evitare una raccolta indiscriminata di dati personali irrilevanti ai fini della protezione dello Stato.»
- Raccomandazione 11: «La DelCG raccomanda al Consiglio federale di proporre alle Camere federali, nel quadro della corrente revisione, segnatamente per quanto riguarda l'articolo 18 LMSI, la sostituzione dell'attuale diritto di consultazione indiretto con un diritto d'accesso secondo le modalità dell'articolo 8 LSIP¹⁷.»

Per l'attuazione delle raccomandazioni 7 e 11 si rimanda al numero 2.3, mentre per la discussione dettagliata del rapporto nel suo complesso e delle altre raccomandazioni si rimanda al parere del Consiglio federale.

¹⁵ FF 2009 2879

¹⁶ FF 2010 6777

¹⁷ Legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione, LSIP; RS 361.

1.6 «LMSI II ridotta»

Il 27 novembre 2009 abbiamo incaricato il DDPS di elaborare un messaggio aggiuntivo limitato alle parti non contestate della revisione originaria. Le rimanenti disposizioni saranno recepite in un disciplinamento globale sui servizi informazioni civili («legge sul servizio informazioni»).

2 Attuazione

2.1 Mandato delle due Camere

Le considerazioni seguenti si limitano ai punti indispensabili al messaggio aggiuntivo.

2.1.1 Perizia Biaggini

2.1.1.1 Mandato di perizia

La Confederazione Svizzera, rappresentata dal DDPS, ha incaricato nel dicembre 2008 il professor dott. iur. Giovanni Biaggini, professore ordinario di diritto pubblico, diritto amministrativo e diritto europeo all'Università di Zurigo, di eseguire accertamenti di diritto costituzionale. Il perito aveva il compito di verificare, sulla base di norme di diritto superiore (Cost. e Convenzione del 4 novembre 1950¹⁸ per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, CEDU), alcune prescrizioni legali di carattere generale e astratto a livello di legge federale (disegno di legge LMSI II).

2.1.1.2 Risultati degli accertamenti di diritto costituzionale

La perizia pubblicata nel 2009 nella Giurisprudenza delle autorità amministrative della Confederazione (GAAC)¹⁹ (Biaggini Giovanni, Accertamenti di diritto costituzionale concernenti la revisione parziale della legge federale sulle misure per la salvaguardia della sicurezza interna, perizia del giugno 2009, nel seguito «perizia Biaggini») precisa che in linea di principio il diritto superiore non si oppone al progetto di revisione. Inoltre giunge alle seguenti conclusioni:

Per quanto concerne i mezzi speciali per la ricerca di informazioni, segnatamente per quanto concerne la definizione di tali mezzi, il disegno di legge non soddisfa ancora in tutti i punti le esigenze di conformità con i diritti fondamentali. Sono necessari miglioramenti soprattutto per quanto riguarda i punti seguenti:

- specificazione dei beni degni di protezione tali da giustificare o da far apparire ragionevoli gravi ingerenze in diritti fondamentali;
- garanzia di una protezione efficace dei diritti fondamentali di terzi, segnatamente per quanto concerne il segreto professionale;

¹⁸ RS 0.101

¹⁹ GAAC 2009.14, pp. 238–330

- garanzia di una protezione efficace del nucleo inviolabile dei diritti fondamentali;
- limitazione e chiarificazione delle possibilità di comunicazione di dati personali acquisiti con i mezzi speciali di raccolta delle informazioni.

Sono inoltre stati individuati alcuni punti poco chiari (ma non tali da costituire una violazione della Cost. o della CEDU) per quanto concerne la procedura di decisione, la procedura di approvazione, la procedura d'urgenza, l'obbligo di comunicazione e l'allestimento di rapporti.

Per quanto riguarda il divieto di determinate attività la perizia constata che il disegno rispetta l'ordinamento delle competenze dello Stato federale e può essere interpretato e applicato in modo conforme ai diritti fondamentali. La norma non costituisce una base legale né per il divieto di organizzazioni né per un'inversione dell'onere della prova.

Sia l'obbligo d'informazione speciale delle autorità sia l'obbligo d'informazione dei trasportatori commerciali sono essenzialmente conformi alla Costituzione federale. Si deplora l'assenza di linee direttrici legali sufficientemente chiare per la comunicazione di dati personali da parte del SIC alle autorità di perseguimento penale.

I previsti disciplinamenti concernenti l'esplorazione radio presenterebbero ancora alcune lacune. Ciò si applica tanto all'ambito delle «emissioni» provenienti dalla Svizzera soggette al segreto delle telecomunicazioni (rimandi non chiari) quanto alle rimanenti «emissioni» (delega troppo ampia al Consiglio federale per quanto concerne i dettagli dell'organizzazione, della procedura e dell'esplorazione radio).

L'impiego delle nozioni di «sicurezza interna e esterna», «terrorismo», «spionaggio politico o militare», «commercio illecito di armi o materiale radioattivo» oppure «trasferimento illegale di tecnologia» è conforme alla Costituzione federale.

Una precisazione o definizione legale delle nozioni di «sicurezza interna e esterna» non è necessaria dal punto di vista costituzionale. Poiché si tratta di nozioni tratte dalla Costituzione federale, per un'eventuale precisazione sarebbe competente il costituente e non il legislatore.

Una precisazione o definizione legale delle nozioni di «terrorismo», «spionaggio politico o militare», «commercio illecito di armi o materiale radioattivo» e «trasferimento illegale di tecnologia» sarebbe possibile, ma anche in questi casi non sussiste alcuna necessità dal punto di vista costituzionale (per la valutazione di pertinenti ponderazioni in materia di diritti fondamentali, nel singolo caso concreto sono ben più importanti altri criteri).

Il diritto «indiretto» d'essere informati può in linea di principio essere interpretato e applicato in modo conforme alla Costituzione federale e alla CEDU; non sussiste pertanto alcuna urgente necessità di agire a livello legislativo.

2.1.2

Mandato 1: definire con esattezza le nozioni di «sicurezza interna e esterna» e «beni giuridici protetti» nonché le caratteristiche di sospettabilità di cui è questione in termini astratti agli articoli 13a e 18a D-LMSI

Secondo la perizia Biaggini l'impiego delle nozioni di «sicurezza interna e esterna», «terrorismo», «spionaggio politico o militare», «commercio illecito di armi o materiale radioattivo» e «trasferimento illegale di tecnologia» è conforme alla Costituzione federale.

In base alla perizia, una precisazione o definizione legale delle nozioni di «sicurezza interna e esterna» non è quindi necessaria dal punto di vista costituzionale. Poiché si tratta di nozioni tratte dalla Costituzione federale, per un'eventuale precisazione sarebbe competente il costituente e non il legislatore. Per difetto di competenza, si rinuncia pertanto a pertinenti proposte nell'ambito della LMSI.

Al riguardo occorre ribadire che la distinzione tra «sicurezza interna» e «sicurezza esterna» è sempre più difficile e talvolta praticamente impossibile. Nondimeno, secondo opinione generale la «sicurezza interna» designa la protezione della società e dello Stato da minacce che si sviluppano in seno alla società stessa. Essa è compromessa quando la stabilità e l'affidabilità delle istituzioni politiche costituzionali dello Stato, l'ordinamento fondamentale dello Stato fondato sulle libertà e sulla democrazia, il funzionamento regolare di tali istituzioni nonché la sicurezza della popolazione della Svizzera sono minacciati. Per «sicurezza esterna», invece, si intende la sicurezza di uno Stato di fronte a minacce di carattere militare provenienti da altri Stati o gruppi di Stati. Negli ultimi anni sono venuti ad aggiungersi anche pericoli non militari quali la migrazione illegale, le pandemie o, ancora, lo «hacking» a fini di spionaggio economico, militare o politico. La «sicurezza esterna» è compromessa quando l'integrità e l'affidabilità dell'indipendenza di uno Stato, la sua capacità di difendere le proprie frontiere e il proprio ordinamento costituzionale nei confronti di minacce esterne nonché i suoi buoni rapporti con gli altri Stati sono minacciati.

In base alla perizia, una precisazione o definizione legale delle nozioni di «terrorismo», «spionaggio politico o militare», «commercio illecito di armi o materiale radioattivo» e «trasferimento illegale di tecnologia» sarebbe possibile, ma non sussiste alcuna necessità dal punto di vista costituzionale. Considerata la possibilità di una precisazione, conformemente al mandato ricevuto il disciplinamento dell'obbligo d'informazione speciale delle autorità è stato completato da opportuni criteri e da un elenco esemplificativo di beni giuridici protetti.

Gli articoli 18a-18m D-LMSI riguardano la ricerca speciale di informazioni, a cui si rinuncia nel quadro del messaggio aggiuntivo. Risultano quindi superflue ulteriori considerazioni in merito.

2.1.3

Mandato 2: precisare la collaborazione degli organi di polizia della Confederazione con le autorità cantonali e il loro obbligo d'informazione come pure, in particolare, la collaborazione con servizi esteri

Collaborazione con le autorità cantonali

Il 1° gennaio 2009 le componenti di fedpol incaricate di compiti informativi sono state trasferite al DDPS e un anno più tardi, il 1° gennaio 2010, raggruppate con il SIS nel nuovo SIC. Nel contempo sono state approvate la LSIC e l'O-SIC. Con l'entrata in vigore dell'O-SIC, l'ordinanza del 27 giugno 2001²⁰ sulle misure per la salvaguardia della sicurezza interna (OMSI) e, di conseguenza, la regolamentazione dettagliata della collaborazione con le autorità cantonali e i servizi esteri, è stata abrogata. Nel contempo, con l'emanazione dell'ordinanza del 4 dicembre 2009²¹ sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia, tutte le pertinenti regolamentazioni dell'OMSI sono recepite in detta ordinanza.

Attualmente la collaborazione del SIC con le autorità cantonali si fonda in primo luogo sulla LSIC, sulla LMSI e sull'O-SIC. Al riguardo, la collaborazione è già stata esaminata e, per quanto necessario, precisata.

Come finora, della sicurezza interna del proprio territorio è responsabile in primo luogo il singolo Cantone. Se in virtù della Costituzione e delle leggi la Confederazione è responsabile della sicurezza interna, i Cantoni la assistono sul piano dell'amministrazione e dell'esecuzione.

La LSIC prevede che le unità del servizio informazioni civile informino altri servizi della Confederazione e dei Cantoni su tutti i fatti concernenti i compiti legali di tali servizi in materia di salvaguardia della sicurezza interna ed esterna. La collaborazione è disciplinata dal Consiglio federale.

Secondo l'O-SIC, nel quadro della legislazione e del mandato fondamentale che gli è assegnato, il SIC può collaborare, tra l'altro, con servizi dei Cantoni. In particolare, può comunicare dati personali alle autorità cantonali che svolgono compiti ai sensi della LMSI (cfr. all. 3, n. 4 O-SIC). Inoltre il SIC collabora strettamente con 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). Quale contropartita le autorità cantonali sono tenute a informare spontaneamente il SIC nei seguenti ambiti:

- attività, mene e operazioni che minacciano la sicurezza esterna della Svizzera o gli interessi svizzeri in materia di politica di sicurezza all'estero;
- attività terroristiche: mene tendenti a influire o a modificare Stato e società, da attuare o favorire commettendo o minacciando di commettere gravi reati nonché propagando paura e timore;
- spionaggio ai sensi degli articoli 272–274 e 301 del Codice penale²² (CP);

²⁰ RS 120.2

²¹ RS 120.52

²² RS 311.0

- estremismo violento: mene di organizzazioni i cui esponenti negano la democrazia, i diritti dell'uomo o lo Stato di diritto e che allo scopo di raggiungere i loro obiettivi commettono, approvano o incoraggiano atti violenti;
- commercio illecito di materiali radioattivi e trasferimento illegale di tecnologia;
- altre attività nonché mene e operazioni condotte in Svizzera o all'estero, che compromettono la sicurezza interna della Svizzera.

Inoltre le autorità cantonali sono tenute, tra l'altro, a comunicare spontaneamente e senza indugio al SIC:

- i fatti e le constatazioni menzionati nella lista confidenziale del DDPS secondo l'articolo 11 capoverso 2 lettera a LMSI, nella misura in cui la lista viene resa nota alle autorità;
- tutte le constatazioni in merito a organizzazioni e gruppi menzionati nella lista confidenziale del DDPS di cui all'articolo 11 capoverso 2 lettera b LMSI o nell'ambito di una procedura di controllo secondo l'articolo 25 O-SIC;
- le informazioni necessarie all'attuazione di operazioni e programmi di ricerche preventivi;
- i fatti e le constatazioni di cui all'allegato 1 O-SIC, ovvero:
 - situazioni e avvenimenti che si delineano o si sono verificati e per i quali le singole autorità cantonali di polizia non sono più in grado di garantire la sicurezza senza l'aiuto di altri Cantoni (impieghi IKAPOL);
 - passaggio illegale della frontiera da parte di persone o gruppi di persone provenienti da Paesi d'origine indicati dal SIC;
 - compromissione della sicurezza lungo la frontiera;
 - informazioni su attività di persone e gruppi a sfondo razzista o di estremismo violento;
 - individuazione di materiale di propaganda a sfondo razzista o di estremismo violento;
 - messa al sicuro di materiale che può servire a scopi propagandistici e il cui contenuto incita concretamente e seriamente a utilizzare la violenza contro persone o beni.

Per quanto riguarda i compiti secondo la LMSI, i Cantoni adempiono di norma in maniera indipendente i mandati e in determinate situazioni di sospetto procedono alla ricerca attiva di informazioni. Il SIC può anche incaricare gli organi di sicurezza cantonali di osservare fatti in luoghi pubblici e liberamente accessibili e di registrarli su supporti video e audio. Del rimanente, i Cantoni presentano una richiesta al SIC se ritengono che determinate persone o organizzazioni debbano essere oggetto di una ricerca di informazioni o ne debbano essere escluse.

Nel settore della protezione dello Stato, la Confederazione finanzia a favore dei Cantoni un'ottantina di posti a tempo pieno, che sul piano organizzativo sono integrati nelle polizie cantonali o, nel Cantone di Basilea Città, nel ministero pubblico. Nei Cantoni la funzione di autorità di vigilanza è assunta da un organo di controllo separato dall'organo esecutivo. L'organo di controllo verifica se le procedure amministrative sono conformi alle pertinenti prescrizioni legali, segnatamente se i dati per

la salvaguardia della sicurezza interna sono trattati separatamente dalle altre informazioni di polizia. Esso può consultare dati della Confederazione se il SIC lo consente espressamente. La consultazione può segnatamente essere rifiutata ove lo richiedano la protezione delle fonti o interessi essenziali in materia di sicurezza.

In sintesi risulta quindi che il SIC collabora strettamente con i Cantoni, concede loro un elevato grado di autonomia nell'adempimento del mandato e coopera anche a livello intercantonale – segnatamente nel quadro della CDDGP o della CCPCS – e che al riguardo già esiste un rigoroso sistema di norme.

Collaborazione con servizi esteri

Il Consiglio federale disciplina la collaborazione tra le unità del servizio informazioni civile e i servizi esteri, definendo segnatamente i principi che presiedono all'utilizzo delle informazioni provenienti da servizi esteri ai fini dell'adempimento dei compiti del servizio informazioni civile (art. 3 cpv. 4 lett. c LSIC).

Conformemente all'O-SIC (cfr. Sezione 4: Collaborazione del SIC con servizi esteri), il SIC assicura i collegamenti con servizi informazioni esteri che adempiono compiti ai sensi della LMSI e della LSIC. Inoltre rappresenta la Svizzera in organismi informativi internazionali e coordina tutti i contatti. Al riguardo, definisce una politica comune in materia di servizi partner e allestisce una pianificazione dei contatti. L'avvio di contatti regolari con servizi informazioni esteri necessita del consenso del Consiglio federale. Il SIC può trasmettere informazioni a servizi esteri, sempre che sia consentito dalla legge o da un trattato internazionale oppure necessario per la sicurezza della Confederazione. Può scambiare direttamente dati personali con autorità estere mediante installazioni di trasmissione comuni. In occasione della comunicazione di dati personali, informa il destinatario sull'affidabilità e l'attualità dei medesimi e lo rende attento allo scopo esclusivo per il quale può utilizzare i dati e sul fatto che si riserva il diritto di esigere informazioni sull'utilizzazione che ne è stata fatta. Il SIC registra la comunicazione, il suo destinatario, l'oggetto e il motivo. Per quanto concerne i rapporti con le autorità di perseguimento penale, esso deve osservare i principi della legge federale del 20 marzo 1981²³ sull'assistenza internazionale in materia penale. I Cantoni informano il SIC in merito alla loro collaborazione con servizi esteri attuata per adempiere compiti ai sensi della LMSI e della LSIC.

Per quanto concerne la sicurezza interna, segnatamente nei settori del terrorismo, dello spionaggio, dell'estremismo violento, del commercio illecito di armi o di materiale radioattivo e del trasferimento illegale di tecnologia, la LMSI stabilisce espressamente che le relazioni con le autorità estere incaricate di compiti di sicurezza incombano alla Confederazione. Per le questioni di sicurezza nella zona di confine i Cantoni possono cooperare con le autorità straniere di polizia competenti. Il SIC può, in casi specifici, comunicare dati personali agli organi di sicurezza degli Stati con i quali la Svizzera ha relazioni diplomatiche, ove lo preveda una legge o una convenzione internazionale approvata oppure se:

- l'informazione è necessaria per prevenire o chiarire un crimine o un delitto punibile anche in Svizzera;
- tali dati sono necessari per motivare una domanda svizzera d'informazioni;

²³ RS 351.1

- la comunicazione avviene nell'interesse della persona di cui si tratta e quest'ultima vi ha acconsentito oppure se le circostanze permettono di presumerne l'accordo;
- la comunicazione è indispensabile alla salvaguardia di interessi considerevoli inerenti alla sicurezza della Svizzera o dello Stato destinatario.

La comunicazione all'estero non può avvenire se la persona interessata dovesse, in ragione della trasmissione dei dati, essere esposta al pericolo di una doppia punizione o a pregiudizi gravi per la salute, la vita, o la libertà ai sensi della CEDU.

Pertanto, nell'ambito dei suoi contatti con l'estero, il SIC è strettamente vincolato alle direttive del Consiglio federale. Va peraltro sottolineato che la collaborazione in ambito informativo con i servizi stranieri avviene su base volontaria, segnatamente sulla base della fiducia reciproca e di interessi strategici comuni. Le informazioni sono messe reciprocamente a disposizione in base al principio di reciprocità (*do ut des*), ciò che non lascia assolutamente alcuno spazio a un atteggiamento esclusivamente passivo. Se la collaborazione con l'estero non può essere garantita in modo adeguato a causa di un margine di manovra legale interno troppo ristretto, la Svizzera rischia di essere esclusa dal flusso d'informazioni provenienti dall'estero. Esiste pure il pericolo che anche servizi d'informazione con i quali già avvengono degli scambi operino illegalmente sul territorio per tutelare i propri interessi se dovessero giudicare insufficiente la collaborazione con le autorità svizzere. Casi simili sono già noti.

2.1.4 Mandato 3: disciplinare in modo chiaro le interfacce tra l'amministrazione (organi di polizia della Confederazione) e i tribunali

Con il trasferimento al DDPS delle componenti del Dipartimento federale di giustizia e polizia (DFGP, fedpol) incaricate di compiti informativi e il successivo raggruppamento del SAP e del SIS nel nuovo SIC si è operata l'auspicata separazione tra i compiti informativi del SIC e i compiti di polizia di fedpol.

Per le indagini di polizia giudiziaria nell'ambito di competenza della Confederazione sono competenti gli organi federali di perseguimento penale, ossia il Ministero pubblico della Confederazione (MPC) e la Polizia giudiziaria federale (PGF).

Vige il principio secondo cui il SIC mette tempestivamente a disposizione di altri servizi della Confederazione e dei Cantoni le sue informazioni, se sono utili per il perseguimento penale o la lotta contro la criminalità organizzata oppure concernono i compiti legali di tali servizi in materia di salvaguardia della sicurezza interna ed esterna (art. 4 LSIC, art. 9 O-SIC e art. 2 cpv. 3 LMSI). Il SIC è quindi tenuto per legge a trasmettere spontaneamente alle autorità nazionali di perseguimento penale le informazioni rilevanti per il perseguimento di reati. A seconda della consistenza delle informazioni trasmesse, le autorità di perseguimento penale aprono direttamente un procedimento penale oppure effettuano ulteriori accertamenti preliminari per verificare il sospetto di reato.

Inversamente, le autorità di cui agli articoli 3 e 4 LSIC e 13 LMSI (segnatamente la PGF, il MPC e gli organi del Corpo delle guardie di confine e delle dogane) hanno l'obbligo di informare spontaneamente il SIC quando vengono a conoscenza di minacce concrete per la sicurezza interna ed esterna (cfr. art. 4 O-SIC). Dal punto di

vista giuridico, tale cooperazione si fonda su un esauriente sistema normativo (legge, ordinanza, convenzioni, istruzioni).

Il disciplinamento delle interfacce tra gli organi di perseguimento penale della Confederazione e i tribunali incombe alla pertinente legislazione formale e materiale (CP e Codice di procedura penale del 5 ottobre 2007²⁴, CPP) e ai regolamenti organizzativi interni del MPC e di fedpol.

Una descrizione dettagliata delle competenze repressive della Confederazione nella lotta contro il terrorismo e la criminalità organizzata e delle relative interfacce figura nel rapporto del Consiglio federale del 9 giugno 2006²⁵ in adempimento del postulato della Commissione della politica di sicurezza del Consiglio degli Stati del 21 febbraio 2005 concernente una lotta più efficace contro il terrorismo e la criminalità organizzata, cui si rimanda.

Occorre distinguere da quanto precede la cooperazione tra gli organi di perseguimento penale e il SIC (vedi più sopra).

In sintesi la collaborazione tra le autorità di perseguimento penale e il SIC si fonda su principi affermati a cui occorre attenersi.

Poiché il messaggio aggiuntivo rinuncia alla ricerca di informazioni con l'ausilio di mezzi speciali prevista dal messaggio del 15 giugno 2007, risultano superflue ulteriori considerazioni concernenti la questione dell'utilizzabilità sotto il profilo giudiziario di informazioni acquisite in tal modo. Per contro, occorrerà tenere conto di questa problematica con l'emanazione di una norma di conflitto dettagliata nel quadro dell'elaborazione, entro la fine del 2013 al più tardi, del disciplinamento globale («legge sul servizio informazioni»).

2.1.5 Mandato 4: strutturare una vigilanza parlamentare più efficace in seno alla Confederazione

Conformemente all'articolo 25 LMSI, il SIC accorda agli organi parlamentari di vigilanza pieno accesso in qualsiasi momento a tutti i locali, gli atti e i sistemi elettronici e risponde dettagliatamente a domande concernenti le sue attività. D'altronde, finora gli organi parlamentari di vigilanza non hanno mai fatto valere di non aver potuto effettuare la loro vigilanza perché disponevano di pochi diritti o perché l'Amministrazione avrebbe limitato in altro modo i mezzi a loro disposizione.

Secondo il Consiglio federale, attualmente la DelCG esercita la sua funzione in modo adeguato e critico. È fatto salvo il parere del Consiglio federale sul rapporto del 21 giugno 2010²⁶ concernente il trattamento dei dati nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS). L'eventuale potenziamento della vigilanza parlamentare dovrebbe essere in primo luogo verificato e formulato dal Parlamento stesso.

²⁴ RS 312.0; RU 2010 1881

²⁵ FF 2006 5223

²⁶ FF 2010 6777

2.1.6

Mandato 5: precisare le ripercussioni finanziarie del progetto legislativo per la Confederazione e i Cantoni

Nel 1997, al momento in cui è stata emanata la LMSI, il messaggio di allora stimava i costi di esecuzione annuali (ossia i costi rimborsati ai Cantoni dalla Confederazione) tra i dieci e i venti milioni di franchi. In effetti, attualmente i pertinenti costi ammontano «soltanto» a circa 8,5 milioni di franchi. Pertanto l'ammontare dei costi di esecuzione indicati a suo tempo al Parlamento non è mai stato raggiunto.

Ripercussioni finanziarie per la Confederazione: secondo il messaggio del 15 giugno 2007 i posti necessari per l'attuazione, gli investimenti e le spese d'esercizio sono compensati internamente dal DFGP. Nel frattempo, con il trasferimento al DDPS delle componenti del DFGP (fedpol) incaricate di compiti informativi e il successivo raggruppamento del SAP e del SIS nel nuovo SIC è venuta a crearsi una nuova situazione. Tuttavia, conformemente alla volontà del Consiglio federale, anche in futuro ci si atterrà alla compensazione dei costi all'interno dell'Amministrazione. Pertanto, il pacchetto legislativo non comporta nuovi costi né nella sua versione originaria né nella sua versione elaborata secondo il messaggio aggiuntivo.

Per quanto riguarda i costi da compensare internamente all'Amministrazione, il messaggio originario indica spese annuali ricorrenti per il personale di circa 6,5 milioni di franchi, spese d'investimento uniche di circa un milione di franchi e spese annue ricorrenti di circa 100 000 franchi. Con la rinuncia alla «ricerca speciale di informazioni», prevista nel presente messaggio aggiuntivo, si calcola ora che il bisogno di personale supplementare sarà considerevolmente inferiore. Si potrà stabilire quanti posti saranno concretamente necessari per l'applicazione del pacchetto legislativo solo quando si conoscerà la struttura concreta delle misure in questione (per es. accertamenti dei fatti e istanze per quanto riguarda il divieto di determinate attività; attività supplementari in relazione al «listing»/«delisting» nell'ambito della lista d'osservazione; accertamenti supplementari in relazione all'obbligo d'informazione delle autorità e dei trasportatori professionali, compreso il chiarimento di pertinenti controversie; misure di protezione a favore degli informatori; creazione, gestione e mantenimento di identità fittizie ecc.). Secondo una stima approssimativa, il bisogno di personale supplementare è valutato in una decina di posti, vale a dire che, con la rinuncia ai mezzi speciali per la ricerca di informazioni, nel presente progetto ridotto si può ipotizzare una diminuzione a circa un quarto dei costi preventivati in origine. Del rimanente, il SIC si sforza per quanto possibile di compensare l'eventuale fabbisogno supplementare sfruttando le sinergie risultanti dal raggruppamento del SAP e del SIS.

Ripercussioni finanziarie per i Cantoni: probabilmente in una prima fase l'estensione dell'obbligo d'informazione nei Cantoni genererà, in misura modesta, oneri di lavoro supplementari. Quale contropartita si conseguirà un livello di sicurezza più elevato sul piano federale, cantonale e comunale. Nondimeno, a media e lunga scadenza, è possibile attendersi anche sgravi grazie alla possibilità di indagini migliorate sotto il profilo dei contenuti e agevolate a livello formale. Pertanto, gli oneri e gli sgravi dovrebbero grossomodo compensarsi.

2.1.7 Mandato 6: verificare in maniera dettagliata la costituzionalità del progetto, segnatamente per quanto concerne la protezione della sfera privata (art. 13 Cost.), della libertà d'opinione e d'informazione (art. 16 Cost.), della libertà dei media (art. 17 Cost.), della libertà di riunione (art. 22 Cost.) e della libertà d'associazione (art. 23 Cost.)

La perizia Biaggini è giunta alla conclusione che in linea di principio il diritto superiore non si oppone al progetto di revisione e quindi che la sua costituzionalità è, di principio, dimostrata. Nella misura in cui, in singoli casi, sono stati ritenuti necessari dei miglioramenti, si rimanda al commento ai singoli articoli.

2.2 Rapporto della CdG-N del 28 novembre 2008²⁷ sulle circostanze della nomina di Roland Nef a capo dell'esercito

Considerata la revisione legislativa in corso, la CdG-N ha raccomandato quanto segue:

«... *Raccomandazione 2 Consultazione degli incarti concernenti procedimenti penali chiusi o sospesi*

La CdG-N raccomanda al Consiglio federale di vegliare affinché, nell'ambito della revisione in corso della LMSI, siano prese le misure necessarie affinché, in occasione di controlli di sicurezza relativi alle persone al più alto livello, il servizio specializzato CSP possa controllare anche gli incarti relativi a procedimenti penali chiusi o abbandonati.

Raccomandazione 5 Momento dell'esecuzione del controllo di sicurezza relativo alle persone

La CdG-N chiede al Consiglio federale di esaminare l'opportunità di effettuare un controllo di sicurezza relativo alle persone prima della nomina a talune alte funzioni di grande responsabilità. Inoltre, la Commissione domanda al Consiglio federale di vegliare affinché, nell'ambito della revisione in corso della LSMI, siano prese le misure necessarie affinché il contenuto dell'articolo 19 capoverso 3 LMSI sia identico nelle tre lingue ufficiali. ...»

Le raccomandazioni 2 e 5 sono state recepite e concretizzate negli articoli 19 capoverso 3 e 20 capoverso 2 lettera d del disegno di legge elaborato secondo il messaggio aggiuntivo.

A ciò si aggiungono adeguamenti in relazione con l'indipendenza dell'autorità di controllo e il trasferimento parziale di settori di controllo alla Cancelleria federale (art. 21 D-LMSI).

Per i dettagli si rimanda al commento ai singoli articoli (cfr. n. 3).

²⁷ FF 2009 2879

2.3

Rapporto della DelCG del 21 giugno 2010 concernente il trattamento dei dati nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS)

La raccomandazione 7 chiede una chiara definizione legale dei cosiddetti «terzi». In tal modo si intende evitare una raccolta indiscriminata di dati personali irrilevanti ai fini della protezione dello Stato.

Attualmente le regole in materia di trattamento dei dati nel sistema d'informazione ISIS-NT sono essenzialmente disciplinate nell'OSI-SIC. Conformemente all'articolo 2 lettera i di tale ordinanza, per «terzi» s'intendono persone o organizzazioni che sono rilevanti ai fini della protezione dello Stato unicamente in virtù di una relazione con un oggetto. Anche la nozione di «oggetti» è disciplinata nell'ordinanza.

Il nostro Collegio ritiene pertanto che l'atto normativo appropriato per il chiarimento della nozione di «terzi» non sia per principio la legge (LMSI) come suggerito dalla DelCG, ma piuttosto l'ordinanza (OSI-SIC). Altrimenti è disposto a procedere alla precisazione auspicata.

Per quanto concerne la modifica del diritto indiretto di essere informati richiesta dalla DelCG nella sua raccomandazione numero 11, con riferimento alle modalità previste all'articolo 8 LSIP, il Consiglio federale ha ritenuto che si trattasse di un'esigenza minima e ha adottato una misura più incisiva, ancorando nella legge il diritto diretto di essere informati; al riguardo si rimanda all'articolo 18 del disegno di legge.

2.4

Messaggio aggiuntivo «LMSI II ridotta»

2.4.1

Disegno di legge precedente

Sia nella procedura di consultazione che nel dibattito politico e nei resoconti dei media, la ricerca speciale di informazioni (ossia la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, l'osservazione in luoghi non liberamente accessibili, anche mediante apparecchi tecnici di sorveglianza, nonché l'accesso segreto a sistemi per l'elaborazione di dati) figurava di gran lunga tra le misure più criticate. Questo vale anche per le disposizioni esecutive inerenti a tali misure (art. 18a-18j, 27 cpv. 1^{bis} lett. b, 14 cpv. 3 del disegno di legge del 15 giugno 2007), principalmente per quanto concerne la procedura di decisione, la procedura di approvazione e la procedura d'urgenza o le disposizioni che riguardano la sorveglianza di terzi e la tutela del segreto professionale. Per questi motivi, e considerato che dopo il raggruppamento del SAP e del SIS nel nuovo SIC in molti ambiti si impongono soluzioni comuni, nel quadro del messaggio aggiuntivo si rinuncia per il momento a tali misure. Risultano quindi superflui anche una nuova articolazione della LMSI e un articolo separato concernente i rimedi giuridici; di quest'ultima esigenza si può tenere conto direttamente nei pertinenti articoli.

Gli articoli restanti del disegno di legge originario hanno palesato un'accettazione a livello politico sensibilmente superiore. Di conseguenza, tali disposizioni sono mantenute, completandole nel contempo come indicato al numero 1.5.2. È fatta salva la disposizione di coordinamento relativa allo scambio di informazioni prevista

nel quadro della collaborazione tra Confederazione e Cantoni, a cui si deve rinunciare in seguito al venir meno, nel frattempo, delle pertinenti basi costituzionali.

Inoltre il disciplinamento dell'esplorazione radio previsto in origine nel messaggio aggiuntivo sarà rimandato alla futura legge sul servizio informazioni: da un lato, va trovata una soluzione uniforme per l'intero servizio informazioni e al riguardo sono necessari dati empirici che oggi ancora mancano; d'altro lato, occorre evitare che l'organismo attualmente competente per i controlli (Istanza di controllo indipendente, ICI), ma praticamente non sufficiente per adempiere le future esigenze, venga disciplinato a livello di legge. Ma, soprattutto, è apparso che a livello funzionale e di contenuti la nozione di «esplorazione radio» è connessa strettamente alla sorveglianza delle telecomunicazioni e che pertanto, ai sensi di un approccio uniforme, dev'essere disciplinata con essa, tanto più che gli attuali canali di comunicazione si situano in un flusso continuo e che proprio nel settore concernente l'estero sussistono ancora numerose questioni che necessitano chiarimenti.

2.4.2 Completamenti

Dal licenziamento del messaggio nel 2007, il contesto giuridico della revisione legislativa si è modificato. In particolare, il 1° gennaio 2009, le componenti di fedpol incaricate di compiti informativi sono state trasferite al DDPS e, dal 1° gennaio 2010, raggruppate con il SIS in un nuovo Ufficio federale (SIC). Nel quadro del messaggio aggiuntivo occorre pertanto tenere conto delle conseguenti ripercussioni dirette e indirette sulla revisione legislativa originaria.

2.4.2.1 Autorità competenti

Con il trasferimento al DDPS, il 1° gennaio 2009, delle componenti di fedpol incaricate di compiti informativi e la successiva creazione del SIC, la responsabilità delle questioni in materia di attività informative civili incombe al capo del DDPS.

2.4.2.2 Armamento del Servizio delle attività informative della Confederazione

La legge federale del 20 giugno 1997²⁸ sulle armi, gli accessori di armi e le munizioni (Legge sulle armi, LArm) esclude esplicitamente le autorità di polizia dal suo campo d'applicazione. Poiché con la creazione del SIC il 1° gennaio 2010, i precedenti nessi con il settore della polizia sono venuti in parte a cadere, va precisato che anche il SIC deve essere escluso dal campo d'applicazione della LArm, poiché non si può escludere l'uso di armi da fuoco per ragioni di servizio in caso di legittima difesa o stato di necessità (cfr. qui di seguito).

Il settore di compiti legale del SIC in Svizzera e pertanto l'eventuale situazione di minaccia che ne deriva per i collaboratori, giustifica di principio l'armamento di parti del SIC (cfr. commento al n. 3). Per questa ragione e per chiarire la situazione giuridica nella LMSI va creata una base legale formale che consenta l'armamento

²⁸ RS 514.54

mirato, per scopi di autodifesa, di collaboratori del SIC particolarmente esposti. I pertinenti criteri di dettaglio – e quelli concernenti la necessaria istruzione – devono essere emanati dal Consiglio federale nel quadro di una norma di delega che menzioni i criteri più importanti. Tuttavia, nella fattispecie, l'impiego delle armi presso il SIC dev'essere consentito – in misura adeguata alle circostanze – esclusivamente in caso di legittima difesa o stato di necessità e non per adempiere un mandato, ciò che equivarrebbe a disporre di competenze esecutive in materia di polizia. Evidentemente una persona ferita in seguito all'uso delle armi dev'essere soccorsa. Questo principio è pure esplicitamente menzionato a livello di legge.

2.4.2.3 Informazioni sui collegamenti di telecomunicazione

Un'ulteriore conseguenza del venir meno di parte dei nessi con il settore della polizia (cfr. n. precedente) è il fatto che, dal 1° gennaio 2010, il SIC non rientra in alcuna delle autorità, menzionate espressamente nell'articolo 14 della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)²⁹, cui si possono fornire informazioni sui collegamenti di telecomunicazione. Poiché le informazioni sui collegamenti di telecomunicazione («A chi appartiene il numero telefonico XY?») rientrano nell'attività quotidiana dei servizi informazioni, risulta indispensabile rettificare l'attuale situazione giuridica. Analogamente alle autorità autorizzate a ricevere informazioni quali, ad esempio, fedpol o i comandi di polizia cantonali e delle città, anche per il SIC va previsto un diritto d'accesso alle informazioni nel quadro del principio di proporzionalità, vale a dire limitato all'adempimento di compiti informativi. Va peraltro sottolineato che il contenuto delle conversazioni, i dati storici del collegamento oppure i dati secondari non sono disponibili, poiché la sorveglianza o/e l'acquisizione dei medesimi possono essere ordinati unicamente dalle competenti autorità inquirenti nel quadro di una sorveglianza dei servizi di telecomunicazione.

2.4.2.4 Lista d'osservazione («listing»/«delisting»)

Secondo l'articolo 11 capoverso 2 LMSI, il DDPS determina in una lista confidenziale (designata anche «lista d'osservazione») le organizzazioni e i gruppi riguardo ai quali è dato il sospetto concreto che mettano in pericolo la sicurezza interna o esterna. La lista dev'essere sottoposta una volta l'anno al Consiglio federale per l'approvazione e alla DelCG per conoscenza. L'iscrizione di un'organizzazione o di un gruppo nella lista ha quale conseguenza che gli organi di sicurezza sono autorizzati a trattare tutte le informazioni disponibili su di essi e sui loro esponenti, e quindi anche quelle che ricadrebbero nei limiti dell'articolo 3 LMSI.

Già nel 2005 la DelCG ha sollevato la questione del «listing» e del «delisting» di gruppi internazionali che figurano su liste internazionali.

In occasione della trattazione del messaggio e del disegno di legge del 15 giugno 2007 in seno alla Commissione degli affari giuridici, il consigliere nazionale Fluri ha presentato la seguente proposta:

²⁹ RS 780.1

«...*Proposta Fluri*
del 20 maggio 2008
Ad art. 11

Il Consiglio federale deve adeguare la lista d'osservazione secondo l'articolo 11 LMSI, e di conseguenza lo stesso articolo 11, alle mutate condizioni in materia di liste internazionali intervenute dall'emanazione della LMSI, segnatamente per quanto riguarda l'inserimento nella lista d'osservazione di dati ripresi da liste internazionali e la relativa cancellazione ...».

La lista d'osservazione è uno strumento di condotta del Consiglio federale. Dal 11 settembre 2001 la comunità internazionale ha intensificato la lotta contro il terrorismo. L'armonizzazione della lista d'osservazione con le misure di prevenzione internazionali ha pertanto assunto un'importanza tale che il legislatore non poteva prevedere. Negli ultimi anni, grazie all'integrazione delle liste internazionali, la lista d'osservazione ha subito un considerevole ampliamento. Di conseguenza, occorre creare un disciplinamento legale per la ripresa di dati dalle liste internazionali, segnatamente per quanto concerne il «listing» e il «delisting».

2.4.2.5 Registrazione con riferimento alle persone interessate secondo l'articolo 3 capoverso 2 LMSI

L'articolo 3 capoverso 2 LMSI disciplina la ricerca e il trattamento di informazioni qualora sussista un sospetto fondato che l'esercizio dei diritti politici o dei diritti fondamentali serva a dissimulare la preparazione o l'esecuzione di attività terroristiche, di spionaggio o di estremismo violento. Nel passato recente la vigilanza sulle attività informative interna all'Amministrazione ha rilevato il bisogno di chiarimento relativamente al termine applicabile nella fattispecie e nell'ambito di una perizia l'Ufficio federale di giustizia (UFG) si è espresso sulla questione se le informazioni acquisite in virtù dell'articolo 3 capoverso 1 LMSI debbano essere confermate prima di poter essere registrate con riferimento alle persone interessate, oppure se le informazioni possano essere acquisite e registrate sulla base dell'articolo 3 capoverso 1 LMSI fino a quando i sospetti relativi a un comportamento punibile sono confermati.

Alla luce delle considerazioni concernenti il diritto in materia di vigilanza, della formulazione poco chiara del capoverso 2 e considerato che il trattamento di dati relativi all'esercizio dei diritti politici costituisce sempre un ambito altamente sensibile, con la presente revisione parziale si provvederà a un chiarimento inequivocabile ai sensi della prassi attuale.

3 Commento ai singoli articoli

3.1 Osservazione preliminare

Il disegno di legge del messaggio aggiuntivo sostituisce il disegno presentato unitamente al messaggio del 15 giugno 2007. Le considerazioni della perizia Biaggini sono state ampiamente recepite e la concretizzazione delle relative raccomandazioni ha avuto luogo direttamente nell'ambito dell'adeguamento delle norme.

Art. 3 cpv. 2

L'attuale capoverso 2 è stato rielaborato in ordine ai tre seguenti indirizzi:

- sostituzione di formulazioni negative con formulazioni positive;
- limitazione temporale mediante l'indicazione di una durata massima;
- sostituzione dell'espressione «comportamento punibile» con l'indicazione di attività concrete, analogamente al capoverso 1.

Nella sua perizia del 12 maggio 2009 concernente l'interpretazione dell'articolo 3 capoverso 2 LMSI³⁰, l'UFG è giunto, tra l'altro, alle seguenti conclusioni: a) per verificare se i sospetti in merito a un eventuale comportamento delittuoso siano fondati, è necessario poter connettere le informazioni raccolte a una persona precisa; b) difatti i sospetti possono essere confermati o esclusi soltanto dopo l'esecuzione di dettagliati accertamenti riguardo alla persona interessata; c) di conseguenza, in caso di sospetti, le informazioni devono essere registrate, durante un certo periodo, con riferimento alle persone interessate, finché vi sia certezza in merito alla fondatezza dei sospetti. Conformemente a tali conclusioni, l'attuale ambigua regolamentazione è stata sostituita con una norma chiara, in cui la procedura legittima è descritta mediante formulazioni positive.

In un secondo momento sono state recepite, mediante la definizione di un limite temporale, le perplessità espresse dall'autorità di vigilanza sulle attività informative: la conferma dei sospetti deve essere fornita entro un anno. Se ciò non è stato possibile o se le attività menzionate hanno potuto essere escluse già in precedenza, tutti i pertinenti dati devono essere cancellati senza indugio dopo l'esclusione dei sospetti.

Infine si è rinunciato al criterio del «comportamento punibile», sostituito ai sensi di quanto indicato sopra. Si è proceduto in tal senso perché la sicurezza interna del Paese può essere minacciata anche da comportamenti non punibili e, soprattutto, perché il comportamento determinante per la decorrenza e quello determinante per la scadenza del termine devono essere della medesima natura.

Art. 5a (nuovo)

Impiego di armi di servizio

Il SIC svolge compiti di intelligence nel settore della sicurezza interna, segnatamente in relazione con il terrorismo, lo spionaggio, l'estremismo violento, il commercio illecito di armi o di materiale radioattivo oppure il trasferimento illegale di tecnologia. Tra i suoi compiti figura la ricerca di informazioni non pubblicamente accessibili. I collaboratori addetti alla ricerca di informazioni devono talvolta muoversi in ambienti altamente criminali nei quali una vita umana conta poco, in particolare quando sono incaricati di avviare o curare contatti con cerchie attive nei summenzionati ambiti illegali. Tali collaboratori prestano pertanto da sempre, nella misura del necessario, il proprio servizio con l'arma. Al momento della creazione del SIC, sono venuti in parte a mancare gli agganci sino ad allora esistenti con il settore della polizia e, di conseguenza, con le relative deroghe alla legge sulle armi. Il porto di un'arma da parte di determinati collaboratori resta tuttavia oggettivamente giustificato, considerate le caratteristiche del settore di compiti proprio all'intelligence e le

relative situazioni di pericolo. Ai sensi di un aggiornamento di una regolamentazione che ha dato buone prove, va pertanto creata un'esplicita base legale per il porto di armi di servizio. Non si tratta dunque in alcun caso di equipaggiare con armi, in maniera capillare, l'intero organico del SIC, ma di far sì che anche in futuro i collaboratori del servizio possano essere dotati di un'arma in caso di effettivo pericolo connesso con lo svolgimento dei loro compiti e unicamente a fini di autodifesa. Nella prassi è interessato dalla norma circa il 10 per cento del personale del SIC. Al riguardo, si rimanda a quanto esplicitamente sancito all'articolo 16 capoverso 4 O-SIC: ai fini della ricerca di informazioni «l'impiego della violenza nei confronti di persone», e pertanto anche il ricorso a mezzi coercitivi, «è proibito» – come è il caso per le autorità di polizia.

Cpv. 1

Conformemente al capoverso 1, il Consiglio federale designa, in base ai rispettivi compiti di servizio, i collaboratori da equipaggiare con un'arma e definisce la necessaria istruzione all'arma. L'obiettivo è limitare l'equipaggiamento con un'arma alle persone esposte a pericoli nello svolgimento della propria funzione di servizio. Si tratta di circa il 10 per cento del personale.

Cpv. 2 e 3

In virtù del capoverso 2, l'impiego dell'arma è ammesso unicamente in caso di legittima difesa e in stato di necessità. Per i collaboratori del SIC equipaggiati con un'arma si applicano pertanto i medesimi principi giuridici già previsti per qualsivoglia persona in situazione analoga. Nel capoverso 3 è esplicitamente stabilito che una persona ferita deve essere soccorsa.

Interesse pubblico e proporzionalità

L'interesse pubblico alla protezione dell'integrità fisica e della vita dei collaboratori del SIC durante lo svolgimento delle rispettive attività è manifesto. Per quanto concerne la proporzionalità, i presupposti della legittima difesa e dello stato di necessità implicano che gli aventi diritto devono rinunciare al bene minacciato nella misura in cui una simile rinuncia può ragionevolmente essere pretesa da essi. Il motivo giustificativo impone dunque già di per sé un impiego proporzionato.

Art. 9 (nuovo)

Divieto di determinate attività

Il divieto di determinate attività è volto a influire già a livello di prevenzione sul comportamento di privati prima ancora che possano svilupparsi minacce concrete per la sicurezza interna o esterna della Svizzera.

Secondo il diritto vigente, divieti del genere devono fondarsi sulla Costituzione federale e soddisfare presupposti molto restrittivi. Il Consiglio federale è autorizzato dalla Costituzione federale a emanare ordinanze e decisioni per tutelare gli interessi del Paese (art. 184 cpv. 3 Cost.) e ad adottare misure per far fronte a gravi turbamenti, esistenti o imminenti, dell'ordine pubblico o della sicurezza interna o esterna della Svizzera (art. 185 cpv. 3 Cost.). Le ordinanze fondate su queste due disposizioni costituzionali devono tuttavia essere limitate nel tempo e non possono essere prorogate a tempo indeterminato. Altrimenti si rischierebbe di invalidare la Costituzione. Di conseguenza è qui proposta a livello di legge la creazione di una possibilità di vietare determinate attività in caso di effettiva minaccia alla sicurezza nazionale.

La nuova disposizione lascia intatte le citate competenze del Consiglio federale secondo gli articoli 184 capoverso 3 e 185 capoverso 3 Cost., che continuano a sussistere in parallelo.

Per i divieti o le misure emanate dal Consiglio federale in virtù della Costituzione federale sono previste vie di ricorso diverse da quelle applicabili a un divieto disposto da un Dipartimento, come è qui il caso secondo il nuovo disciplinamento proposto. Le decisioni del Consiglio federale sono atti di governo e in quanto tali possono essere impugnate dinanzi a un Tribunale della Confederazione soltanto se il diritto internazionale pubblico conferisce un diritto al giudizio da parte di un tribunale³¹, altrimenti sono definitive. Le disposizioni emanate in virtù della LMSI secondo quanto qui proposto saranno dunque impugnabili mediante ricorso presentato al Tribunale amministrativo federale, la cui decisione potrà essere impugnata dinanzi al Tribunale federale. Le critiche espresse esplicitamente o implicitamente al riguardo da singoli partecipanti alla consultazione, secondo cui la possibilità di ricorso aprirebbe la via a un'inversione dell'onere della prova, sono state chiaramente confutate dalla perizia Biaggini (cfr. n. 2.1.1). Al contrario: la nuova competenza deve giustappunto essere controbilanciata da incisivi rimedi giuridici.

Rientrando il divieto di determinate attività nell'ambito della coercizione di polizia, dovrà a suo tempo essere valutata l'opportunità di un eventuale trasferimento della norma nella legge federale sui compiti di polizia della Confederazione (LCPol), attualmente in fase di elaborazione. Poiché, da quanto è dato sapere, la LCPol sarà trattata in Parlamento a una data ulteriore, nulla si oppone al trattamento della norma nel quadro del presente pacchetto legislativo.

Del rimanente, in considerazione di precedenti disposizioni comparabili e in base a un'esperienza pluriennale, si può ipotizzare che si verificheranno pochissimi casi l'anno, motivo per cui il conseguente onere del DFGP non è separatamente indicato.

Cpv. 1

Al capo del DFGP è attribuita la competenza per pronunciare un divieto di diritto amministrativo contro attività che comportano una concreta minaccia per la sicurezza interna o esterna della Svizzera. A tal fine deve essere preliminarmente consultato il SIC; di regola sarà piuttosto quest'ultimo a presentare relative richieste motivate. Si è pertanto optato per una procedura analoga a quella vigente per la messa al sicuro, il sequestro e la confisca di materiale di propaganda conformemente all'attuale articolo 13a LMSI (decisione del DFGP/di fedpol previa consultazione del DDPS/del SIC).

Vi sono attività che a prima vista possono sembrare innocue o addirittura degne di sostegno, quali le raccolte di fondi a favore di vedove e orfani in una zona di conflitto all'estero. Tuttavia, sempreché una raccolta di fondi non abbia luogo per iniziativa di un'opera assistenziale riconosciuta, non di rado in simili contesti sono esercitate pressioni che rasentano l'estorsione (per es. si avvicinano i membri di una comunità straniera residente nel nostro Paese minacciando che, se si rifiutano di fare una donazione, i familiari rimasti in patria ne subiranno le conseguenze). Inoltre, talvolta i fondi raccolti non vengono destinati allo scopo indicato in Svizzera, ma impiegati, almeno in parte, in tutt'altro modo, ad esempio per l'acquisto di armi per

³¹ Cfr. DTF 125 II 417 segg. La giurisprudenza su questo aspetto è sancita anche nell'art. 83 lett. a della legge federale del 17 giugno 2005 sul Tribunale federale (RS 173.110) e nell'art. 32 cpv. 1 lett. a della legge sul Tribunale amministrativo federale (RS 173.32).

un movimento di resistenza operante nella zona di conflitto. Simili macchinazioni sono difficili da provare in via diretta. In Svizzera i donatori coatti tacciono per paura di nuocere a se stessi e ai familiari, amici e conoscenti rimasti in patria. Presto si perdono le tracce del denaro a causa della complessità dei trasferimenti di capitali, dell'attestazione dell'uso dei fondi per mezzo di certificati stranieri lacunosi, contraffatti oppure autentici perché ottenuti grazie alla corruzione, ma dal contenuto fasullo ecc. Per non mettere in pericolo le persone coinvolte non è nemmeno possibile rivolgersi direttamente ai Paesi di destinazione dei fondi. Del resto le organizzazioni adoperate per raccogliere le donazioni cambiano spesso nome, si presentano in modo sempre diverso e non di rado incaricano terzi residenti all'estero di «raccolgere le donazioni».

Il capo del DFGP deve definire i termini e il contenuto del divieto con la massima precisione possibile. La richiesta avanzata da alcuni partecipanti alla procedura di consultazione di elencare nella legge le attività da vietare è stata esaminata e respinta. Un elenco di attività suscettibili di essere vietate equivarrebbe a un invito diretto a eluderlo e inoltre diverrebbe impossibile prevenire tempestivamente nuove forme di minaccia. Una definizione ancora più restrittiva dei criteri non consentirebbe di contemplare l'intera gamma dei comportamenti indesiderati e costituenti una minaccia per la sicurezza.

Contrariamente al timore espresso da alcuni partecipanti alla consultazione, il divieto di determinate attività non è uno strumento per combattere l'opposizione. Il divieto riguarda soltanto mene destinate a promuovere attività terroristiche o di estremismo violento e che costituiscono pertanto una minaccia concreta per la sicurezza interna o esterna della Svizzera. Pertanto il fine qui perseguito è impedire lo svolgimento di attività non punibili *a priori*, ma comportanti minacce concrete.

Se il mancato rispetto del divieto è punibile, il divieto deve contenere un riferimento alla comminatoria di pena di cui all'articolo 292 CP. Non occorre che la legge rimandi alla norma penale, in quanto tale riferimento avrebbe carattere puramente dichiaratorio.

Cpv. 2

I divieti ai sensi del capoverso 1 possono impedire agli interessati di esercitare i loro diritti fondamentali e devono pertanto 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 i presupposti sono ancora adempiuti, la durata di un divieto può essere prorogata fintantoché le circostanze lo esigono. La limitazione massima ammessa, di volta in volta pari a cinque anni, obbliga il Dipartimento a verificare a intervalli regolari i presupposti all'origine della disposizione. Se i presupposti non sono più adempiuti, il divieto deve essere revocato senza indugio dal capo del DFGP, vale a dire dalla medesima autorità da cui è stato disposto.

Cpv. 3 e 4

Sono qui create le basi legali per l'impugnazione dinanzi al Tribunale amministrativo federale, con pieno potere d'esame, dei divieti di diritto amministrativo di determinate attività pronunciati in virtù della LMSI. Sono altresì create le basi per una successiva impugnazione dinanzi al Tribunale federale.

Interesse pubblico e proporzionalità

Vietare determinate attività tutelate lede fortemente i diritti fondamentali in questione e può sfociare nella lesione di più di un diritto, ad esempio la libertà d'associazione (art. 23 Cost.), la libertà di credo e di coscienza (art. 15 Cost.), la libertà d'opinione e d'informazione (art. 16 Cost.), la libertà di riunione (art. 22 Cost.) o la garanzia della proprietà (art. 26 Cost.). Secondo l'articolo 36 Cost., tali restrizioni devono essere giustificate da un interesse pubblico e proporzionate allo scopo. L'interesse pubblico risulta dall'obbligo, iscritto tra i compiti della LMSI, di rilevare e combattere tempestivamente i pericoli dovuti ad attività terroristiche e di estremismo violento. Quanto alla proporzionalità, va rilevato che vietare una determinata attività alle condizioni indicate nella legge non è sproporzionato *a priori*: la necessaria ponderazione degli interessi deve aver luogo per ogni singolo caso concreto. La perizia Biaggini (cfr. n. 2.1.1) ha confermato che la norma è conforme alle competenze nonché interpretabile e applicabile in conformità ai diritti fondamentali.

Art. 10a (nuovo)

Rappresentazione della situazione

La disposizione disciplina un compito affidato già oggi agli organi di sicurezza della Confederazione (cfr. l'ordinanza sull'organizzazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport³², in particolare l'art. 8 cpv. 3 lett. c e d nonché l'art. 15 cpv. 3 LMSI e l'art. 25 cpv. 2 lett. g OSI-SIC).

Il SIC provvede a una valutazione e a una rappresentazione globali della situazione di minaccia. A tale scopo gestisce, tra l'altro, il Centro federale di situazione, che integra in un quadro generale le informazioni rilevanti che riceve dai singoli settori della sicurezza interna (dai Cantoni e da altri servizi federali) e che in occasione di eventi particolari (per es. grandi manifestazioni) fornisce un contributo decisivo alla gestione della rete informativa integrata svizzera. Per svolgere i propri compiti, il Centro federale di situazione gestisce un sistema d'informazione elettronico (presentazione elettronica della situazione, PES). Tra il sistema d'informazione elettronico per la rappresentazione della situazione e il sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS) non esiste alcun collegamento tecnico. A condizione che simili dati siano indispensabili per la rappresentazione della situazione, il sistema può contenere anche dati personali e dati personali degni di particolare protezione (cfr. art. 3 della legge federale del 19 giugno 1992³³ sulla protezione dei dati, LPD). Ciò è necessario perché nella LPD i concetti di «persona» e «dati personali» sono stati definiti in maniera molto ampia e perché la rappresentazione e la valutazione di eventi rilevanti per la sicurezza spesso non sono possibili senza il ricorso a dati personali (per es. rete informativa integrata per il World Economic Forum (WEF) a Davos: in quanto fondazione, il WEF è una persona giuridica protetta dal diritto in materia di protezione dei dati). In occasione di eventi particolari quali l'EURO 08, nell'ambito dei quali vi è una stretta collaborazione tra gli Stati partner (nel caso concreto l'Austria), a titolo eccezionale parti della PES possono essere rese accessibili anche ad autorità di sicurezza e di polizia estere. Ciò vale pure per gli enti privati, nel qual caso con il termine di «privati» si intendono soltanto le persone che adempiono una funzione importante nella gestione dell'evento e sono coinvolte nella rete informativa integrata. Tale può essere ad esempio il caso delle FFS.

³² RS 172.214.1

³³ RS 235.1

Art. 11 cpv. 2, 3, 4-7 (nuovi)

Conformemente all'articolo 11 capoverso 2 lettera b LMSI, il DDPS determina in una lista confidenziale le organizzazioni e i gruppi in merito a cui sussiste il «sospetto concreto che mettano in pericolo la sicurezza interna o esterna». Conformemente all'articolo 11 capoverso 3 LMSI, la lista deve essere sottoposta «una volta all'anno all'approvazione del Consiglio federale e in seguito alla Delegazione delle commissioni della gestione per conoscenza». La lista (chiamata anche «lista d'osservazione») deve essere sottoposta «ogni quattro anni (...) a una valutazione complessiva» (art. 27 cpv. 3 O-SIC).

La lista d'osservazione è uno strumento di condotta del Consiglio federale. Dal 11 settembre 2001 la comunità internazionale ha intensificato la lotta contro il terrorismo. Il coordinamento della lista d'osservazione con le misure di prevenzione a livello internazionale ha pertanto assunto un grado di importanza che non poteva essere previsto dal legislatore. Negli ultimi anni la lista d'osservazione ha subito un considerevole ampliamento soprattutto a causa dell'inclusione di dati provenienti dalle liste internazionali.

L'iscrizione di un'organizzazione o di un gruppo nella lista d'osservazione non comporta sanzioni (per es. un divieto di organizzazione), a differenza di quanto previsto nel sistema di liste ONU istituito in virtù della risoluzione n. 1267 del Consiglio di sicurezza dell'ONU. Un'ulteriore differenza è costituita dal fatto che la lista d'osservazione non comprende singoli individui. Infine, la procedura annuale d'approvazione da parte del Consiglio federale assicura il margine di manovra necessario per la cancellazione di organizzazioni o gruppi dalla lista.

La questione dell'iscrizione nella lista d'osservazione di gruppi internazionali già iscritti in liste internazionali e della loro eventuale successiva cancellazione dalla lista d'osservazione («listing» e «delisting») era già stata sollevata nel 2005 – in una lettera al capo del DFGP – dalla DelCG, alla quale la lista d'osservazione è annualmente sottoposta per conoscenza. Alla fine di agosto 2007 fedpol, allora competente in materia, è stato incaricato di elaborare – in collaborazione con l'Ufficio federale di giustizia – una proposta concreta per l'ancoraggio nella legislazione della prassi già in vigore per l'inclusione di dati provenienti dalle liste internazionali nella lista d'osservazione.

La richiesta della DelCG è stata recepita nell'ambito della proposta revisione parziale della LMSI, che comprende pertanto anche una sufficiente regolamentazione legale dell'elaborazione di dati provenienti da liste internazionali.

Cpv. 2

Il nuovo capoverso 2 corrisponde all'attuale capoverso 2 lettera a LMSI.

Cpv. 3

Rispetto all'attuale regolamentazione dell'iscrizione nella lista d'osservazione di organizzazioni e gruppi «in merito a cui sussiste il sospetto concreto che mettano in pericolo la sicurezza interna o esterna» (primo periodo), la lista d'osservazione è estesa ai dati ripresi dalle liste internazionali (secondo periodo).

Per l'iscrizione dei dati valgono diversi presupposti. Di regola un'organizzazione o un gruppo sono iscritti nella lista d'osservazione se sussiste il sospetto concreto che mettano in pericolo la sicurezza interna o esterna. Per quanto concerne le organizzazioni e i gruppi già iscritti nelle liste internazionali, la loro presenza in una di tali

liste costituisce già di per sé il presupposto per l'iscrizione nella lista d'osservazione. In tal caso, soprattutto in considerazione degli aspetti formali, si verifica a intervalli regolari se le organizzazioni e i gruppi interessati figurano ancora nelle liste internazionali e se non può essere sostanzialmente escluso che costituiscano una minaccia per la sicurezza della Svizzera. Quest'ultimo punto non è sempre materialmente accertabile, soprattutto nei casi in cui un'organizzazione non è (ancora) attiva in Svizzera. Ad ogni modo, il fatto di figurare in una lista internazionale costituisce il criterio determinante: in tal caso è esclusa la cancellazione dalla lista d'osservazione. Senza questa regolamentazione non sarebbe ad esempio possibile individuare tempestivamente i tentativi messi in opera da un'organizzazione classificata come pericolosa a livello internazionale per insediarsi in Svizzera e adottare le misure del caso per impedirne l'espansione.

Il concetto di «liste internazionali» è precisato nella legge. Si tratta di liste allestite da organizzazioni internazionali di sicurezza collettiva quali l'Organizzazione delle Nazioni Unite o da comunità sovranazionali quali l'Unione europea. Tale precisazione consente di escludere altri generi di liste, ad esempio liste redatte da singoli Paesi o da organizzazioni che non dispongono al riguardo di alcuna autorizzazione in virtù del diritto internazionale o il cui relativo mandato non ha valore a livello internazionale. Le liste internazionali ai sensi della legge sono invece allestite da organizzazioni internazionali o comunità sovranazionali a cui è stato assegnato un mandato in materia di salvaguardia della sicurezza internazionale e di lotta al terrorismo.

Cpv. 4

L'iscrizione di un'organizzazione o di un gruppo nella lista di cui al capoverso 3 ha quale conseguenza che gli organi di sicurezza sono autorizzati a trattare tutte le informazioni disponibili su di essi e sui loro esponenti, e quindi anche quelle che ricadrebbero entro i limiti di cui all'articolo 3 LMSI (per es. informazioni concernenti la preparazione di una pacifica manifestazione o lo svolgimento di attività di propaganda). Il trattamento di simili informazioni può essere determinante per una visione d'insieme delle attività, del potenziale e delle strutture di comando di un'organizzazione classificata come pericolosa.

Cpv. 5, 6 e 7

Nel capoverso 5 sono disciplinati i presupposti per il cosiddetto «delisting»: l'organizzazione o il gruppo interessati non devono più essere menzionati in alcuna lista internazionale conformemente al capoverso 3 e non deve più sussistere alcun sospetto concreto in merito all'esistenza di una minaccia per la sicurezza interna o esterna della Svizzera.

Il capoverso 6 delega al Consiglio federale la designazione delle organizzazioni internazionali e delle comunità sovranazionali le cui liste vanno prese in considerazione nonché la definizione dei pertinenti criteri di verifica. Nel capoverso 7 è sancito il principio dell'approvazione da parte del Consiglio federale e della notifica alla DelCG.

Interesse pubblico e proporzionalità

La revisione parziale dell'articolo 11 si inserisce nel solco della LMSI, fondata sulla competenza non scritta della Confederazione di salvaguardare la sicurezza interna ed esterna della Svizzera e sui compiti della Confederazione per la tutela della sicurezza.

za interna (art. 173 Cost.). Ci si è attenuti sotto ogni profilo al settore di compiti ancorato nell'articolo 2 capoversi 1 e 2 LMSI.

L'estensione della lista d'osservazione proposta nel quadro della presente modifica potrebbe generare ingerenze nei diritti fondamentali. Ciò vale segnatamente per la sfera privata (art. 13 Cost.), la libertà d'associazione (art. 23 Cost.) e la libertà di riunione (art. 22 Cost.).

A tenore dell'articolo 36 Cost., le restrizioni dei diritti fondamentali devono fondarsi su una base legale, devono essere giustificate da un interesse pubblico o dalla tutela dei diritti fondamentali di terzi e devono rispettare il principio della proporzionalità. Inoltre, non deve essere violata l'essenza dei diritti fondamentali. La restrizione di un diritto fondamentale è ammessa a condizione che vengano minacciati o lesi in modo grave specifici beni giuridici di terzi o della collettività.

L'iscrizione di organizzazioni o gruppi nella lista d'osservazione è sancita in una legge formale, la LMSI. Il primo criterio è pertanto soddisfatto. L'interesse pubblico consiste nella protezione della sicurezza interna o esterna e nell'individuazione tempestiva di minacce derivanti dal terrorismo o dall'estremismo violento. L'esistenza di un interesse pubblico legittimo è pertanto incontrovertibile. Nell'ambito della verifica della proporzionalità di un intervento statale, vanno in linea di principio prese in considerazione anche le circostanze connesse in ogni singolo caso con le misure in questione. Se dall'iscrizione nella lista d'osservazione di organizzazioni e gruppi già menzionati in liste internazionali conseguono una sensibilizzazione delle autorità competenti e una maggiore attenzione di quest'ultime verso le attività all'estero di tali organizzazioni e gruppi, l'iscrizione nella lista d'osservazione è lo strumento adatto per mettere a disposizione informazioni utili che consentano di valutare e prevenire un'eventuale minaccia. Quanto alla necessità dello strumento, è evidente che l'iscrizione nella lista d'osservazione può consentire di ottenere la necessaria visione d'insieme riguardo a eventuali potenziali di minaccia. Va inoltre sottolineato che la lista d'osservazione è uno strumento di condotta del Consiglio federale e che l'iscrizione di un'organizzazione o di un gruppo non comporta alcuna sanzione. Per quanto concerne l'esame della proporzionalità in senso stretto, ossia la valutazione se l'interesse pubblico prevalga su quello di un'organizzazione o di un gruppo, tale esame può essere eseguito soltanto per ogni singolo caso concreto. La costituzionalità è data.

Art. 13 cpv. 1^{bis} (nuovo), 3 e 4

Cpv. 1^{bis} (nuovo)

Dal 1° gennaio 2010 il SIC non fa più parte di nessuna delle autorità esplicitamente menzionate nell'articolo 14 della legge federale del 6 ottobre 2000³⁴ sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT), alle quali possono essere comunicate informazioni concernenti i collegamenti di telecomunicazione (nome, indirizzo e, se disponibile, professione dell'utente o parametri di comunicazione ed elementi numerici quali identificazioni, numeri di chiamata e numeri brevi oppure i generi di collegamento). Poiché la richiesta di simili informazioni è parte integrante delle attività quotidiane di intelligence, è necessario adeguare di conseguenza la LSCPT (cfr. «Modifica del diritto vigente»)

e, per ragioni di trasparenza, indicare nella LMSI il servizio competente per le informazioni. Tale esigenza è stata recepita in un capoverso autonomo, al fine di mettere in risalto la distinzione tra autorità di perseguimento penale e SIC. Nel quadro del principio di proporzionalità, il diritto a ricevere informazioni è con ogni evidenza limitato all'adempimento di compiti di intelligence. Va osservato che i contenuti delle comunicazioni rimangono integralmente protetti e non sono in alcun modo disponibili. Lo stesso vale per i cosiddetti dati di traffico o i cosiddetti dati secondari, disponibili soltanto per le autorità di perseguimento penale previa autorizzazione da parte di un giudice dei provvedimenti coercitivi.

Cpv. 3

Poiché le informazioni su una minaccia derivante dal terrorismo, dallo spionaggio politico o militare, dal commercio illecito di armi o materiale radioattivo oppure dal trasferimento illegale di tecnologia devono essere comunicate permanentemente (cfr. art. 13a), l'articolo 13 delega al Consiglio federale soltanto i settori rimanenti, ossia l'estremismo violento e lo spionaggio economico.

Cpv. 4

La disposizione finora contenuta in questo capoverso è abrogata e inserita in un nuovo articolo autonomo (cfr. art. 13b).

Art. 13a Obbligo d'informazione speciale delle autorità

A causa della modifica strutturale della legge il vigente articolo 13a LMSI (Messa al sicuro, sequestro e confisca di materiale di propaganda) diventa il nuovo articolo 13e. Lo spostamento non comporta una modifica del contenuto (cfr. il commento all'art. 13e).

Rispetto all'articolo 13, il *nuovo* articolo 13a è una norma speciale. Essa è circoscritta a una parte dei compiti previsti dalla legge, ma risulta più incisiva in quanto si applica a tutte le autorità federali e cantonali nonché alle organizzazioni che esercitano funzioni pubbliche. Di queste organizzazioni non fanno tuttavia parte ad esempio le banche cantonali, poiché non sono investite di competenze ufficiali.

Cpv. 1

Il capoverso 1 stabilisce un obbligo d'informazione per determinati generi di minaccia se quest'ultimi rischiano di ledere importanti beni giuridici.

I generi di minaccia sono elencati in maniera esaustiva alla lettera b: attività terroristiche; spionaggio politico o militare e proliferazione. Si tratta di minacce che, considerato il loro potenziale, possono pregiudicare i valori fondamentali della Svizzera, minando le istituzioni parlamentari, giudiziarie o governative e mettendo a repentaglio l'esistenza o il corretto funzionamento del nostro Paese. Se i cittadini vengono ostacolati o intimiditi nell'esercizio dei loro diritti popolari, nasce un senso di insicurezza e lo Stato rischia l'erosione del suo sistema democratico. Conformemente alla proposta presentata in occasione del rinvio al Consiglio federale, le minacce sono state, per quanto possibile, esplicitate – in sintonia con il tenore dell'O-SIC (cfr. art. 4 cpv. 1 O-SIC) – e sono stati menzionati a mo' di esempio alcuni beni giuridici determinanti in materia. È stata pertanto tracciata una chiara delimitazione rispetto ai casi di limitata importanza.

Nel quadro e secondo i principi dell'assistenza amministrativa, la disposizione obbliga in linea di principio tutte le autorità e unità amministrative della Confederazione e dei Cantoni a fornire informazioni. La cerchia di autorità interessate si fonda sull'articolo 13 capoverso 3 LMSI e sull'ordinanza del 7 novembre 2001³⁵ concernente l'estensione degli obblighi di informazione e del diritto di comunicazione di autorità, servizi e organizzazioni a tutela della sicurezza interna ed esterna. In questo modo, in caso di una minaccia concreta per la sicurezza della Svizzera che riguarda specificatamente il campo d'applicazione della disposizione (attività terroristiche, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo e trasferimento illegale di tecnologia), tutti i poteri pubblici (Confederazione, Cantoni e Comuni) devono contribuire a respingere la minaccia. Fanno ad esempio parte delle unità amministrative della Confederazione anche l'Ufficio di comunicazione in materia di riciclaggio di denaro (MROS) e le autorità competenti per i documenti d'identità. Per «unità amministrative dei Cantoni» si intendono anche quelle dei Comuni, compresi nella nozione di «Cantone». Le organizzazioni che esercitano funzioni pubbliche sono anch'esse tenute a fornire informazioni. Secondo l'articolo 2 capoverso 4 della legge federale del 21 marzo 1997³⁶ sull'organizzazione del Governo e dell'Amministrazione (LOGA), si tratta di organizzazioni di diritto pubblico o privato alle quali sono attribuiti compiti amministrativi e che non fanno parte dell'Amministrazione federale. Allestire direttamente nella LMSI un elenco delle organizzazioni interessate non è possibile per motivi di ordine pratico. Inoltre, un simile elenco a livello di legge risulterebbe troppo restrittivo perché non consentirebbe di tener conto tempestivamente di circostanze in rapida evoluzione. È pertanto opportuno rinunciare a elencare nel testo di legge le organizzazioni soggette all'obbligo d'informazione, delegandone la designazione al Consiglio federale (cfr. cpv. 3).

L'espressione «in casi specifici» evidenzia che le autorità vincolate dall'obbligo d'informazione devono informare costantemente il SIC o le autorità cantonali di sicurezza che agiscono su suo mandato soltanto riguardo a determinati casi concreti e soltanto su specifica richiesta. La cerchia piuttosto ampia di autorità interessate è giustificata alla luce dell'obbligo d'informazione limitato a casi specifici e a minacce concrete.

Le informazioni raccolte presso le autorità e le organizzazioni vanno indirizzate al SIC, che ne è il destinatario. Le autorità cui i Cantoni hanno affidato compiti in materia di sicurezza possono operare su mandato della Confederazione e richiedere le informazioni direttamente alle autorità e alle organizzazioni vincolate dall'obbligo d'informazione, per poi metterle a disposizione del SIC. Tale procedura è conforme al sistema previsto dalla legge (cfr. art. 7 cpv. 1, art. 13 cpv. 1, art. 14 cpv. 1 LMSI). Eventuali divergenze d'opinione in merito all'obbligo d'informazione sono considerate controversie che contrappongono l'autorità o l'organizzazione che rifiuta di comunicare l'informazione al SIC, e non all'autorità cantonale che, su mandato del SIC, ha richiesto l'informazione contestata.

In occasione delle missioni all'estero, va garantita in particolar modo la sicurezza dei periti appartenenti al Pool svizzero di esperti per la promozione civile della pace e dei collaboratori messi a disposizione di organizzazioni umanitarie o che promuovono i diritti dell'uomo. Vanno inoltre debitamente osservati eventuali clausole di

³⁵ RS 120.1

³⁶ RS 172.010

riservatezza, codici di condotta particolari o procedure operative standard (standard operating procedures, SOP). Sono determinanti le circostanze specifiche del caso.

Cpv. 2

L'articolo 13a disciplina la sospensione del segreto d'ufficio. Al riguardo le assicurazioni sociali e le autorità fiscali hanno fatto valere che nei rispettivi ambiti non sarebbero sospesi semplici segreti d'ufficio, bensì segreti d'ufficio qualificati e che sarebbe pertanto necessaria una norma specifica.

Nel settore delle assicurazioni sociali la comunicazione dei dati è disciplinata dettagliatamente nelle pertinenti leggi speciali e costituisce un ordinamento esaustivo a sé stante. Di conseguenza, nelle pertinenti leggi speciali il segreto d'ufficio nei confronti delle autorità di sicurezza della Confederazione e dei Cantoni è sospeso se sono adempiute le condizioni dell'articolo 13a. Pertinenti leggi speciali contengono già regolamentazioni analoghe applicabili alle autorità d'assistenza sociale, ai tribunali civili e penali, alle autorità istruttorie penali, agli uffici d'esecuzione e alle autorità fiscali.

La situazione in ambito fiscale è meno omogenea. Anche se alcune disposizioni contengono prescrizioni sull'obbligo di mantenere il segreto e sull'obbligo di discrezione, per la comunicazione dei dati non esiste un sistema paragonabile a quello in vigore per le assicurazioni sociali. Non esiste nemmeno una definizione esplicita di segreto fiscale (se ne trovano alcune definizioni nella letteratura specializzata, ad esempio: «Steuergeheimnis ist jede einer mit steuerlichen Aufgaben betrauten Person in Ausübung ihrer hoheitlichen Tätigkeit anvertraute oder ihr sonst wie zur Kenntnis gelangte persönliche Tatsache eines Steuerpflichtigen, die Steuerakten sowie die Verhandlungen innerhalb der Steuerbehörden³⁷»). Per contro, oltre al segreto d'ufficio, il segreto fiscale protegge anche interessi privati (protezione della personalità). Tutto sommato è quindi giustificato disciplinare il segreto fiscale in una regolamentazione specifica. Innanzitutto viene sancito il principio che obbliga anche le autorità fiscali a fornire informazioni. Esse devono comunicare le informazioni all'autorità federale o cantonale competente a seconda del genere di imposta. In caso di parere favorevole del SIC e dell'autorità competente, è consentito trasmettere le informazioni senza ulteriori formalità. In caso di dissenso si applica la procedura prevista all'articolo 13b (Controversie in merito all'obbligo d'informazione), il che significa che il Consiglio federale decide in via definitiva sulla comunicazione di informazioni concernenti le imposte federali e il Tribunale amministrativo federale su quelle riguardanti le imposte cantonali e comunali. Questa procedura favorisce anche un'applicazione uniforme del diritto di comunicazione ai sensi dell'articolo 13a capoverso 5 del disegno di legge.

Cpv. 3

Gli organi di sicurezza non decidono autonomamente sull'obbligo d'informazione cui è sottoposta un'organizzazione. Il Consiglio federale deve quindi sancire mediante ordinanza l'elenco esaustivo delle organizzazioni soggette a tale obbligo.

³⁷ Weber, M., Berufsgeheimnis im Steuerrecht und Steuergeheimnis, Zurigo 1982, pag. 139.

Cpv. 4

Il capoverso 4 disciplina la comunicazione dei dati alle autorità di perseguimento penale. Conformemente alla perizia Biaggini (cfr. n. 2.1.1), si è tenuto conto del fatto che si tratta della comunicazione di dati personali:

- rilevati da autorità non facenti parte del settore della «sicurezza», per scopi di tutt'altro genere, e
- di cui il SIC ha potuto venire a conoscenza soltanto a condizioni qualificate (art. 13a).

Di questo fatto si è tenuto conto stabilendo che la comunicazione di dati alle autorità di perseguimento penale ha luogo unicamente nei casi in cui le informazioni consentono di far luce su gravi reati ai sensi dell'articolo 141 CPP (l'articolo 13a deve consentire accertamenti di intelligence mirati nei confronti di persone sospette, ma non condurre a [disdicevoli] «fishing expedition» a favore delle autorità di perseguimento penale).

Cpv. 5

I servizi menzionati nel capoverso 1, che comprendono anche i servizi menzionati al capoverso 3, sono altresì autorizzati a informare spontaneamente le autorità federali e cantonali che eseguono i compiti previsti dalla LMSI in merito a fatti che ritengono legati al terrorismo, allo spionaggio politico o militare, al commercio illecito di armi o materiale radioattivo oppure al trasferimento illegale di tecnologia. Si intende evitare che ai servizi menzionati nei capoversi 1 e 3 venga mossa l'accusa di violare il segreto d'ufficio. Non esiste invece alcun obbligo di comunicazione sistematico.

Interesse pubblico e proporzionalità

Il nuovo articolo 13a ribadisce nella legge il contenuto dell'attuale articolo 13 capoverso 3 LMSI, che conferisce al Consiglio federale la facoltà di estendere, per un periodo limitato, l'obbligo d'informazione anche ad autorità diverse da quelle indicate nell'articolo 13 capoverso 1 LMSI. Ci siamo avvalsi di tale facoltà emanando, dopo gli attentati terroristici di Al-Qaïda dell'11 settembre 2001, l'ordinanza concernente l'estensione degli obblighi di informazione e del diritto di comunicazione di autorità, servizi e organizzazioni a tutela della sicurezza interna ed esterna. L'ordinanza è stata prorogata tre volte e rimarrà in vigore fino al 31 dicembre 2011 (RU 2008 6269).

In virtù dell'articolo 13 capoverso 3 LMSI, su cui si basa la suddetta ordinanza, la validità dei relativi atti normativi del Consiglio federale deve essere limitata nel tempo. Un'ordinanza fondata su dette disposizioni non può pertanto essere prorogata oltre un certo limite. La limitazione temporale sancita dal legislatore è volta a rendere necessaria la trasposizione nel diritto ordinario di norme contenenti disposizioni che devono restare in vigore per un periodo più lungo. Occorre legiferare non appena si prospetta che le regolamentazioni ivi contenute sono indispensabili a lungo termine. Questa condizione è soddisfatta nel caso presente.

Dopo gli attentati terroristici compiuti a Madrid nel 2004, la minaccia del terrorismo islamista nei confronti dell'Europa ha assunto nuove dimensioni nel luglio 2005³⁸. Secondo la valutazione attuale, la Svizzera non è un obiettivo diretto e primario del terrorismo, ma il rischio generale di atti terroristici resta elevato e riguarda anche la

³⁸ Rapporto sulla sicurezza interna della Svizzera 2005, pag. 25.

Svizzera, alla stregua di altri Paesi. Il bacino del Mediterraneo e l'Europa continentale non fungono più soltanto da rifugio e da luogo di preparazione. Si deve invece presumere che le organizzazioni terroristiche siano pronte alla prima occasione a sferrare attacchi tesi a ledere gli interessi occidentali. La situazione si prospetta di lunga durata e al momento attuale non è possibile prevedere quando la minaccia rientrerà.

Nel dicembre del 2002 abbiamo incaricato il DFGP di valutare l'efficacia dell'ordinanza concernente l'estensione degli obblighi di informazione e del diritto di comunicazione di autorità, servizi e organizzazioni a tutela della sicurezza interna ed esterna e di presentarci un rapporto. È stata quindi svolta un'inchiesta in proposito presso i corpi di polizia cantonali e delle città di Zurigo e Berna, incentrata prevalentemente sul valore del contenuto delle comunicazioni (qualità) e meno sul loro numero (quantità).

In un primo tempo, si è pensato di procedere alla valutazione contrassegnando, nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS), le comunicazioni fornite in seguito all'ampliamento delle competenze. Questo progetto si è tuttavia rivelato troppo oneroso ed è stato necessario abbandonarlo. È emerso inoltre che contrassegnare le comunicazioni a livello di Confederazione non consentiva di rilevare o consentiva di rilevare soltanto in maniera insufficiente l'impatto a livello cantonale dell'ordinanza concernente l'estensione degli obblighi di informazione e del diritto di comunicazione di autorità, servizi e organizzazioni a tutela della sicurezza interna ed esterna – segnatamente nei casi in cui l'ampliamento delle competenze ha comportato a livello cantonale una corrispondente diminuzione degli oneri per la verifica delle informazioni senza che il SAP ricevesse specifiche comunicazioni al riguardo.

È stato inoltre constatato che l'ordinanza era sufficientemente nota agli organi di polizia, ma non alle persone autorizzate o tenute a fornire informazioni. In occasione dell'ultima proroga, si è tenuto conto di tale circostanza diramando ai Cantoni una circolare ad ampia diffusione.

Nel complesso, il numero di comunicazioni è aumentato di poco, mentre il loro contenuto è nettamente migliorato.

Riassumendo, l'ordinanza ha avuto un impatto importante sul piano della politica interna ed esterna (a livello nazionale ha fornito indicazioni sulla nostra volontà di combattere il terrorismo, mentre all'estero è stato inviato un segnale sulla disponibilità della Svizzera ad assumersi, in seno alla comunità internazionale, le proprie responsabilità nella lotta al terrorismo). In altre parole, vi è un interesse pubblico preponderante a mantenere l'ordinanza, o meglio, a trasporla nel diritto permanente.

Sebbene il numero delle comunicazioni pervenute sia esiguo, la loro elevata qualità suffraga la proporzionalità della disposizione proposta.

Art. 13b (nuovo)

Controversie in merito all'obbligo d'informazione

L'articolo 13b si applica quando il SIC o un organo di sicurezza cantonale operante su suo mandato richiede un'informazione in virtù dell'articolo 13 o 13a, ma il servizio interpellato non è disposto a fornirla.

Cpv. 1

In caso di controversie in merito all'obbligo d'informazione, se le divergenze d'opinione sussistono tra unità amministrative dell'Amministrazione federale centrale (cfr. art. 7 dell'ordinanza del 25 novembre 1998³⁹ sull'organizzazione del Governo e dell'Amministrazione, OLOGA), esse sono risolte dall'autorità di vigilanza comune, ossia dal capo del Dipartimento che presenta l'istanza, oppure, per i casi concernenti più dipartimenti, dal Consiglio federale (cfr. art. 9 cpv. 3 della legge federale del 20 dicembre 1968⁴⁰ sulla procedura amministrativa, PA). Ad esempio, in caso di controversia in merito a un'informazione richiesta dal SIC all'Ufficio federale della migrazione, la decisione spetterebbe al Consiglio federale.

Cpv. 2

Conformemente all'articolo 36a della legge del 17 giugno 2005⁴¹ sul Tribunale amministrativo federale, «sempreché una legge federale lo preveda, il Tribunale amministrativo federale giudica le divergenze di opinione in materia di assistenza amministrativa e giudiziaria tra autorità federali e tra autorità della Confederazione e dei Cantoni». La decisione del Tribunale amministrativo federale è definitiva (art. 83 lett. v della legge del 17 giugno 2005⁴² sul Tribunale federale, LTF). Il capoverso 2 comprende pertanto un pertinente rimando alla norma succitata.

Art. 13c (nuovo)

Obbligo d'informazione dei trasportatori commerciali

Cpv. 1

Questo nuovo obbligo d'informazione è analogo a quello sancito all'articolo 13a ed è fondato sui medesimi presupposti; si rimanda pertanto al riguardo alle considerazioni sull'articolo 13a capoverso 1. Per ragioni di proporzionalità la cerchia degli interessati è stata circoscritta ai trasportatori commerciali. La disposizione si applica, ad esempio, alle imprese di taxi, alle compagnie aeree, alle società ferroviarie e di autonoleggio o ai trasportatori su strada.

Spesso è possibile ricostruire le attività delle persone che sono state riconosciute pericolose (per es. spie, persone sospettate di terrorismo, ingegneri attivi nel settore della proliferazione), soltanto raccogliendo informazioni sui loro spostamenti (per es. documenti sul noleggio di automobili ecc.). Questo vale anche per i sospetti in materia di trasporti imminenti o già avvenuti di merci nel settore della proliferazione o il trasferimento di tecnologia corrispondente.

I trasportatori sono tenuti a fornire i dati rilevati ai fini della propria attività che sono già in loro possesso. L'articolo 13c non li obbliga quindi a raccogliere o conservare dati supplementari. Dal momento che la comunicazione di informazioni già raccolte non cagiona ai trasportatori oneri supplementari di rilievo, non è prevista alcuna indennità da parte degli organi di sicurezza; le informazioni vanno comunicate gratuitamente.

L'espressione «in casi specifici» evidenzia che l'obbligo d'informazione sussiste soltanto quando il SIC o un organo di sicurezza cantonale che opera su suo mandato

³⁹ RS 172.010.1

⁴⁰ RS 172.021

⁴¹ RS 173.32

⁴² RS 173.110

si rivolgono al trasportatore in un caso specifico concreto richiedendo un'informazione.

Cpv. 2

Se, in caso di controversie in merito all'obbligo d'informazione dei trasportatori commerciali, non intende rinunciare a un'informazione, il SIC deve emanare una relativa decisione comprendente segnatamente indicazioni riguardo alle restrittive condizioni per ordinare misure in materia. La decisione del SIC può essere impugnata dal trasportatore commerciale in prima istanza dinanzi al Tribunale amministrativo federale, contro la cui decisione può essere presentato ricorso dinanzi al Tribunale federale. Sussiste pertanto un'esauritiva protezione giuridica in materia.

Cpv. 3

Si rimanda alle considerazioni sull'articolo 13a capovero 4, di tenore identico, le quali sono applicabili in questa sede per analogia.

Interesse pubblico e proporzionalità

Secondo l'articolo 14 capovero 2 lettera b LMSI, gli organi di sicurezza possono richiedere informazioni per adempiere i propri compiti. Talvolta i privati interpellati (persone fisiche o giuridiche) si rifiutano di fornire informazioni, appellandosi alla legislazione in materia di protezione dei dati. Affinché ciò non accada nel settore dei trasporti commerciali, che riveste grande importanza per gli organi di sicurezza, s'intende obbligare i trasportatori a fornire le informazioni richieste. Tale obbligo d'informazione costituisce un'ingerenza sia nella sfera professionale del trasportatore sia nella sfera privata della persona posta sotto osservazione. Occorre pertanto appurare se l'ingerenza è proporzionata agli interessi pubblici in gioco. Va sottolineato che le informazioni dei trasportatori commerciali possono essere determinanti per valutare una potenziale minaccia. Non di rado sono proprio gli spostamenti di determinate persone (per es. il personale di imprese fittizie straniere) o merci (per es. il trasporto di materiale di proliferazione) oppure le informazioni sulla frequenza di tali spostamenti a permettere di verificare l'esattezza di determinati indizi concreti. L'accesso a questo tipo di informazioni costituisce uno strumento adeguato e necessario per consentire al SIC di adempiere i propri compiti prevenendo con successo le minacce.

La proporzionalità della misura dipende dalle circostanze concrete nel singolo caso specifico. Come già esposto più sopra, il presupposto essenziale per obbligare i trasportatori commerciali a fornire informazioni è che queste siano necessarie, nel singolo caso specifico, per scoprire e sopprimere una minaccia concreta per la sicurezza interna o esterna della Svizzera inerente a uno dei ristretti settori di compiti della LMSI, in precedenza descritti, e concernente un bene giuridico importante quale l'integrità fisica o la vita. In questo contesto strettamente circoscritto, i trasportatori sono tenuti a fornire unicamente informazioni a loro già note. Essi non sono obbligati ad acquisire attivamente informazioni né a conservare in maniera particolare determinati dati. Pertanto l'ingerenza nella loro sfera professionale non può essere considerata sproporzionata. Inoltre, le informazioni non riguardano alcun settore protetto dal segreto professionale o da un particolare rapporto di fiducia. Di solito si tratta piuttosto di informazioni su fatti che si verificano in luoghi liberamente accessibili quali strade o treni. In questo contesto non è pertanto data un'ingerenza sproporzionata nella sfera privata. Ciononostante, nella prassi dovrà aver luogo in ogni singolo caso concreto, come in occasione di altre ingerenze in diritti fonamen-

tali, un'accurata ed esaustiva ponderazione dell'interesse pubblico e dell'interesse privato (segnatamente la protezione della sfera privata), entrambi da tutelare. In conclusione, i trasportatori commerciali sono tenuti a fornire soltanto informazioni utili per scoprire e sopprimere minacce di rilievo.

Art. 13d (nuovo) Segreto professionale

L'esercizio di talune professioni può svolgersi normalmente e correttamente solo ispirando nel pubblico, mediante una seria garanzia di discrezione, l'indispensabile fiducia nel professionista (DTF 84 IV 108). Tale condizione è garantita sia dalla punibilità delle violazioni del segreto professionale (per es. art. 321 CP⁴³, art. 35 LPD), sia dal diritto di rifiutare di comunicare informazioni soggette al segreto professionale, anche se a richiederle sono le autorità. Questo diritto è quindi stato istituito a tutela di un particolare rapporto di fiducia, di cui occorre tener conto non soltanto nei procedimenti giudiziari, ma ogniqualvolta un privato sia tenuto a fornire informazioni alle autorità.

La presente revisione non intacca il segreto professionale. Considerata la sua importanza questo principio è sancito espressamente nell'articolo 13d. Ad esempio, nell'esercizio delle proprie competenze ufficiali, un medico cantonale è di conseguenza obbligato a fornire, conformemente all'articolo 13a, informazioni generiche, ma non informazioni su quanto rientra nel segreto medico.

Art. 13e (nuovo) Messa al sicuro, sequestro e confisca di materiale di propaganda

A causa della modifica strutturale della legge, l'attuale articolo 13a LMSI deve essere spostato all'interno dell'articolo 13. Esso diventa il nuovo articolo 13e. Il suo tenore è identico alla versione vigente e non comporta alcuna modifica materiale.

Del rimanente, poiché rientra nell'ambito della coercizione di polizia, anche per questa norma dovrà essere valutata a suo tempo l'opportunità di un eventuale trasferimento nella LCPol.

Art. 14a (nuovo) Informatori

Per poter adempiere i propri compiti, gli organi di sicurezza necessitano della cooperazione e delle comunicazioni di persone che hanno accesso a informazioni rilevanti. La LMSI vigente ammette implicitamente l'impiego di informatori (cfr. in particolare l'art. 14 cpv. 2 lett. b e d che disciplina la richiesta di informazioni e la ricezione di comunicazioni; per il settore concernente l'estero cfr. art. 16 cpv. 1 lett. a O-SIC), ma non contiene disposizioni specifiche in merito al loro impiego, ai loro diritti e obblighi o alle prestazioni da parte dello Stato. Tale situazione giuridica imprecisa va chiarita.

Cpv. 1

La disposizione autorizza esplicitamente il SIC a servirsi di informatori nel quadro del campo di applicazione della LMSI. Gli informatori trasmettono al SIC, saltuariamente o sistematicamente, informazioni a essi già note o da essi acquisite su base volontaria.

⁴³ RS 311.0

Gli informatori sono persone che collaborano su base volontaria con gli organi di sicurezza senza che sia in tal modo stipulato un contratto di lavoro ai sensi dell'articolo 319 del Codice delle obbligazioni⁴⁴ (CO) o della legislazione sul personale federale. La possibilità di ricompensare tali persone o di rimborsare loro le spese (cfr. cpv. 2), non giustifica in alcun modo la qualifica di tale rapporto come un contratto di lavoro. Un contratto di lavoro ai sensi dell'articolo 319 CO presuppone la presenza di altri elementi costitutivi, quali un rapporto di subordinazione formale che porrebbe l' informatore alle dipendenze del SIC ai sensi del diritto in materia di personale, a livello organizzativo e nel quadro di un orario di lavoro. Una tale subordinazione non è assolutamente data.

Cpv. 2

È previsto il rimborso spese per evitare perdite finanziarie a chi, più o meno regolarmente, fornisce informazioni al SIC. Tali indennità non costituiscono redditi o salari imponibili ai sensi della legislazione sull'AVS. Sono considerate spese ai sensi di questo capoverso quelle cagionate all' informatore nello svolgimento della sua attività, segnatamente le spese di viaggio e di telecomunicazione.

È inoltre possibile ricompensare gli informatori in singoli casi per le informazioni particolarmente utili. Nella prassi corrente, le ricompense si situano a livelli alquanto modesti, ammontano al massimo ad alcune migliaia di franchi l'anno e sono ben lungi dal raggiungere il minimo vitale. Per evitare una controproducente corsa al successo, l'incentivo finanziario non deve evidentemente determinare la decisione di fungere da informatore. Sono concesse ricompense modeste a chi è in grado di fornire ragguagli che agevolano in maniera considerevole l'ulteriore ricerca di informazioni o la valutazione della situazione di minaccia. Già attualmente il SIC informa a un ritmo annuale la DelCG in merito a corrispondenti attività e riguardo ai relativi costi e risultati.

Cpv. 3

Il rapporto tra gli organi di sicurezza e gli informatori poggia sulla reciproca fiducia e sulla confidenzialità. Se la persona oggetto della ricerca di informazioni giungesse a conoscenza dell'attività che l' informatore svolge per conto degli organi di sicurezza nei settori d'intervento rilevanti per la protezione dello Stato, l' informatore potrebbe correre gravi rischi. Gli informatori non possono quindi essere registrati negli incarti concernenti il personale del servizio né essere annunciati alle assicurazioni sociali (nemmeno per indicare l'esonero dall'obbligo d'assicurazione). Per contro, la legalità e l'opportunità dell'impiego di informatori sono già attualmente verificate dalla vigilanza sulle attività informative interna al DDPS e dalla Delegazione delle Commissioni della gestione, in qualità di organi di controllo designati dalla LMSI.

Il nuovo capoverso 3 specifica che eventuali indennità non sono soggette a alcun obbligo fiscale, se e finché la protezione della fonte e l'ulteriore ricerca di informazioni lo esigono. Vista l'esiguità degli importi elargiti, tale disposizione non arreca danni concreti né ai diretti interessati né alla comunità: gli oneri amministrativi per registrare gli importi e riscuotere i contributi sarebbero nettamente superiori ai benefici.

Per il settore concernente l'estero valgono considerazioni analoghe. Al riguardo cfr. il nuovo articolo 7 capoverso 2 LSIC (i concetti di «informatori» e «fonti» menzionati all'art. 16 cpv. 1 lett. a O-SIC per il settore concernente l'estero sono compresi nel concetto di «informatori»: il tenore dell'ordinanza sarà adeguato di conseguenza).

Art. 14b (nuovo)

Protezione degli informatori

Questa disposizione è finalizzata a proteggere chi si espone a rischi per raccogliere informazioni utili agli scopi della LMSI. Vi sono in particolare due tipologie di informatori da proteggere: coloro che devono temere rappresaglie perché cooperano con gli organi di sicurezza di propria iniziativa e coloro che sono disposti a cooperare purché venga loro garantita un'adeguata protezione. Tale garanzia consente di acquisire le informazioni necessarie e di evitare (come già accaduto più volte in passato) che informatori importanti disposti a cooperare debbano essere «affidati» a servizi informazioni stranieri in grado di assicurarne la protezione perché la Svizzera non ne ha la possibilità.

Chi coopera con gli organi di sicurezza di propria iniziativa in certi casi si espone a rischi notevoli e deve temere ritorsioni, sia da parte delle cerchie che frequenta (per es. se fa parte di gruppi violenti), sia da parte di Stati esteri (per es. se in apparenza si è messo a disposizione dei servizi informazioni di uno Stato estero, ma in realtà lavora per le autorità svizzere). Il pericolo a cui si espongono tali persone è paragonabile a quello corso dagli agenti infiltrati, che godono di ampia protezione. Di conseguenza appare giustificato creare i presupposti per garantire una protezione efficace anche agli informatori.

La normativa per la protezione degli informatori va chiaramente distinta da quella per la protezione dei pentiti, che deriva dal diritto penale anglo-americano. In linea di massima i pentiti hanno presumibilmente preso parte al reato in questione, ma sono disposti a testimoniare contro i coimputati, ottenendo in cambio l'impunità, una riduzione della pena o altri benefici processuali. L'esenzione da una pena sul modello della normativa sui pentiti sopra descritta non rientra nelle presenti considerazioni. La prevenzione non è incentrata sul chiarimento di precisi reati, che può essere agevolato grazie a testimonianze particolari, bensì sulla ricerca di informazioni rilevanti ai fini della sicurezza, con lo scopo di individuare e di sopprimere le minacce e di prevenire, per quanto possibile, futuri reati.

La misura è destinata a essere impiegata soltanto in rari casi eccezionali, in presenza di una fonte potenziale di informazioni di grande valore. È ad esempio ipotizzabile proteggere persone in grado di fornire informazioni importanti per prevenire gravi rischi a livello di politica di sicurezza, quali notizie sulla progettazione e la programmazione di attacchi terroristici, su concrete attività di spionaggio rivolte contro la Svizzera o su organizzazioni che si servono della Svizzera per procurarsi armi di distruzione di massa. Al fine di minimizzare i rischi inerenti a una collaborazione, dopo un primo contatto sono previsti diversi colloqui esplorativi, dopodiché, a condizione che i pertinenti presupposti siano adempiuti, è convenuto un accordo di protezione comprendente obblighi e diritti reciproci. La collaborazione vera e propria ha inizio soltanto dopo questa prima fase. La misura non comporta alcuna protezione contro il perseguimento penale in Svizzera o all'estero.

Cpv. 1

Questo capoverso istituisce le basi giuridiche per la protezione degli informatori. Le misure necessarie a tutela della vita e dell'integrità fisica degli informatori adottate dal SIC comprendono la protezione della persona e gli spostamenti della dimora. La protezione della persona implica misure quali l'impiego di guardie del corpo, di veicoli o impianti protetti oppure provvedimenti edili. Lo spostamento della dimora può consistere nel trasferimento, con il consenso della persona interessata, in un altro luogo in Svizzera o all'estero. Per provvedimenti adeguati a tutela di una persona trasferita all'estero si intende il suo trasferimento in un luogo più sicuro all'estero qualora le circostanze non permettano di offrirle una protezione adeguata in Svizzera. Al fine di compensare le spese derivanti da tale provvedimento, come pure un'eventuale perdita di guadagno, è previsto un sostegno finanziario limitato nel tempo.

Il SIC può eseguire direttamente le misure di protezione o finanziarle. Nella prassi, risulterà necessario e attuabile soltanto un numero limitato di simili misure. Considerate le dimensioni della Svizzera, per determinate minacce il Paese non è in grado di adottare misure di protezione esaustive; in tali casi potrebbe risultare necessario il ricorso all'assistenza di autorità estere, con conseguenti costi. Può inoltre essere considerata la possibilità di concedere una protezione parziale, ad esempio garantendo il soggiorno in Svizzera o in uno Stato amico. Il secondo periodo del capoverso 1 indica esplicitamente tale possibilità.

Cpv. 2

Dalle medesime considerazioni consegue che il SIC deve poter adottare misure per la protezione di persone vicine a un informatore se da tali provvedimenti dipende la sicurezza di quest'ultime. Il carattere potestativo della disposizione garantisce il potere discrezionale necessario per attuare le misure adeguate al caso specifico.

Cpv. 3

La disposizione prevede la possibilità di proteggere l'informatore fornendogli un'identità fittizia. Al contrario delle misure previste ai capoversi 1 e 2, in questo caso la misura è adottata soltanto dopo l'interruzione dei contatti tra il SIC e l'informatore e soltanto qualora la fonte non sia più impiegata dal Servizio. Se la persona in questione è in grave pericolo per aver collaborato con il SIC, quest'ultimo può proteggerla fornendole un'identità fittizia permanente. La persona è in seguito autorizzata a utilizzare tale identità seguendo le istruzioni del SIC. La creazione di un'identità fittizia presuppone l'autorizzazione del capo del Dipartimento (cfr. quanto illustrato qui di seguito).

La ricerca di informazioni con il ricorso a un'identità fittizia (cfr. al riguardo il commento all'art. 14c) va distinta dalla presente disposizione.

Conformemente all'articolo 27 capoverso 1^{bis} del presente disegno di legge, il Dipartimento è tenuto a informare regolarmente il Consiglio federale e gli organi di controllo del Parlamento sul numero di identità fittizie create, sullo scopo per il quale sono state fornite e sul loro concreto utilizzo. Tale disposizione si applica anche alle identità fittizie di cui al capoverso 3.

Cpv. 4

Questo capoverso stabilisce che le misure di protezione sono abitualmente limitate nel tempo. Tuttavia, la legge non può indicare in via definitiva una durata determina-

ta, dal momento che vanno prese in considerazione le esigenze di ogni caso specifico. In via del tutto eccezionale, il capo del Dipartimento può rinunciare a fissare un limite temporale se una persona è manifestamente esposta a un rischio grave e permanente; in un caso del genere, le misure di protezione possono essere mantenute a tempo indeterminato. Per contro, il Dipartimento è tenuto a verificare regolarmente se i presupposti sono ancora adempiuti e, se ciò non dovesse più essere il caso, a sospendere le misure di protezione.

Art. 14c (nuovo) Identità fittizie

Per adempiere i propri compiti e proteggere i propri collaboratori, i servizi informazioni e le autorità della polizia preventiva devono potersi servire di identità fittizie quando cercano informazioni in determinati ambienti. Tali identità fittizie sono di regola create per lunghi periodi e raramente possono essere attribuite soltanto nel momento in cui si avviano le ricerche su un determinato caso. Anzi, per perfezionare un'identità fittizia sono spesso necessari, indipendentemente dalla complessità dell'identità fittizia richiesta, diversi anni di preparativi.

Dal 1998 il Servizio informazioni strategico SIS aveva la facoltà, in virtù dell'articolo 99 della legge militare, di fornire identità fittizie ai membri dei suoi organi di ricerca (cfr. il Rapporto annuale 2002/2003 delle Commissioni della gestione e della Delegazione delle Commissioni della gestione delle Camere federali del 23 gennaio 2004; FF 2004 1435). Il controllo in merito era affidato al capo del DDPS e alla Giunta del Consiglio federale in materia di sicurezza. In seguito alla fusione del SAP e del SIS nella nuova unità organizzativa SIC, l'articolo 16 capoverso 1 lettera e O-SIC prevede esplicitamente l'impiego di «documenti fittizi e identità fittizie» in relazione con la ricerca di informazioni all'estero.

La regolamentazione della ricerca di informazioni in Svizzera è ispirata a quella della ricerca di informazioni all'estero, che ha dato buone prove. Essa prevede che in singoli casi specifici il capo del DDPS può autorizzare il SIC a fornire un'identità fittizia a determinate persone. L'identità fittizia può essere impiegata unicamente per due scopi, ovvero ai fini della sicurezza e della ricerca di informazioni.

Va rilevato che, in virtù dell'articolo 27 capoverso 1^{bis} del presente disegno di legge, il conferimento e l'uso di identità fittizie sono soggetti a un controllo politico mirato e intenso, nel cui ambito il Dipartimento deve informare, a scadenza annuale, il Consiglio federale e la Delegazione delle Commissioni della gestione.

Cpv. 1

Il presente capoverso pone le basi dell'impiego di identità fittizie per raccogliere informazioni e garantire la sicurezza degli informatori. Il capoverso 1 elenca in modo esaustivo le persone a cui può essere fornita un'identità fittizia:

- *lettere a e b*: dopo il raggruppamento del SAP e del SIS e la creazione del nuovo SIC gli organi di sicurezza ai sensi della LMSI continuano, seppur in misura minore, a far parte dell'apparato di polizia svizzero e possono ancora contare su di esso, almeno parzialmente, nell'ambito della loro ricerca di informazioni. Tuttavia, per poter instaurare contatti con determinate realtà, segnatamente nell'ambiente terroristico e spionistico, è talvolta necessario agire sotto copertura, segnatamente per proteggere i collaboratori degli organi di sicurezza e i loro familiari;

- *lettera c*: anche gli informatori devono potersi servire di identità fittizie se la ricerca di informazioni lo richiede. Si tratta in particolare di persone che solo con questo sistema possono infiltrarsi in determinati ambienti rilevanti ai fini della protezione dello Stato e che necessitano di un'identità fittizia per cautelarsi. Nella ricerca di informazioni, gli informatori sono vincolati alle direttive degli ufficiali di collegamento degli organi di sicurezza, ma non sottostanno al controllo diretto della relativa autorità di vigilanza. In questi casi, l'impiego di identità fittizie è pertanto limitato nello spazio e nel tempo e possibile soltanto per determinate operazioni.

Creare un'identità fittizia comprende il diritto di servirsene per concludere negozi giuridici e, in particolare, per costituire strutture fittizie. Le persone provviste di un'identità fittizia hanno piena personalità giuridica e possono stipulare contratti (per es. affittare locali e veicoli o collegamenti di telecomunicazione oppure costituire strutture fittizie quali ditte o altre persone giuridiche).

Cpv. 2

In linea di principio un'identità fittizia dovrà poter essere mantenuta per il tempo necessario allo svolgimento dell'operazione. Va invece revocata non appena sono stati raggiunti gli obiettivi perseguiti con la sua creazione. Per garantire la necessaria flessibilità e migliorare il controllo sui rischi inerenti all'impiego di identità fittizie, le autorizzazioni sono limitate a dodici mesi al massimo (informatori) o cinque anni al massimo (collaboratori), con, di volta in volta, possibilità di proroga di rispettivamente sei mesi o tre anni.

Tanto le autorizzazioni corredate della limitazione temporale di base quanto ogni proroga sono da intendersi come concesse soltanto finché necessario, oltre che al massimo sino allo scadere del termine.

Cpv. 3 e 4

Per la creazione di un'identità fittizia è necessaria l'autorizzazione del capo del DDPS, previa pertinente richiesta del direttore del SIC. Il capo del DDPS può approvare la richiesta, approvarla con l'apposizione di limitazioni o condizioni supplementari (ciò che corrisponde a un'approvazione parziale), rifiutarla oppure rinviarla al SIC in vista del completamento.

Come menzionato poc'anzi, un'autorizzazione deve essere preceduta da una corrispondente richiesta del direttore del SIC. Quest'ultimo verifica per ogni singolo caso se sono adempiuti i presupposti per l'impiego di un'identità fittizia. Ai fini di tale verifica, che deve essere motivata agli atti, si applicano i seguenti quattro criteri:

- *lettera a*: la ricerca di informazioni deve essere in relazione con una minaccia concreta per la sicurezza interna ed esterna della Svizzera;
- *lettera b*: la ricerca di informazioni deve concernere uno degli ambiti di minaccia indicati (attività terroristiche, spionaggio, estremismo violento, proliferazione);
- *lettera c*: il principio di proporzionalità è applicato ponendo la condizione che il ricorso a mezzi abituali deve essere risultato inefficace o che l'impiego di un'identità fittizia deve essere giustificato dalla gravità e dalla natura della minaccia;

- *lettera d*: infine, l'impiego di un'identità fittizia non deve essere in alcun modo sproporzionato alle informazioni da acquisire.

Poiché i quattro criteri legali sopraesposti sono stati definiti in maniera talmente restrittiva da non concedere alcun margine di manovra, è possibile rinunciare all'esame della richiesta da parte di un tribunale (esame che, per quanto concerne gli elementi essenziali, dovrebbe comunque essere fondato sulle indicazioni del SIC ed essere eseguito applicando i medesimi criteri).

Se i criteri sopraesposti sono adempiuti (e soltanto a questa condizione), il direttore del SIC può presentare al capo del DDPS una richiesta per la creazione di un'identità fittizia.

Cpv. 5

La procedura per una proroga è identica a quella per la decisione; deve segnatamente essere verificato, con modalità motivate agli atti, che tutti i presupposti siano adempiuti.

Cpv. 6

Il capoverso 6 disciplina l'origine dei documenti d'identità: le autorità competenti in materia sono tenute a collaborare con il SIC.

Cpv. 7

La creazione di un'identità fittizia e l'allestimento di relativi documenti comprendono anche misure atte a prevenire uno smascheramento (ad opera di terzi oppure occasionato in altro modo). Nel peggiore dei casi, le corrispondenti misure sono in grado di assicurare il tempo necessario per una «fuga» mirata.

Interesse pubblico e proporzionalità

L'impiego di un'identità fittizia può costituire un'ingerenza nei diritti fondamentali delle persone oggetto della ricerca o di terzi non implicati. Mediante l'articolo 14c è pertanto creata una pertinente base legale, indipendentemente dall'entità dell'ingerenza. L'interesse pubblico determinante è manifesto. La verifica della legalità e della proporzionalità da parte del direttore del SIC è sempre immediatamente preliminare o concomitante a una valutazione o autorizzazione politica da parte del capo del DDPS. Quest'ultimo può far dipendere la sua autorizzazione (anche in assenza di un'esplicita base legale) da condizioni, presupposti o altre misure. In considerazione delle innumerevoli possibilità di impiego e degli altrettanto innumerevoli possibili punti di contatto tra terzi e un'identità fittizia, la legge non può comprendere una regolamentazione definitiva; la verifica deve poter essere di volta in volta orientata a criteri aperti. La presenza di controlli incisivi ed efficaci assume di conseguenza una ancor maggiore importanza. I controlli sono garantiti con l'obbligo di presentare dettagliati rapporti, sancito all'articolo 27 capoverso 1^{bis} del presente disegno di legge, in virtù del quale il DDPS è tenuto a informare di propria iniziativa e esaustivamente sia il Consiglio federale sia l'autorità di vigilanza parlamentare, ossia la Delegazione delle Commissioni della gestione.

Art. 15 cpv. 6

La disposizione si fonda sulla regolamentazione definita per la precedente Polizia federale, a cui erano affidati compiti di polizia giudiziaria e di prevenzione. La separazione di questi due compiti e le conseguenti implicazioni organizzative hanno

reso obsoleta la disposizione. Secondo il diritto e la concezione attuali, la trasmissione delle informazioni dal settore della repressione al settore della prevenzione ne muta lo scopo; i dati divengono di natura preventiva e vanno pertanto trattati secondo il diritto applicabile alla prevenzione. L'abrogazione di questa disposizione non significa che lo scambio di informazioni non possa più aver luogo.

Art. 17 cpv. 1, 1^{bis} (nuovo), 1^{ter}(nuovo), cpv. 3 lett. e (nuova) e 5

Cpv. 1

Dagli accertamenti di diritto costituzionale del professor Biaggini (cfr. n. 2.1.1) è risultato che la comunicazione agli organi di perseguimento penale di informazioni raccolte nel quadro di attività di polizia preventiva corrisponde in linea di principio a un interesse pubblico. Tuttavia, non vi sarebbero al riguardo linee direttrici legali sufficientemente chiare, soprattutto per quanto concerne le condizioni per la possibilità o l'obbligo di una comunicazione senza indugio alle autorità penali.

In considerazione di tale critica, l'attuale capoverso 1 è stato suddiviso e rielaborato; la nuova struttura comprende ora i capoversi 1, 1^{bis} e 1^{ter}. Il nuovo capoverso 1 è identico al primo periodo dell'attuale capoverso 1; il capoverso 1^{bis} disciplina le condizioni alle quali una comunicazione dei dati è obbligatoria e il capoverso 1^{ter} disciplina le condizioni alle quali una comunicazione dei dati può essere procrastinata, ovvero provvisoriamente sospesa.

Cpv. 1^{bis} (nuovo)

È qui precisato che la comunicazione di dati deve aver luogo senza indugio se:

- le informazioni ottenute possono essere utili per il perseguimento penale o la lotta contro la criminalità organizzata;
- sussiste un sospetto di reato sufficiente; e
- per perseguire il reato può essere disposta la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (ciò che presuppone una relativa gravità dei delitti in questione).

Cpv. 1^{ter} (nuovo)

Per quanto concerne tutte le ulteriori informazioni non sottostanti al capoverso 1^{bis}, la comunicazione dei dati può essere rinviata. Un rinvio della comunicazione è ammesso se e nella misura in cui interessi pubblici preponderanti (da motivare agli atti) in materia di salvaguardia della sicurezza interna ed esterna della Svizzera o in materia di protezione di interessi privati prevalgono sull'interesse a un perseguimento penale. Tale criterio, fondato sul principio di proporzionalità, è volto a consentire alle autorità di prevenzione di proseguire, in casi di minore gravità, i loro accertamenti sino al chiarimento della situazione, senza che sorgano sovrapposizioni con le autorità penali. Tuttavia, se sin dall'inizio non sono dati i presupposti per un rinvio della comunicazione dei dati o se tali presupposti vengono meno durante la procedura (per es. perché ciò che inizialmente era soltanto un vago sospetto assume vieppiù i connotati di una certezza), le relative informazioni devono essere comunicate senza indugio alle autorità penali.

Cpv. 3 lett. e (nuova)

Il cosiddetto clearing è un compito che il servizio informazioni (ora SIC) esegue da tempo nelle relazioni con l'estero. Su richiesta di un servizio straniero, il SIC esegue controlli di sicurezza aventi per oggetto cittadini svizzeri o cittadini stranieri residenti in Svizzera, allo scopo di consentire a quest'ultimi di collaborare a progetti esteri classificati. Come richiesto da numerosi partecipanti alla procedura di consultazione, è stato stabilito espressamente che lo Stato richiedente deve garantire per scritto che la persona interessata ha acconsentito al clearing.

Da sempre, per eseguire il clearing il Servizio informazioni (ora SIC) si basa sull'articolo 17 capoverso 3 lettera c LMSI. In passato, tuttavia, tale base giuridica è stata messa in discussione da più parti. Pertanto s'intende ora istituire una base legale formale per il clearing. Ciò è necessario per garantire le possibilità di accesso a VOSTRA (casellario giudiziale informatizzato). Gli estratti del casellario giudiziale costituiscono un elemento di valutazione importante per il clearing. Senza di essi, il clearing effettuato dal SIC per conto di uno Stato estero risulterebbe di minor valore. Ne subirebbe le conseguenze la persona in questione, che, anche in caso di esito positivo del clearing, potrebbe non essere ritenuta abbastanza affidabile per poter cooperare a progetti segreti o confidenziali all'estero.

Cpv. 5

L'attuale capoverso 5 rimane in vigore; l'ampliamento con un ulteriore periodo è volto a chiarire la questione, sorta recentemente, se in caso di procedura di assistenza giudiziaria (cfr. per es. l'art. 27 della legge federale del 15 giugno 1934⁴⁵ sulla procedura penale, PP) la protezione della fonte informativa continua a prevalere in maniera immutata oppure assume i tratti di una protezione negoziabile dalle autorità penali.

Il mantenimento della protezione della fonte informativa riveste un'assoluta importanza per il SIC: le fonti umane sono tra i più importanti canali di acquisizione del Servizio e non sono né reclutabili né gestibili se i contatti non sono basati, sia verso l'interno sia verso l'esterno, sulla confidenzialità. A ciò si aggiunge l'obbligo del SIC di garantire in ogni caso la protezione delle fonti nell'ambito delle sue relazioni con l'estero. Se non è più in grado di garantire la necessaria confidenzialità, il SIC rischia di essere immediatamente e senza valide alternative escluso da buona parte dei canali di provenienza delle sue informazioni. Al fine di evitare una simile situazione, la preminenza della protezione delle fonti è stata sancita nella legge.

Art. 18

Dagli accertamenti di diritto costituzionale del professor Biaggini (cfr. n. 2.1.1) è risultato che il diritto «indiretto» di essere informati conformemente all'attuale articolo 18 LMSI può in linea di principio essere interpretato e applicato in modo conforme alla Costituzione federale e alla CEDU e che non sussiste pertanto alcuna urgente necessità d'intervento in materia di legislazione.

Per contro, nella mozione 08.3852 Leutenegger Oberholzer Susanne («Collezioni di dati della Confederazione. Diritto d'informazione») era stato chiesto al Consiglio federale di «garantire alle persone interessate un diritto d'accesso a tutte le collezioni di dati della Confederazione che contengono informazioni che le concernono,

⁴⁵ RS 312.0

conformemente agli articoli 8 e 9 della legge sulla protezione dei dati». Abbiamo proposto di accogliere la mozione, osteggiata dalla consigliera nazionale Jasmin Hutter (UDC).

Durante la sessione primaverile 2010, il Consiglio nazionale si è chinato sulla questione. A quella data l'onorevole Hutter non era più titolare di un seggio in Consiglio nazionale; contro la mozione si è espresso in sua vece il consigliere nazionale Christoph Mörgeli (UDC), che nel corso della propria argomentazione si è esplicitamente riferito al cosiddetto diritto indiretto di essere informati ai sensi della LMSI. Gli argomenti adottati dall'onorevole Mörgeli hanno convinto il Consiglio nazionale, che, contro il parere del Consiglio federale, ha respinto la mozione con 95 voti contro 64.

La DelCG, invece, nella *raccomandazione numero 11* del suo Rapporto del 21 giugno 2010 concernente il trattamento dei dati nel sistema per il trattamento dei dati relativi alla protezione dello Stato (ISIS), ha chiesto al Consiglio federale di proporre alle Camere, nel quadro della revisione della LMSI, di sostituire il «diritto indiretto di consultazione» ai sensi dell'attuale articolo 18 LMSI con un diritto di essere informati secondo le modalità previste all'articolo 8 della legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione (LSIP).

Il nostro Collegio ha ritenuto che detta richiesta della DelCG corrispondesse a un'esigenza minima e ha adottato una misura più incisiva (in conformità con la mozione di cui ha raccomandato l'approvazione, cfr. più sopra), ancorando nella legge il diritto diretto di essere informati conformemente agli articoli 8 e 9 della legge federale sulla protezione dei dati.

Art. 19 cpv. 3

Se concerne funzioni di massima responsabilità, il controllo di sicurezza relativo alle persone deve essere eseguito prima che i futuri titolari siano proposti per la nomina o per l'elezione alla funzione. Con l'espressione «funzioni di massima responsabilità» sono designati i titolari di cariche nominati dal Consiglio federale. Può trattarsi sia di cosiddetti quadri top della Confederazione (segretari generali, direttori di Uffici ecc.) sia di massimi quadri dell'esercito nonché di membri di gruppi di esperti, di giudici istruttori straordinari ecc. Nel caso di persone da sottoporre a controllo e che non sono elette dal Consiglio federale, l'elezione alla funzione o alla carica oppure la concessione dell'accesso a informazioni, materiali o impianti classificati possono aver luogo soltanto dopo la conclusione del controllo di sicurezza relativo alle persone.

Inoltre, conformemente agli standard internazionali, il controllo di sicurezza dovrà essere ripetuto per principio e non soltanto in casi eccezionali. I controlli di sicurezza sono ripetuti di regola ogni cinque anni. Ciò consentirà di colmare ulteriori essenziali lacune in materia di sicurezza.

L'aggiunta «è fatto salvo l'articolo 113 capoverso 1 lettera d della legge militare del 3 febbraio 1995» è stata decisa dalle Camere federali già in data 19 marzo 2010 nel quadro della revisione della legge militare e, scaduto inutilizzato il termine di referendum, entrerà in vigore il 1° gennaio 2011.

Art. 20 cpv. 2 lett. c e d

Let. c

Si rimanda al commento all'articolo 21.

Let. d

I controlli di sicurezza relativi alle persone sono una componente della gestione statale dei rischi. Se persone che occupano posizioni chiave commettono un tradimento, agiscono contro lo Stato o aspirano a modificarne in maniera illegale le istituzioni, lo Stato si trova di fronte a una delle maggiori minacce a cui può essere esposto. I controlli di sicurezza relativi alle persone sono volti segnatamente a mettere lo Stato al riparo da simili rischi.

In virtù dell'attuale articolo 20 capoverso 2 lettera d LMSI, nel quadro dei controlli di sicurezza relativi alle persone possono essere richieste agli organi incaricati del perseguimento penale informazioni concernenti procedimenti penali in corso. Condividiamo il parere della CdG-N secondo cui, nel quadro di controlli concernenti i massimi livelli, dovrà essere data in futuro anche la possibilità di visionare gli atti di procedimenti penali conclusi o abbandonati.

Ai fini della valutazione dei rischi in materia di sicurezza, l'autorità di controllo ha l'obbligo, indipendentemente dal livello di controllo, di visionare atti relativi a procedimenti penali conclusi o abbandonati, poiché anche persone sottoposte ad altri livelli di controllo (accesso a informazioni, impianti militari o materiali classificati CONFIDENZIALE o SEGRETO) rivestono funzioni sensibili in materia di sicurezza. In occasione dei controlli di sicurezza, anche per queste categorie di personale l'autorità di controllo deve poter acquisire certezze riguardo ai contenuti di procedimenti penali conclusi o abbandonati e poter procedere a una pertinente valutazione; altrimenti il controllo di sicurezza relativo alle persone si ridurrebbe a una farsa.

Art. 21 cpv. 1, 2 e 4

La CdG-N ha raccomandato al Consiglio federale di provvedere affinché l'autorità di controllo (servizio specializzato) sia trasferita all'esterno del DDPS e di valutare l'opportunità di incorporarla nella Cancelleria federale oppure in un Dipartimento con un numero ridotto di funzioni soggette all'obbligo del controllo di sicurezza relativo alle persone.

Il settore dei controlli di sicurezza relativi alle persone riveste un'importanza centrale per tutti gli altri settori inerenti alla sicurezza e per il sistema globale «Sicurezza integrale». Per questo motivo siamo convinti che sia opportuno mantenere l'autorità di controllo nel DDPS, più precisamente in seno alla Protezione delle informazioni e delle opere (PIO). Un suo trasferimento all'esterno di tale «rete integrata per la sicurezza» non soltanto annienterebbe l'approccio integrale sviluppato in materia di sicurezza nell'ultimo decennio e radicato nei Dipartimenti, ma indebolirebbe duramente la sicurezza stessa del Paese.

Il nostro Collegio è convinto che la questione dell'indipendenza dell'autorità di controllo del DDPS possa in linea di principio porsi eventualmente soltanto per una parte del processo, ovvero soltanto in occasione di audizioni e valutazioni aventi per oggetto i rischi in materia di sicurezza rappresentati da quadri top del DDPS (quadri top: persone nominate dal Consiglio federale) e in occasione delle verifiche a cui è sottoposto il personale della PIO. Nell'ambito della maggior parte dei controlli di

sicurezza relativi alle persone non vi sono dubbi sull'indipendenza dell'autorità di controllo. Come menzionato poc'anzi, riteniamo dunque che l'indipendenza dell'autorità di controllo sia suscettibile di subire limitazioni soltanto in occasione dei controlli aventi per oggetto quadri top del DDPS: l'esecuzione dei controlli all'esterno del DDPS è stata per contro chiesta in maniera perentoria dalla CdG-N per tutti i casi in cui le verifiche concernono quadri top della Confederazione conformemente all'articolo 12 dell'ordinanza del 19 dicembre 2001⁴⁶ sui controlli di sicurezza relativi alle persone (OCSP). Al riguardo, il Consiglio federale invita in questa sede a considerare che l'autorità di controllo del DDPS ha in passato più volte espresso il parere che quadri top della Confederazione rappresentassero un rischio per la sicurezza e che tra le persone interessate figuravano sia collaboratori di Dipartimenti civili sia quadri del DDPS.

Per dare seguito alla raccomandazione della CdG-N, nel quadro di controlli aventi per oggetto quadri top della Confederazione è previsto di far eseguire le fasi di controllo «audizioni», «analisi dei rischi» e «emanazione della decisione» dalla Cancelleria federale. In futuro saranno inoltre eseguiti dalla Cancelleria federale anche i controlli relativi a collaboratori della PIO (collaboratori dell'autorità di controllo del DDPS compresi). In tal modo l'auspicata indipendenza delle autorità di controllo potrà essere totalmente garantita. I rimanenti controlli di sicurezza relativi alle persone conformemente agli articoli 10, 11 e 12 OCSP continueranno a essere eseguiti dal DDPS. Affinché non sorgano problemi di indipendenza in seno alla Cancelleria federale, i controlli relativi a quadri top di quest'ultima (vicecancelliere) saranno eseguiti dal DDPS. L'adozione di tali misure consentirà di fugare qualsiasi dubbio sull'indipendenza delle autorità di controllo, sia in seno al DDPS sia in seno alla Cancelleria federale.

In questo ambito vanno inoltre debitamente considerati aspetti quali l'economicità, il know-how e l'economia amministrativa. A tal fine la Cancelleria federale e il DDPS opereranno congiuntamente, nel quadro di una chiara delimitazione delle responsabilità. Nell'ambito dei controlli relativi a quadri top, ad esempio, il rilevamento dei dati contenuti nei registri della Confederazione e dei Cantoni sarà eseguito per la Cancelleria federale dal DDPS. Quest'ultimo metterà a disposizione della Cancelleria federale, ai fini dell'ulteriore elaborazione e valutazione, tutti i dati rilevati, allo stato grezzo, sotto forma cartacea e in forma elettronica. La Cancelleria federale provvederà all'esecuzione delle audizioni, alla valutazione dei rischi in materia di sicurezza e all'emanazione della relativa decisione. Per i quadri top (eccettuati i quadri top della Cancelleria federale) sarà pertanto istanza precedente rispetto al Tribunale amministrativo federale in caso di ricorso contro decisioni da essa emane.

L'indipendenza delle autorità di controllo sarà inoltre sancita a livello di legge.

Art. 27 cpv. 1^{bis} (nuovo), 1^{ter} (nuovo)

L'articolo 27 della legge impone al Consiglio federale di informare annualmente, o secondo necessità, le Camere federali, i Cantoni e l'opinione pubblica sulla sua valutazione dello stato della minaccia nonché sulle attività degli organi di sicurezza della Confederazione. Allo stesso modo, si intende obbligare il DDPS e il DFGP a informare annualmente, o secondo necessità, sull'utilizzo dei mezzi introdotti con la

presente revisione. Alla luce delle possibili restrizioni dei diritti fondamentali della popolazione, è del tutto naturale che tale informazione abbia luogo. L'informazione concerne l'uso delle identità fittizie (DDPS) e il divieto di determinate attività (DFGP). Del resto, il Dipartimento e la Delegazione delle Commissioni della gestione ricevono già oggi rendiconti completi senza che esista un espresso obbligo legale.

Modifica del diritto vigente

1. Legge federale del 3 ottobre 2008⁴⁷ sul servizio informazioni civile

Art. 7 capoverso 2 (nuovo)

Come previsto per il settore delle attività di intelligence all'interno del territorio nazionale (cfr. art. 14a cpv. 3 D-LMSI), anche le indennità o ricompense versate agli informatori del settore concernente l'estero non devono figurare né come reddito imponibile né come reddito ai sensi della legge federale del 20 dicembre 1946⁴⁸ sull'assicurazione per la vecchiaia e per i superstiti.

2. Codice penale⁴⁹

Art. 317bis

La falsità in documenti è un atto punibile (cfr. art. 251, 252, 255, 317 CP). L'attuale articolo 317^{bis} CP fa tuttavia salvi l'allestimento e l'uso di documenti falsi atti a costituire o conservare, con l'approvazione del giudice, un'identità fittizia. Questa disposizione penale va adeguata affinché sia fatto salvo anche l'impiego di identità fittizie conformemente alla LMSI.

A quanto appena esposto si aggiunge la necessità di adeguare il capoverso 2 a causa di un'incoerenza con l'attuale disciplinamento nel settore della procedura penale: se, da un lato, conformemente all'articolo 288 CPP, anche il pubblico ministero è autorizzato ad assegnare un'identità fittizia ad agenti infiltrati, dall'altro, conformemente all'attuale articolo 317^{bis} CP, l'allestimento, l'alterazione o l'uso di documenti necessari per un'inchiesta mascherata non sono punibili unicamente se hanno luogo con l'approvazione del giudice. Quest'ultima tuttavia, conformemente all'articolo 289 capoverso 4 lettera a CPP, è concessa dal competente giudice dei provvedimenti coercitivi soltanto dopo che una relativa richiesta di approvazione dell'intervento gli è stata presentata dal pubblico ministero. L'approvazione del giudice alla creazione di un'identità fittizia ha pertanto luogo in un momento troppo tardivo. La necessità di adeguare il tenore del capoverso è già stata riconosciuta e considerata nel quadro dei lavori relativi alla LCPol. Tuttavia, poiché la questione si porrà concretamente già al momento dell'entrata in vigore del CPP, la modifica dovrebbe aver luogo quanto prima possibile.

⁴⁷ RS 121

⁴⁸ RS 831.10

⁴⁹ RS 311.0

3. Legge federale del 20 giugno 1997⁵⁰ sulle armi, gli accessori di armi e le munizioni

L'articolo 5 D-LMSI crea una base legale formale per la dotazione con un'arma di elementi del SIC; quest'ultimo è inoltre nel contempo escluso – come l'esercito e le autorità doganali e di polizia – dal campo di applicazione della legge sulle armi. L'esclusione da detto campo di applicazione è giustificata innanzitutto da ragioni di ordine pratico.

4. Legge federale del 6 ottobre 2000⁵¹ sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni

Trattandosi dell'introduzione «parallela» del diritto di essere informati, si rimanda alle considerazioni nel commento all'articolo 13 capoverso 1^{bis} D-LMSI.

5–11: leggi sulle assicurazioni sociali

5. Legge federale del 20 dicembre 1946⁵² sull'assicurazione per la vecchiaia e per i superstiti

6. Legge federale del 19 giugno 1959⁵³ sull'assicurazione per l'invalidità

7. Legge federale del 25 giugno 1982⁵⁴ sulla previdenza professionale per la vecchiaia, i superstiti e l'invalidità

8. Legge federale del 18 marzo 1994⁵⁵ sull'assicurazione malattie

9. Legge federale del 20 marzo 1981⁵⁶ sull'assicurazione contro gli infortuni

10. Legge federale del 19 giugno 1992⁵⁷ sull'assicurazione militare

11. Legge del 25 giugno 1982⁵⁸ sull'assicurazione contro la disoccupazione

Nell'ambito delle assicurazioni sociali, il legislatore ha disciplinato la comunicazione dei dati di volta in volta nelle rispettive leggi, costituendo un ordinamento esautivo a sé stante. Di conseguenza, la sospensione del segreto d'ufficio nei confronti degli organi di sicurezza della Confederazione e dei Cantoni conformemente all'articolo 13a del presente disegno necessita di un adeguamento specifico in ognuna di tali leggi. La sospensione del segreto d'ufficio non è globale, bensì limitata alle condizioni di cui all'articolo 13a. La disposizione non contempla i segreti legali professionali (per es. dei medici, degli avvocati, degli ecclesiastici) che rimangono garantiti. Del resto il segreto d'ufficio è già abrogato mediante norme analoghe nei confronti delle autorità istruttorie penali, delle autorità di assistenza sociale, degli uffici d'esecuzione, delle autorità fiscali ecc.

50 RS 514.54

51 RS 780.1

52 RS 831.10

53 RS 831.20

54 RS 831.40

55 RS 832.10

56 RS 832.20

57 RS 833.1

58 RS 837.0

Va sottolineato che l'obbligo di comunicazione è di per sé circoscritto ai settori del terrorismo, dello spionaggio politico o militare e della proliferazione. Il segreto d'ufficio è abrogato unicamente in questo settore di minaccia strettamente limitato.

