07.057

Messaggio concernente la modifica della legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI) (Mezzi speciali per la ricerca di informazioni)

del 15 giugno 2007

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di modifica della legge federale sulle misure per la salvaguardia della sicurezza interna.

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

15 giugno 2007 In nome del Consiglio federale svizzero:

La presidente della Confederazione, Micheline Calmy-Rey
La cancelliera della Confederazione, Annemarie Huber-Hotz

Compendio

La legge federale del 21 marzo 1997[1] *sulle misure per la salvaguardia della sicurezza interna (LMSI) è entrata in vigore il 1° luglio 1998 con lo scopo di garantire i fondamenti democratici e costituzionali della Svizzera nonché di proteggere la libertà della sua popolazione.*

Per riconoscere tempestivamente le minacce che attentano alla sicurezza della Svizzera è necessario valutare continuamente la situazione di pericolo. Il Consiglio federale e il Parlamento, ma anche i Cantoni, dovrebbero riconoscere tempestivamente i pericoli che minacciano l'esistenza dello Stato, tenerne conto nell'ambito della politica di sicurezza e prendere per tempo contromisure concrete. Il principale compito della protezione preventiva dello Stato consiste nel reperire tempestivamente le informazioni necessarie a questo scopo (rapporto sulla politica di sicurezza della Svizzera 2000, pagg. 32 e 54).

Ogni analisi dei rischi necessita di molte informazioni e di una solida rete per venirne in possesso. Raccogliere informazioni importanti per la sicurezza è un compito dei servizi d'informazione. Il Servizio di analisi e prevenzione (SAP) dell'Ufficio federale di polizia (fedpol) è preposto alla raccolta d'informazioni sul territorio nazionale. Tra i suoi compiti vi sono il riconoscimento tempestivo delle minacce terroristiche, dello spionaggio, dell'estremismo violento, del commercio illegale di armi e di materiale radioattivo e del trasferimento illegale di tecnologie (proliferazione), oltre alla ricerca di informazioni confidenziali.

In Svizzera la situazione relativa alla sicurezza e alle minacce è negli ultimi anni gradualmente peggiorata, in particolare a causa della crescente probabilità di attentati terroristici di matrice islamica. Da tempo non si è più in grado di soddisfare in modo adeguato il fabbisogno di informazioni, necessarie per valutare la situazione e prendere decisioni, ma anche per riconoscere tempestivamente le minacce nascoste. Il dispositivo di difesa dei servizi d'informazione presenta lacune e non basta più contro l'odierna situazione di pericolo. Le lacune non possono essere colmate né con uno sfruttamento più coerente delle possibilità esistenti né con il miglioramento del flusso d'informazioni e della coordinazione tra il servizio d'informazione e le autorità di perseguimento penale né potenziando il diritto penale formale e materiale. È invece indispensabile che la ricerca delle informazioni da parte dei servizi segreti venga migliorata, rendendola più mirata, ma anche circoscrivendola e controllandola più rigorosamente, in modo da renderla più efficace e da avvicinarla agli standard europei.

A questo scopo saranno prese in particolare le seguenti misure:

– *limitatamente alla prevenzione dalle minacce gravi (terrorismo, spionaggio politico o militare e commercio illegale di beni nel settore della proliferazione) le autorità e le unità amministrative della Confederazione e dei Cantoni saranno tenute a fornire tutte le informazioni richieste. Alle stesse*

[1] RS **120**

condizioni anche i trasportatori commerciali dovranno fornire informazioni sui dati in loro possesso;

– *sarà inoltre possibile impiegare, a condizioni molto severe e come ultima ratio, mezzi speciali per la ricerca di informazioni. In caso di sospetto fondato, sempre limitatamente ai settori del terrorismo, dello spionaggio politico o militare e della proliferazione, saranno consentiti: la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, l'osservazione di persone pericolose in luoghi non liberamente accessibili, anche ricorrendo ad apparecchi tecnici di sorveglianza, e l'accesso segreto a sistemi per l'elaborazione dei dati. L'impiego di questi mezzi è sottoposto a un doppio obbligo d'autorizzazione (esame giudiziario da parte del Tribunale amministrativo federale e verifica dal punto di vista politico da parte dei capi del DFGP e del DDPS);*

– *il capo del DFGP riceverà la competenza di vietare attività finalizzate a promuovere operazioni terroristiche o di estremismo violento che minacciano de facto la sicurezza interna o esterna della Svizzera. È altresì prevista una base legale formale per l'impiego di informatori, la loro protezione e il loro indennizzo. Allo scopo di proteggere gli informatori e i collaboratori del SAP durante la ricerca di informazioni, potranno essere fornite anche identità fittizie;*

– *il presente ampliamento delle competenze comporta un equivalente rafforzamento della protezione giuridica. Per poter ordinare mezzi speciali per la ricerca di informazioni, occorrerà sottoporli all'autorizzazione del Tribunale amministrativo federale e dell'Esecutivo, mentre le decisioni sul dovere di comunicare e il divieto di determinate attività soggiaceranno ad un efficace controllo giudiziario da parte del Tribunale amministrativo federale e del Tribunale federale.*

Grazie a criteri restrittivi e a molteplici controlli si eviterà una limitazione illecita dei diritti fondamentali di terzi non coinvolti.

Tutte le misure sono conformi alla Costituzione e compatibili con i diritti fondamentali. Si basano infatti su un interesse pubblico comprovato e rispettano il principio della proporzionalità. Il progetto è inoltre compatibile con la CEDU e il Patto internazionale del 16 novembre 1996 relativo ai diritti civili e politici.

I posti necessari per l'attuazione, gli investimenti e le spese di gestione sono compensati internamente dal DFGP.

Indice

Elenco delle abbreviazioni

AIMP	Legge federale del 20 marzo 1981 sull'assistenza internazionale in materia penale (RS *351.1*)
CEDU	Convenzione del 4 novembre 1950 per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (RS *0.101*)
CO	Criminalità organizzata
Cost.	Costituzione federale della Confederazione Svizzera del 18 aprile 1999 (RS *101*)
CP	Codice penale svizzero del 21 dicembre 1937 (RS *311.0*)
CPP	Codice di procedura penale svizzero (FF *2006* 1291)
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
D-CPP	Disegno concernente il Codice di procedura penale svizzero
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DFGP	Dipartimento federale di giustizia e polizia
DGE	Divisione della guerra elettronica del DDPS
DTF	Decisione del Tribunale federale
Europol	Ufficio europeo di polizia
fedpol	Ufficio federale di polizia
FF	Foglio federale
Interpol	Organizzazione internazionale di polizia giudiziaria
LM	Legge federale del 3 febbraio 1995 sull'esercito e sull'amministrazione militare (RS *510.10*)
LMSI	Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (RS *120*)
LPD	Legge federale del 19 giugno 1992 sulla protezione dei dati (RS *235.1*)
LSCPT	Legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (RS *780.1*)
LUC	Legge federale del 7 ottobre 1994 sugli Uffici centrali di polizia giudiziaria della Confederazione (RS *360*)
MPC	Ministero pubblico della Confederazione
OCGE	Ordinanza del 15 ottobre 2003 concernente la condotta della guerra elettronica (RS *510.292*)
OMSI	Ordinanza del 27 giugno 2001 sulle misure per la salvaguardia della sicurezza interna (RS *120.2*)
ONU	Organizzazione delle Nazioni Unite
OUC	Ordinanza del 30 novembre 2001 sull'adempimento di compiti di polizia giudiziaria in seno all'Ufficio federale di polizia (RS *360.1*)
PGF	Polizia giudiziaria federale
PP	Legge federale del 15 giugno 1934 sulla procedura penale (RS *312.0*)
SAP	Servizio di analisi e prevenzione

SCS	Servizio per compiti speciali della Segreteria generale del DATEC
SFS	Servizio federale di sicurezza
UE	Unione europea

Messaggio

1 Linee direttrici del progetto

1.1 Situazione iniziale

1.1.1 Genesi del progetto

Il servizio d'informazione interno mostra da anni deficit nella prevenzione delle minacce, che vanno ricondotti alla lacunosa gamma di strumenti disponibile per scoprirli. Preso atto della situazione l'Organo direttivo in materia di sicurezza e la Giunta del Consiglio federale in materia di sicurezza hanno ordinato l'esame di misure atte a colmare queste lacune.

Dopo gli attentati terroristici dell'11 settembre 2001 sono stati depositati molti interventi parlamentari che sollecitano un rafforzamento del ruolo degli organi di sicurezza dello Stato e dei servizi d'informazione, come pure dei mezzi e degli strumenti a loro disposizione. Si richiedono inoltre rapporti circostanziati sulla situazione in materia di sicurezza (cfr. in particolare le mozioni PLR[2], Leu[3], Merz[4] e Burkhalter[5]; gli interventi PLR[6], Fünfschilling[7], Suter[8], PPD[9], Leutenegger Oberholzer[10] e Pfister[11]).

Di conseguenza, nel novembre del 2001 abbiamo incaricato il Dipartimento federale di giustizia e polizia (DFGP), di sottoporci un rapporto e una proposta sulle misure per migliorare la lotta contro il terrorismo. Nel giugno 2002 abbiamo approvato il rapporto «Analisi della situazione attuale e dei rischi per la Svizzera dopo gli attacchi terroristici dell'11 settembre 2001» e abbiamo preso nel contempo conoscenza della ripartizione in due pacchetti dei progetti legislativi. Il secondo pacchetto (ovvero la presente revisione) riguarda specialmente il tema del terrorismo.

Dopo approfonditi lavori preliminari e dopo un primo dibattito, il 20 ottobre 2004 abbiamo incaricato il DFGP di sottoporci un avamprogetto per la consultazione nel corso del 2005. L'avamprogetto è stato inviato in consultazione presso gli Uffici la prima volta nel luglio del 2005, la seconda nel febbraio 2006 dopo rielaborazione. Il 5 aprile 2006 ci siamo espressi sugli aspetti risultati particolarmente critici nell'ambito della consultazione degli Uffici, decidendo il seguito da dare al progetto. In

2 01.3545 Mozione del Gruppo liberale-radicale: Ottimizzare i servizi d'informazione e la protezione dello Stato
3 01.3626 Mozione Leu: La nuova cultura dei servizi d'informazione per nuove sfide
4 01.3569 Mozione Merz: Ottimizzare i servizi d'informazione e di protezione dello Stato
5 04.3216 Mozione Burkhalter: Lotta al terrorismo. Misure preventive
6 01.3552 Interpellanza del Gruppo liberale-radicale: Valutazione della situazione in seguito agli attentati terroristici
7 01.3576 Interpellanza Fünfschilling: Valutazione della situazione in seguito agli attentati terroristici
8 01.3612 Interpellanza Suter: Lotta al terrorismo nell'UE – Ripercussioni in Svizzera?
9 01.3702 Mozione del Gruppo popolare-democratico: Mantenimento a distanza di persone indesiderate in Svizzera per ragioni di sicurezza; 01.3704 Mozione del Gruppo popolare-democratico: Eliminazione dei punti deboli nella prevenzione del terrorismo; 01.3705 Mozione del Gruppo popolare-democratico: Cooperazione e professionalità nei servizi informazioni
10 01.3633 Postulato Leutenegger Oberholzer: Attentati terroristici. Nuova valutazione dei rischi in Svizzera
11 01.1114 Interrogazione ordinaria Pfister: Indagine combinata

base al mandato è stato elaborato il progetto da inviare in consultazione. Il 5 luglio 2006 abbiamo incaricato il DFGP di svolgere la procedura di consultazione.

La procedura di consultazione è durata dal 5 luglio al 15 ottobre 2006. Dati i molti pareri talvolta controversi emersi dalla stessa, abbiamo ricevuto in un primo tempo il rapporto sui risultati della procedura di consultazione e una proposta sul seguito da dare al progetto. Con la decisione del 4 aprile 2007 abbiamo preso conoscenza del risultato della procedura di consultazione e incaricato il DFGP di elaborare il presente messaggio, definendone le linee direttrici.

1.1.2 Servizio di analisi e prevenzione (SAP): servizio d'informazione interno civile

Compiti del SAP

Servizio d'informazione interno

Il Servizio di analisi e prevenzione (SAP) nell'Ufficio federale di polizia (fedpol) è il servizio d'informazione interno di polizia della Svizzera.

I compiti del SAP sono disciplinati nella LMSI e nelle relative ordinanze. Esso ha l'incarico di fornire tempestivamente agli organi di polizia della Confederazione e dei Cantoni informazioni sulle minacce per la sicurezza interna, affinché sia possibile adottare misure preventive in tempo utile. Le informazioni riguardano principalmente minacce alla sicurezza per tutta la Svizzera e i suoi abitanti. Esse comprendono in particolare il riconoscimento e l'analisi di attività collegate alla criminalità grave. Per individuare tempestivamente queste minacce contro i fondamenti democratici e costituzionali della Svizzera nonché contro la libertà e la sicurezza dei cittadini, il SAP ha l'obbligo di osservare permanentemente e di analizzare periodicamente la situazione relativa alle minacce. Dal momento che la LMSI vincola le misure preventive, di regola segrete, e gli interventi che ne conseguono alla prevenzione dei rischi per la sicurezza dello Stato, le attività del servizio d'informazione hanno uno scopo esclusivamente preventivo. Nei tempi di pace il SAP assolve anche i compiti di difesa militare.

Minacce alla sicurezza interna

La salvaguardia della sicurezza interna è un compito originario e primordiale dello Stato. Comprende la garanzia delle norme fondamentali della convivenza pacifica, la protezione delle istituzioni statali, la tutela della società e del singolo contro pericoli elementari e la difesa del Paese contro le situazioni di crisi sociale[12].

Il giudizio sul pericolo per la sicurezza interna di certi comportamenti è in primo luogo una valutazione politica che dipende dalla situazione generale. Una situazione di minaccia non scaturisce solo da un atteggiamento concreto, ma soprattutto dal contesto politico in cui si situa. In altre parole lo stesso atteggiamento, in un ambito differente, può diventare da neutro a una minaccia per la sicurezza interna e viceversa.

12 Messaggio del 20 novembre 1996 concernente la revisione della Costituzione federale, pag. 375

Si prenda ad esempio un'organizzazione terroristica che, dopo una lunga fase di tregua nella propria patria, durante la quale la minaccia sulla sicurezza della Svizzera era solo latente, riprende le violenze in modo che le conseguenze sulla nostra sicurezza interna diventino repentinamente concrete. Entrano in gioco in particolare attentati terroristici in Svizzera, reciproci atti di violenza delle comunità di diaspora locali, riscossione vessatoria di «offerte» e conseguente trasferimento di fondi dalla Svizzera alla madre patria per finanziare la lotta armata o il reclutamento di adepti o di terroristi ecc. Gli attentati terroristici all'estero possono danneggiare sempre sia i cittadini svizzeri sia gli interessi svizzeri.

Dimensione preventiva della protezione

La ricerca, l'esame e la diffusione permanente di informazioni da parte del SAP ha lo scopo di informare gli organi direttivi dello Stato sulle possibili minacce per l'esistenza e la sicurezza del Paese, per il suo libero ordinamento sociale e per le sue istituzioni democratiche.

Questa dimensione della protezione dello Stato, che riguarda la società e la nazione nel suo complesso, si riflette nell'articolo 1 LMSI, secondo cui la protezione dello Stato serve a garantire i fondamenti costituzionali e democratici della Svizzera e a proteggere la libertà.

Informazione del Governo e dell'opinione pubblica

Le informazioni raccolte devono consentire alle autorità competenti della Confederazione e dei Cantoni di intervenire per tempo conformemente al loro diritto determinante. Il fine del riconoscimento tempestivo consiste nello svelare strutture pericolose e nel trattare le informazioni ottenute affinché servano come base per le decisioni degli organi politici responsabili della Confederazione e dei Cantoni. Il direttore di fedpol e il capo del SAP sono membri permanenti dell'Organo direttivo in materia di sicurezza e pertanto direttamente coinvolti nella valutazione della situazione e nel riconoscimento tempestivo degli organi di conduzione della politica di sicurezza.

La lotta contro le attività terroristiche deve avvenire tempestivamente per poter intervenire già nella fase di pianificazione e preparazione. A questo scopo sono necessarie le misure di osservazione delle persone e dei gruppi pericolosi nonché una collaborazione ottimale su scala internazionale. Tuttavia anche dopo un attentato terroristico - come confermano le esperienze all'estero - le informazioni dei servizi d'informazione hanno un'importanza decisiva per la rapida identificazione degli autori.

Ciclo d'informazioni

I servizi d'informazione dirigono la propria attività secondo i principi del ciclo d'informazione, che comprende la pianificazione (che cosa interessa?), la ricerca (p. es. colloqui con informatori), l'esame (p. es. riguardo alla pertinenza dell'informazione), la valutazione (p. es. elaborazione di rapporti e indicazioni degli organi di ricerca) e diffusione (p. es. stesura di rapporti per l'Esecutivo). Un punto debole nel corso della ricerca si ripercuote direttamente su tutto il ciclo.

Ricerca delle informazioni: tutte le analisi delle minacce e tutte le attività che ne scaturiscono si basano su molteplici informazioni. Le fonti accessibili al pubblico permettono di raccogliere soltanto una parte delle informazioni necessarie. Uno dei compiti principali del servizio d'informazione consiste pertanto nel raccogliere

informazioni su fatti riservati. Non può tuttavia procurarsi informazioni più numerose e più approfondite rispetto a quelle che la legge consente di raccogliere.

A livello operativo la ricerca d'informazioni del SAP va dalla direzione degli informatori, fonti particolarmente sensibili, fino alle contro-operazioni con agenti smascherati o che hanno cambiato campo. Molti casi sono affrontati in collaborazione con i Cantoni e/o con le autorità straniere e da questa strategia risultano informazioni indispensabili per la sicurezza della Confederazione e dei Cantoni.

Di particolare importanza è lo scambio d'informazioni con le autorità straniere. Il flusso di comunicazioni riguarda annualmente circa 20 000 comunicazioni di natura confidenziale e segreta. Tale collaborazione internazionale è particolarmente importante anche per far fronte ai compiti della polizia degli stranieri. Infatti ad esempio, se la Francia espelle predicatori che incitano all'odio, questi non devono poter trovare rifugio in Svizzera. Oppure se un concerto di skinhead con famosi gruppi tedeschi e italiani del giro è annunciato in Svizzera, è meglio impedire che possano venire nel nostro Paese a diffondere pubblicamente le proprie idee razziste. In entrambi i casi il SAP ha la competenza di emanare i divieti di entrata. Per esaminare i criteri in base ai quali ordinare i divieti, esso dipende dalle informazioni fornitegli dalle autorità straniere.

Esame delle informazioni: l'esame delle informazioni raccolte consente di studiare la loro affidabilità, di confrontarle tra loro e di elaborarle in modo da poterle utilizzare. I dati devono infatti essere sempre raggiungibili con facilità dalle persone abilitate, ma devono anche essere sicuri e presentati in forma corretta.

Valutazione e diffusione delle informazioni: il settore d'analisi del SAP è il servizio centrale di analisi nazionale. Tutte le informazioni dei servizi segreti e della polizia giudiziaria vengono valutate integralmente in questa sede. Negli ultimi anni questo settore è stato cresciuto dal punto di vista sia qualitativo sia quantitativo. Il SAP collabora strettamente con i servizi interessati della Confederazione e dei Cantoni.

L'analisi in senso stretto comporta la raccolta delle informazioni per avere un quadro generale, dove le ipotesi vengono verificate o scartate e si traggono le conclusioni.

Le analisi ad esempio possono essere elaborate come analisi delle minacce o analisi di politica comparata oppure indicare gli sviluppi, i fenomeni e gli scenari.

Tra le analisi più conosciute del SAP, anche perché pubblicate, si annoverano il Rapporto sulla sicurezza interna della Svizzera e il Rapporto sull'estremismo che appaiono quasi ogni anno. Tuttavia la maggior parte di ciò che è prodotto dal SAP è di natura confidenziale e riguarda questioni specifiche concernenti la sicurezza interna (come p. es. la lotta contro le ideologie estremiste violente a livello giuridico, tecnico e ideologico). Allo stesso tempo questi rapporti individuano anche le carenze nelle conoscenze e di conseguenza danno un orientamento su dove pianificare la ricerca delle informazioni.

Un altro elemento che garantisce la sicurezza della Svizzera è la continua valutazione e diffusione delle informazioni sulla situazione attuale. Il Centro federale di situazione del SAP diffonde quotidianamente a questo scopo i rapporti di situazione e le valutazioni a più di 300 servizi della Confederazione e dei Cantoni.

Inoltre il riconoscimento dell'importanza di Internet e della vulnerabilità dell'infrastruttura svizzera ha portato alla creazione di nuovi settori: SCOCI (Servizio di coordinazione nazionale per la lotta contro la criminalità su Internet) e MELANI (Centrale d'annuncio e d'analisi per la sicurezza dell'informazione).

Ricerca di informazioni da parte del SAP

In virtù del diritto vigente, il SAP si occupa delle minacce dovute al terrorismo, all'estremismo violento, allo spionaggio, al commercio illecito di armi e materiale radioattivo nonché al trasferimento illegale di tecnologie. Assiste inoltre le autorità di polizia e di perseguimento penale competenti, trasmettendo loro informazioni sulla criminalità organizzata, in particolare quelle scaturite dalla cooperazione con le autorità di sicurezza straniere.

L'articolo 14 capoverso 2 LMSI enumera esaustivamente i mezzi per la ricerca di informazioni consentiti nell'ambito della prevenzione. In virtù di questo articolo i dati personali possono essere raccolti con:

a. la valutazione delle fonti accessibili al pubblico;
b. la richiesta di informazioni;
c. la consultazione di fascicoli ufficiali;
d. la ricezione e valutazione di comunicazioni;
e. la ricerca dell'identità o del luogo di soggiorno delle persone;
f. l'osservazione dei fatti in luoghi pubblici e liberamente accessibili, anche ricorrendo a registrazioni di immagini e suoni;
g. l'accertamento dei movimenti e contatti delle persone.

L'articolo 14 capoverso 3 LMSI, che risale al 1997, esclude l'impiego da parte del SAP di misure coercitive e di osservazioni di fatti in ambienti privati ammissibili nel quadro di una procedura penale. Di conseguenza attualmente non è consentito raccogliere informazioni per scopi preventivi nel settore della comunicazione (posta, telefono, fax, posta elettronica).

1.1.3 Ulteriori compiti e competenze nel settore della sicurezza

Servizi d'informazione stranieri

Il Servizio informazioni strategico (SIS) in seno al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) è il servizio informazioni concernente l'estero.

Il SIS, quale servizio d'informazione esterno della Svizzera, conformemente all'articolo 99 capoverso 1 della legge militare del 3 febbraio 1995[13] (LM), raccoglie, valuta e distribuisce, per conto dei più alti dirigenti politici e militari, in particolare il capo del DDPS, il capo dell'esercito, la Giunta del Consiglio federale in materia di sicurezza e l'Organo direttivo in materia di sicurezza, informazioni concernenti l'estero rilevanti per la sicurezza della Confederazione. In virtù dell'arti-

13 RS **510.10**

colo 99 capoverso 5 LM, il SIS è direttamente subordinato al capo del DDPS. Al SIS è assegnata un mandato di base approvato dalla Giunta del Consiglio federale in materia di sicurezza. L'attività di ricerca e di analisi del SIS si concentra su temi politici, economici, militari e tecnico-scientifici. Vi rientrano soprattutto minacce quali il terrorismo, la criminalità organizzata e la diffusione di armi di distruzione di massa e dei loro vettori (proliferazione). I compiti del SIS sono disciplinati nell'ordinanza del 26 settembre 2003[14] sui servizi d'informazione del DDPS (OSINF).

Polizia

La polizia, sottoposta prevalentemente alla sovranità cantonale, salvaguarda la sicurezza, la tranquillità e l'ordine pubblico e combatte la criminalità in generale. La Confederazione interviene in caso di avvenimenti che i Cantoni non sono in grado di fronteggiare con i propri mezzi e possibilità. Se la situazione lo richiede, essa può assumere la direzione.

Perseguimento penale

Il perseguimento penale intende chiarire dal punto di vista giuridico il sospetto di reato già esistente e l'eventuale colpevolezza dei singoli autori.[15]

Distinzione dei compiti e dei mezzi del servizio d'informazione interno da quelli delle autorità di perseguimento penale

Finalità della ricerca d'informazioni: il lavoro degli organi di perseguimento penale è finalizzato a chiarire nel caso specifico, i sospetti su un individuo. La ricerca di informazioni da parte dei servizi segreti ha invece il fine di riconoscere tempestivamente le minacce o i turbamenti della sicurezza, i piani pericolosi o gli atti preparatori concreti. Una volta individuate dal SAP, le competenti autorità della Confederazione e dei Cantoni adottano le misure di polizia o di diritto amministrativo necessarie per contrastare o eliminare tali minacce.

Mezzi della ricerca d'informazioni: le inchieste di diritto penale sono condotte nell'ambito di una procedura penale o di un'inchiesta formale qualora si debbano chiarire sospetti sufficientemente sicuri su reati concreti. Le autorità di perseguimento penale possono impiegare se necessario, per adempiere alle proprie inchieste penali, misure coercitive procedurali (p. es. citazione, consegna, fermo, detenzione di polizia, detenzione preventiva, messa al sicuro e custodia degli oggetti, sequestro, sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, perquisizione di persone, misure d'identificazione, osservazioni, inchieste mascherate). In virtù della ripartizione delle competenze tra Confederazione e Cantoni in materia di perseguimento penale, oltre alla normativa federale sono di principio applicabili le 26 leggi cantonali di procedura penale a cui si aggiungono le rispettive leggi che regolano l'attività della polizia. Un codice di procedura penale unico a livello federale è attualmente in discussione in Parlamento. Il legislatore ha vietato al servizio d'informazione interno l'impiego di simili mezzi e le osservazioni in spazi

14 RS **510.291**

15 Per un confronto esaustivo dei compiti di polizia per il perseguimento penale e di polizia preventiva cfr. il rapporto del Consiglio federale del 21 febbraio 2005 relativo al postulato 05.3006 della Commissione della politica di sicurezza del Consiglio degli Stati sulla «Lotta più efficace contro il terrorismo e la criminalità organizzata», numero 3.2.4, lettera a (FF **2006** 5223).

privati. La questione se e in quale misura tale divieto debba essere mantenuto, alla luce delle attuali minacce terroristiche e di altri siffatti pericoli, è oggetto della presente revisione parziale della LMSI.

Competenze per il riconoscimento tempestivo di crimini gravi di stampo terroristico o mafioso: il SAP è responsabile del riconoscimento tempestivo delle minacce alla sicurezza interna, che oltre all'uso della violenza contro la società e lo Stato, si contraddistinguono anche per la motivazione politico-ideologica degli autori. Si devono distinguere da ciò le organizzazioni di stampo mafioso, che agiscono a scopo di lucro e vogliono essere riconosciute a livello sociale. In questo caso infatti il contesto commerciale è in primo piano e il riconoscimento tempestivo rientra nella sfera di competenza della polizia giudiziaria.[16]

Compiti di polizia giudiziaria: il riconoscimento tempestivo va distinto l'istruzione dei reati e il perseguimento degli autori. In caso di giurisdizione federale, le indagini riguardanti i reati a sfondo mafioso (criminalità organizzata) sono di esclusiva competenza della polizia giudiziaria federale PGF sotto la direzione del Ministero pubblico della Confederazione (MPC).[17]

Limiti del perseguimento penale

Lo scopo del perseguimento penale è al tempo stesso il suo limite. Il puntuale chiarimento di sospetti concreti non è fatto per il riconoscimento tempestivo delle minacce o delle interconnessioni superiori. I fatti di rilevanza penale definiscono esaustivamente il comportamento punibile e non sono affatto legati a qualsiasi minaccia per lo Stato o per la sua popolazione. Le fattispecie di reato per perseguire le organizzazioni criminali, gli autori dei principali reati terroristici o le cellule terroristiche non sono finalizzate primariamente a impedire gli attentati. Anche gli atti preparatori non sono punibili in base a una situazione di minaccia precisa, ma solo in quanto attività individuali concrete. Da tale situazione si evince che gli strumenti per il perseguimento penale non sono né concepiti né adatti per riconoscere tempestivamente le minacce e i rischi da parte di individui pericolosi e di organizzazioni o delle loro strutture. A questo serve il lavoro dei servizi d'informazione che si orienta in base a situazioni di minaccia e non di reati.

1.1.4 Scambio d'informazioni e cooperazione con altre autorità

Organizzazione delle autorità presso il DFGP

In vista dell'estensione della giurisdizione penale federale alle organizzazioni criminali, il 1° settembre 1999 abbiamo trasferito l'allora Polizia federale e il Servizio federale di sicurezza dal MPC a fedpol, che all'epoca era ancora il vecchio Ufficio federale di polizia. Con la decisione di riunire tutti i servizi di polizia in seno a fedpol, abbiamo soddisfatto l'esigenza dei Cantoni di potersi rivolgere a un unico partner nel settore della polizia a livello federale e adempito alla richiesta della CPI DFGP di sollevare il Procuratore generale della Confederazione dal suo incarico di capo della Polizia federale di quell'epoca, poiché quest'ultima, oltre a fungere da

16 Cfr. rapporto relativo al postulato CPS, numero 3.2.4, lettera c
17 Cfr. rapporto relativo al postulato CPS, numero 3.2.4, lettera d

polizia giudiziaria della Confederazione, svolgeva anche compiti di prevenzione in quanto servizio d'informazione interno[18].

Il 1° gennaio 2001, con la conclusione del progetto di riorganizzazione delle strutture nel settore della polizia della Confederazione, i compiti di prevenzione della polizia e quelli del perseguimento penale in seno a fedpol sono stati separati dal punto di vista organizzativo. La divisione «Uffici centrali di polizia giudiziaria» e la «Polizia federale» sono state sostituite dalle nuove divisioni principali «PGF» e «SAP». Mentre la PGF, in quanto polizia giudiziaria, svolge compiti di perseguimento penale, le competenze del SAP, in quanto servizio d'informazione, si concentrano sulla prevenzione mediante la ricerca di informazioni.

Collaborazione con il servizio d'informazione esterno del DDPS

Se le minacce si manifestano a livello internazionale e rientrano nella sfera di competenza sia del servizio d'informazione interno sia di quello esterno entrambi i servizi operano in stretta collaborazione, oggi in particolare nei settori del terrorismo, della criminalità organizzata e della proliferazione in base a uno schema di gruppi comuni.

Collaborazione con altri organi del DDPS

Il SAP, il Servizio informazioni militare (SIM), il Servizio informazioni delle Forze aeree (SIFA), gli altri organi militari di informazione nonché di sicurezza militare si sostengono nell'adempimento dei loro compiti. Il sostegno avviene segnatamente mediante lo scambio di informazioni, la consultazione vicendevole nell'ambito dei settori speciali nonché nella formazione.

Cooperazione del SAP con gli organi di perseguimento penale della Confederazione

La parziale sovrapposizione tematica dei compiti richiede uno scambio d'informazioni regolare e rapido: il SAP e la PGF sono tenuti a trasmettersi[19] reciprocamente le informazioni che rientrano nell'ambito di competenza dell'altra divisione.

Trasmissione di informazioni del SAP alla PGF e al MPC: se il SAP entra in possesso di informazioni sul crimine organizzato, secondo l'articolo 2 capoverso 3 LMSI le deve trasmettere alle autorità di perseguimento penale della Confederazione o dei Cantoni. Inoltre è tenuto a trasmettere immediatamente ogni indizio rilevante per il perseguimento penale alle autorità nazionali preposte al perseguimento penale[20].

Trasmissione di informazioni della PGF e del MPC al SAP: per la trasmissione delle informazioni in direzione inversa, la legge[21] obbliga il MPC e la PGF a informare il SAP. Entrambi hanno l'obbligo di informare spontaneamente il SAP quando vengono a conoscenza di minacce concrete per la sicurezza interna ed esterna[22]. Oltre allo scambio di informazioni operative, il MPC deve inoltre comunicare le sentenze e le

18 Rapporto della Commissione parlamentare d'inchiesta (CPI) del 22 novembre 1989, 89.006, Avvenimenti in seno al DFGP, FF **1990** 473, cap. VII numero 1.
19 Cfr. rapporto relativo al postulato CPS, numero 3.2.5, lettera a
20 Cfr. art. 17 cpv. 1 LMSI e l'obbligo di collaborazione secondo l'art. 4 LUC; cfr. il rapporto relativo al postulato CPS, numero 3.2.5, lettera b
21 Art. 13 cpv. 1 lett. a LMSI
22 Art. 13 cpv. 2 LMSI

dichiarazioni di non doversi procedere che riguardano i settori contemplati dalla LMSI[23].

Scambio di informazioni online: il SAP e la PGF dispongono reciprocamente di accessi limitati ai rispettivi sistemi di informazioni. Nella nuova legge federale sui sistemi d'informazione di polizia della Confederazione è prevista la creazione di un registro nazionale di polizia per rendere più rapida e facile l'assistenza amministrativa in materia di polizia[24].

Garanzie di procedura per la trasmissione delle informazioni: oltre alla protezione dei dati, il servizio d'informazione interno e le autorità di perseguimento penale devono tenere conto anche degli interessi pubblici preponderanti che nel caso concreto possono limitare o vietare del tutto la trasmissione di informazioni oppure sottoporre a restrizioni la trasmissione di informazioni a terzi. Per la trasmissione di informazioni il SAP deve ad esempio non solo valutare se vi si oppongono in generale interessi preponderanti pubblici o privati, bensì anche tenere conto della cosiddetta protezione della fonte[25]. Mentre nelle relazioni con l'estero la protezione della fonte dev'essere garantita in ogni caso[26], la necessità di proteggere la fonte in Svizzera dev'essere confrontata in ogni singolo caso con gli interessi dell'assistenza amministrativa o giudiziaria. La trasmissione avviene sotto forma di rapporti di valutazione e non di informazioni allo stato grezzo.

Anche il MPC e la PGF possono rifiutare, limitare o vincolare a oneri la trasmissione delle informazioni. Ciò è d'obbligo se lo richiedono[27] gli interessi degni di protezione di una persona interessata o interessi importanti del perseguimento penale[28].

Traffico con l'estero

In virtù della LMSI il SAP assicura le relazioni con le autorità estere incaricate di compiti di sicurezza (art. 8 LMSI) e rappresenta la Svizzera in seno a istanze internazionali (art. 6 dell'ordinanza del 27 giugno 2001[29] sulle misure per la salvaguardia della sicurezza interna [OMSI]). La prevenzione del terrorismo costituisce oggi la parte preponderante del flusso internazionale di informazione tra i servizi segreti.

Il SAP intrattiene in particolare uno scambio d'informazioni continuo e una collaborazione di polizia con circa 90 servizi partner di diversi Stati o organizzazioni straniere (p. es. ONU e UE) [30]. Il SAP è membro di quattro organi multilaterali informali: il «Counter-Terrorism Group» (composto di un servizio di ciascuno Stato dell'UE nonché di uno della Norvegia e della Svizzera), il «Club de Berne» (servizi di 22 Paesi europei), la «Middle European Conference» (servizi di 17 Paesi soprattutto dell'Europa sud-orientale, oltre a 8 Paesi con statuto di osservatori) e il «Police Working Group on Terrorism» (unità antiterrorismo delle autorità di polizia di 26 Paesi). Come condizione per lo scambio di informazioni con il «Situation

23 Cfr. rapporto relativo al postulato CPS, numero 3.2.5, lettera c
24 Cfr. rapporto relativo al postulato CPS, numero 3.2.5, lettera d
25 Art. 18 cpv. 5 OMSI
26 Cfr. art. 17 cpv. 7 LMSI e art. 20a OMSI
27 Cfr. art. 102^{quater} cpv. 2 in combinato disposto con l'art. 27 cpv. 2 PP e l'art. 7 cpv. 2 dell'ordinanza sull'adempimento di compiti di polizia giudiziaria in seno all'Ufficio federale di polizia
28 Cfr. rapporto « relativo al postulato CPS, numero 3.2.5, lettera e
29 RS **120.2**
30 La strategia di cooperazione internazionale del SAP è stata stabilita in un documento classificato confidenziale e approvato dal Consiglio federale nel giugno 2005.

Center» del Consiglio dell'UE, è prevista la conclusione di un accordo sulle procedure di sicurezza per lo scambio di documenti riservati[31]. Inoltre nell'ambito dell'EAPC (Euro-Atlantic Partnership Council) il SAP assolve per la Svizzera i compiti di un'Intelligence Liaison Unit (ILU) della NATO.

Tale cooperazione corrisponde, per quanto riguarda la cerchia dei servizi partner stranieri, alle esigenze attuali della Svizzera in tutti i settori specifici della LMSI.

La cooperazione del servizio d'informazione con i servizi stranieri è informale. Essa poggia sui principi della confidenzialità – la cosiddetta regola del servizio a terzi – e sulla reciproca fiducia. Le informazioni sono messe a disposizione in base al principio dell'interesse comune, confidando nel fatto che il servizio partner trasmetta a sua volta le informazioni rilevanti per la sicurezza interna («do ut des», dare per avere). Tuttavia non c'è un obbligo che lo garantisca.

31 L'accordo è stato approvato dal Consiglio dell'UE il 24 giugno 2005 e dal Consiglio federale il 29 giugno 2005. Al momento si stanno regolando i dettagli tecnici con l'UE.

1.1.5 Raffronto schematico

Sospetto di	
Minacce della sicurezza della Svizzera dovute al terrorismo, all'estremismo violento, allo spionaggio, alla proliferazione di armi	**Reati concreti o atti preparatori secondo il diritto penale federale o cantonale**
Prevenzione	*Repressione*
Competenze	
Servizio di analisi e prevenzione servizi cantonali d'informazione	Ministero pubblico della Confederazione Polizia giudiziaria federale autorità di perseguimento penale cantonali
Attività	
accertamenti dei servizi segreti e ricerca di informazioni analisi nell'ambito della sicurezza interna	chiarimento giuridico di un concreto sospetto di reato (eventuale impiego di misure coercitive del procedimento penale)
Oggetto	
tutti gli atti che costituiscono una minaccia per la sicurezza, indipendentemente dalla loro qualifica come reati	atti per cui è comminata una pena e sospetti sufficienti per aprire un procedimento penale
Scopo	
accertamenti finalizzati a verificare una possibile minaccia per i fondamenti democratici e costituzionali della Svizzera o la libertà della sua popolazione strategico (osservazione a lungo termine)	accertamenti finalizzati a verificare l'effettivo compimento di un reato o di un atto preparatorio focalizzato sul singolo caso (reato specifico)
Risultato	
rapporto alle autorità politiche misure politiche o amministrative	esecuzione del procedimento da parte delle autorità penali (decreto d'abbandono, condanna o assoluzione) eventualmente con conseguente esecuzione della pena
Scambio d'informazioni	
scambio informale d'informazioni con i servizi d'informazione e di sicurezza stranieri	scambio formale con autorità giudiziarie e di polizia straniere
Vigilanza	
organi di protezione dei dati e autorità politiche	organi di protezione dei dati e autorità giudiziarie penali
Basi legali	
legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI)	legge sugli Uffici centrali (LUC) diritto penale federale e cantonale diritto di procedura penale federale e cantonale

1.1.6 Situazione in materia di sicurezza in Svizzera

Terrorismo

Analisi della situazione

Dagli attentati di Madrid (2004; attentato ai treni di pendolari) e di Londra (2005; attentati alla metropolitana e agli autobus) l'Europa occidentale non è più soltanto un'area di rifugio e di preparazione, ma è diventata anche l'area operativa del terrorismo islamico. Le minacce terroristiche in generale prendono di mira gli interessi occidentali, di cui, secondo i fondamentalisti islamici, fanno parte anche l'ONU o il CICR che hanno sede in Svizzera. L'attuale situazione è caratterizzata da cellule molto piccole (e quindi molto difficili da infiltrare) che agiscono in modo autonomo, in parte in maniera del tutto indipendente le une dalle altre, sono impenetrabili dall'esterno e non sono organizzate gerarchicamente. Queste cellule si servono con abilità dei moderni mezzi di comunicazione, sia per comunicare al loro interno, sia per diffondere l'ideologia e quindi radicalizzarsi. Questo vale in particolare per i mezzi tecnici legati a Internet. Inoltre gli autori dei reati vengono reclutati sempre più spesso fra i figli di immigrati stranieri, nati e cresciuti sul posto, che fino a quel momento non si erano distinti per attivismo ideologico, che conoscono perfettamente la situazione locale (e pertanto anche i punti deboli) e che suscitano l'impressione di essere ben integrati. Le conclusioni tratte dai procedimenti penali in Svizzera e le informazioni provenienti dai Paesi limitrofi dimostrano chiaramente che taluni sostenitori di Al Qaeda si servono della Svizzera. Le forze di sicurezza europee sono già più volte riuscite con anticipo a scoprire e a sventare i piani e i preparativi di attentati terroristici. Ad esempio impedendo l'attentato al mercatino di Natale di Strasburgo (2000), gli attentati suicidi sulle linee aeree transatlantiche dall'Inghilterra con l'uso di esplosivo liquido (2006) oppure scoprendo tempestivamente i piani segreti di attentati contro le istituzioni danesi da parte di un gruppo jihadista (2006).

Nel contesto degli sviluppi su scala internazionale sopra descritti, la situazione relativa alla sicurezza in Svizzera si è negli ultimi anni costantemente deteriorata ed è sensibilmente peggiorata. Gli attentati terroristici di matrice islamica sono sempre più probabili anche in Europa occidentale. Nel passato recente la Svizzera è stata risparmiata da attacchi terroristici. Tuttavia tale situazione può cambiare in qualsiasi momento. L'attuale situazione in Svizzera è in parte paragonabile alle circostanze che all'estero hanno portato all'esecuzione o al tentativo di attentati. La Svizzera quindi rientra nella zona di pericolo dell'Europa occidentale, essa è indicata dagli jihadisti tra gli Stati che partecipano alla crociata - motivo che legittimerebbe gli attentati - ed inoltre qui si trovano strutture islamiste attive, propense alla violenza e in parte tra loro collegate. Pertanto c'è fondamentalmente il potenziale per attentati terroristici. I mezzi attuali per scoprire informazioni, fondati principalmente su fonti pubbliche, non consentono di sapere quando e se si realizzeranno le minacce esistenti. In Svizzera sono stati scoperti anche islamisti che volevano partecipare come volontari alla Jihad in Iraq. In questo contesto la città di Ginevra serviva quale zona di passaggio e i volontari vi sono transitati dalla Svizzera occidentale e dalla vicina Francia.

In base alla valutazione odierna la Svizzera non rientra però tra i principali obiettivi del terrorismo islamico. Tuttavia, il pericolo di attacchi terroristici è elevato in tutta l'Europa e quindi anche la Svizzera risulta coinvolta alla stregua degli altri Stati dell'Europa occidentale. In questo contesto occorre osservare che la Svizzera valuta-

zione della situazione approfitta delle informazioni e delle competenze molto più ampie dei servizi di sicurezza esteri incaricati di fare ricerche. Una collaborazione insoddisfacente, dovuta a basi legali deficitarie, può rapidamente portare i partner stranieri a mostrarsi molto più restrittivi nel fornire informazioni alla Svizzera. La penuria di informazioni può comportare valutazioni erronee con le relative conseguenze nell'ambito delle misure da adottare.

Lacune riscontrate nel dispositivo preventivo di difesa

Senza violare la sfera privata non è possibile né individuare tempestivamente gruppi terroristici come quelli descritti né sorvegliarli o controllarli sufficientemente in altro modo.

In base al diritto in vigore il traffico postale e delle telecomunicazioni non può essere oggetto di chiarimenti per valutare la minaccia in base alla LMSI. Ne conseguono lacune nel riconoscimento tempestivo e nella collaborazione internazionale.

Le autorità italiane, dopo le esplorazioni radio in Italia delle cerchie islamiste di Milano, hanno ad esempio concluso che esse organizzavano e finanziavano la formazione di estremisti in Afghanistan per il tramite persone in Svizzera. Poiché non c'erano le premesse per avviare una procedura penale contro residenti in Svizzera, i servizi d'informazione italiani hanno contattato il SAP chiedendogli di chiarire l'ambiente delle persone sospettate. Il SAP non ha potuto condurre le ricerche richieste a livello internazionale, relative alla sfera privata di queste persone e del loro ambiente. La ragione risiede nel fatto che esso non può accedere a osservazioni nella sfera privata o alle informazioni che soggiacciono al segreto postale. Poiché non si potevano interpellare direttamente i sospettati per non pregiudicare le indagini italiane, queste persone sono rimaste in Svizzera senza essere indagate (in base al diritto in vigore è vietato anche l'uso di apparecchiature tecniche di sorveglianza nella sfera privata). Conclusione: le indagini dei servizi d'informazione sulle reti terroristiche o estremiste possono fermarsi alla frontiera con la Svizzera.

Un altro esempio è dato da tre cittadini turchi arrestati nel Liechtenstein nel dicembre del 2005. Sono stati accusati di sostenere finanziariamente e logisticamente un gruppo estremista turco responsabile di attentati suicidi a Istanbul. Dalle inchieste è emerso che gli accusati avevano compiuto numerosi viaggi in Svizzera, in particolare per visitare una determinata moschea. I dettagli relativi alla rete di contatti in Svizzera sarebbero stati di particolare interesse per scoprire i legami esistenti nel nostro Paese con i gruppi terroristici o con i loro simpatizzanti. Anche in questo caso la mancanza di accesso ai dati relativi alle telecomunicazioni ha impedito di svolgere i chiarimenti necessari.

I servizi europei di informazione interna quantificano all'80 per cento la quota attuale delle scoperte importanti per la lotta contro il terrorismo che deriva dalla sorveglianza preventiva delle comunicazioni.

Laddove manca questo tipo di comunicazione, le autorità di protezione dello Stato devono cercare informazioni entrando in contatto sotto copertura con i gruppi e le persone in questione, per cui è necessario utilizzare identità fittizie che oggi ancora mancano.

Un'ulteriore aggravante è la lacuna esistente nel settore di Internet. Le persone e le fazioni che minacciano la sicurezza interna della Svizzera, utilizzano ormai da tempo per scopi di propaganda, per diffondere il loro pensiero e per scambiarsi

reciprocamente informazioni le moderne infrastrutture informatiche e in particolare Internet.

Malgrado sia tecnicamente possibile, l'accesso ai settori protetti dalle password, in cui ad esempio è diffusa la propaganda jihadista, è vietato trattandosi di settori annoverabili nella sfera privata (art. 143bis CP Accesso indebito a un sistema per l'elaborazione di dati). Ciò vale anche se con molta probabilità si può dedurre che un sistema o una rete di dati vengono usati al fine di registrare dati per sé o per altri di tale entità da poter concretamente minacciare la sicurezza interna della Svizzera e che i sistemi si trovano all'estero. Non è quasi possibile eseguire accertamenti sulle situazioni di sospetto pertinenti senza aver accesso né ai dati grezzi dello scambio di e-mail criptato né ai forum radicali sui siti jihadisti.

Con la completa esclusione dalla ricerca preventiva d'informazioni in un mass-media divenuto oggi di centrale importanza, si deve mettere in conto una pericolosa lacuna nelle conoscenze.

Le carenze nei mezzi mettono la Svizzera in condizione di dipendenza dalle informazioni che provengono dall'estero. Pertanto le scoperte della radicalizzazione di parte della comunità della diaspora bosniaca/slava per mezzo di interpretazioni radicali del Corano si basano essenzialmente sulle informazioni ottenute dai servizi partner stranieri. Senza la richiesta d'assistenza giudiziaria dall'estero la Svizzera non avrebbe saputo della locale struttura che sosteneva un'organizzazione terroristica algerina. Una simile dipendenza dall'estero potrebbe rivelarsi fatale.

Spionaggio

Analisi della situazione

Da sempre taluni servizi segreti stranieri sono attivi in Svizzera o contro gli interessi svizzeri all'estero. Raccolgono informazioni di genere politico, economico e militare.

Riteniamo che occorra distinguere lo spionaggio politico e militare da quello economico. Contro quest'ultimo sono soprattutto le imprese a dover prendere le misure preventive adeguate.

La situazione è diversa per quanto riguarda lo spionaggio politico e militare. In questo caso sono da sempre indispensabili misure preventive appropriate dello Stato.

Va rilevato che, dopo l'entrata in vigore della LMSI, sono state scoperte meno spie, identificate meno strutture spionistiche e sventati meno atti di spionaggio rispetto al passato. Eppure l'impressione che la Svizzera non sia più interessata da questo fenomeno o lo sia soltanto marginalmente non è corretta. Il numero di agenti (presunti o identificati con certezza) dei servizi segreti che determinati Paesi inviano in Svizzera conferma implicitamente questo genere di attività. Certe rappresentanze straniere in Svizzera assumono personale addestrato per il servizio d'informazione. Gli «agenti» appartengono al personale dell'ambasciata, sono protetti dall'immunità diplomatica e sono formati per raccogliere anche informazioni per i servizi d'informazione utilizzando la propria copertura. Di regola all'inizio il sospetto scaturisce solo dalla valutazione della minaccia operata dai servizi d'informazione (p. es. sulla base di un avviso di un servizio d'informazione amico oppure perché una persona è stata identificata quale successore di un membro di un servizio d'informazione nemico). A ciò si aggiungono le ricerche effettuate da agenzie investigative private

attive su scala internazionale che agiscono frequentemente (con identità fittizia) per conto di un Governo.

Lacune riscontrate nel dispositivo preventivo di difesa

In base al diritto in vigore i luoghi che non sono liberamente accessibili (p. es. camere d'albergo) sono esclusi in virtù della LMSI da ogni accertamento sulle minacce. Ne consegue che le ricerche sulla sicurezza interna della Svizzera terminano letteralmente sulla porta d'entrata della sfera privata. Di conseguenza possono sorgere gravi lacune nel dispositivo di difesa.

Poiché la ricerca di informazioni dei servizi segreti, per esempio con incontri cospirativi, avviene in genere in ambienti privati e con particolari precauzioni, l'autorità di controspionaggio svizzero può nutrire solo un sospetto di minaccia. Avendo accesso solo agli spazi pubblici, essa può indagare unicamente sulle attività di cui sospetta senza poter però concretizzare il sospetto in una fattispecie rilevante a livello penale. Per aprire un'inchiesta penale inoltre non vi è ancora un sospetto di reato sufficiente (escludendo la problematica dell'immunità diplomatica che esclude il perseguimento penale). Pertanto rimangono aperte le questioni centrali: quali sono i contatti che la persona in oggetto intrattiene? Chi è la sua persona di contatto in Svizzera? Che cosa spia e perché? Che metodi impiega? Come si può muovere il controspionaggio?

Nei casi di spionaggio l'autorità di controspionaggio non può chiarire i sospetti senza accedere alla sfera privata; inoltre le persone prese di mira sono addestrate proprio a sfruttare i punti deboli della legislazione in vigore e a nascondere e a camuffare da professionisti le proprie attività. Senza identità fittizie solo eccezionalmente si possono condurre contro-operazioni; le scoperte importanti rilevanti per la sicurezza sfuggono alla Svizzera a causa delle contromisure che non può adottare.

Con le indagini sulle locali comunità di diaspora si è potuto ripetutamente constatare che le persone coinvolte tacevano per paura delle ritorsioni con cui esse o i loro parenti erano stati minacciati. Se si vuole spezzare l'omertà, gli accertamenti dei servizi d'informazione nella sfera privata sono indispensabili (le autorità penali hanno spesso le mani legate, poiché manca un sospetto di reato sufficiente).

Estremismo violento

Analisi della situazione

Per estremismo violento s'intendono attività 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, incoraggiano o approvano atti violenti (cfr. art. 8 cpv. 1 lett. c LMSI).

Le attività degli estremisti sono potenzialmente violente e possono minacciare la sicurezza interna di un Paese. Si tratta dunque d'individuare tempestivamente e di prevenire le possibili azioni violente delle organizzazioni estremiste.

In Svizzera, sia gli ambienti di estrema destra, sia quelli di estrema sinistra sono composti da numerosi piccoli gruppi, in parte collegati fra loro. Si stima che attualmente vi siano in Svizzera circa 1200 estremisti di destra, mentre negli ambienti di estrema sinistra si contano circa 2000 militanti. Anche i gruppi estremisti stranieri sfruttano il margine di manovra relativamente ampio offerto in Svizzera dai diritti fondamentali.

Lacune riscontrate nel dispositivo preventivo di difesa

Riteniamo che l'insieme delle leggi vigenti sia di per sé sufficiente per affrontare l'attuale situazione di minaccia. Fanno eccezione quei comportamenti indesiderati e potenzialmente pericolosi per la sicurezza interna della Svizzera di determinate persone o fazioni indesiderate che vanno impediti. Si pensi ad esempio alle collette di denaro effettuate dalle organizzazioni estremiste violente in Svizzera. Esse trasferiscono il denaro all'estero dove se ne perdono le tracce e dove non si ha alcuna certezza sul suo successivo impiego e non si può escludere che il denaro sia utilizzato per il finanziamento di attentati.

Commercio illecito di armi e materiale radioattivo e trasferimento illegale di tecnologie (proliferazione)

Analisi della situazione

Per proliferazione s'intende la diffusione di armi nucleari, chimiche e biologiche, dei loro vettori (p. es. missili) e di beni a duplice impiego civili e militari, necessari per la fabbricazione. La definizione comprende anche il trasferimento delle tecnologie necessarie.

La Svizzera è uno Stato firmatario di tutti gli accordi internazionali volti a impedire il trasferimento di armi di distruzione di massa e di tutti i trattati sul controllo degli armamenti.

Nel settore della proliferazione operano generalmente organizzazioni molto complesse, spesso attive su scala internazionale per cui nei singoli Paesi è solitamente possibile scoprirne soltanto alcune parti. Le contrattazioni e gli avvenimenti decisivi si svolgono con la massima discrezione in spazi privati. Spesso questo genere di affari comporta il pagamento di grosse somme di denaro, inducendo le persone coinvolte a una segretezza e prudenza ancora maggiori. In base all'esperienza, in una prima fase sussistono unicamente vaghi elementi che lasciano sospettare una minaccia alla sicurezza, ad esempio se una persona conosciuta nell'ambiente entra in Svizzera, senza che sia noto il vero motivo del viaggio oppure se quest'ultimo suscita dubbi o preoccupazioni. La scoperta della complessa organizzazione del dottor Abdul Qadeer Khan (padre della bomba atomica pachistana), specializzata nel trasferimento di tecnologia nucleare, non solo ha mostrato la struttura complessa e professionale di simili organizzazioni, ma anche che la Svizzera viene spesso implicata in simili trame e che la sua infrastruttura può essere e viene anche sapientemente sfruttata per attività di spionaggio. Inoltre l'interesse degli Stati a rischio di proliferazione nucleare è rivolto alla qualità svizzera in genere e in particolare ad alcune aziende del segmento hi-tech.

Un ulteriore esempio è dato dagli sforzi dell'Iran di arricchire l'uranio o dal programma nucleare della Corea del Nord. In relazione alla minaccia di bombe sporche (bombe dotate di un ordigno convenzionale con un'incamiciatura non convenzionale, per esempio radioattiva) i contrabbandieri hanno moltiplicato i loro sforzi in particolare in Europa, tanto che la quantità di materiale confiscato dalle autorità negli ultimi tre anni (2003–2006) è pari a quella dei precedenti sette anni.

Da parte di terzi il SAP riceve costantemente avvertimenti su probabili traffici di proliferazione di ditte svizzere. Gli indizi a disposizione tuttavia non possono confortare un sospetto di reato sufficiente per aprire una procedura penale a causa delle

possibilità troppo ristrette di ricercare le informazioni. In conclusione il SAP di fronte ad un reato deve accettare di avere un margine di manovra molto limitato.

Lacune riscontrate nel dispositivo preventivo di difesa

Se non può sorvegliare la sfera segreta o privata, esattamente come nel caso del terrorismo e dello spionaggio, il servizio d'informazione ha anche pochissime possibilità di verificare con successo i sospetti nel settore della proliferazione.

Generalmente, ad esempio, la vendita o l'acquisto di una macchina utensile non comporta un pericolo per la sicurezza interna o esterna. Tuttavia la situazione è diversa se si tratta di un acquisto segreto per lo sviluppo di armi di distruzione di massa (cosiddetti beni a duplice impiego). Anche in questo caso l'impossibilità di accedere allo spazio privato impedisce di approfondire le indagini, ovvero quando ci sono indizi che si svolgono attività di siffatta natura (p. es. sulla base di comunicazioni dei servizi d'informazione stranieri), ma non si ha un sospetto di rilevanza penale che suffraghi un'attività vietata. Questo è il caso, ad esempio, quando i servizi d'informazione stranieri avvertono la Svizzera dell'arrivo di un uomo d'affari, collegato con l'ambiente in cui si sviluppa un programma nucleare indesiderato all'estero. In questa circostanza sarebbe di massimo interesse conoscere i suoi contatti, i suoi partner in Svizzera e in particolare il vero fine del viaggio. Le basi giuridiche in vigore invece non permettono di approfondire le indagini su una simile situazione di sospetto.

Criminalità organizzata (CO)

Analisi della situazione

La criminalità organizzata è diffusa ovunque e a medio termine può diventare una delle minacce più gravi per la società, lo Stato e l'economia. Infatti il riciclaggio di denaro, la corruzione e l'acquisizione di società e immobili che si insinuano nel regolare mondo degli affari possono costituire una minaccia per la stabilità economica e politica. Tuttavia anche gli Stati stessi, la loro politica economica, la polizia e le autorità giudiziarie sono spesso gli obiettivi dell'infiltrazione della criminalità organizzata. Le attività principali dei gruppi criminali, in parte collegati fra loro, sono il traffico di stupefacenti, la tratta di esseri umani, il traffico d'armi, la corruzione, il ricatto e il riciclaggio di denaro che ne scaturisce. Suscitano inoltre preoccupazione i possibili contatti con gruppi terroristici.

Le economie nazionali altamente sviluppate e collegate fra loro offrono alle organizzazioni criminali molte possibilità di infiltrazione e di riciclaggio dei profitti.

Dispositivo di difesa

Riteniamo che con il potenziamento del MPC e della PGF avvenuto negli scorsi anni (Progetto Efficienza), si sia tenuto sufficientemente conto dell'attuale minaccia.

1.1.7 Cooperazione del servizio d'informazione e delle autorità di perseguimento penale

Le procedure secondo la LMSI e il CP non coincidono

Sia le investigazioni preventive dei servizi d'informazione sia le inchieste penali la cui finalità è repressiva cominciano in presenza di concreti elementi di sospetto. Per il lavoro dei servizi d'informazione si tratta del sospetto di una grave minaccia alla sicurezza della Svizzera o della sua popolazione, mentre per gli organi di perseguimento penale si tratta di sospettare un reato concreto.

Le ricerche in base alla LMSI hanno il fine di chiarire il sospetto di una possibile minaccia alla sicurezza della Svizzera o dei suoi abitanti dovuta a terrorismo, estremismo violento, spionaggio o proliferazione. Le investigazioni possono essere indotte sia da un comportamento in definitiva non punibile sia da comportamenti punibili. I risultati delle indagini sono trasmessi a coloro che prendono le decisioni politiche, ovvero agli organi esecutivi della Confederazione e dei Cantoni, affinché possano intervenire per tempo conformemente al diritto determinante oppure agli organi di perseguimento penale quando si conferma il sospetto di un reato.

La situazione è diversa per quanto riguarda il perseguimento penale (repressione). La ricerca delle informazioni serve in questo caso a chiarire un sospetto di reato e a valutare la colpevolezza dei singoli autori; essa si limita ai corrispettivi elementi costitutivi del reato. Gli organi di perseguimento penale presentano i risultati delle loro inchieste nelle procedure giudiziarie e non alle istanze politiche.

La verifica delle situazioni di minaccia secondo la LMSI si distingue quindi dalle indagini per gli atti penalmente rilevanti conformemente al CP. Le investigazioni si differenziano sia in base all'avvenimento che le ha provocate (da una parte sospetta minaccia alla sicurezza della Svizzera e dei suoi abitanti e dall'altra invece il sospetto che sia stato commesso un reato concreto), sia all'oggetto dell'investigazione (da una parte la scoperta di strutture e reti che rientrano nell'ambito di competenza della LMSI, dall'altra la prova di un comportamento che costituisce reato in base al CP) sia per lo scopo perseguito (da una parte fornire una base informativa su cui l'Esecutivo possa prendere misure e dall'altra verificare il sospetto di un reato o di una colpa individuale).

Vi sono punti in comune laddove gli accertamenti in ambito repressivo su un comportamento punibile si sovrappongono ad accertamenti in ambito preventivo concernenti minacce per la sicurezza nazionale, perché la persona sospettata o il presunto reato sono contemporaneamente oggetto di diversi generi di accertamenti in ambito preventivo. In altri termini è possibile che la stessa persona o lo stesso reato siano oggetto di accertamenti comuni anche se da prospettive diverse. Nel primo caso si tratta di confermare il sospetto di un reato concreto, nel secondo di effettuare accertamenti per valutare una minaccia per la sicurezza interna. Le due procedure possono dunque in parte completarsi, ma non sostituirsi.

Per chiarire i diversi punti di vista si prenda ad esempio un'organizzazione straniera di natura terroristica. Si sa che essa raccoglie fondi dai connazionali in Svizzera con metodi poco ortodossi. È stato anche constatato che le persone appartenenti a questa organizzazione viaggiano con regolarità all'estero portando con sé grosse quantità di denaro in contanti. Dal punto di vista penale non c'è alcuna prova concreta sull'impiego a fini criminali del denaro esportato. Di conseguenza manca il reato, ovvero l'elemento indispensabile per un procedimento penale, aspetto che esclude

qualsiasi condanna. Dal punto di vista del servizio d'informazione invece è evidente che il denaro in questione proviene dalle «collette» e serve a finanziare attentati terroristici o la guerra contro il loro Paese d'origine. Siccome la Svizzera non ammette la promozione di atti terroristici, questo comportamento non è accettabile. Sulla base delle informazioni del servizio segreto, l'Esecutivo ha il compito di decidere sugli ulteriori sviluppi, cioè sulle misure preventive da adottare (p. es. il divieto di collette di denaro a favore di certi partiti o cittadini stranieri).

La sicurezza interna della Svizzera può essere minacciata da atti non punibili e punibili

La prima condizione per gli accertamenti in base alla LMSI sono indizi su comportamenti o su sviluppi delle situazioni che comportano una minaccia per la sicurezza interna dovuta a terrorismo, estremismo violento, spionaggio o proliferazione.

Inoltre la sicurezza interna delle Svizzera può essere minacciata sia da atti non punibili sia da atti punibili. Ad esempio il regime iracheno di Saddam Hussein a suo tempo aveva minacciato, se fosse scoppiata la guerra, di far commettere attentati terroristici in tutto il mondo, sotto la protezione delle missioni diplomatiche dell'Iraq. Per la Svizzera non sussisteva alcuna prova concreta che si predisponessero reati, su cui poter investigare in un procedimento penale. Tuttavia rientrava sotto la responsabilità del governo svizzero valutare la situazione e prendere le misure per arginare i rischi di attentati sul proprio territorio o commessi partendo da esso. A questo scopo sono state necessarie e lo sono ancora le informazioni dei servizi segreti.

Quindi per valutare a livello di politica di sicurezza una situazione di minaccia, né l'impunibilità né la presunta punibilità di un certo comportamento sono i soli criteri determinanti.

La mancanza di mezzi del servizio d'informazione impedisce di sostenere meglio le autorità di perseguimento penale

La premessa per ogni attività delle autorità di perseguimento penale è l'iniziale sospetto di un reato. A livello federale per esempio si richiede per l'apertura di un'inchiesta che vi siano «sufficienti» indizi di reato (cfr. art. 101 cpv. 1 PP e art. 194 cpv. 1 n. 2, D-CPP).

Nella prassi le indagini dei servizi d'informazione sulle minacce alla sicurezza interna forniscono spesso indizi sulla presenza o la pianificazione di possibili reati, senza che vi sia tuttavia un sospetto rilevante di reato sul possibile giro degli autori o sul grado di avanzamento del piano in preparazione.

Ne consegue che il servizio d'informazione deve supporre la presenza di un reato, senza però disporre degli strumenti necessari per avvalorare gli indizi conosciuti a un sospetto di reato sufficiente. Le autorità penali da parte loro dispongono invece di strumenti sufficienti, ma non sono, a causa dei sospetti insufficienti, autorizzati a impiegarli in una simile costellazione.

Se si vogliono evitare simili lacune e procedimenti penali aperti per un sospetto di reato insufficiente, allora si devono creare possibilità di indagini approfondite per il riconoscimento tempestivo da parte del servizio d'informazione.

1.1.8 Valutazione dei rischi

Un certo rischio per la sicurezza

La LMSI disciplina la protezione preventiva dello Stato in Svizzera. La legge risente fortemente del cosiddetto «affare delle schedature» e conferisce una grande importanza alle questioni inerenti alla protezione dei dati nell'ambito dei servizi d'informazione. Si rinuncia sostanzialmente alla ricerca di informazioni che interferiscono nella sfera privata. L'accento è posto sui limiti della protezione dello Stato piuttosto che sulla protezione offerta alla popolazione. Questo approccio è stato menzionato espressamente anche nel messaggio.

«La legge prevede il trattamento delle informazioni preliminarmente al perseguimento penale soltanto in caso di assoluta necessità. Con questo modo d'agire la Confederazione accetta un certo rischio di sicurezza …» (messaggio concernente la LMSI, FF *1994* II 1007).

Con l'inasprimento della situazione di minaccia è da considerare che il rischio per la sicurezza allora tollerato è aumentato. L'esigenza di informazioni utili per il riconoscimento tempestivo non sono più soddisfatte già da molto tempo. Avevamo messo in rilievo le lacune nella lotta alle minacce terroristiche già nel rapporto approvato il 26 giugno 2002 presentato al Parlamento «Analisi della situazione attuale e dei rischi per la Svizzera dopo gli attacchi terroristici dell'11 settembre 2001».

Lacune riconosciute nel dispositivo preventivo di difesa

Le ricerche previste dalla LMSI devono permettere il riconoscimento tempestivo delle minacce alla sicurezza della Svizzera o dei suoi abitanti al fine, se possibile, di poterle prevenire. Il riconoscimento tempestivo tuttavia manca della strumentazione che gli permetterebbe di condurre ricerche approfondite nella sfera privata nei casi in cui vi sia ragion di causa.

Se le situazioni di minaccia non sono individuate o lo sono troppo tardi, le misure preventive possono essere attuate soltanto con ritardo o non possono più essere attuate.

Nella collaborazione con l'estero il dislivello eccessivo nella strumentazione per la sicurezza nazionale porta a standard molto differenti, fino a mettere in discussione la propria credibilità. Nel rapporto del Dipartimento di Stato degli USA «Country Reports on Terrorism 2006» si conclude tra l'altro riguardo alla Svizzera: «… however, law and practice continued to limit the scope of intelligence sharing and joint investigations …» (pag. 75). Esiste il pericolo che anche i servizi d'informazione amici diventino operativi sul suolo svizzero per garantire i propri interessi, cosa confermata già da parecchi casi.

Nessuna possibilità di sorveglianza strategica

Le minacce di matrice terroristica contro la sicurezza dello Stato si fondano generalmente su motivazioni politiche e ideologiche. Le convinzioni fondamentaliste e radicali non hanno la tendenza a scemare da sole poiché si chiudono di fronte a qualsiasi argomentazione e sono di durata imprecisa.

L'esperienza mostra che da queste situazioni di minaccia possono in qualsiasi momento scaturire azioni concrete che mettono in pericolo la sicurezza della Svizzera. I fattori che possono influire in queste situazioni spesso non sono ponderabili. In molti casi le opinioni estremistiche sono tramutate in estremismo violento e in

singoli casi sono addirittura stati commessi attentati. Non può essere escluso che un tale attentato si verifichi anche in Svizzera; il potenziale non manca e sono state manifestate intenzioni in questo senso.

Sono state ad esempio sequestrate sostanze chimiche a un cittadino svizzero simpatizzante per il terrorismo che avrebbero permesso la fabbricazione di diversi chilogrammi di esplosivo. Dopo la sospensione della procedura penale a causa della mancanza di prove giuridicamente tangibili, molti indizi permettono di concludere che le idee di questa persona si siano ulteriormente radicalizzate (senza mai varcare la soglia di un atto preparatorio punibile penalmente, motivo per cui non può seguire nessun perseguimento penale).

Un'irragionevole lassismo verso simili persone o fazioni rappresenta un rischio che la Svizzera non può permettersi. Si porrà sempre più spesso la domanda di sorvegliare a lungo termine le persone che, per esempio, sono state condannate penalmente per attività terroristiche, ma che hanno scontato la loro pena e sono di nuovo in libertà, oppure coloro che, per mancanza di prove, sono stati assolti da reati concretamente punibili, pur continuando a sostenere la propria ideologia orientata alla violenza e a non escludere atti di violenza.

C'è dunque necessità di basi legali per la sorveglianza da parte dei servizi d'informazione in Svizzera, tali da permettere che essa sia strategica, efficace a lungo termine, ma anche mirata, limitata alle necessità, giuridicamente e politicamente controllata.

Divieto di attività rilevanti per la sicurezza

Per la protezione della sicurezza interna alcune attività dovrebbero essere vietate. Specialmente l'incitamento alle attività terroristiche o all'estremismo violento si dovrebbero poter vietare, quando attentano concretamente alla sicurezza interna o esterna della Svizzera (p. es. vietare le collette di denaro in Svizzera per il finanziamento di una guerra o di un partito belligerante all'estero).

Tali divieti sono in base al diritto in vigore limitati e possibili solo in situazioni straordinarie di pericolo, in base all'articolo 184 capoverso 3 e all'articolo 185 capoverso 3 Cost. Tuttavia essi devono essere limitati nel tempo e non è possibile prolungarne più volte o in maniera indeterminata la validità, poiché non sarebbe conforme alla Costituzione. Per questo dev'essere creata una base giuridica ed essere delegata al DFGP la competenza decisionale nei casi di applicazione in base alla LMSI. Al contempo si potenzierà la protezione giuridica.

L'enumerazione esaustiva delle attività da vietare non è regolamentata, poiché i dettagli di un divieto che devono essere adattati ai casi particolari non si possono fissare con precisione. Inoltre ciò equivarrebbe a un avvicinamento al diritto penale e il Governo potrebbe garantire solo in modo insoddisfacente la propria responsabilità di mantenere la sicurezza interna. È imperativo che la persona o l'organizzazione coinvolta dopo l'inflizione di un divieto conosca i suoi doveri e prenda conoscenza dei suoi diritti. Questa situazione si può al meglio raggiungere quando gli obblighi da rispettare in ogni singolo caso vengono adeguati individualmente ai fatti da giudicare. La procedura proposta in questa sede permette di tener conto al meglio di questa esigenza.

Tale procedura permette di migliorare la prevenzione delle minacce, creando la possibilità sul piano giuridico di poter reagire rapidamente e direttamente di fronte al comportamento di persone o fazioni.

1.2 Soluzioni analizzate

1.2.1 Uso sistematico di tutte le possibilità del diritto penale e della protezione preventiva dello Stato

Le competenze legali attuali sono già largamente sfruttate, per quanto si possa influire su di esse a livello politico. Tuttavia pur interpretando e applicando il diritto attuale in modo più largo, non è possibile fornire alla sfera politica e all'Esecutivo le informazioni necessarie per colmare le lacune in materia di sicurezza. Si deve però scartare la strumentalizzazione politica del diritto penale per scopi preventivi. Non si possono condurre procedimenti penali per soddisfare il bisogno d'informazione della direzione politica o per la ricerca d'informazioni dei servizi segreti, per esempio riducendo i criteri legati all'apertura di tali procedure oppure aprendole su ordine degli organi preposti alla politica di sicurezza. L'indipendenza del perseguimento penale deve continuare a essere garantita anche se esso talvolta potrebbe fornire informazioni importanti per la salvaguardia della sicurezza interna. Le lacune esistenti nel riconoscimento tempestivo e nell'analisi della situazione non possono dunque essere colmate con queste informazioni.

1.2.2 Miglioramento del flusso delle informazioni e coordinamento tra repressione e prevenzione

Abbiamo già esaminato in maniera approfondita la collaborazione tra le autorità di perseguimento penale della Confederazione e il servizio interno d'informazione[32]. All'epoca non abbiamo riscontrato, in questo contesto, alcuna necessità di nuove misure legali.

1.2.3 Sviluppo del diritto penale formale e materiale

Abbiamo esaminato nell'ambito del nostro rapporto, che dava seguito al postulato 05.3006, in che misura fosse necessario legiferare al fine di combattere più efficacemente il terrorismo e la criminalità organizzata. Allora avevamo concluso che era prematuro prendere misure per legiferare. Sarebbe invece più idoneo aspettare prima le conclusioni delle sentenze ancora pendenti o ancora da trattare nonché i risultati della discussione parlamentare sul presente progetto di revisione LMSI.

1.2.4 Sviluppo della protezione preventiva dello Stato

Le lacune riscontrate gravano sul riconoscimento preventivo e sulla soppressione delle minacce e quindi in particolare sulla protezione preventiva dello Stato. La LMSI disciplina i compiti e i mezzi della protezione preventiva dello Stato e deve quindi essere migliorata. Inoltre anche in questo caso è possibile basarsi su un sistema collaudato dalle strutture già esistenti.

32 Rapporto relativo al postulato CPS.

Depongono a favore di un ampliamento della LMSI anche i punti seguenti:

- la prevenzione è uno strumento gestito dalla politica di sicurezza. Il potere politico, ossia il Governo, definisce il proprio fabbisogno di informazioni nel rispetto della legge e assegna i relativi compiti. Esso deve avere la possibilità di riconoscere tempestivamente le minacce su scala nazionale in materia di politica di sicurezza e di includerle nella valutazione politica della situazione. Infine il potere politico prende le decisioni in materia di politica di sicurezza, basandosi fra l'altro sulle informazioni delle autorità di sicurezza federali e cantonali, e se ne assume la responsabilità sul piano politico. Pertanto è corretto colmare in seno alla LMSI, sottoposta al controllo e alla vigilanza delle autorità politiche, le lacune riscontrate nel dispositivo preventivo di difesa;
- in base al diritto in vigore il riconoscimento tempestivo e la valutazione della situazione sono possibili solo in maniera limitata, poiché con la strumentazione attuale non si è in grado né di raccogliere sufficienti informazioni sugli avvenimenti nel Paese né di condurre osservazioni strategiche efficaci sui gruppi riconosciuti pericolosi;
- per combattere il terrorismo e le minacce simili, occorre utilizzare tutti i mezzi disponibili conformi alla legge, ossia applicare l'insieme degli strumenti sia repressivi che preventivi. Per individuare tempestivamente le minacce e sventare il pericolo, ossia per impedire gli attentati terroristici o di analoga natura, è necessaria innanzitutto la prevenzione e quindi il lavoro dei servizi d'informazione;
- la lotta alle azioni terroristiche dev'essere messa in atto con particolare anticipo, per poterle riconoscere e disinnescare ancora allo stadio di pianificazione e di preparazione. A questo scopo sono necessarie misure efficaci per l'osservazione delle persone e delle strutture pericolose nonché una collaborazione ottimale a livello internazionale. Spesso le informazioni fornite dai servizi d'informazione sono comunque estremamente importanti, anche dopo un attentato terroristico, come dimostrano gli esempi dall'estero dato che permettono d'identificare rapidamente gli autori;
- un gran divario fra gli strumenti di sicurezza dei vari servizi segreti nazionali comporta livelli di qualità differenti. Uniformando alcune funzioni del nostro servizio d'informazione a quelle di diversi Paesi limitrofi, intendiamo evitare che la Svizzera divenga un territorio meno sicuro;
- con l'ampliamento della LMSI si rafforza nel tempo la collaborazione internazionale;
- l'ampliamento della LMSI non mette in discussione i principi della procedura penale, che presuppongono un sospetto sufficientemente fondato per avviare le inchieste penali e un comportamento punibile precisamente descritto;
- il rafforzamento della prevenzione consente nel tempo di ottenere informazioni fondate e dettagliate sui settori sensibili della sicurezza, che in ultima analisi comprendono anche forme gravi di criminalità. Queste informazioni («intelligence») possono sostenere efficacemente gli organi preposti al perseguimento penale, consentendo loro di impiegare con efficacia le proprie risorse;

– grazie alle ricerche mirate dei servizi d'informazione e alle misure tempestive del caso si possono prevenire gravi reati, evitando procedure penali dispendiose e di conseguenza sgravando efficacemente le autorità di perseguimento penale.

1.2.5 Ulteriori progetti di legge

La legislazione nel settore della polizia e del perseguimento penale viene costantemente adeguata e rinnovata. Attualmente numerosi accordi internazionali, leggi e ordinanze sono in fase di realizzazione o di revisione. Tra questi progetti e il presente pacchetto legislativo non esistono connessioni dirette rilevanti.

In questo contesto citiamo soprattutto la revisione in corso del diritto federale di polizia (cfr. 06.3285, Interpellanza Banga, Sicurezza interna: ordinamento costituzionale e ripartizioni delle competenze tra Confederazione e Cantoni nel diritto in materia di polizia) nonché i lavori legislativi per la legge federale sui sistemi d'informazione di polizia della Confederazione (LSIP) e la legge federale sull'impiego della coercizione nell'ambito del diritto degli stranieri e dei trasporti di persone su mandato delle autorità federali (legge sull'impiego della coercizione, LICo) o ancora la creazione di una disposizione costituzionale relativa alla tifoseria violenta.

La presente revisione ha soprattutto lo scopo di migliorare la ricerca preventiva delle informazioni necessarie per valutare la situazione in materia di politica di sicurezza e le misure che ne scaturiscono nell'interesse della sicurezza interna e esterna.

L'adeguamento delle basi giuridiche per il Servizio informazioni strategico del DDPS è esaminato separatamente. Per il servizio d'informazione esterno vi sono esigenze nell'ambito giuridico essenzialmente differenti rispetto al servizio d'informazione interno, per questo nella presente revisione viene trattato solo un ambito del settore particolarmente importante per i due servizi (esplorazione radio strategica).

1.3 Le nuove norme richieste

La revisione della legge mira ad attuare le conclusioni tratte dagli interventi parlamentari presentati dopo l'11 settembre 2001 e dal rapporto approvato il 26 giugno 2002 all'attenzione del Parlamento e intitolato «Analisi della situazione attuale e dei rischi per la Svizzera dopo gli attacchi terroristici dell'11 settembre 2001».

Per raggiungere tale obiettivo l'insieme degli strumenti impiegati dai servizi d'informazione per raccogliere informazioni dovrà essere strutturato in modo ottimale, conformandolo agli standard europei. In casi specifici concernenti esclusivamente la prevenzione del terrorismo, dello spionaggio politico o militare e del commercio illegale di beni nel settore della proliferazione (diffusione di armi di distruzione di massa), le autorità e le unità amministrative della Confederazione e dei Cantoni potranno essere tenute a fornire informazioni circostanziate. Anche i trasportatori commerciali potranno essere tenuti a fornire informazioni alle stesse condizioni, purché siano richiesti dati che essi hanno già rilevato. È inoltre previsto l'impiego di strumenti per la ricerca speciale di informazioni, a condizioni molto severe. Sempre limitatamente ai settori del terrorismo, dello spionaggio politico o militare e della proliferazione, in caso di sospetto fondato saranno consentiti la sorveglianza della

corrispondenza postale e del traffico delle telecomunicazioni, l'osservazione in luoghi non liberamente accessibili, anche ricorrendo ad apparecchi tecnici di sorveglianza, nonché l'accesso segreto a sistemi per l'elaborazione dei dati.

L'impiego di mezzi speciali per la ricerca di informazioni è sottoposto a un doppio controllo: su incarico dell'Ufficio federale di polizia il Tribunale amministrativo federale deciderà se le misure sono legittime (procedura d'autorizzazione). Nell'ambito della decisione i capi del DFGP e del DDPS esamineranno in seguito la domanda dal punto di vista politico e decideranno di comune accordo le misure (procedura di decisione). Se il Tribunale amministrativo federale nega la legittimità delle misure, la procedura di decisione è annullata.

L'osservazione con mezzi speciali dev'essere comunicata successivamente alla persona in oggetto; fanno eccezione i singoli casi in cui prevalga un interesse pubblico preponderante o la sicurezza di terzi. Il Tribunale amministrativo federale o il capo del DFGP o del DDPS decidono sulle deroghe all'obbligo di comunicazione nel quadro della procedura d'approvazione o della procedura di decisione quando si tratta di ordinare i mezzi speciali per la ricerca di informazioni.

Il capo del DFGP deve avere le competenze di vietare a una persona, a un'organizzazione o a una fazione certe attività (p. es. le collette) che, in via diretta o indiretta, propugnino, appoggino o sostengano in altro modo operazioni terroristiche o di estremismo violento e che minaccino concretamente la sicurezza interna o esterna della Svizzera. Finora solo il Consiglio federale aveva la facoltà, in base alle sue competenze speciali sancite dalla Costituzione, di imporre un divieto temporaneo. Le persone coinvolte d'altra parte avranno il diritto di ricorso, che non potrebbero di principio esercitare contro le decisioni e ordinanze del Consiglio federale fondate direttamente sulla Costituzione.

È inoltre prevista una base legale formale per l'impiego di informatori e il tipo di indennità loro concesse (reddito esente da imposte e da contributi AVS); inoltre tali persone saranno protette in caso di necessità. Per proteggere gli informatori e i collaboratori del SAP durante la ricerca di informazioni viene estesa la possibilità già esistente per il Servizio informazioni strategico di impiegare identità fittizie anche al servizio d'informazione interno. Verrà poi disciplinata la descrizione della situazione da parte del Centro federale di situazione (che da tempo dà buoni risultati), mentre un'aggiunta nel settore dei controlli di sicurezza delle persone (il cosiddetto «*clearing*») garantisce ai cittadini svizzeri e agli stranieri domiciliati nel nostro Paese di poter collaborare anche in futuro a progetti classificati di Paesi stranieri.

1.4 Motivazione e valutazione della soluzione proposta

La situazione in materia di sicurezza e di pericolo negli ultimi anni in Svizzera è gradualmente peggiorata in particolare a causa degli sviluppi internazionali. Essa si è lentamente ma costantemente deteriorata, soprattutto in seguito alla crescente probabilità di attentati terroristici di matrice islamica. Con i mezzi per svolgere ricerche oggi a disposizione dei servizi d'informazione, non è più possibile riconoscere con tempestività e in modo adeguato l'evolversi di una situazione di pericolo. Esiste un pericoloso vuoto nel rilevamento delle informazioni. Se una situazione di pericolo non è rilevata o è rilevata troppo tardi (per quanto sia ancora possibile ad

esempio dopo un attentato terroristico), ciò comporta indugi nell'adottare le misure di prevenzione e con questo rischi per la popolazione.

Per avere misure di prevenzione tempestive è necessario migliorare la ricerca delle informazioni, per cui in alcuni casi possono rendersi indispensabili specifiche ingerenze nella sfera privata. La possibilità di ricorrere a simili deroghe ai diritti fondamentali dev'essere consentita quando vi siano indizi concreti di minacce gravi alla sicurezza interna della Svizzera e sotto il controllo giudiziario e la responsabilità politica del capo del DFGP. In altre parole l'attuale divieto generale di violare la sfera privata, istituito in base a una situazione di pericolo diversa da quella attuale, dev'essere sostituito da un divieto con riserva,. Si tratterebbe di un esiguo numero di casi, ma che potenzialmente potrebbero essere importanti.

Nella lotta contro il terrorismo e altri pericoli analoghi si devono impiegare tutti i mezzi a disposizione, cioè sia gli strumenti repressivi sia quelli preventivi. Per il riconoscimento tempestivo e la prevenzione dalle minacce, ovvero per impedire gli attentati terroristici o i pericoli della stessa portata, è necessaria la prevenzione e con essa il lavoro dei servizi d'informazione.

1.4.1 Risultati della procedura di consultazione

Tutti i Cantoni ad eccezione di Berna sono esplicitamente oppure sostanzialmente favorevoli all'avamprogetto. Tuttavia, una parte dei pareri è corredata di riserve nonché della richiesta di spiegazioni più approfondite sulla necessità della revisione.

Il Partito evangelico popolare e il Partito liberale approvano il progetto. È fondamentalmente positivo il giudizio del Partito popolare democratico. Il Partito liberale radicale sostiene l'orientamento della revisione della legge, ma chiede alcune modifiche e tematizza il bisogno di chiarire il problema della gestione e del coordinamento dei servizi d'informazione. Il progetto è respinto dall'Unione democratica di centro (neutralità invece di misure preventive di sorveglianza), dal Partito socialista (sufficienti mezzi di perseguimento penale e all'occorrenza ampliabili) e dai Verdi (contrari alle indagini preliminari senza sospetto di reato). Secondo il Tribunale federale si potrà valutare la proporzionalità delle misure nell'uso concreto che ne farà l'autorità e con le decisioni dei tribunali. Se ne deduce che il Tribunale federale ha giudicato le misure applicabili e conformi ai diritti fondamentali.

L'Associazione dei Comuni svizzeri e l'Unione delle Città svizzere sono favorevoli all'avamprogetto. Economiesuisse appoggia un adeguamento degli strumenti alla nuova situazione di minaccia e reputa indispensabile rafforzare i rimedi giuridici. Swiss Banking comprende le necessità delle misure proposte. L'Unione sindacale svizzera si pronuncia negativamente sul progetto (la legislazione vigente sarebbe sufficiente).

Molti pareri sono diametralmente opposti. Hanno espresso un parere negativo organizzazioni come Amnesty International (sufficienti i mezzi del diritto penale), le Giuriste e i Giuristi democratici svizzeri (inammissibile che aumenti la sorveglianza quando i sospetti diminuiscono) oppure gli Incaricati svizzeri della protezione dei dati (insufficienti garanzie del rispetto dei diritti fondamentali). Hanno invece approvato il progetto le organizzazioni di polizia come la Conferenza dei comandanti delle polizie cantonali della Svizzera, la Federazione svizzera dei funzionari di polizia oppure la Conferenza dei comandanti delle polizie delle città. Gli organi

preposti al perseguimento penale ritengono che vi sia ancora un potenziale di miglioramento nelle attuali strutture, pur ammettendo comunque la necessità di metodi di investigazione idonei. Essi ricordano inoltre la fondamentale importanza dei rimedi giuridici.

Le critiche si focalizzano sulla necessità stessa del progetto. Altre critiche di principio fanno il punto sulla mancanza di definizioni legali di terrorismo e di estremismo violento, sulle procedure d'esecuzione e di autorizzazione relative alla ricerca speciale di informazioni (p. es. poco chiari la procedura o il concetto di parere del Tribunale amministrativo federale e il suo effetto vincolante) e sulla protezione giuridica (p. es. la mancanza del potere d'esame del Tribunale amministrativo federale impedirebbe l'efficacia della procedura di ricorso).

Oggetto di critiche (piuttosto specifiche) sono la presentazione elettronica della situazione (p. es. si tratterebbe di una raccolta di dati in base alla legge sulla protezione dei dati), la regolamentazione a livello federale dell'ispezione dei dati della Confederazione da parte delle autorità cantonali di controllo (p. es. in disaccordo con l'autonomia d'organizzazione di Cantoni/Città/Comuni), il dovere d'informazione delle autorità e dei trasportatori professionali (p. es. non chiara la necessità di una regolamentazione non limitata temporalmente), la regolamentazione sugli informatori (p. es. sistema che non stimola i privati) nonché le identità fittizie (p. es. identità fittizie solo nei procedimenti penali), l'assoluta protezione delle fonti (p. es. nessuna protezione per gli informatori condannati o in malafede), i mezzi speciali di ricerca delle informazioni (p. es. verifica dell'estensione dell'ambito di validità all'estremismo violento e alla criminalità organizzata), l'obbligo di comunicare ulteriormente (p. es. necessità di chiarire il rapporto tra l'obbligo di comunicare ulteriormente e il diritto indiretto di essere informato), la procedura d'urgenza (p. es. garantire la distruzione dei dati già trasmessi all'estero nel caso in cui la misura non sia ulteriormente autorizzata), il divieto di attività (p. es. nessun divieto per le attività senza azioni rilevanti a livello penale).

1.4.2 Modifica dell'avamprogetto

Abbiamo preso conoscenza del risultato della procedura di consultazione il 4 aprile 2007 e abbiamo incaricato il DFGP di redigere il messaggio. Lo stesso giorno abbiamo approvato il principio di continuare il progetto.

Per l'elaborazione del messaggio è servito come base il progetto messo in consultazione, anche se si è tenuto largamente in conto delle principali obiezioni e delle proposte della consultazione.

I cambiamenti più importanti rispetto al progetto posto in consultazione sono:

- il riesame e l'approfondimento dell'argomentazione sulla necessità del progetto così come dei termini e delle procedure giudicate poco chiare, in particolare la procedura del Tribunale amministrativo federale e la procedura di decisione del Governo;
- il rafforzamento efficace della protezione giuridica con l'estensione del potere d'esame del Tribunale amministrativo federale;
- la rinuncia a una regolamentazione federale per permettere alle autorità cantonali di prendere visione dei dati della Confederazione;

– la rinuncia a una protezione completa delle fonti;
– l'organizzazione della presentazione elettronica della situazione come un insieme di dati in base alla legge sulla protezione dei dati;
– la definizione della forma scritta per garantire i dati dello Stato richiedente nelle procedure di clearing.

Per il momento si è rinunciato a uniformare la protezione delle fonti tra il SAP e il SIS. Durante la procedura di consultazione è stato espresso il timore che, sostituendo la protezione relativa delle fonti con una protezione assoluta, delatori malintenzionati avrebbero potuto nuocere alla reputazione di onesti cittadini rilasciando dichiarazioni false. Questo aspetto aveva del resto già allora attirato l'attenzione del legislatore che aveva rinunciato a una disposizione in tal senso, temendo che gli informatori avrebbero potuto commettere reati. Ciò che tuttavia conta maggiormente è che le disposizioni vigenti consentono già oggi al SAP un ampio margine di manovra per adeguare la protezione delle fonti alle esigenze del caso e prevengono i disaccordi con le autorità di vigilanza.

La possibilità di definire legalmente i termini di «terrorismo» e di «estremismo violento», come era stato richiesto da molti partecipanti alla consultazione, è stata a sua volta esaminata approfonditamente, prima di essere respinta principalmente per due motivi. Il primo è che già nell'ordinanza d'esecuzione (OMSI) è descritto che cosa si deve intendere per «attività terroristiche» («mene tendenti a influire o a modificare Stato e società da attuare o favorire commettendo o minacciando di commettere gravi reati nonché propagandando paura e timore») oppure per «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, incoraggiano o approvano atti violenti»). In altre parole esistono già definizioni precise delle attività di cui si dibatte e non si tratta dunque di concetti giuridici vaghi e indefiniti. In secondo luogo non esiste ad oggi una definizione esaustiva di terrorismo che sia riconosciuta a livello internazionale. Creando una definizione si anticiperebbero gli sviluppi delle normative internazionali, compromettendo la possibilità di adeguare la legislazione nazionale al diritto internazionale. Inoltre il disciplinamento a livello di ordinanza semplifica e snellisce i futuri adeguamenti agli ulteriori sviluppi del diritto internazionale. A ciò si aggiunga che la separazione tra combattenti per la libertà e terrorismo di Stato non è ancora sufficientemente chiara. La decisione quadro adottata dall'Unione europea (Decisione quadro 2002/475/GAI) stabilisce i reati terroristici e le sanzioni che gli Stati membri devono iscrivere nelle loro legislazioni nazionali. L'obiettivo è di adeguare la descrizione della fattispecie dei reati terroristici. Tuttavia ciò non influisce sul settore dei servizi d'informazione (prevenzione) bensì soltanto sul perseguimento penale (repressione).

Il testo di legge è infine stato rivisto a livello strutturale tenendo conto della revisione della LMSI relativa alle misure contro la propaganda violenta e contro la violenza in occasione di manifestazioni sportive.

1.5 Compatibilità tra i compiti e le finanze

La sicurezza ha un prezzo (USIS II, tesi strategica 10). I costi per un lavoro di prevenzione di successo tuttavia sono sempre molto più bassi del prezzo da pagare (morti, feriti, danni materiali, disorientamento della popolazione, ripercussioni sull'economia ecc.) se si realizzasse un rischio (p. es. un attentato terroristico). Nel confronto europeo, anche dopo l'ampliamento dell'effettivo di 40 posti (il SAP attualmente dispone di 140 posti di cui circa 90 nell'ambito di centrale importanza della protezione preventiva dello Stato secondo la LMSI) il numero di posti della protezione preventiva dello Stato è nettamente inferiore ai servizi dei Paesi comparabili (p. es. Austria, Belgio, Paesi Bassi, Danimarca, sia in termini assoluti (quantità totale di posti) sia percentuali (quantità di posti per ogni abitante). Grazie al suo radicamento nel sistema di polizia, la protezione preventiva dello Stato continua a trarre vantaggio delle ampie sinergie con il sistema di polizia svizzero.

Gli interessi e i valori in gioco giustificano nel complesso i costi correlati all'applicazione della revisione della legge.

1.6 Diritto comparato e rapporto con il diritto europeo

1.6.1 In generale

Non è possibile trasporre automaticamente in Svizzera le leggi straniere in vigore prima degli attacchi terroristici dell'11 settembre 2001 e quelle in seguito promulgate o inasprite, poiché le situazioni di minaccia, i sistemi politici e le esperienze dei singoli Paesi in relazione al terrorismo (p. es. ETA in Spagna) sono diversi.

L'aumento delle minacce terroristiche ha indotto in generale i servizi responsabili della sicurezza interna della comunità internazionale a intensificare la cooperazione. È stata riconosciuta la necessità di lottare uniti contro il terrorismo e di formalizzare la cooperazione internazionale in quest'ambito. Il «Counter Terrorist Group» istituito dal «Club de Berne» funge ad esempio da centro di contatto fra l'UE e i direttori dei servizi di sicurezza e d'informazione degli Stati membri.

All'inizio del 2003 e a metà del 2005, l'Istituto svizzero di diritto comparato (ISDC) ha confrontato le basi giuridiche sulla sicurezza interna degli Stati europei più importanti.

La legislazione di tutti i Paesi elencati di seguito è stata influenzata dagli attentati dell'11 settembre 2001 negli Stati Uniti.

Le strutture organizzative e le possibilità d'intervento politiche e giuridiche sono diverse in ogni Stato. Pertanto non è facile effettuare paragoni e trarne conclusioni chiare per la Svizzera. Le due seguenti tabelle illustrano in modo schematico le misure e le competenze previste dalla legislazione di alcuni Paesi nonché i relativi rimedi giuridici e i sistemi di controllo. Le spiegazioni dettagliate sono contenute nell'allegato 1. Se manca un'esplicita norma di legge non significa necessariamente che il Paese in questione non applichi una determinata misura. È probabile che il suo disciplinamento non sia ritenuto necessario oppure che la misura sia parte integrante di altre norme.

1.6.2 Confronto con l'estero

Misura	Repressione/perseguimento penale	Prevenzione
Esplorazione radio art. 14*a* D		Germania, Francia, Italia, Paesi Bassi
Indennità degli informatori art. 14*b* D	Francia, Italia	Italia, Francia
Protezione degli informatori art. 14*c* D	Austria, Germania, Francia, Italia	Austria, Germania, Francia, Paesi Bassi
Identità fittizie art. 14*d* D	Austria, Germania, Francia, Italia, Paesi Bassi	Austria, Germania, Francia, Paesi Bassi
Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni art. 18*k* D	Austria, Germania, Francia, Italia, Lussemburgo, Paesi Bassi	Germania, Francia (esclusa la corrispondenza postale), Italia, Lussemburgo, Paesi Bassi
Osservazione di spazi privati art. 18*l* D	Austria, Germania, Francia, Italia, Lussemburgo, Paesi Bassi	Austria, Germania, Francia, Italia, Paesi Bassi
Accesso segreto a un sistema per l'elaborazione di dati art. 18*m* D	Germania, Francia, Lussemburgo, Paesi Bassi	Francia, Paesi Bassi
Divieto per una persona o organizzazione di compiere determinate attività art. 18*n* D	Austria, Germania, Italia, Lussemburgo, Paesi Bassi	Francia, Germania, Austria

1.6.3 Rimedi giuridici e controlli da parte delle istituzioni nei Paesi stranieri

Paese	Controlli regolari	Controlli speciali
Germania	*In generale:* alta vigilanza dell'incaricato della protezione dei dati, controllo parlamentare, obbligo di denuncia al tribunale amministrativo.	*Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni:* richiesta del presidente o di un rappresentante dell'Ufficio federale di tutela della Costituzione, ordine del ministro dell'interno, organo di revisione: commissione G-10. Eccezioni: se vi è pericolo nel ritardo, esecuzione immediata e in seguito comunicazione alla commissione. *Identità fittizie:* previa approvazione del ministro dell'interno
Austria	Possibilità di ricorso dinanzi alla commissione per la protezione dei dati, al tribunale amministrativo o alla corte costituzionale.	*In generale:* controllo da parte dell'incaricato per i rimedi giuridici, controllo parlamentare, le autorità di sicurezza informano senza indugio il ministro dell'interno. *Inchieste mascherate e impiego sotto copertura di apparecchi per registrare immagini e suoni:* sotto la vigilanza dell'incaricato per i rimedi giuridici.

Paese	Controlli regolari	Controlli speciali
Francia	Richieste di consultazione alla «Commission nationale de l'information et des libértés» (CNIL)	*Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni:* richiesta del ministro della difesa, del ministro dell'interno, del ministro delle dogane o dei loro supplenti, ordine del primo ministro o di due persone da lui designate. *Organo di revisione:* «Commission nationale de contrôle des interceptions de sécurité» esterna all'amministrazione.
Italia	Il Governo presenta al Parlamento un resoconto semestrale delle attività dei servizi. Il Garante per la protezione dei dati personali controlla tutti i dati.	*Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni:* richiesta del presidente del consiglio dei ministri, approvazione del giudice, il presidente del consiglio può delegare le proprie competenze ai servizi, ordine della Procura di Stato. Se vi è pericolo nel ritardo, ordine immediato. Entro 24 ore dev'essere inoltrata al giudice per via ordinaria la richiesta del permesso. Entro 48 ore il giudice deve esprimersi in proposito.
Lussemburgo	Commissione parlamentare di controllo, il procuratore generale dello Stato o un suo rappresentante e due membri di una commissione speciale designati dal ministro dell'interno vigilano sul controllo dei dati. L'alta autorità di protezione dei dati (ANS) vigila sulla sicurezza dei dati classificati.	*Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni:* richiesta del Service de Renseignement D'Etat (SRDE) previa approvazione di una commissione speciale, ordine del direttore dei servizi di telecomunicazione che incarica della sorveglianza e del relativo controllo un servizio creato appositamente. La commissione parlamentare di controllo viene informata ogni sei mesi sulle misure di sorveglianza delle telecomunicazioni eseguite.
Paesi Bassi	Commissione di vigilanza, difensore civico indipendente, commissione parlamentare di vigilanza. *Identità fittizie:* è consentito aprire lettere di terzi se il tribunale distrettuale dell'Aja approva una richiesta in tal senso del direttore dei Servizi.	*Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni:* richiesta del direttore dell'AIVD e del MIVD, ordine del ministro dell'interno. Se vi è pericolo nel ritardo è consentita un'autorizzazione a posteriori, a condizione che venga posta la richiesta il prima possibile. *Osservazione:* in generale consentita l'osservazione previa approvazione scritta del ministro competente. Consentita l'osservazione in spazi privati, previa approvazione del ministro dell'interno o del direttore dei servizi.

1.6.4 Confronto con la Svizzera

Le strutture in materia di sicurezza e le possibilità d'intervento delle autorità di sicurezza previste dalla legge sono diverse da Stato a Stato. Eppure, dal paragone risulta che le misure preventive e i mezzi attualmente disponibili in Svizzera sono

notevolmente al di sotto delle possibilità ammesse in numerosi Paesi dell'Europa occidentale.

Tale situazione causa lacune pericolose, percettibili anche all'estero e, come è già avvenuto in diversi casi, può indurre le autorità straniere a procurarsi illegalmente informazioni sul territorio svizzero.

L'insufficiente capacità di rilevazione tempestiva nel proprio Paese e di cooperazione internazionale può inoltre ripercuotersi sulla Svizzera, poiché riduce la propensione allo scambio di informazioni, aspetto questo che potrebbe comportare un ulteriore indebolimento della prevenzione contro il terrorismo in Svizzera.

I recenti attentati dimostrano che le organizzazioni terroristiche vengono individuate troppo tardi se il lavoro di collaborazione si interrompe. I mezzi per la ricerca di informazioni di cui la Svizzera attualmente non può disporre a scopo preventivo hanno permesso di sventare svariati attacchi terroristici in passato. Nel 2000 fu ad esempio evitata una strage al mercatino di Natale di Strasburgo, nel 2003 fu scoperto a Londra un laboratorio che fabbricava ricino, una tossina naturale, lo stesso anno in Olanda fu individuata la rete di Hofstad, un'organizzazione di terroristi islamici, e in Germania fu impedito l'attentato progettato dal gruppo neonazista «Kameradschaft Süd» in occasione dell'inaugurazione del centro culturale ebreo.

La Svizzera deve essere in grado di avvicinarsi allo standard minimo degli Stati europei. Per il momento si rinuncia ad adottare misure ulteriori.

1.7 Applicazione

Le misure saranno attuate facendo quasi completamente ricorso alle strutture federali e cantonali esistenti (Tribunale amministrativo federale, SAP, Servizio per compiti speciali del DATEC, autorità cantonali di polizia e di sicurezza).

1.8 Interventi parlamentari

La mozione Burkhalter[33] chiede che al Parlamento vengano sottoposte le modifiche di legge necessarie per migliorare la lotta preventiva al terrorismo. Non è ancora possibile sapere in quale misura con il presente messaggio si risponde a tale richiesta, che non può essere stralciata, poiché la mozione è dibattuta e non è ancora stata discussa nelle Camere.

2 Spiegazioni dei singoli articoli

Struttura sistematica

Per l'attuale revisione della LMSI non è necessario modificare la struttura della legge. S'intendono infatti distinguere chiaramente i mezzi «generali» per la ricerca di informazioni attuali e che saranno mantenuti dai mezzi «speciali» per la ricerca di informazioni e dai presupposti per ordinarne l'impiego. Pertanto nella legge viene aggiunto il capitolo intitolato «Ricerca speciale di informazioni» suddiviso nelle due

33 04.3216 Mozione Burkhalter. Lotta al terrorismo. Misure preventive.

sezioni «Disposizioni generali» e «Mezzi speciali per la ricerca di informazioni». La prima sezione del nuovo capitolo sancisce i presupposti generali per ordinare l'impiego dei mezzi speciali per la ricerca di informazioni, la seconda sezione descrive i singoli mezzi, ossia: la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, l'osservazione in luoghi non liberamente accessibili (anche per mezzo di apparecchi tecnici di sorveglianza) e l'accesso segreto a un sistema per l'elaborazione di dati. A causa della nuova struttura è necessario spostare l'articolo 13*a* che è stato introdotto dalla cifra I della legge federale del 24 marzo 2006 (in vigore dal 1° gennaio 2007, cfr. la spiegazione dell'articolo 18*o*).

Art. 2 cpv. 4 lett. b^{bis} e b^{ter}

L'articolo 2 capoverso 4 della legge in vigore elenca tutte le misure preventive. L'elenco va integrato aggiungendovi i mezzi speciali per la ricerca di informazioni disciplinati nel capitolo 3*a* (lett. b^{bis}) e il divieto di attività di cui al capitolo 3*b* (lett. b^{ter}).

Art. 7 cpv. 2 terzo periodo

Conformemente all'articolo 7 capoverso 2 LMSI, i Cantoni adempiono in maniera indipendente i mandati secondo la presente legge. Qualora più Cantoni debbano cooperare o vi sia pericolo nel ritardo, l'Ufficio federale di polizia può assumere la direzione. Tale competenza viene ampliata per consentire all'Ufficio federale di polizia di coordinare lo scambio di informazioni se il suo intervento semplifica in maniera considerevole le attività della Confederazione e dei Cantoni. L'Ufficio federale di polizia assicura quindi lo scambio coordinato di informazioni fra le unità amministrative (cantonali) che continueranno come finora ad essere a loro volta competenti in materia. Il termine «coordinamento» pone l'accento sul carattere cooperativo dell'intervento. Il qualificativo «considerevole» specifica che dallo scambio reciproco di informazioni deve risultare un netto vantaggio. Il coordinamento assicurato dall'Ufficio federale di polizia, mira quindi a migliorare in maniera ragguardevole la resa informativa di tutti i servizi coinvolti. Si tratta peraltro di una disposizione potestativa; l'Ufficio federale di polizia non è obbligato a coordinare i lavori.

Interesse pubblico e proporzionalità

La crescente internazionalizzazione del terrorismo, dell'estremismo violento e dei loro militanti, rende sempre più difficile prevenire i rischi. È pertanto opportuno adeguare la funzione coordinatrice dell'Ufficio federale di polizia nello svolgimento delle funzioni attribuitegli dalla legge. Per individuare in tempo le eventuali minacce, è indispensabile una conoscenza approfondita delle fitte reti di contatti personali e degli eventi complessi, i quali hanno spesso carattere transfrontaliero. È indispensabile scambiare assiduamente informazioni con le autorità omologhe straniere. Il coordinamento proposto rispetta il principio di sussidiarietà sancito nella Costituzione e determinante per la ripartizione dei compiti tra Confederazione e Cantoni (cfr. il nuovo art. 5*a* Cost., che popolo e Cantoni hanno approvato nel novembre del 2004 la cui entrata in vigore è prevista per il 1° gennaio 2008).

Capitolo 3: Ricerca generale e trattamento delle informazioni

A causa della nuova struttura sistematica della legge, l'attuale sezione 3 («Trattamento delle informazioni») diventa il nuovo capitolo 3 intitolato «Ricerca generale e trattamento delle informazioni».

L'adeguamento del titolo del capitolo 3 permette di meglio delimitare la nozione di ricerca speciale di informazioni. Infatti, la «ricerca generale e il trattamento delle informazioni» corrisponde alla ricerca di informazioni ammessa attualmente, che si basa sull'assistenza amministrativa fra le autorità, non lede i diritti fondamentali e rispecchia la concezione di polizia preventiva su cui il legislatore si è basato nel 1997.

La presente revisione non modifica affatto il nucleo dell'attuale LMSI, ossia la parte che disciplina il trattamento delle informazioni. Le norme pertinenti conservano la loro validità e si applicano anche ai dati raccolti con l'ausilio di mezzi speciali per la ricerca di informazioni, purché il capitolo 3*a* non preveda espressamente altrimenti.

Art. 10a Descrizione della situazione

La disposizione disciplina un compito affidato già oggi agli organi di sicurezza della Confederazione (cfr. l'ordinanza sull'organizzazione del Dipartimento federale di giustizia e polizia[34], in particolare l'art. 9 cpv. 2 lett. a n. 2 nonché l'art. 15 cpv. 3 LMSI e l'art. 4 cpv. 2 lett. k dell'ordinanza ISIS[35]).

L'Ufficio federale di polizia ha il compito permanente di descrivere la situazione in materia di sicurezza interna. A tale scopo gestisce il Centro federale di situazione, che integra in una panoramica generale le informazioni rilevanti che riceve dai singoli settori della sicurezza interna (dai Cantoni e da altri servizi federali). In occasione di eventi particolari (p. es. grandi manifestazioni), il Centro federale di situazione fornisce inoltre un contributo decisivo alla gestione della rete dei servizi d'informazione nazionali. Per svolgere i propri compiti gestisce un sistema d'informazione elettronico. 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. Il sistema può contenere anche dati personali degni di particolare protezione, a condizione che siano indispensabili per la descrizione della situazione (cfr. art. 3 della legge federale del 19 giugno 1992[36] sulla protezione dei dati, LPD).

Art. 13, rubrica, nonché cpv. 3 e 4 Obbligo d'informazione generale delle autorità

L'inserimento dell'articolo 13*a* implica un adeguamento dell'articolo 13 per mettere maggiormente in rilievo la differenza tra le due tipologie di obbligo d'informazione.

Rubrica

La modifica del titolo dell'articolo 13, in particolare l'aggiunta della parola «generale» sottolinea che l'obbligo d'informazione si applica a tutti i compiti previsti dalla LMSI.

34 RS **172.213.1**
35 RS **120.3**
36 RS **235.1**

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. 13*a*), 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. 13*b*).

Art. 13a Obbligo d'informazione speciale delle autorità

A causa della modifica strutturale della legge il vigente articolo 13*a* LMSI (Messa al sicuro, sequestro e confisca di materiale di propaganda) diventa il nuovo articolo 18*o*. Lo spostamento all'interno della legge non comporta una modifica del contenuto (cfr. la spiegazione dell'art 18*o*).

Rispetto all'articolo 13, il *nuovo* articolo 13*a* 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, e 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

Questo capoverso istituisce un obbligo d'informazione in presenza di determinate minacce (cfr. lett. a–c) 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. Pericoli di questo tipo sono peculiarità tipiche del terrorismo, dello spionaggio politico o militare, del commercio illecito di armi o materiale radioattivo e del trasferimento illegale di tecnologia.

La disposizione sottopone di principio all'obbligo d'informazione tutte le autorità e le unità amministrative della Confederazione e dei Cantoni. Questa cerchia di autorità interessate si fonda sull'articolo 13 capoverso 3 LMSI e sull'ordinanza del 7 novembre 2001[37] 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 (terrorismo, 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. Anche l'Ufficio di comunicazione in materia di riciclaggio di denaro (MROS) o le autorità competenti per i documenti d'identità fanno ad esempio parte delle unità amministrative della Confederazione. Le unità amministrative dei Cantoni comprendono quelle dei Comuni; la nozione di «Cantone» si riferisce anche ad esse. Le organizza-

37 RS **120.1**

zioni che esercitano funzioni pubbliche sono, a loro volta, tenute a fornire informazioni. Secondo l'articolo 2 capoverso 4 della legge federale del 21 marzo 1997[38] sull'organizzazione del Governo e dell'Amministrazione (LOGA), si tratta di organizzazioni di diritto pubblico o privato che non fanno parte dell'Amministrazione federale cui sono attribuiti compiti amministrativi. Motivi pratici impediscono di elencare nella legge tutte le organizzazioni in questione, senza contare che un tale elenco risulterebbe alquanto limitativo perché non permetterebbe di reagire tempestivamente al rapido mutare delle circostanze. Si rinuncia pertanto 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 l'Ufficio federale di polizia o le autorità cantonali di sicurezza che agiscono su suo mandato, comunicando loro tuttavia soltanto le informazioni riguardanti determinati casi specifici e soltanto su speciale richiesta. La cerchia piuttosto ampia di autorità interessate appare giustificata alla luce dell'obbligo d'informazione soltanto in casi specifici e unicamente su minacce concrete.

Le informazioni raccolte presso le autorità e le organizzazioni vanno indirizzate all'Ufficio federale di polizia, che ne è il destinatario. Le autorità cui i Cantoni hanno affidato mansioni 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 dell'Ufficio federale di polizia. 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 e l'Ufficio federale di polizia, e non l'autorità cantonale che, su mandato dell'Ufficio federale di polizia, ha richiesto l'informazione contestata.

In occasione delle missioni all'estero, va garantita in particolar modo la sicurezza degli specialisti appartenenti al Pool svizzero di esperti per la promozione della pace e dei collaboratori messi a disposizione di organizzazioni umanitarie o che difendono i diritti dell'uomo. Eventuali clausole di riservatezza, codici di condotta particolari o procedure operative permanenti (Standing operating Procedures, SOP) vanno inoltre rispettati nel modo dovuto. Sono determinanti le circostanze specifiche del caso.

Cpv. 2

L'articolo 13*a* disciplina la soppressione del segreto d'ufficio. A questo proposito le assicurazioni sociali e le autorità fiscali hanno fatto notare che nel loro ambito non si tratterebbe soltanto di sopprimere il segreto d'ufficio, ma anche il segreto d'ufficio qualificato ed è quindi necessaria una norma specifica.

Nel settore delle assicurazioni sociali la trasmissione dei dati è disciplinata dettagliatamente nelle pertinenti leggi speciali e costituisce un ordinamento esaustivo a se stante. Di conseguenza, nelle pertinenti leggi speciali viene soppresso il segreto d'ufficio nei confronti delle autorità di sicurezza della Confederazione e dei Cantoni se le condizioni dell'articolo 13*a* sono adempiute. Le leggi speciali contengono già

[38] RS **172.010**

disposizioni 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 trasmissione dei dati non esiste un sistema paragonabile a quello utilizzato dalle assicurazioni sociali. Non esiste nemmeno una definizione esplicita di segreto fiscale (se ne trovano alcune definizioni nella letteratura , 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 Steuerbehörden[39]»). Oltre al segreto d'ufficio, il segreto fiscale protegge anche gli interessi privati (protezione della personalità). Tutto sommato è quindi giustificato tenere conto del segreto fiscale mediante una disposizione 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 a seconda del genere di imposta. In caso di parere favorevole dell'Ufficio federale e dell'autorità competente, è consentito trasmettere le informazioni senza ulteriori formalità. In caso di dissenso si applica la procedura prevista dall'articolo 13*b* (Controversie in merito all'obbligo d'informazione), il che significa che il Consiglio federale decide in via definitiva sulla trasmissione 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 informazione ai sensi dell'articolo 13*a* capoverso 4 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.

Cpv. 4

I servizi menzionati nel capoverso 1 che comprendono 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 13*a* 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 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

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

esterna. L'ordinanza è stata prorogata due volte e rimarrà in vigore fino al 31 dicembre 2008 (RU *2005* 5423).

In virtù dell'articolo 13 capoverso 3 LMSI, su cui si basa la suddetta ordinanza la validità delle relative ordinanze del Consiglio federale deve essere limitata nel tempo. Pertanto un'ordinanza che si basa su questa disposizione non può essere prorogata oltre un certo limite. La limitazione temporale sancita dal legislatore rende necessaria la trasposizione delle norme nel diritto ordinario, nel caso in cui le loro disposizioni debbano restare in vigore per un periodo più lungo. Occorre legiferare non appena si prospetta che le norme contenute nell'ordinanza sono indispensabili a lungo termine. Nel caso in questione questa condizione è soddisfatta.

Dopo gli attentati terroristici compiuti a Madrid nel 2004, la minaccia del terrorismo islamista nei confronti dell'Europa ha assunto nuove dimensioni nel luglio 2005[40]. 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 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 sono 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 non era sufficiente a rilevare l'impatto dell'ordinanza a livello cantonale, in particolare laddove l'ampliamento delle competenze ha agevolato i Cantoni nella verifica delle informazioni loro pervenute senza dover inviare una comunicazione apposita al SAP.

È inoltre stato appurato che l'ordinanza era ben nota agli organi di polizia, ma non altrettanto alle persone autorizzate o tenute a fornire informazioni. In occasione dell'ultima proroga, si è tenuto conto di tale circostanza diramando una circolare ad ampio raggio.

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

Tutto sommato, 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 le proprie responsabilità in seno alla comunità

40 Rapporto Sicurezza interna della Svizzera 2005.

internazionale per combattere il terrorismo). In altre parole, vi è un interesse pubblico preponderante a mantenere l'ordinanza, o meglio, a trasporla nel diritto «ordinario».

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

Art. 13b Controversie in merito all'obbligo d'informazione

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

Cpv. 1

Le divergenze d'opinione tra unità amministrative dell'Amministrazione federale centrale (cfr. art. 7 dell'ordinanza del 25 novembre 1998[41] sull'organizzazione del Governo e dell'Amministrazione [OLOGA]) sono risolte dall'autorità di vigilanza comune, ossia dal capo del Dipartimento che presenta l'istanza oppure dal Consiglio federale (cfr. art. 9 cpv. 3 della legge federale del 20 dicembre 1968[42] sulla procedura amministrativa [PA]). Se, ad esempio, sorge una controversia in merito a un'informazione che l'Ufficio federale di polizia richiede all'Ufficio federale della migrazione, la decisione spetterebbe al capo del DFGP.

Cpv. 2

In tutti gli altri casi, l'Ufficio federale di polizia può adire il Tribunale amministrativo federale chiedendo una decisione definitiva (cfr. la modifica proposta dell'art. 83 lett. d della legge del 17 giugno 2005[43] sul Tribunale amministrativo federale). L'Ufficio federale di polizia può procedere in questo modo anche quando l'informazione negata è stata richiesta da un organo di sicurezza cantonale. Dal momento che quest'ultimo opera su mandato della Confederazione, appare logico che la facoltà di rivolgersi al Tribunale amministrativo federale sia riservata all'Ufficio federale di polizia e non all'organo di sicurezza cantonale.

La procedura dinanzi al Tribunale amministrativo federale sostituisce la procedura dinanzi al Tribunale penale federale prevista dall'attuale articolo 13 capoverso 4. Conformemente al nuovo articolo 29*a*, al Tribunale amministrativo federale compete anche la composizione di altre controversie riguardanti il campo di applicazione della LMSI.

Le controversie in merito all'obbligo d'informazione possono sorgere tra autorità federali o cantonali, organizzazioni che esercitano funzioni pubbliche o servizi esterni all'Amministrazione federale decentralizzata (cfr. art. 8 OLOGA, p. es. il MPC).

Art. 13c Obbligo d'informazione dei trasportatori commerciali

Questo nuovo obbligo d'informazione è analogo a quello previsto dall'articolo 13*a* e si rivolge ai trasportatori commerciali. Per ragioni di proporzionalità la cerchia degli interessati è stata circoscritta ai trasportatori commerciali. La disposizione si applica,

41 RS **172.010.1**
42 RS **172.021**
43 RS **173.32**

ad esempio, alle imprese di taxi, alle compagnie aeree, alle società ferroviarie e di autonoleggio, ai trasportatori su strada, ecc. Analogamente all'obbligo d'informazione secondo l'articolo 13*a*, anche quello dei trasportatori commerciali è valido unicamente in relazione a determinate minacce, ossia: terrorismo, spionaggio politico o militare, commercio illecito di armi o di materiale radioattivo e trasferimento illegale di tecnologia.

Spesso è possibile ricostruire le attività delle persone che sono state riconosciute pericolose (p. es. spie, terroristi, ingegneri attivi nel settore della proliferazione), soltanto raccogliendo informazioni sui loro spostamenti (p. es. documenti sul noleggio di automobili ecc.). Questo vale anche per i 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 13*c* non li obbliga quindi a raccogliere 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 l'Ufficio federale di polizia o un organo di sicurezza cantonale che opera su suo mandato si rivolgono al trasportatore in un caso specifico concreto richiedendo un'informazione.

Interesse pubblico e proporzionalità

Secondo l'articolo 14 capoverso 2 lettera b LMSI, gli organi di sicurezza possono richiedere informazioni per adempiere i propri compiti. Talvolta le persone interpellate (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 (p. es. il personale di imprese fittizie straniere) o merci (p. es. il trasporto di materiale di proliferazione) oppure le informazioni sulla frequenza di tali spostamenti a permettere di verificare l'esattezza di certi indizi concreti. È indubbio che l'accesso a questo tipo di informazioni costituisce uno strumento adeguato e necessario per consentire all'Ufficio federale di polizia di adempiere il suo compito prevenendo con successo le minacce.

La proporzionalità della misura dipende dal grado di concretezza delle circostanze nel singolo caso. Come già affermato il presupposto essenziale per obbligare i trasportatori commerciali a fornire informazioni è che queste siano necessarie nel singolo caso per scoprire e sopprimere una minaccia concreta per la sicurezza interna o esterna della Svizzera nel campo d'applicazione della LMSI, descritto in precedenza. Va ricordato che in questo contesto chiaramente definito, i trasportatori sono tenuti a fornire unicamente le informazioni di cui sono già al corrente. Non sono obbligati a cercarne attivamente altre. Pertanto l'ingerenza nella sfera professionale non può essere considerata sproporzionata. Inoltre le informazioni non riguardano

nessun 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, come le strade, i treni ecc. Non si tratta quindi nemmeno di un'ingerenza sproporzionata nella sfera privata. Ciononostante in ogni singolo caso concreto si dovrà ponderare accuratamente e dettagliatamente, come in occasione di altre ingerenze nei diritti fondamentali, l'interesse pubblico e l'interesse privato (soprattutto la protezione della sfera privata) che vanno tutelati entrambi. In conclusione i trasportatori commerciali saranno tenuti a fornire soltanto le informazioni utili per scoprire e sopprimere le minacce di grande portata.

Art. 13d 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 (p. es. art. 321 CP[44], 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 13*d*. Di conseguenza un medico cantonale è ad esempio obbligato a fornire informazioni ai sensi dell'articolo 13*a* nell'esercizio delle proprie competenze ufficiali, ma non su quanto rientra nel segreto medico.

Art. 14 cpv. 3

L'articolo 14 LMSI elenca tutti i mezzi che sono attualmente consentiti per la ricerca di informazioni e che ingeriscono solo in minima parte nei diritti fondamentali. Questi mezzi conservano tutta la loro importanza e gli organi di sicurezza continueranno a cercare informazioni soprattutto con il loro aiuto, mentre i mezzi speciali elencati nel capitolo 3*a* saranno utilizzati soltanto a determinate condizioni e a titolo sussidiario.

Cpv. 3

La disposizione riveste grande importanza nella legge in vigore. Vieta di principio agli organi di sicurezza incaricati della prevenzione di adottare misure coercitive procedurali penali o di osservare fatti in ambienti privati. La revisione introduce però l'impiego di queste misure in ambito preventivo, vale a dire che, in casi eccezionali e nel rispetto di condizioni molto restrittive, sarà consentito cercare informazioni con l'ausilio di mezzi speciali. Se finora vigeva un divieto generalizzato, la revisione prevede ora un sistema di deroghe soggette ad autorizzazione. Sebbene i nuovi mezzi speciali non siano misure coercitive ai sensi della procedura penale, ma piuttosto mezzi per raccogliere informazioni segrete, la disposizione del capoverso 3 non è più necessaria ed è abrogata. La prevista ricerca speciale di informazioni è

44 RS **311.0**

tuttavia formulata in modo molto restrittivo ed è soggetta a controlli molto severi delle autorità esecutive e giudiziarie (cfr. le spiegazioni relative al capitolo 3*a*).

Art. 14a Esplorazione radio

Da decenni gli organi di sicurezza della Confederazione esplorano le emissioni radio di servizi segreti stranieri che possono essere connesse ad attività di spionaggio contro la Svizzera. Si tratta tuttora di emissioni a onde corte che non sono particolarmente protette contro l'intercettazione da parte di terzi (cfr. il rapporto del 2000 sulla protezione dello Stato, pag. 149 seg.). Al momento in cui è stata emanata la LMSI, tale attività è stata pertanto considerata una misura di ricerca nell'ambito dell'osservazione di fatti in luoghi pubblici e liberamente accessibili (art. 14 cpv. 2 lett. f LMSI).

Per esplorazione radio all'estero s'intende oggi il rilevamento di emissioni elettromagnetiche di sistemi di telecomunicazione provenienti dall'estero o trasmesse via satellite che si possono captare in Svizzera. Oggi queste emissioni si possono registrare con il sistema ONYX per quanto riguarda le comunicazioni trasmesse via satellite e con gli apparecchi in grado di captare le onde corte. Sarà lo sviluppo della tecnologia a determinare quali mezzi e sistemi si dovranno utilizzare in futuro per l'esplorazione radio. Con il termine generico di «esplorazione radio» il disegno di legge istituisce il margine di manovra necessario per rimanere al passo con gli sviluppi futuri in campo tecnologico.

Negli ultimi anni, il DDPS ha potenziato mediante il progetto ONYX le capacità di esplorazione delle comunicazioni internazionali trasmesse via satellite. Il sistema capta e valuta le emissioni dei satelliti trasmesse alla terra, che sono registrate e riutilizzate anche dai fornitori di servizi di telecomunicazione nel contesto delle loro attività commerciali. Dall'aprile del 2001, il SAP utilizza il sistema ONYX nell'ambito di una fase operativa di prova. La base giuridica è stata istituita con l'articolo 9*a* OMSI, che nell'ambito della presente revisione verrà integrato nella legge. Così si esaudisce anche una richiesta avanzata dalla Delegazione delle Commissioni della gestione, che chiede una base legale esplicita per l'impiego di ONYX. Viene inoltre modificata la legge militare affinché anche i servizi d'informazione del DDPS possano ricorrere all'esplorazione radio (cfr. le modifiche del diritto vigente, n. 3 art. 99 cpv. 1 e 1bis e art. 99*a* LM). In questo modo entrambi i servizi d'informazione dispongono nei rispettivi settori di competenza previsti dalla legge di basi legali formali che li autorizzano a servirsi dell'esplorazione radio.

Il nuovo articolo 14*a* LMSI corrisponde in larga misura alle attuali disposizioni dell'OMSI. In aggiunta contempla la possibilità di sorvegliare obiettivi nazionali alle condizioni e secondo la procedura prevista dai nuovi articoli 18*d* e 18*e*.

Cpv. 1

Questo capoverso fornisce la base all'attività esplorativa di fedpol, permettendogli di rilevare obiettivi esteri e di valutare le informazioni; definisce altresì il concetto di esplorazione radio, precisando che racchiude tutti i tipi di emissioni elettromagnetiche provenienti dall'estero. Alla luce del rapido sviluppo della tecnologia delle telecomunicazioni, limitare il raggio d'azione a determinate applicazioni tecniche, quali le onde corte oppure ONYX, non sarebbe opportuno né in termini materiali né sul piano giuridico.

Pertanto l'impiego di ONYX è retto da una base legale formale. Il SAP cerca autonomamente i dati nell'esercizio dei suoi compiti legali, mentre il DDPS è incaricato di rilevarli (cfr. le spiegazioni del cpv. 3).

Cpv. 3

La disposizione sancisce la prassi attuale della cooperazione tecnica tra i servizi federali, autorizzando l'Ufficio federale di polizia a cooperare con altre unità amministrative della Confederazione e dei Cantoni ai fini dell'esplorazione radio. fedpol gestisce direttamente soltanto pochi impianti d'intercettazione di onde corte e in sostanza funge da mandante autonomo della Divisione della guerra elettronica del DDPS. Ai sensi della presente disposizione, resta escluso il collegamento a una rete di ascolto straniera (p. es. ECHELON).

Cpv. 4

Il capoverso 4 garantisce che l'esplorazione radio permanente sia sempre controllata con gli strumenti previsti dagli articoli 99 e seguenti della legge militare (cfr. modifica del diritto vigente, n. 3, legge militare, in particolare l'art. 99*a*). Per evitare discrepanze rispetto all'esplorazione radio a favore dei servizi d'informazione del DDPS, l'esplorazione di obiettivi situati esclusivamente all'estero continuerà ad essere controllata dalla stessa autorità di vigilanza («Autorità di controllo indipendente»). Nel caso di eventuali obiettivi nazionali va tuttavia seguita la procedura di cui agli articoli 18*d* e 18*e* (cfr. quanto esposto più avanti), purché la misura o l'esplorazione radio riguardino telecomunicazioni soggette al segreto.

Interesse pubblico e proporzionalità

L'esplorazione radio è uno strumento per raccogliere informazioni provenienti da fonti in genere accessibili al pubblico. Chiunque sia provvisto dei mezzi adeguati può captare queste informazioni. L'esplorazione radio non costituisce pertanto né una grave ingerenza nella sfera privata in generale né una grave violazione del segreto delle telecomunicazioni in particolare. Talune forme di radiocomunicazione, che è possibile sorvegliare con l'esplorazione radio sono tuttavia soggette al segreto delle telecomunicazioni. In tal caso, l'esplorazione radio può ledere gravemente la sfera privata, e si applicano le disposizioni sulla ricerca speciale di informazioni, segnatamente l'articolo 18*k* che riguarda la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Altre considerazioni in merito si trovano nelle spiegazioni dell'articolo summenzionato.

Art. 14b Informatori

Per poter adempire i propri compiti, i servizi d'informazione 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 e valutazione di comunicazioni), ma non contiene disposizioni specifiche in merito al loro intervento, ai loro diritti e doveri o alle prestazioni da parte dello Stato. Tale situazione giuridica imprecisa va chiarita.

Cpv. 1

La disposizione autorizza esplicitamente l'Ufficio federale di polizia a servirsi di informatori. Si tratta di persone che collaborano su base volontaria con gli organi di

sicurezza, ma senza che sia stipulato un contratto di lavoro ai sensi dell'articolo 319 del Codice delle obbligazioni[45] (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 ad esempio un rapporto di subordinazione formale che porrebbe l'informatore alle dipendenze dell'Ufficio federale di polizia per quanto riguarda le disposizioni della legislazione sul personale, l'organizzazione e l'orario di lavoro. Una tale subordinazione non è assolutamente prevista.

Cpv. 2

È previsto il rimborso spese per evitare perdite finanziarie a chi, più o meno regolarmente, fornisce informazioni agli organi incaricati della protezione dello Stato. 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. Le ricompense modeste vengono concesse 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.

Cpv. 3

Il rapporto tra i servizi 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 dell'ufficio né annunciati alle assicurazioni sociali (nemmeno per indicare l'esonero dall'obbligo d'assicurazione). Per contro, il DFGP e la Delegazione delle Commissioni della gestione attualmente controllano già, in qualità di organi di controllo designati dalla LMSI, la legalità e l'opportunità dell'impiego di informatori. Il nuovo capoverso 3 specifica che eventuali indennità non sono soggette ad 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.

Art. 14c Protezione degli informatori

Questa disposizione è finalizzata a proteggere chi si espone a rischi per raccogliere informazioni utili allo scopo della LMSI. Vi sono due tipologie di informatori da proteggere: coloro che devono temere rappresaglie perché cooperano con i servizi

45 RS **220**

d'informazione di propria iniziativa e coloro che sono disposti a cooperare purché venga loro garantita un'adeguata protezione. Tale garanzia permette la ricerca delle informazioni necessarie ed evita che informatori importanti disposti a cooperare debbano essere «affidati» a servizi segreti stranieri in grado di assicurarne la protezione perché la Svizzera non ne ha la possibilità (come già accaduto più volte in Svizzera nel passato).

Chi coopera con i servizi d'informazione di propria iniziativa in certi casi si espone a rischi notevoli e deve temere ritorsioni, sia da parte delle cerchie che frequenta (p. es. se fa parte di gruppi violenti), sia da parte di Stati esteri (p. es. se in apparenza si è messo al servizio 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. In un rapporto dedicato all'unificazione della procedura penale, una commissione peritale della Confederazione ha ritenuto inopportuno introdurre nella procedura penale svizzera una normativa per la protezione dei pentiti. Lo stesso vale sul piano della prevenzione: è esclusa un'esenzione dalla pena sul modello della normativa sui pentiti sopra descritta. La prevenzione non pone l'accento sulla scoperta di precisi reati, che può essere agevolata 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, reati futuri.

Del resto la misura verrà verosimilmente impiegata soltanto in casi eccezionali alquanto rari dai quali si presume possano emergere informazioni di grande valore. È ad esempio ipotizzabile proteggere persone in grado di fornire informazioni importanti per prevenire gravi rischi alla sicurezza, quali notizie sulla progettazione e la programmazione di attacchi terroristici, su concrete attività di spionaggio rivolte contro la Svizzera o sulle organizzazioni che si servono della Svizzera per procurarsi armi di distruzione di massa. Per minimizzare il pericolo inerente a una collaborazione, a un primo contatto farebbero seguito vari colloqui esplorativi e, se le condizioni sono adempite, verrebbe stipulata una convenzione di protezione che stabilisce obblighi e diritti reciproci. Soltanto allora inizierebbe la collaborazione vera e propria. La misura non comporterebbe una protezione contro il perseguimento penale in Svizzera.

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 sono eseguite dall'Ufficio federale di polizia e 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.

L'Ufficio federale di polizia può eseguire direttamente le misure di protezione o finanziarle. Nella prassi, solo poche misure saranno necessarie e attuabili. Dal momento che la Svizzera, considerate le sue dimensioni, non è in grado di adottare misure di protezione complete per determinate minacce, sarebbe necessario in un caso del genere richiedere l'assistenza di autorità estere, quantificando quindi i costi. È inoltre ipotizzabile la concessione di 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

Le medesime considerazioni impongono che l'Ufficio federale di polizia possa altresì adottare misure per la protezione di persone prossime a un informatore, se la loro sicurezza dipende da tali provvedimenti. Il carattere potestativo della disposizione garantisce all'Ufficio federale di polizia 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. Tale misura, al contrario di quelle previste dai capoversi 1 e 2, viene adottata soltanto qualora l'Ufficio federale di polizia abbia interrotto i contatti con un informatore e non si serva più della fonte. Se la persona in questione è in grave pericolo per aver collaborato con l'Ufficio federale di polizia, quest'ultimo può proteggerla fornendole un'identità fittizia permanente. La persona è in seguito autorizzata a utilizzare tale identità seguendo le istruzioni dell'Ufficio federale di polizia. La creazione di un'identità fittizia presuppone l'approvazione del Tribunale amministrativo federale e l'autorizzazione del capo del Dipartimento (cfr. quanto illustrato qui di seguito).

Questa disposizione non disciplina tuttavia la ricerca di informazioni sotto copertura. Infatti, l'identità fittizia può essere impiegata per la ricerca di informazioni soltanto a determinate condizioni e seguendo l'apposita procedura (cfr. le spiegazioni dell'art. 14*d*).

Conformemente all'articolo 27 capoverso 1bis 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 in genere limitate nel tempo. Tuttavia, la legge non può indicare una durata definitiva, dal momento che vanno prese in considerazione le esigenze del 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.

Art. 14d Identità fittizie

Per adempire i propri compiti e proteggere i propri collaboratori, i servizi d'informazione e le autorità della polizia preventiva sono costrette a servirsi di identità fittizie quando cercano informazioni in determinati ambienti. Tali identità fittizie sono sempre create per lunghi periodi e raramente possono essere attribuite soltanto nel momento in cui si avviano le ricerche su un determinato caso. Il disciplinamento delle identità fittizie non rientra quindi nel settore dei mezzi speciali per la ricerca di informazioni, per il quale vigono condizioni molto restrittive (cfr. le spiegazioni sul cpv. 1).

Dal 1998 il Servizio informazioni strategico SIS ha 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 del 23 gennaio 2004 delle Commissioni della gestione e della Delegazione delle Commissioni della gestione delle Camere federali; FF *2004* 1435). Il controllo in merito è affidato al capo del DDPS e alla Giunta del Consiglio federale in materia di sicurezza.

Il capo del Dipartimento può autorizzare l'Ufficio federale di polizia a creare un'identità fittizia in un caso specifico. Prima di tutto, il Tribunale amministrativo federale (procedura di approvazione conformemente all'art. 18*d*) verifica la legittimità della misura, ossia esamina se vi sono le premesse legali per adottarla. Soltanto allora il capo del Dipartimento può valutare gli aspetti politici e, se del caso, dare il suo benestare.

Va peraltro sottolineato che i servizi d'informazione possono servirsi di identità fittizie unicamente per proteggere i collaboratori e raccogliere le informazioni. In tutti gli altri casi, l'impiego è vietato. Poiché la ricerca di informazioni in virtù della LMSI e le indagini penali sono due cose distinte, soprattutto per quanto riguarda il motivo per cui vengono avviate, i fatti su cui si concentrano e gli obiettivi perseguiti, non è possibile ricorrere alle misure di sorveglianza previste dal diritto di procedura penale.

Cpv. 1

Il presente capoverso pone le basi dell'impiego di identità fittizie per raccogliere informazioni e garantire la sicurezza degli informatori. Va segnalato innanzitutto che le identità fittizie sono di norma utilizzate nell'ambito della ricerca generale di informazioni, ossia di misure ai sensi dell'articolo 14 capoverso 2 LMSI. Se, per contro, l'uso di un'identità fittizia è richiesto nel corso di una ricerca di informazioni con l'ausilio di mezzi speciali (p. es. l'osservazione in luoghi non liberamente accessibili, anche ricorrendo a un'identità fittizia), per ordinare la misura si applicano le procedure di cui agli articoli 18*a* e seguenti. Il capoverso 1 elenca in modo esaustivo le persone a cui può essere fornita un'identità fittizia.

Lettere a e b. Gli organi di sicurezza designati dalla LMSI mantengono uno stretto contatto con le forze di polizia svizzere e possono svolgere gran parte della loro attività di ricerca alla luce del sole in qualità di membri delle forze di polizia. Talvolta è tuttavia necessario poter instaurare dei contatti agendo sotto copertura, segnatamente nell'ambiente terroristico e spionistico. Tali misure servono anche a proteggere i collaboratori degli organi di sicurezza e i loro familiari.

Lettera c. Anche gli informatori possono servirsi 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 loro autorità di vigilanza. Ecco perché, in questi casi, l'impiego di identità fittizie sarà limitato nello spazio e nel tempo e sarà concesso soltanto per determinate operazioni.

Creare un'identità fittizia comprende il diritto di servirsene per concludere negozi giuridici e, in particolare, per costituire reti di contatti fittizie. Le persone provviste di un'identità fittizia hanno piena personalità giuridica e possono stipulare contratti (p. es. affittare locali e veicoli o collegamenti di telecomunicazione, 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 meglio controllare i rischi inerenti all'uso di un'identità fittizia, conviene limitare il tempo in cui essa può essere impiegata. Tale precauzione si impone in particolar modo per gli informatori che non sono impiegati dell'Ufficio federale di polizia e che quindi sfuggono al suo potere disciplinare. La limitazione significa che l'autorizzazione va concessa finché è necessaria, ma non oltre un certo limite. Se allo scadere del termine e di una sua eventuale proroga, l'identità fittizia è ancora necessaria, bisogna presentare una nuova richiesta.

Cpv. 3

Il capoverso 3 precisa che l'identità fittizia può essere usata soltanto per gli scopi perseguiti dalla LMSI. Va inoltre rilevato che, in virtù dell'articolo 27 capoverso 1bis lettera a 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.

Art. 15 cpv. 6

La disposizione si fonda sulla normativa relativa alla precedente Polizia federale, a cui erano affidati compiti di repressione e di prevenzione. La separazione di questi due compiti e della loro realizzazione sul piano organizzativo ha reso obsoleta tale disposizione. Secondo il diritto e la concezione attuali, la trasmissione delle informazioni dalla repressione alla 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 sia d'ora in avanti escluso.

Art. 17 cpv. 3 lett. e

Cpv. 3 lett. e

Il cosiddetto clearing è un compito che il SAP esegue da tempo nelle relazioni con l'estero. Su richiesta di un servizio straniero, il SAP effettua controlli di sicurezza relativi a cittadini svizzeri o a cittadini stranieri residenti in Svizzera, allo scopo di

permettere la loro collaborazione a progetti (o impieghi) 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, il SAP per eseguire il clearing 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. È una misura necessaria affinché anche i servizi dell'Ufficio federale di polizia che effettuano il clearing possano essere presi in considerazione nell'ambito del progetto legislativo preparato dall'Ufficio federale di giustizia per un nuovo disciplinamento dei diritti d'accesso dell'Ufficio federale di polizia a VOSTRA (casellario giudiziale informatizzato). Infatti, sotto il profilo della protezione dei dati, l'accesso dell'Ufficio federale di polizia a VOSTRA per scopi di clearing richiede anche un'esplicita base legale negli articoli 365 e seguenti CP. La presente modifica della LMSI crea pertanto le premesse per un futuro disciplinamento preciso dell'accesso ai dati del casellario giudiziale informatizzato. Gli estratti del casellario giudiziale costituiscono un elemento di valutazione importante per il clearing. Senza di essi, il clearing effettuato dal SAP per conto di uno Stato estero risulterebbe di minor valore. Ne subirebbe le conseguenze la persona in questione, che probabilmente, anche in caso di un esito positivo del clearing, non verrebbe ritenuta abbastanza fidata da poter cooperare a progetti segreti o confidenziali all'estero.

Capitolo 3*a*: Ricerca speciale di informazioni

Il capitolo 3*a* racchiude le disposizioni sostanziali della revisione. Esse permettono agli organi di sicurezza di impiegare in futuro mezzi speciali per raccogliere informazioni a titolo preventivo.

Il titolo del capitolo riflette il concetto fondamentale alla base di questo tipo di ricerca. La ricerca speciale di informazioni si distingue da quella effettuata con i mezzi generali indicati al capitolo 3 e avviene con l'ausilio di mezzi speciali il cui utilizzo non è sempre consentito e lo è soltanto durante un periodo limitato.

Il capitolo 3*a* si suddivide in due sezioni: la prima contiene le disposizioni generali che disciplinano l'impiego della ricerca speciale di informazioni, la seconda illustra i mezzi speciali da utilizzare per la ricerca.

Art. 18a Principio

Cpv. 1

Lo scopo della ricerca speciale di informazioni è la scoperta o la soppressione di una minaccia concreta per la sicurezza interna o esterna della Svizzera. Conformemente all'articolo 18*b* del presente disegno di legge, prima di impiegare i mezzi speciali per la ricerca di informazioni, gli organi di sicurezza devono nutrire il sospetto che una determinata persona, organizzazione o fazione minacci la sicurezza (cfr. DTF *109* Ia 273, 288–289, secondo cui la sorveglianza non deve servire a confermare un sospetto).

Le minacce la cui soppressione giustifica l'impiego di mezzi speciali per la ricerca di informazioni sono: il terrorismo, lo spionaggio politico o militare, il commercio illecito di armi o materiale radioattivo oppure il trasferimento illegale di tecnologia. Contrariamente a quanto richiesto da diversi partecipanti alla procedura di consultazione, si è rinunciato a estendere il campo d'applicazione all'estremismo violento, allo spionaggio economico e alla criminalità organizzata. Riteniamo che, per quanto riguarda la lotta alla criminalità organizzata, sia necessario attendere innanzitutto i risultati del Progetto Efficienza.

Cpv. 2

Il capoverso 2 elenca in modo esaustivo i mezzi speciali per la ricerca di informazioni. Non possono quindi essere impiegati altri mezzi.

Art. 18b Condizioni

L'impiego di mezzi speciali per la ricerca di informazioni presuppone l'adempimento cumulativo di cinque condizioni.

Le prime quattro condizioni sono di tipo materiale e adempiono quanto previsto dall'articolo 36 Cost. Dapprima sono definiti l'interesse pubblico e le circostanze che giustificano la restrizione dei diritti fondamentali nel caso specifico (lett. a), poi vengono indicati i vari aspetti del principio della proporzionalità (lett. b–d).

Il concetto di interesse pubblico comprende la salvaguardia della sicurezza interna ed esterna della Svizzera come pure la protezione dei collaboratori dell'Ufficio federale di polizia da persone, organizzazioni o fazioni sospettate di costituire una minaccia per la sicurezza interna o esterna della Svizzera. Queste persone, organizzazioni o fazioni sono definiti presunti autori della minaccia; cfr. lettera a.

Soprattutto l'aspetto della protezione non è da sottovalutare. I collaboratori dell'Ufficio federale di polizia (compresi gli informatori) si espongono a rischi elevati, in particolare quando svolgono operazioni per la ricerca di informazioni. In caso di comprovata necessità, dev'essere pertanto possibile adottare misure cautelari per proteggerli. Si tratta normalmente di assistere queste persone durante il loro intervento e di portarle tempestivamente al sicuro in caso di pericolo (p. es. se vengono smascherate).

Il principio di proporzionalità impone, per quanto possibile, una distinzione tra le componenti di fondo: l'adeguatezza del mezzo impiegato per raggiungere lo scopo perseguito nell'interesse pubblico (lett. d *in initio*), la necessità (lett. c e d *in fine*) se tutti i mezzi convenzionali si sono rivelati inefficaci e la proporzionalità in senso stretto (lett. b) allorché prevale l'interesse pubblico e giustifica l'ingerenza nei diritti della persona in questione.

Art. 18c Sorveglianza di terzi e tutela del segreto professionale

Cpv. 1

La disposizione disciplina il coinvolgimento indiretto di terzi. È ipotizzabile che il presunto autore della minaccia, sorvegliato con l'ausilio di mezzi speciali per la ricerca di informazioni, si serva di mezzi di comunicazione o di luoghi che appartengono a un terzo invece che a lui, ad esempio un apparecchio telefonico o un sistema informatico privato. È senz'altro possibile che il terzo sia all'oscuro dell'uso

dei suoi mezzi e dei suoi locali; tuttavia, è indispensabile che questi possano essere posti sotto sorveglianza.

Dalla disposizione risulta inequivocabilmente che l'obiettivo della sorveglianza è l'ambiente del terzo, e non il terzo stesso, a meno che non venga anch'egli considerato un presunto autore della minaccia.

Cpv. 2

Questa disposizione non si applica esclusivamente a terze persone, ma disciplina qualsiasi coinvolgimento diretto o indiretto di una persona vincolata dal segreto professionale. La disposizione ha lo scopo di tutelare al meglio ogni tipo di segreto professionale. Pertanto essa si applica sia ai terzi il cui ambiente è sorvegliato conformemente al capoverso 1, sia alle persone sorvegliate con l'ausilio di mezzi speciali per la ricerca di informazioni. Il testo richiama l'articolo 4 capoverso 6 della legge federale del 6 ottobre 2000[46] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT). Secondo la giurisprudenza della Corte europea dei diritti dell'uomo (decisione Kopp vs Confederazione Svizzera, 25 marzo 1998), la selezione dei risultati della sorveglianza dev'essere controllata da un'autorità giudiziaria. Questa sentenza che verte su un procedimento penale può essere applicata alla prevenzione. Appare pertanto opportuno affidare tale compito al Tribunale amministrativo federale (cfr. il messaggio del 1° luglio 1998 concernente la legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni e la legge federale sull'inchiesta mascherata (FF *1998* 3319).

Le persone vincolate dal segreto professionale ai sensi dell'articolo 321 CP sono: gli ecclesiastici, gli avvocati, i difensori, i notai, i revisori tenuti al segreto professionale in virtù del Codice delle obbligazioni, i medici, i dentisti, i farmacisti, le levatrici, come pure gli ausiliari di questi professionisti per quanto riguarda i fatti loro confidati per ragione della loro professione o di cui hanno avuto notizia nell'esercizio della medesima. L'articolo 321 CP non si applica ad esempio ai detentori di segreti ai sensi dell'articolo 47 della legge dell'8 novembre 1934[47] sulle banche (LBCR). In questo caso, analogamente alla procedura penale, una protezione particolare non è giustificata, perché l'impiego di mezzi speciali per la ricerca di informazioni dev'essere autorizzato dal Tribunale amministrativo federale e dai capi del DFGP e del DDPS, i quali possono tenere conto di eventuali interessi da proteggere. Inoltre una banca non è tenuta a fornire spontaneamente informazioni (in questo modo rispetta il segreto bancario) e qui si tratta unicamente di stabilire se un giudice del Tribunale amministrativo federale debba controllare la selezione dei dati raccolti durante una sorveglianza. L'articolo 47 LBCR obbliga peraltro tutti gli organi e gli impiegati di una banca a mantenere il segreto e quindi una deroga per una categoria così ampia non sarebbe opportuna.

Art. 18d Procedura di approvazione

L'impiego di mezzi speciali per la ricerca di informazioni lede i diritti fondamentali, in particolare il diritto al rispetto della vita privata garantito dall'articolo 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[48] (CEDU) e dall'articolo 13 della Costituzione federale. Inoltre, la natura della ricerca

46 RS **780.1**
47 RS **952.0**
48 RS **0.101**

speciale non consente a una persona sorvegliata di opporsi alla misura finché questa perdura. È quindi indispensabile che l'applicazione delle pertinenti disposizioni normative sia disciplinata con la massima precisione possibile e che il loro rispetto sia controllato rigorosamente.

Il controllo è duplice e scaglionato nel tempo. Le persone oggetto di una ricerca di informazioni con l'ausilio di mezzi speciali devono esserne informate al termine dell'operazione; possono impugnare la misura mediante ricorso dinanzi al Tribunale amministrativo federale (verifica *ex post*). L'obbligo di rivelare alle persone interessate *ex post* l'avvenuta ricerca speciale di informazioni e i rimedi giuridici è disciplinato nell'articolo 18*i* (Obbligo di comunicazione) e nell'articolo 29*a* (Rimedi giuridici).

Ma questo non è sufficiente. Infatti i diritti fondamentali sono già stati lesi quando giunge la comunicazione *ex post*. Oltretutto, a determinate condizioni la legge ammette di rinunciare alla comunicazione (in via temporanea o definitiva, cfr. art. 18*i* cpv. 2 del presente disegno di legge). Alla verifica *ex post* va pertanto abbinata una verifica *ex ante* di modo che già nel momento in cui viene richiesto l'impiego di mezzi speciali per la ricerca di informazioni sia effettuata una verifica altrettanto severa di quella che viene eseguita durante una procedura di ricorso.

Per le misure in ambito penale, la legge prevede di norma la verifica di un'istanza giudiziaria dopo che è stato ordinato un provvedimento. Dal momento che la ricerca speciale di informazioni a titolo preventivo costituisce una lesione analoga dei diritti fondamentali, non si giustifica la rinuncia alla verifica da parte di un'istanza giudiziaria. Nella sua decisione di principio del 1983 (DTF *109* Ia 273), il Tribunale federale ha stabilito che gli abusi perpetrati nel settore della prevenzione rischiano di danneggiare l'ordine democratico liberale molto di più di quanto non faccia la sorveglianza repressiva. Sorge quindi la domanda se la verifica preliminare di una misura preventiva pianificata vada considerata un appannaggio delle autorità giudiziarie o se possa essere affidata a un ente paragiudiziale, a condizione che quest'ultimo non faccia parte dell'Amministrazione.

La risposta della Corte europea dei diritti dell'uomo (Corte eur. DU) e del Tribunale federale non sono del tutto identiche: la Corte eur. DU ha stabilito che basta una verifica paragiudiziale, ma il Tribunale federale sembra prediligere una verifica da parte di un'istanza giudiziaria ufficiale.

Nella decisione Klass vs Repubblica Federale di Germania del 6 settembre 1978, la Corte eur. DU ha stabilito che, per quanto attiene alla sorveglianza preventiva, la legge tedesca in materia soddisfa i requisiti dell'articolo 8 capoverso 2 CEDU. La legge prevede che la sorveglianza telefonica vada prima autorizzata da un comitato indipendente composto da tre membri nominati da una commissione parlamentare. La legge presuppone tuttavia che le ingerenze nella sfera privata sono ammesse soltanto se l'intervento è giustificato dall'interesse pubblico (p. es. per motivi di sicurezza nazionale o pubblica), è necessario in una società democratica (cfr. in particolare § 21, 53 e 60 della decisione Klass) ed è conforme allo scopo perseguito in considerazione dell'articolo 13 CEDU (Diritto ad un ricorso effettivo).

La Corte ha statuito che sarebbe di per sé auspicabile che, in un ambito in cui nel caso specifico vi è il rischio di gravi abusi a detrimento di una società democratica, la verifica sia affidata a un giudice. È tuttavia giunta alla conclusione che il sistema tedesco di un comitato indipendente, anche se soltanto paragiudiziale, soddisfa il

criterio della necessità, com'è inteso in una società democratica (§ 56 della decisione Klass).

In alcune considerazioni più recenti (DTF *109* Ia 273), il Tribunale federale fornisce un'interpretazione leggermente diversa da quella della Corte eur. DU. Nel contesto di un caso in cui dovevano verificare se una legge del Cantone di Basilea Città sulla sorveglianza a scopo preventivo e repressivo fosse conforme all'articolo 8 CEDU e all'articolo 36 capoverso 4 della vecchia Costituzione federale (Garanzia del segreto epistolare), i giudici federali hanno stabilito che la procedura in questione andava giudicata considerando in particolare che la sorveglianza richiedeva l'autorizzazione di un giudice. A loro parere, tale obbligo di un controllo approfondito tutela a sufficienza gli interessati (DTF *109* Ia 273). Dodici anni dopo, il Tribunale federale, richiamandosi a tale decisione, ha ribadito che l'intercettazione telefonica dev'essere esaminata dal giudice (DTF *122* I 182; 2 maggio 1996). Il secondo caso verteva tuttavia sulle misure di sorveglianza durante le procedure penali formali.

Resta tuttavia incerto se i giudici federali si siano limitati a esaminare la legge del Cantone di Basilea Città concludendo che era conforme alla CEDU e alla Costituzione, oppure se abbiano voluto indicare l'obbligatorietà costituzionale di una verifica giudiziale, anche se questa non è prevista dalla CEDU (cfr. decisione Klass). In altre parole, la giurisprudenza del Tribunale federale non permette di stabilire con certezza se esso concorda con la Corte eur. DU ritenendo auspicabile, ma non indispensabile, l'intervento di un'istanza giudiziaria, oppure se, basandosi sulla Costituzione, propende per una maggiore severità rispetto alla CEDU, reputando obbligatorio l'intervento di un giudice.

Considerata questa incertezza, nel presente disegno di legge privilegiamo l'approvazione da parte di un'istanza giudiziaria.

Tuttavia, poiché la prevenzione è un'attività diretta e controllata politicamente nel rispetto della legge, il disegno di legge prevede un duplice controllo con il coinvolgimento di un'ulteriore istanza politica. La procedura viene avviata dall'Ufficio federale di polizia che presenta una richiesta scritta e motivata. Il Tribunale amministrativo federale esamina la richiesta e decide se approvare la misura (procedura di approvazione). Dopo che e soltanto se il Tribunale amministrativo federale ha autorizzato la misura, il capo del DFGP la esamina, consulta il capo del DDPS e, in caso di vicendevole consenso, approva definitivamente l'esecuzione della misura (procedura di decisione). Pertanto la richiesta è sottoposta a una verifica giuridica dal potere giudiziario e anche a un (duplice) esame di tipo politico dal potere esecutivo. L'impiego di mezzi speciali per la ricerca di informazioni è consentito soltanto se tutti lo approvano.

Questa procedura, che è stata snellita e corretta dopo la consultazione, soddisfa diverse richieste avanzate dai partecipanti alla stessa che, pur approvando la duplice verifica, avevano criticato la procedura proposta nell'avamprogetto posto in consultazione, giudicandola poco trasparente.

Sebbene non esista una base legale specifica, alla luce degli interessi e dei beni giuridici in gioco, si presuppone inoltre che, esaminando i casi, i giudici competenti terranno sufficientemente conto delle esigenze in materia di tutela del segreto. Pertanto il capoverso dell'avamprogetto posto in consultazione che disciplinava questo aspetto è stato stralciato.

Cpv. 4

Il Tribunale amministrativo federale è tenuto a verificare il rispetto dei requisiti di legge nella creazione di identità fittizie (cfr. art. 14*c* cpv. 3 e 4 e art. 14*d*). Si tratta di un controllo della legalità, vale a dire che il Tribunale deve accertare l'adempimento delle condizioni previste dall'articolo 14*c* capoverso 3 e dall'articolo 14*d* capoversi 1 e 2. Per contro non si esprime sull'opportunità di creare le identità fittizie; è una competenza che spetta al capo del DFGP. Anche per le identità fittizie è quindi indispensabile l'autorizzazione del Tribunale amministrativo federale (cfr. art. 14*c* cpv. 3 e 14*d* cpv. 1). Le sue decisioni in quest'ambito sono definitive.

Art. 18e Procedura di decisione

Cpv. 1

Dopo la procedura di approvazione di cui all'articolo 18*d*, segue la procedura di decisione di cui all'articolo 18*e*. L'Ufficio federale di polizia può richiedere al Dipartimento di impiegare i mezzi speciali per la ricerca di informazioni soltanto se il Tribunale amministrativo federale ha precedentemente autorizzato la misura. In seguito alle richieste di diversi partecipanti alla procedura di consultazione, il capoverso sancisce espressamente che la decisione deve rispettare sempre le condizioni stabilite dal Tribunale amministrativo federale («nel rispetto della decisione del Tribunale amministrativo federale»), la cui decisione deve quindi essere allegata alla richiesta.

L'ultimo periodo del capoverso 1 stabilisce che l'Ufficio federale di polizia deve informare il Dipartimento su tutte le richieste respinte dal Tribunale amministrativo federale. Questa procedura mira a offrire ai vertici del Dipartimento una panoramica completa delle richieste presentate dall'Ufficio federale di polizia (e non solo di quelle approvate dal Tribunale amministrativo federale).

Cpv. 2 e 3

Il capo del DFGP consulta il capo del DDPS e, in caso di vicendevole consenso, decide in via definitiva l'impiego dei mezzi speciali per la ricerca di informazioni autorizzati dal Tribunale amministrativo federale. La delega di tale competenza è esclusa. Se il capo del DFGP e il capo del DDPS non sono d'accordo sull'impiego dei mezzi speciali per la ricerca di informazioni, richiesti e autorizzati dal Tribunale amministrativo federale, non è consentito ordinare l'esecuzione.

Anche se il Tribunale amministrativo federale ha autorizzato una misura richiesta, il capo del DFGP e il capo del DDPS possono, in caso di vicendevole consenso, rinunciare del tutto o parzialmente ad adottare la misura o vincolarla a ulteriori restrizioni o oneri (esigendo p. es. di essere aggiornati regolarmente sulla sua esecuzione).

A seconda dei casi, il capo del DFGP prima di decidere può consultare i capi di altri Dipartimenti (p. es. il capo del DFAE per i casi che riguardano interessi di politica estera).

Art. 18f Procedura d'urgenza

L'articolo 18*f* prevede una procedura specifica per i casi in cui vi è pericolo nel ritardo. Se la decisione tardiva del Tribunale amministrativo federale o dei capi del DFGP e del DDPS compromette o rende impossibile la riuscita della ricerca speciale

di informazioni, dev'essere possibile agire senza indugio. È quanto succede quando un obiettivo di spicco entra di sorpresa in Svizzera e va subito posto sotto stretto controllo, ad esempio sorvegliandone anche le telecomunicazioni.

Cpv. 1

In casi urgenti, l'impiego di mezzi speciali è ordinato direttamente dal direttore dell'Ufficio federale di polizia e avviato immediatamente. Le condizioni materiali per l'impiego dei mezzi speciali in virtù dell'articolo 18*b* del disegno di legge devono essere pienamente adempite anche nei casi urgenti. Il direttore dell'Ufficio federale di polizia ha l'obbligo di verificare che le condizioni per ordinare le misure siano adempite, informando nel contempo il capo del Dipartimento.

Cpv. 2

Il direttore dell'Ufficio federale di polizia è tenuto a presentare al Tribunale amministrativo federale l'istanza ordinaria entro 24 ore, motivando l'urgenza. La procedura segue poi il suo corso abituale. Il Tribunale amministrativo federale deve comunicare entro 72 ore la sua decisione all'Ufficio federale di polizia (come per la procedura ordinaria).

Cpv. 3

L'istanza dell'Ufficio federale di polizia per ordinare *ex post* l'impiego dei mezzi speciali per la ricerca di informazioni dev'essere presentata al Tribunale amministrativo federale che decide in merito alla sua legalità. La richiesta dev'essere presentata senza indugio. Anche l'ordine di esecuzione presuppone il consenso del capo del DFGP e del capo del DDPS.

Cpv. 4

Se il Tribunale amministrativo federale non autorizza l'impiego o se il capo del DFGP, dopo aver consultato il capo del DDPS, non ordina entro 48 ore di proseguirlo, l'Ufficio federale di polizia deve distruggere senza indugio tutti i dati tratti dalla ricerca e raccolti fino a quel momento (cfr. la disposizione analoga di cui all'art. 7 cpv. 4 LSCPT).

Se ha già trasmesso ad altri organi o autorità le informazioni ottenute con una misura non autorizzata, l'Ufficio federale di polizia deve chiedere la distruzione di tutti i dati registrati che riguardano queste informazioni.

A questo proposito durante la procedura di consultazione è stata sollevata la questione su come garantire la distruzione di eventuali dati già trasmessi all'estero se una misura non viene autorizzata.

Di solito, durante le procedure d'urgenza è probabile che anche l'eventuale trasmissione di dati ai servizi partner stranieri deve avvenire rapidamente (ossia nel giro di poche ore, p. es. in caso di informazioni sugli spostamenti previsti di una persona sorvegliata). Non c'è quindi tempo per procedure giudiziarie anticipate (p. es. decisioni superprovvisionali). Il diritto vigente autorizza peraltro i servizi partner stranieri a utilizzare le informazioni ottenute soltanto per lo scopo per cui sono state trasmesse e il SAP può esigere di essere informato sull'uso che ne è stato fatto. Questo implica anche che deve informare le autorità straniere interessate sui dati che devono rettificare o distruggere. Anche se i servizi dell'Amministrazione svizzera non possono controllare come i servizi d'informazione o le autorità di sicurezza straniere utilizzano i dati o se li distruggono realmente, è tuttavia lecito presumere che esse

distruggano i dati loro inviati se il SAP lo richiede perché un'istanza è stata respinta. I servizi d'informazione svizzeri e stranieri non sono interessati a dati dichiarati «falsi» o illeciti. Inoltre di solito il SAP trasmette all'estero le informazioni a condizione che non siano trasmesse ulteriormente senza la sua esplicita approvazione (la cosiddetta regola dei servizi terzi). È evidente che il SAP non concederebbe una tale autorizzazione durante una procedura d'urgenza e quindi i dati sarebbero inutili per il servizio straniero in questione. Infine va ricordato che lo scambio d'informazioni con servizi stranieri, non è obbligatorio come nel caso di una procedura di assistenza giudiziaria, ma avviene su base volontaria. Se un servizio partner straniero non rispetta le regole, la Svizzera può limitare o sospendere la cooperazione in qualsiasi momento.

Art. 18g Sospensione dell'impiego

L'Ufficio federale di polizia interrompe senza indugio l'impiego se questo non è più necessario (lett. a), risulta infruttuoso (lett. b), non viene prorogato (lett. c) o, nella procedura d'urgenza, non è considerato legale dal Tribunale amministrativo federale, non viene autorizzato dal capo del DFGP dopo consultazione del capo del DDPS oppure il capo del DFGP non lo ordina entro 48 ore (lett. d ed e). In questi casi, per rispettare il principio di proporzionalità è giustificato sospendere gli impieghi non soltanto totalmente ma anche parzialmente, se si protraggono nel tempo.

Art. 18h Trattamento dei dati personali raccolti impiegando mezzi speciali

Cpv. 1

La disposizione disciplina le condizioni generali per la conservazione dei dati elencati nell'articolo 15 LMSI. I dati raccolti vanno distrutti entro 30 giorni dalla fine dell'impiego, purché non abbiano una relazione con la minaccia che ha dato adito all'impiego di mezzi speciali per la ricerca di informazioni.

Alcuni partecipanti alla procedura di consultazione hanno chiesto che l'Ufficio federale di polizia non selezioni da solo le informazioni o che la selezione sia perlomeno controllata dal Tribunale amministrativo federale, ma per motivi pratici e giuridici non è possibile soddisfare questa richiesta. La selezione presuppone conoscenze approfondite sui casi ed è pressoché impossibile che le persone esterne siano in grado di procurarsele in tempo utile e senza oneri eccessivi. In ogni caso l'attività dell'Ufficio federale di polizia è inoltre già severamente controllata da diversi servizi (ispettorato interno al Dipartimento, commissioni parlamentari di vigilanza ecc.) e quindi un nuovo strumento di controllo non è necessario.

Art. 18i Obbligo di comunicazione

Questa disposizione è un elemento cardine del disegno di legge ed è determinante per lo svolgimento della verifica *ex post*. La persona interessata ha la possibilità di far valere il proprio diritto di ricorso dinanzi a un tribunale ai sensi dell'articolo 29*a*, soltanto dopo che è stata informata della sorveglianza.

L'obbligo di informare gli interessati è di natura costituzionale e deriva implicitamente dalla garanzia di rispettare la vita privata e la corrispondenza epistolare. Tale garanzia si basa sugli articoli 8 CEDU e 13 Cost.. Secondo la decisione *109* Ia 273, 298–299 del Tribunale federale, l'obbligo vale per la sorveglianza a titolo preventi-

vo e repressivo, nei confronti di imputati, sospettati e terzi. In linea di massima, si può quindi partire dal presupposto che le misure di sorveglianza vadano comunicate agli interessati.

Se eccezionalmente, una volta terminato l'intervento, l'Ufficio federale non mette la persona al corrente del fatto che sono state raccolte informazioni sul suo conto impiegando mezzi speciali, essa di norma non ha alcuna possibilità di difendersi a fatto avvenuto, a meno che non ne sia venuta a conoscenza per altri canali. Analogamente a quanto avviene nei procedimenti penali, in questi casi un'ulteriore procedura giudiziaria deve garantire la legittimità.

Cpv. 1

Per ottemperare alla giurisprudenza di cui sopra, il presente disegno di legge sancisce il principio dell'obbligo di comunicazione *ex post*. Al termine di un'operazione, l'Ufficio federale di polizia è tenuto, in linea di massima, a mettere al corrente entro un mese gli interessati della ricerca speciale di informazioni (per il concetto di operazione, cfr. l'art. 14 OMSI).

Alcuni partecipanti alla consultazione hanno chiesto di estendere l'obbligo di comunicazione alla ricerca generale di informazioni o a tutte le persone coinvolte nella sorveglianza, ma ciò non è giustificato ed è anche irrealizzabile. Innanzitutto la ricerca generale di informazioni lede solo marginalmente i diritti fondamentali. Inoltre l'estensione dell'obbligo di comunicazione causerebbe oneri amministrativi sproporzionati, poiché ogni anno si dovrebbero notificare migliaia di ricerche (anche se si sono concluse senza esito) e identificare un numero ancora maggiore di persone (non soltanto quelle sorvegliate ma anche quelle rimaste coinvolte casualmente). Non è necessario nemmeno informare terze persone coinvolte per caso sulla sorveglianza o sulle procedure in corso nei confronti dei diretti interessati.

Cpv. 2 e 3

Nella citata decisione Klass (§§ 57–59; cfr. le spiegazioni dell'art. 18*d*), la Corte eur. DU ha stabilito che la comunicazione *ex post* poteva senz'altro mettere in questione lo scopo ultimo di una sorveglianza. Ha inoltre riconosciuto che sussiste il rischio di rivelare i metodi di lavoro dei servizi segreti, i settori sorvegliati ed eventualmente persino l'identità degli inquirenti. Sono state pertanto giudicate lecite le deroghe all'obbligo di comunicazione previste dalla legge tedesca.

Nella sua decisione del 1983, il Tribunale federale si è allineato a tali considerazioni (DTF *109* Ia 273), ammettendo pressappoco lo stesso tipo di deroghe e sottolineando che andavano comunque concesse con moderazione. Riserva a parte, nella prassi, l'obbligo di comunicazione è ridimensionato dalle esigenze del procedimento penale. Le deroghe elencate nelle lettere a-d del capoverso 2 riprendono quasi integralmente l'articolo 10 capoverso 3 LSCPT e l'articolo 22 capoverso 2 della legge federale del 20 giugno 2003[49] sull'inchiesta mascherata. L'elenco contenuto nelle lettere a-d è esaustivo.

Una persona è considerata non reperibile (lett. d), ad esempio anche se è possibile scoprirne il luogo di soggiorno soltanto con un onere di lavoro sproporzionato oppure se quest'ultimo è noto, ma contattare la persona comporta un onere di lavoro sproporzionato (in particolare se si trova all'estero).

49 RS **312.8**

La decisione di procrastinare la comunicazione o di rinunciarvi non è peraltro di competenza dell'Ufficio federale di polizia. Dal momento che viene leso un diritto costituzionale, la procedura deve garantire che l'interesse individuale del singolo a opporsi alle ingerenze nella propria sfera privata possa essere limitato soltanto a condizione che un interesse pubblico preponderante renda palesemente necessario rinviare la comunicazione o rinunciarvi. Tale ponderazione dei vari interessi è particolarmente delicata in quanto la procedura di comunicazione prevede anche la possibilità di far accertare in giudizio la legalità dell'impiego dei mezzi speciali per la ricerca di informazioni. È pertanto giustificato prevedere regole severe per procrastinare la comunicazione o rinunciarvi. Se del caso, l'Ufficio federale di polizia presenta un'istanza motivata chiedendo una deroga all'obbligo di comunicazione. In seguito il Tribunale amministrativo federale verifica la legalità della richiesta e, se emette un parere favorevole, il capo del DFGP consulta il capo del DDPS come previsto dall'articolo 18*e* e decide. In altre parole si applica la stessa procedura valida per ordinare l'impiego dei mezzi speciali per la ricerca di informazioni.

L'obbligo di comunicazione *ex post* va distinto dal diritto d'essere informati disciplinato dagli articoli 8–10 LPD su cui verte l'articolo 18 LMSI (il cosiddetto diritto indiretto d'essere informati). Secondo questa disposizione chiunque può richiedere all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) di verificare se nel sistema d'informazione dell'Ufficio federale di polizia sono trattati, in conformità con la legge, dati che lo concernono. L'IFPDT comunica al richiedente, con una risposta standard, che in modo non conforme alla legge non è stato trattato alcun dato che lo concerne o che, nel caso di eventuali errori nel trattamento dei dati, ha indirizzato all'Ufficio federale di polizia una raccomandazione volta a correggerli.

A differenza della comunicazione *ex post* che presuppone una misura di ricerca speciale delle informazioni, il diritto indiretto d'essere informati non presuppone alcuna condizione. Chiunque può quindi chiedere in ogni momento all'IFPDT di verificare se i dati che lo riguardano sono trattati in conformità con la legge. La persona interessata può chiedere che il presidente della corte del Tribunale amministrativo federale competente in materia di protezione dei dati esamini la comunicazione dell'IFPDT o l'esecuzione della raccomandazione da lui emanata.

Questa possibilità permanente di verificare il trattamento dei dati effettuato dal SAP presuppone controlli di qualità elevata, ma è giustificata dal fatto che di norma la persona interessata non può consultare gli atti. Questa soluzione garantisce che gli interessi della persona coinvolta siano tutelati pienamente e in modo competente e impedisce inoltre che una persona che potrebbe essere pericolosa possa giungere a conoscenza di ricerche concluse o ancora in corso sul suo conto.

Del resto, a determinate condizioni, sono possibili deroghe al diritto indiretto d'essere informati. L'IFPDT, eccezionalmente e secondo i disposti della LPD, può informare il richiedente in modo adeguato, se ciò non pregiudica la sicurezza interna o esterna e se altrimenti il richiedente dovesse subire un danno rilevante e irreparabile.

A questo proposito diversi partecipanti alla procedura di consultazione hanno richiamato l'attenzione su una decisione del 15 febbraio 2006 della Commissione federale della protezione dei dati e della trasparenza che in passato era competente in materia. Questo tipo di decisioni, unitamente al resto della giurisprudenza (p. es. sulla CEDU) vengono costantemente analizzate. Si tratta di verificare la necessità di

aggiornare le disposizioni della LMSI, della legge militare e della legge sui sistemi d'informazione di polizia della Confederazione (LSIP). Il Parlamento sta già discutendo la LSIP. Se necessario, durante il dibattito parlamentare sulla revisione della presente legge, il Dipartimento proporrà di discutere questo problema e suggerirà soluzioni.

Art. 18j Esecuzione da parte dei Cantoni

Questo articolo stabilisce che la ricerca speciale di informazioni da parte degli organi di sicurezza cantonali su mandato della Confederazione è retta dalle disposizioni della LMSI. Pertanto se gli organi di sicurezza cantonali osservano luoghi non liberamente accessibili o vi installano apparecchi di sorveglianza operando su mandato della Confederazione, si applicano gli articoli 18*a*–18*i* del presente disegno di legge e non eventuali disposizioni del diritto cantonale.

Le conseguenze che i nuovi mezzi avranno per i Cantoni dipendono in larga misura dal genere e dalle modalità delle singole misure, ma soprattutto dalla necessità di utilizzarle (che dipende dagli eventi). A seconda del loro coinvolgimento, i Cantoni impiegheranno quindi personale supplementare per i servizi che si occupano dell'esecuzione della LMSI (cfr. art. 6 LMSI) e la Confederazione accorderà loro un'equa indennità (art. 28 LMSI).

Sezione 2: Mezzi speciali per la ricerca di informazioni

Secondo gli articoli 36 capoverso 1 e 164 capoverso 1 lettera a Cost., le restrizioni gravi dei diritti fondamentali devono essere sanciti in una legge. Tuttavia, non basta elencare i vari mezzi che potrebbero limitare i diritti fondamentali. Occorre invece esporre dettagliatamente la portata delle limitazioni, specificare i punti su cui vertono e disciplinare nei particolari le azioni ammesse.

È stato peraltro già ricordato che lo scopo preventivo della ricerca di informazioni non ostacola una loro trasmissione alle autorità di perseguimento penale svizzere e straniere (l'art. 17 cpv. 1 LMSI sancisce anzi l'obbligo di trasmettere alle autorità nazionali di perseguimento penale le informazioni utili per il perseguimento penale). In questo modo è possibile integrare i dati raccolti dai servizi d'informazione («Intelligence») in varie fasi di un procedimento penale, ad esempio durante l'analisi e mediante rapporti ufficiali, consentendo fra l'altro un impiego efficiente delle risorse del perseguimento penale.

Art. 18k Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni

La sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni ai fini del procedimento penale è disciplinata nella LSCPT. La sorveglianza preventiva da definire in questa sede non è tuttavia finalizzata al perseguimento penale, ma mira a riconoscere minacce concrete derivanti dal terrorismo, dallo spionaggio politico o militare, dal commercio illecito di armi o materiale radioattivo oppure dal trasferimento illegale di tecnologia. Pertanto è opportuno un disciplinamento speciale nella LMSI.

Comunque, la LMSI istituisce regole speciali soltanto laddove occorrono varianti o precisazioni rispetto alla LSCPT. Per le questioni tecniche e organizzative, la LMSI rimanda alla LSCPT, poiché di principio non s'intendono definire altre procedure e altri requisiti tecnici per la sorveglianza preventiva.

L'articolo 18*i* capoverso 1 del presente disegno di legge stabilisce inequivocabilmente che altre autorità coinvolte nella procedura, quali ad esempio il Servizio per compiti speciali (SCS) del DATEC, non sono né tenute né autorizzate a fornire informazioni sull'applicazione delle misure di sorveglianza previste dalla LMSI.

Cpv. 1

In questo capoverso si descrive lo scopo perseguito con la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Essi vengono denominati in generale: mezzi di comunicazione. Come nella legge sulle telecomunicazioni e nella LSCPT, anche in questo contesto si rinuncia ad indicare i mezzi tecnici speciali per garantire il necessario margine di manovra in questo settore, in cui il progresso tecnico procede a velocità particolarmente sostenuta. Obiettivamente occorrono indizi concreti per confermare il sospetto che il presunto autore della minaccia si serva di tali mezzi per scambiare informazioni o commettere atti direttamente connessi alla reale minaccia alla sicurezza interna o esterna. Per giustificare la sorveglianza in un determinato momento, tali indizi devono essere sufficientemente concreti e attuali. Informazioni generiche del passato su possibili minacce non sono sufficienti.

Cpv. 2

La disposizione sulla sorveglianza di un posto pubblico di telecomunicazione corrisponde alla norma speciale di cui all'articolo 4 capoverso 2 LSCPT. All'atto pratico, si tratta di casi in cui, ad esempio osservando una persona sospetta o intercettandone le telefonate, si è potuto appurare che essa utilizza, regolarmente o in determinate occasioni, una cabina telefonica pubblica ben precisa.

Cpv. 3

Se una persona sospetta cambia in rapida successione i collegamenti di telecomunicazione, ad esempio utilizzando carte prepagate di telefonia mobile, la disposizione rischia quasi sempre di giungere in ritardo. In questi casi può essere ordinata la sorveglianza di tutti i collegamenti identificati di cui si serve la persona o l'organizzazione. Anche questa disposizione si rifà alla LSCPT (art. 4 cpv. 4).

Cpv. 4

Per la sorveglianza preventiva della corrispondenza postale e del traffico delle telecomunicazioni non s'intendono creare strutture parallele a quelle previste dalla LSCPT. Pertanto, le varie forme di sorveglianza, la loro attuazione tecnica e le indennità sono rette per analogia dalla LSCPT e dalle sue disposizioni esecutive.

Interesse pubblico e proporzionalità

La sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni lede in modo grave la sfera privata. Secondo l'articolo 36 Cost., le restrizioni dei diritti fondamentali devono essere giustificate da un interesse pubblico e proporzionate allo scopo perseguito. A tutela dell'interesse pubblico, la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, come pure tutti gli altri mezzi speciali per la ricerca di informazioni, possono essere impiegati unica-

mente nei tre ambiti da cui può scaturire una minaccia che rischia di minare i fondamenti della nostra società (cfr. le spiegazioni dell'art. 13*a* cpv. 1). È quindi indubbio che l'interesse pubblico giustifichi la misura. Per giudicare la proporzionalità, occorre valutare se la misura è adeguata e necessaria e se è ragionevolmente proporzionata allo scopo perseguito. Se vi sono indizi a sufficienza per sospettare che il presunto autore della minaccia si serva di mezzi di telecomunicazione per le sue attività, questa forma di sorveglianza è lo strumento adatto per ottenere informazioni che permettono di giudicare meglio la minaccia e prevenirla.

Gli organi di sicurezza non sono invece autorizzati a effettuare sorveglianze di tipo prettamente esplorativo, soltanto perché sospettano che una persona possa minacciare la sicurezza interna. Occorrono anzi in ogni caso indizi concreti di una minaccia e la persona interessata deve servirsi di mezzi specifici di telecomunicazione per le sue attività.

Per quanto riguarda la necessità della misura, è indubbio che è possibile apprendere informazioni sufficienti sulla rete di contatti di una persona che costituisce una minaccia o sul contenuto delle comunicazioni scambiate mediante mezzi di telecomunicazione soltanto sorvegliando il traffico delle telecomunicazioni. È pressoché impossibile procurarsi tali informazioni ricorrendo alla sola ricerca generale secondo l'articolo 14 capoverso 2.

Non è possibile stabilire su un piano generico e astratto se la misura è proporzionata in senso stretto, ossia se l'interesse pubblico prevale al punto da giustificare la lesione dei diritti fondamentali dell'individuo. La descrizione molto circostanziata dei compiti previsti dalla LMSI limita già per legge in modo molto restrittivo l'ambito dell'impiego. Un'ulteriore limitazione mediante un elenco di reati, come nel diritto di procedura penale, sarebbe inopportuna soprattutto perché bisogna evitare una commistione con i sospetti fondati penalmente rilevanti e perché per definizione l'attività preventiva non si focalizza su fattispecie concrete del diritto penale. Gli organi competenti possono ponderare l'interesse pubblico e la tutela dei diritti fondamentali del singolo e giungere a una decisione fondata, soltanto se sono a conoscenza delle circostanze specifiche. È importante che gli aspetti giuridici non siano valutati soltanto dagli organi di sicurezza, ma anche da un'autorità giudiziaria indipendente, in grado di ponderare al meglio, in base dei criteri sanciti dalla legge, le esigenze degli organi di sicurezza e la legittima pretesa di ciascuno di comunicare e intrattenere contatti senza ingerenze statali.

Nell'ambito di tale apprezzamento e tenuto conto delle restrizioni e dei provvedimenti previsti dal disegno di legge, la sorveglianza preventiva della corrispondenza postale e del traffico delle telecomunicazioni costituisce uno strumento proporzionato alla salvaguardia dell'interesse pubblico, e può essere impiegato in conformità con i principi della Costituzione e della Convenzione sui diritti dell'uomo.

Art. 18l Osservazione in luoghi non liberamente accessibili, anche mediante apparecchi tecnici di sorveglianza

In base alle disposizioni attuali della LMSI, gli organi di sicurezza possono osservare fatti in luoghi pubblici e liberamente accessibili, anche ricorrendo a registrazioni di immagini e suoni (art. 14 cpv. 2 lett. f LMSI). La nuova disposizione permette l'osservazione e la registrazione anche in luoghi non liberamente accessibili (p. es. locali adibiti a uso commerciale, sale di riunione, appartamenti e camere d'albergo; cfr. cpv. 1). A tal fine è anche previsto l'impiego di apparecchi tecnici di sorveglian-

za (cfr. cpv. 2). La legge in vigore vieta l'impiego di tali mezzi per intercettare o registrare conversazioni non pubbliche (cfr. art. 179bis e 179ter CP). È altresì vietato osservare o registrare, con un apparecchio da presa un fatto rientrante nella sfera personale o riservata di una persona (art. 179quater CP) che si verifica in un luogo liberamente accessibile, se l'osservazione o la registrazione vengono tenute intenzionalmente segrete. Non sono per contro tutelati fatti privati di natura generale che avvengono in pubblico.

Cpv. 1

La disposizione definisce i particolari e le condizioni dell'osservazione. Devono sussistere fatti concreti e attuali che inducono a presumere che la persona in questione si serva di un determinato luogo per scambiare informazioni o commettere atti direttamente connessi alla concreta minaccia alla sicurezza interna o esterna.

Cpv. 2

L'impiego di apparecchi tecnici di sorveglianza corrisponde, per contenuto e portata, alla disposizione dell'articolo 66 capoverso 2 della legge federale del 15 giugno 1934[50] sulla procedura penale. Si tratta di apparecchi per la ripresa di suoni e immagini, che possono essere impiegati anche in ambienti privati, purché siano adempite le condizioni necessarie. Rientra in questo ambito anche l'osservazione e la registrazione tecnica di fatti privati in luoghi liberamente accessibili, come ad esempio una conversazione privata in un ristorante.

Interesse pubblico e proporzionalità

L'osservazione in un luogo non liberamente accessibile o con l'ausilio di apparecchi tecnici di sorveglianza costituisce una grave ingerenza nella sfera privata. Come accennato in precedenza, secondo l'articolo 36 Cost., un tale intervento dev'essere giustificato da un interesse pubblico e proporzionato allo scopo perseguito. Riguardo alla giustificazione di tale mezzo speciale alla luce dell'interesse pubblico, rimandiamo alle spiegazioni degli articoli 13*a* e 18*k*.

Per quanto riguarda la proporzionalità, si possono fare le seguenti considerazioni: se vi sono fatti sufficienti che dimostrano che il presunto autore della minaccia si serve di un determinato luogo per le sue attività, allora l'osservazione è lo strumento adatto per ottenere informazioni che permettono di giudicare e prevenire la minaccia. Gli organi di sicurezza non sono invece autorizzati a osservare l'intera sfera privata di una persona soltanto perché hanno motivo di sospettare che essa possa minacciare la sicurezza interna. L'osservazione deve mirare a un obiettivo specifico ben definito che costituisce un elemento chiave delle attività del presunto autore della minaccia. La misura è considerata adeguata a condizione che sia reso verosimile il nesso tra gli atti considerati minacciosi e l'utilizzo di un luogo.

Quanto alla necessità, appare evidente che, a prescindere dall'eventuale intervento di un informatore, la sola ricerca generale di informazioni secondo l'articolo 14 capoverso 2 LMSI non permette di venire a sapere quanto accade negli spazi privati. Tali situazioni però non consentono sempre di trovare o impiegare informatori.

50 RS **312.0**

Come spiegato in precedenza, soltanto gli organi competenti possono giudicare se la misura è proporzionata in senso stretto, ossia se, nel caso specifico, l'interesse pubblico prevale su quello individuale. La decisione se, nel caso specifico, sussiste un legittimo interesse pubblico, compete al Tribunale amministrativo federale.

L'impiego di apparecchi tecnici di sorveglianza non costituisce tanto una misura di sorveglianza autonoma, quanto piuttosto uno strumento ausiliario per osservare fatti che avvengono nella sfera privata. Nell'osservazione con l'ausilio di apparecchi tecnici, questi si sostituiscono semplicemente all'agente osservatore che è presente fisicamente in un luogo privato. Ne consegue che, per i medesimi motivi per i quali l'osservazione di fatti in un luogo privato può essere considerata proporzionata, l'osservazione effettuata con l'ausilio di apparecchi tecnici può essere ritenuta a priori uno strumento conforme al principio della proporzionalità. L'esistenza di un interesse pubblico preponderante va decisa alla luce delle circostanze concrete.

Art. 18m Accesso segreto a un sistema per l'elaborazione di dati

L'impiego di moderne infrastrutture EED riveste un'importanza crescente in seno alla società odierna. Soprattutto Internet è divenuto uno strumento importante per scambiare informazioni. Dal momento che le autorità preposte alla sicurezza stanno già conducendo intense ricerche di informazioni su Internet, i gruppi che sono oggetto di queste ricerche (p. es. le organizzazioni terroristiche) affidano sempre più la diffusione di informazioni sensibili a settori riservati, protetti ad esempio da password. L'intrusione in tali sistemi è fattibile sul piano tecnico, ma penalmente perseguibile (art. 143bis CP, Accesso indebito a un sistema per l'elaborazione di dati).

L'articolo 18*m* definisce in che cosa consiste questo strumento di ricerca speciale di informazioni e ne descrive l'impiego. In conformità alle disposizioni pertinenti del Codice penale (cfr. art. 143 e 143bis CP), il campo d'applicazione si estende ai dati registrati elettronicamente o con modalità simili e specialmente protetti contro l'accesso di terzi. Al contrario della perquisizione effettuata nell'ambito di un'istruzione penale, questo tipo di accesso avviene all'insaputa del presunto autore della minaccia. Anche in questo caso devono sussistere fatti chiari e attuali che fanno presumere che la persona in questione si serva del sistema informatico per le proprie attività. L'accesso ha tuttavia carattere passivo, vale a dire che non consente di interferire nel sistema al punto da renderlo inoperativo, di comprometterne le funzioni o di distruggere dati. Sono ad esempio ipotizzabili la ricerca di indirizzi di contatto sul computer portatile del presunto autore della minaccia o la decodificazione di un messaggio di posta elettronica cifrato, scoperto durante una sorveglianza autorizzata delle telecomunicazioni, ma che non è stato possibile leggere.

Un possibile campo d'applicazione concreto è indubbiamente l'analisi della propaganda jihadista. Anche se non è rivolta direttamente contro la Svizzera, è potenzialmente molto pericolosa e quindi rilevante per la sicurezza. Nel recente passato abbiamo assistito a una crescente tendenza al fondamentalismo diffuso mediante siti Internet di propaganda jihadista e contatti in rete. Sebbene il SAP sia autorizzato a consultare i siti Internet liberamente accessibili e a partecipare alle chat non protette, la legge vigente non gli consente di accedere ad ambiti protetti da password o in altro modo, dove si intrattengono i contatti cruciali (p. es. nei settori riservati delle chat pubbliche). Il SAP rimane quindi escluso dai settori determinanti e questa situazione va modificata nell'interesse della sicurezza della Svizzera.

Interesse pubblico e proporzionalità

Accedere a un sistema per l'elaborazione di dati costituisce una grave ingerenza nella sfera privata. Come accennato in precedenza, secondo l'articolo 36 Cost. un tale intervento dev'essere giustificato da un interesse pubblico e proporzionato allo scopo perseguito. Riguardo alla giustificazione di tale mezzo speciale alla luce dell'interesse pubblico, rimandiamo alle considerazioni sugli articoli 13*a* e 18*l*. In fatto di proporzionalità vale quanto segue: se appare alquanto verosimile che il presunto autore della minaccia utilizzi un sistema e delle reti per lo scambio di dati per trattare o memorizzare, ad uso proprio o di terzi, dati che minacciano concretamente la sicurezza interna ed esterna, l'accesso al sistema costituisce uno strumento adeguato e necessario per procurare le informazioni necessarie a valutare la minaccia. Per accedere a questi dati non vi è altro modo che introdursi nel sistema informatico. Sarà consentito soltanto accedere ai sistemi informatici, mentre sarà ad esempio vietato perquisire locali o veicoli, per i quali si adopereranno altri mezzi per cercare informazioni (p. es. l'osservazione fisica o gli apparecchi tecnici di sorveglianza). La revisione propone una gamma ristretta di mezzi, al fine di preservare la proporzionalità già a livello di legge. Come spiegato in precedenza, è possibile giudicare soltanto nel caso specifico se la misura è proporzionata in senso stretto, ossia se l'interesse pubblico prevale su quello individuale. La decisione se, nel caso specifico, sussiste un legittimo interesse pubblico, compete al Tribunale amministrativo federale.

Capitolo 3*b*: Divieto di determinate attività e lotta alla propaganda violenta

Quale nuova misura viene introdotto il divieto di determinate attività. Con la revisione della LMSI, sottoposta al Parlamento il 24 marzo 2006 (propaganda violenta e violenza nel corso di manifestazioni sportive), era stato compiuto un primo passo in questa direzione. Il divieto di accedere a un'area, il divieto di recarsi in un Paese determinato, l'obbligo di presentarsi alla polizia e il fermo preventivo di polizia hanno lo scopo di indurre i privati cittadini a mutare il loro comportamento e di prevenire in tal modo gli atti violenti durante le manifestazioni sportive. La presente revisione costituisce un ulteriore passo nella stessa direzione. Si intende rafforzare la prevenzione dei pericoli creando la possibilità di reagire con flessibilità ai comportamenti dei privati.

Art. 18n Divieto di determinate attività

La disposizione autorizza il capo del Dipartimento a vietare determinate attività in virtù del diritto amministrativo, purché siano connesse a una minaccia concreta per la sicurezza interna o esterna.

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.) o per far fronte a gravi turbamenti, esistenti o imminenti, dell'ordine pubblico o della sicurezza interna o esterna (art. 185 cpv. 3 Cost.). Tutte 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. Ecco perché si intende creare

a livello di legge la possibilità di vietare determinate attività in caso di 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 (cfr. anche le spiegazioni degli art. 18*e in fine* e 29*a* cpv. 1).

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 dal Dipartimento secondo il nuovo disciplinamento proposto. Le decisioni del Consiglio federale sono atti di governo; possono essere impugnate dinanzi a un Tribunale della Confederazione soltanto se il diritto internazionale pubblico conferisce un diritto al giudizio da parte di un tribunale[51], altrimenti sono definitive. Per contro, le disposizioni emesse in virtù della LMSI sono impugnabili mediante ricorso presentato al Tribunale amministrativo federale, la cui decisione può essere impugnata dinanzi al Tribunale federale.

Il nuovo disciplinamento proposto implica un rafforzamento dei rimedi giuridici che sono indipendenti dal diritto internazionale pubblico e più incisivi (le vie di ricorso giungono fino al Tribunale federale, passando per il Tribunale amministrativo federale). Alcuni partecipanti alla procedura di consultazione hanno criticato le possibilità di ricorso, affermando che finiscono per invertire l'onere della prova. Questa affermazione non trova riscontro nel disegno di legge e non corrisponde nemmeno allo scopo perseguito. La nuova competenza comporta anzi rimedi giuridici incisivi.

Per quanto riguarda la richiesta avanzata durante la procedura di consultazione di creare all'interno di questo articolo una base legale per sequestrare gli emblemi di organizzazioni estremiste, rinviamo ai lavori legislativi sulla legge federale sulle misure contro il razzismo.

Cpv. 1

La disposizione permette di vietare determinate attività. Vi sono ad esempio 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. Non di rado, però, in tale contesto vengono esercitate pressioni che rasentano l'estorsione (p. es. si avvicinano i membri di una comunità straniera residente nel nostro Paese minacciando che, se si rifiutano di fare una donazione, i loro familiari rimasti in patria ne subiranno le conseguenze). Inoltre, molto probabilmente, i fondi raccolti non vengono destinati allo scopo indicato in Svizzera, ma finiscono, almeno in parte, ad alimentare tutt'altre cause, quali ad esempio l'acquisto di armi per un movimento di resistenza operante nella zona di conflitto. Tuttavia, tali macchinazioni sono difficili da provare in via diretta. In Svizzera i donatori coatti tacciono per paura di nuocere a sé stessi e ai loro familiari, amici e conoscenti rimasti in patria. Presto si perdono le tracce del denaro a causa della complessità dei trasferimenti di capitali, dell'uso dei fondi attestato da certificati stranieri lacunosi, contraffatti o autentici perché ottenuti grazie alla corruzione, ma dal contenuto fasullo e via dicendo. Per non mettere in pericolo le persone coinvolte non è nemmeno possibile rivolgersi direttamente ai Paesi di destinazione dei fondi. Del resto le organizzazioni che sono state adoperate per raccogliere le donazioni cambiano spesso nome, si presentano in

51 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**).

modo sempre diverso e non di rado incaricano terzi residenti all'estero di «raccogliere le donazioni».

Il capo del Dipartimento 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 vietate è stata esaminata e respinta. Un elenco di questo tipo equivarrebbe a un invito diretto a eluderlo e inoltre diverrebbe impossibile prevenire tempestivamente nuove forme di minaccia. Per contemplare l'intera gamma dei comportamenti indesiderati, non è possibile determinare i criteri in modo più restrittivo.

Il timore espresso da alcuni partecipanti alla consultazione che il divieto di determinate attività sia uno strumento per combattere l'opposizione è ingiustificato. Il divieto riguarda invece tutti coloro che promuovono attività terroristiche o di estremismo violento che mettono seriamente a repentaglio la sicurezza interna o esterna della Svizzera. Lo scopo principale di questo divieto in virtù del diritto amministrativo non è di prevenire un reato, bensì una minaccia per la sicurezza interna (che non deve essere un reato in quanto tale).

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

Cpv. 2

I divieti ai sensi del capoverso 1 possono impedire agli interessati di esercitare i loro diritti fondamentali. Pertanto è importante limitarli nel tempo. La limitazione obbliga le autorità a riesaminare il divieto dopo la sua scadenza per verificare se le condizioni valide al momento dell'emanazione sono ancora soddisfatte o se non sussistono più.

Se le condizioni sono ancora soddisfatte, la durata di un divieto può essere prorogata fintantoché le circostanze lo esigono. La limitazione obbliga esplicitamente il Dipartimento a verificare, a intervalli regolari, se le condizioni all'origine della disposizione continuano a essere soddisfatte e, eventualmente, a revocare senza indugio il divieto. Il Dipartimento è quindi tenuto a intervenire sia per emanare un divieto sia per revocarne uno emanato in precedenza.

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 senz'altro dall'obbligo, inserito tra i compiti della LMSI, di rilevare e combattere tempestivamente i pericoli dovuti alle attività terroristiche e di estremismo violento. Quanto alla proporzionalità, va rilevato che vietare una determinata attività alle condizioni indicate nella legge non è sproporzionato per definizione, ma che vanno piuttosto ponderati gli interessi in causa nel caso specifico.

Art. 18o Messa al sicuro, sequestro e confisca di materiale di propaganda

L'articolo 13*a*, introdotto nel numero I della modifica della legge federale del 24 marzo 2006 (in vigore dal 1° gennaio 2007), dev'essere spostato in un altro punto della legge a causa della nuova struttura della LMSI. Esso diventa il nuovo articolo 18*o*. Il suo tenore è identico alla versione vigente e il contenuto non è stato modificato.

Art. 27 cpv. 1bis

L'articolo 27 della legge impone al Consiglio federale di informare annualmente, o secondo necessità, l'Assemblea federale, 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, s'intende obbligare il Dipartimento a informare annualmente, o secondo necessità, sull'utilizzo dei mezzi introdotti con la presente revisione (p. es. nell'ambito del Rapporto sulla sicurezza interna della Svizzera). Alla luce delle eventuali restrizioni dei diritti fondamentali della popolazione, questa informazione appare naturale. L'informazione deve vertere sull'uso delle identità fittizie, sull'impiego di mezzi speciali per la ricerca di informazioni e sul divieto di determinate attività. Del resto, il Dipartimento e la Delegazione delle Commissioni della gestione ricevono già oggi rendiconti completi senza che esista un espresso obbligo legale.

Capitolo 6*a*: Procedura e rimedi giuridici

Art. 29a

L'introduzione della ricerca di informazioni impiegando mezzi speciali richiede un adeguamento dei rimedi giuridici ai principi della Costituzione federale e della CEDU. Appaiono particolarmente rilevanti a tal proposito l'articolo 29*a* Cost. (Garanzia della via giudiziaria) e l'articolo 13 CEDU (Diritto ad un ricorso effettivo).

Durante la procedura di consultazione è stata aspramente criticata la disposizione di cui al capoverso 2 dell'avamprogetto, che limitava il potere d'esame alle violazioni del diritto federale. La critica è stata ritenuta giustificata e il potere d'esame è stato esteso agli accertamenti inesatti o incompleti di fatti giuridicamente rilevanti (cfr. la spiegazione nel cpv. 3). In tal modo sono stati creati rimedi giuridici efficaci da affiancare alle accresciute competenze dei servizi d'informazione.

Cpv. 1

La disposizione sancisce il diritto di ricorrere contro le decisioni pronunciate dalle autorità federale in virtù della LMSI. Essa precisa inoltre l'articolo 32 capoverso 1 lettera a della legge sul Tribunale amministrativo federale, specificando che le citate decisioni secondo la LMSI sono atti amministrativi impugnabili e non atti di governo. Questi ultimi, di norma, non sono impugnabili dinanzi al Tribunale amministrativo federale (cfr. anche la spiegazione dell'articolo18*n*).

Cpv. 3

Il ricorrente può far valere una violazione del diritto federale, compreso l'eccesso o l'abuso del potere d'apprezzamento oppure l'accertamento inesatto o incompleto di fatti giuridicamente rilevanti.

Allegato: Modifica del diritto vigente

1. Legge del 17 giugno 2005[52] sul Tribunale amministrativo federale

L'introduzione dell'articolo 13*b* LMSI richiede l'adeguamento dell'articolo 35 lettera d della legge sul Tribunale amministrativo federale. Infatti, l'articolo 13*b* LMSI stabilisce che il Tribunale amministrativo federale è competente per comporre le controversie tra l'Ufficio federale di polizia e le autorità, le unità amministrative dei Cantoni, le organizzazioni che esercitano funzioni pubbliche e le unità amministrative dell'Amministrazione federale decentralizzata (cfr. la spiegazione dell'art. 13*b*).

2. Codice penale svizzero[53]

Art. 179octies

L'impiego, nella sfera segreta, di apparecchi tecnici di sorveglianza, quali registratori e macchine da presa, costituisce un reato ai sensi dell'articolo 179 e seguenti CP. L'articolo 179octies autorizza tuttavia la sorveglianza statale in base alla legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

La disposizione penale va pertanto modificata affinché la deroga comprenda anche le nuove misure di sorveglianza ammesse nel contesto della procedura prevista dalla LMSI.

Art. 317bis

La falsità in atti è reato (cfr. art. 251, 252, 255, 317 CP). L'attuale articolo 317bis CP autorizza tuttavia l'allestimento e l'utilizzo, nel quadro di un'inchiesta mascherata, di documenti falsi atti a costituire o conservare un'identità fittizia nell'ambito di un'inchiesta mascherata autorizzata dal giudice. La norma penale va adeguata affinché la deroga comprenda anche l'utilizzo delle identità fittizie secondo la LMSI.

3. Legge federale sull'esercito e sull'amministrazione militare[54]

Art. 99 cpv. 1 secondo periodo, cpv. 1bis e 2

Cpv. 1 secondo periodo

Limitando (in linea di principio) l'esplorazione radio a obiettivi situati all'estero, come previsto dall'articolo 99 capoverso 1 del disegno di legge, si intende mettere in atto quanto raccomandato dalla Delegazione delle Commissioni della gestione nel

52 RS **173.32**
53 RS **311.0**
54 RS **510.10**

punto 1 del suo rapporto del 10 novembre 2003 sul progetto ONYX. Per esplorazione radio all'estero s'intende il rilevamento di emissioni elettromagnetiche provenienti dall'estero. Oggi a tale scopo vengono impiegati il sistema ONYX per le comunicazioni trasmesse via satellite e apparecchi riceventi capaci di captare le onde corte. Sarà lo sviluppo tecnico a determinare quali mezzi e sistemi saranno utilizzati in futuro per l'esplorazione radio all'estero. Il disegno di legge rinuncia volutamente a una definizione più specifica e utilizza l'espressione generica di «esplorazione radio».

Cpv. 1bis

Conformemente al secondo periodo del capoverso 1, l'esplorazione radio va in linea di massima impiegata per obiettivi situati all'estero. Tuttavia, l'esercito necessita tuttora dell'esplorazione radio in Svizzera. Alla luce del carattere generale della norma istituita con il secondo periodo del capoverso 1 e considerato che le restrizioni dei diritti fondamentali, come quello a tutela della sfera privata, richiedono una base legale formale, l'impiego dell'esplorazione radio contro civili in Svizzera va disciplinato esplicitamente. Il capoverso 1bis ammette pertanto l'esplorazione radio da parte dell'esercito in Svizzera nei due casi illustrati qui di seguito.

La lettera a si riferisce alla sorveglianza delle frequenze utilizzate per scopi militari in Svizzera. Nel corso dei suoi interventi, l'esercito deve poter controllare se civili si stanno eventualmente servendo delle frequenze riservate ai militari. Inoltre deve essere in grado di individuare e sorvegliare con i propri mezzi tutte le frequenze utilizzate per scopi militari. Se del caso, identificherà e isolerà le frequenze civili. Solo così si può garantire che le frequenze siano utilizzate soltanto dall'esercito e impedire gli abusi.

La lettera b riguarda la salvaguardia della sovranità sullo spazio aereo. Secondo l'ordinanza del 23 marzo 2005[55] concernente la salvaguardia della sovranità sullo spazio aereo (OSS), tale compito spetta alle Forze aeree. A questo scopo devono potersi avvalere dell'esplorazione radio per intercettare le comunicazioni radio trasmesse tra aerei militari e civili e le loro stazioni terrestri (civili o militari). Ciò permette di riconoscere e identificare, tra l'altro, aeromobili sconosciuti e, se del caso, di adottare le misure di difesa adeguate. Le Forze aeree si servono dell'esplorazione radio anche per sorvegliare lo spazio aereo in generale e descrivere la situazione aerea, come prescritto dall'articolo 5 OSS.

L'impiego dell'esplorazione radio da parte dell'esercito contro obiettivi civili in Svizzera (o all'estero) è ammesso peraltro anche nell'ambito della legittima difesa o di uno stato di necessità, ad esempio per proteggere i militari da un imminente attacco sferrato da civili. Si tratta di un classico motivo giustificativo, che la legge militare non deve prevedere esplicitamente in quanto è già disciplinato dagli articoli 25 e 26 del Codice penale militare del 13 giugno 1927[56] (CPM).

Art. 99 cpv. 2

Il contenuto del capoverso 2 attualmente in vigore autorizza il Sevizio informazioni strategico a trattare dati personali. Questa disposizione non è più del tutto in linea con i principi della protezione dei dati, soprattutto alla luce del trattamento di dati

55 RS **748.111.1**
56 RS **321**

personali degni di particolare protezione e di profili della personalità. Per soddisfare i nuovi requisiti s'intende completare l'articolo 99 capoverso 2 riprendendo in sostanza i principi sul trattamento dei dati sanciti nei capoversi 1 e 2 dell'articolo 15 LMSI.

Il contenuto del secondo e del terzo periodo del capoverso 2 riprende l'articolo 15 capoverso 1 LMSI. I due periodi disciplinano il trattamento di tutti i dati personali e sanciscono i principi generali, ossia che si devono valutare i dati in merito a esattezza e rilevanza e distruggere le informazioni inesatte o inutili (cfr. art. 4 e 5 della LPD.

Inoltre è stato ripreso l'attuale articolo 9 capoverso 1 lettere a-c dell'ordinanza del 26 settembre 2003[57] sui servizi d'informazione del DDPS (OSINF), di modo che ora i presupposti per il trattamento di dati personali degni di particolare protezione e di profili della personalità sono disciplinati direttamente nella LM. Spetta al Consiglio federale disciplinare ulteriormente i particolari mediante un'ordinanza.

Il risultato che si ottiene con la modifica proposta dell'articolo 99 capoverso 2 LM è che il SIS e il SAP trattano i dati personali in base agli stessi principi.

Art. 99a

In conformità con l'articolo 164 capoverso 1 Cost., tutte le disposizioni importanti che contengono norme di diritto vanno emanate sotto forma di legge federale. Le attuali disposizioni in materia di esplorazione radio contenute nell'ordinanza concernente la condotta della guerra elettronica comprendono norme di diritto, ma non hanno una base legale formale esplicita nella legge militare. Occorre pertanto istituire una base legale adeguata per tali disposizioni.

Cpv. 1

La disposizione sancisce nella legge la designazione dell'Autorità di controllo indipendente, l'equivalente dell'istanza di controllo indipendente (ICI) attualmente retta dalle disposizioni degli articoli 14 e seguenti dell'ordinanza del 15 ottobre 2003[58] concernente la guerra elettronica (OGEL).

L'Autorità di controllo indipendente, in linea di massima, controlla unicamente i mandati di esplorazione che non richiedono una particolare autorizzazione (individuale) sul piano politico, com'è il caso per i mandati di esplorazione radio permanente (p. es. del Servizio informazioni strategico del DDPS). L'esplorazione radio all'estero (effettuata dall'esercito) può avvenire anche durante gli interventi per la promozione della pace. In questo caso, la decisione parlamentare in merito include anche l'autorizzazione per l'esplorazione radio. Dal momento che tale autorizzazione è stata concessa dall'autorità politica competente, l'Autorità di controllo indipendente non è tenuta a un ulteriore esame del mandato di esplorazione radio.

L'Autorità di controllo indipendente verifica la legalità dell'esplorazione radio permanente, compresa la proporzionalità della misura, ma non si pronuncia in merito alla sua adeguatezza.

L'indipendenza è assicurata in quanto l'Autorità di controllo indipendente non è vincolata a istruzioni.

57 RS **510.291**
58 RS **510.292**

4. Legge sulle telecomunicazioni del 30 aprile 1997[59]

Art. 44

L'articolo 44 va completato dal momento che in futuro la sorveglianza del traffico delle comunicazioni non sarà più retta soltanto dalla LSCPT bensì anche dalla LMSI. La corrispondenza postale e il traffico delle telecomunicazioni sono sorvegliati in base alla LSCPT nell'ambito di un procedimento penale della Confederazione o di un Cantone, oppure per l'esecuzione di una domanda di assistenza giudiziaria in virtù della legge federale del 20 marzo 1981[60] sull'assistenza internazionale in materia penale (AIMP). Lo scopo della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni prevista dalla LMSI è di individuare minacce derivanti dal terrorismo, dallo spionaggio politico o militare, dal commercio illecito di armi o materiale radioattivo oppure dal trasferimento illegale di tecnologia.

5.–11.: Leggi sull'assistenza sociale

Legge federale del 20 dicembre 1946[61] **su l'assicurazione per la vecchiaia e per i superstiti (LAVS)**

Legge federale del 19 giugno 1959[62] **su l'assicurazione per l'invalidità (LAI)**

Legge federale del 25 giugno 1982[63] **sulla previdenza professionale per la vecchiaia, i superstiti e l'invalidità (LPP)**

Legge federale del 18 marzo 1994[64] **sull'assicurazione malattie (LAMal)**

Legge federale del 20 marzo 1981[65] **sull'assicurazione contro gli infortuni (LAINF)**

Legge federale del 19 giugno 1992[66] **sull'assicurazione militare (LAM)**

Legge federale del 25 giugno 1982[67] **su l'assicurazione obbligatoria contro la disoccupazione e l'indennità per insolvenza (LADI)**

Nel settore delle assicurazioni sociali, la trasmissione dei dati è disciplinata direttamente nelle diverse leggi ed è quindi riunita in un ordinamento esaustivo a se stante. Pertanto l'abrogazione del segreto d'ufficio nei confronti delle autorità di sicurezza della Confederazione e dei Cantoni sancita dall'articolo 13*a* del presente disegno di

59 RS **784.10**
60 RS **351.1**
61 RS **831.10**
62 RS **831.20**
63 RS **831.40**
64 RS **832.10**
65 RS **832.20**
66 RS **833.1**
67 RS **837.0**

legge implica un adeguamento specifico di queste leggi. Il segreto d'ufficio non viene abrogato integralmente, bensì soltanto alle condizioni di cui all'articolo 13*a*. La disposizione non contempla i segreti professionali legali (p. es. dei medici, degli avvocati, degli ecclesiastici ecc.) 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.

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.

La revisione del Codice civile (protezione degli adulti, diritto delle persone e diritto della filiazione) attualmente in corso (cfr. FF *2006* 6391) introduce nel settore delle assicurazioni sociali alcune disposizioni identiche a quelle della presente revisione della LMSI. Per uniformare questi due progetti paralleli di revisione, il Dipartimento presenterà proposte a tempo debito in base al loro avanzamento.

3 Ripercussioni

3.1 Ripercussioni per la Confederazione

3.1.1 Impatto finanziario

L'impatto finanziario dipende in larga misura dal genere e dalle modalità delle singole misure, ma soprattutto dalla necessità di utilizzarle (che dipende dagli eventi). Non esistono ancora valori empirici in merito, in particolare per quanto concerne la prassi d'autorizzazione giudiziaria ed esecutiva (per molti aspetti decisiva). Per gli stessi motivi non è possibile formulare indicazioni concrete su una possibile eventualità di risparmio (p. es. sostituire le osservazioni con la sorveglianza delle telecomunicazioni). Dalle stime effettuate, per il settore tecnico (apparecchi, equipaggiamento) le spese d'investimento uniche si aggirano attorno a un milione di franchi, le spese annuali ricorrenti sono di circa 100 000 franchi e le spese annuali ricorrenti per il personale di circa 6,5 milioni di franchi (compresi i contributi del datore di lavoro). Il finanziamento avviene facendo ricorso a risorse all'interno del Dipartimento.

3.1.2 Impatto sull'effettivo del personale

Le misure saranno attuate facendo ampio ricorso alle strutture federali e cantonali esistenti (Tribunale amministrativo federale, SAP e servizi d'informazione dei Cantoni). Complessivamente occorreranno una quarantina di posti supplementari, che tuttavia non richiederanno l'assunzione di personale esterno.

Il fabbisogno di personale supplementare sussiste negli ambiti seguenti:

– 35 posti presso il SAP per raccogliere ed esaminare le informazioni (agenti di polizia, interpreti, tecnici e analisti) e per uniformare il trattamento dei dati (registrazione dei dati, controllo della qualità e comunicazione con l'estero);

– altri 5 posti per adeguare le strutture delle unità amministrative che devono contribuire all'esecuzione dei compiti, ma che non fanno parte dei servizi d'informazione (p. es. i servizi tecnici e amministrativi del SCS del DATEC), per il Tribunale amministrativo federale e per la direzione di fedpol.

Pertanto le nuove competenze dovranno essere introdotte utilizzando poche risorse supplementari.

Nella procedura di consultazione talvolta si è messo in dubbio che la collaborazione attuale dei servizi coinvolti soddisfi i requisiti ed è stato chiesto di verificare i compiti, le procedure e le strutture degli enti amministrativi coinvolti.

In questo contesto rinviamo al nostro parere del 2 dicembre 2005 concernente la mozione Schlüer (05.3637: Raggruppamento dei servizi d'informazione in seno al DDPS e al DFGP): «Nel 2001, seguendo le richieste della CPI DFGP (affare delle schedature), l'Ufficio federale di polizia (fedpol) è stato riorganizzato di modo che, conformemente ai principi dell'organizzazione in funzione dei processi, le funzioni del servizio informazioni interno e di polizia giudiziaria sono state separate e attribuite internamente a differenti divisioni principali. Quest'ultime sono subordinate al direttore di fedpol, il quale è direttamente subordinato al capo del DFGP. Il Consiglio federale ritiene efficiente e adeguata questa ripartizione dei compiti e questa organizzazione interna al DFGP …».

D'altro canto il numero 3 del rapporto «Lotta più efficace contro il terrorismo e la criminalità organizzata»[68] si occupa dettagliatamente della cooperazione tra gli organi di perseguimento penale e il servizio d'informazione interno. In considerazione di queste circostanze riteniamo che non vi sia una necessità immediata di nuovi provvedimenti legislativi o politici in ambito strutturale. Non vi è motivo per tornare sull'argomento, poiché anche nelle decisioni del 24 gennaio 2007 sulla politica dei servizi d'informazione e la loro cooperazione abbiamo ritenuto non vi fosse ulteriore necessità di intervento.

3.1.3 Altre ripercussioni

Non sono state individuate altre ripercussioni specifiche.

3.2 Ripercussioni per i Cantoni e i Comuni

I Cantoni e i Comuni stanno innalzando il livello di sicurezza. L'intensificazione degli obblighi d'informazione e di comunicazione delle unità amministrative cantonali e comunali secondo gli articoli 13 e 13*a* del presente disegno di legge è compensata con determinati sgravi a media e lunga scadenza (accertamenti facilitati, parziale sostituzione delle osservazioni, particolarmente dispendiose in termini di personale, eseguite da agenti di polizia cantonali con i mezzi speciali per la ricerca di informazioni ecc.), che non sono ancora enumerabili allo stato attuale delle cose. A dipendenza del genere e delle modalità delle nuove misure, sono ipotizzabili oneri di lavoro supplementari nei Cantoni.

68 Cfr. rapporto relativo al postulato CPS.

3.3 Impatto economico

In base alle nostre direttive del 15 settembre 1999 concernenti la presentazione delle conseguenze per l'economia dei progetti di atti normativi federali (cfr. rapporto del Consiglio federale concernente misure di deregolamentazione e sgravio amministrativo; FF *2000* 888), vanno esaminati i punti seguenti.

3.3.1 Necessità e possibilità d'intervento dello Stato

L'attuazione del disegno aumenta la sicurezza della Svizzera e mira tra l'altro all'attuazione degli interventi parlamentari.

3.3.2 Conseguenze per i singoli gruppi della società

Le disposizioni proposte rafforzano la sicurezza interna ed esterna e quindi migliorano la protezione della popolazione.

3.3.3 Conseguenze per l'insieme dell'economia

Non si prevedono ripercussioni dirette sull'economia in generale. Indirettamente, invece, un contesto sicuro ed economicamente stabile migliora le condizioni quadro economiche e rafforza quindi la piazza economica svizzera.

3.3.4 Disciplinamenti alternativi

Ogni singolo Cantone è responsabile in primo luogo della sicurezza interna del proprio territorio. Per quanto in virtù della Costituzione e della legge la Confederazione sia responsabile della sicurezza interna, i Cantoni devono assisterla sul piano dell'amministrazione e dell'esecuzione. Secondo la legge in vigore, alla Confederazione compete in particolare di individuare tempestivamente le minacce derivanti da terrorismo, spionaggio politico o militare, estremismo violento, commercio illecito di armi o di materiale radioattivo oppure trasferimento illegale di tecnologia (non proliferazione). La Confederazione assiste le competenti autorità di polizia e di perseguimento penale comunicando loro informazioni in merito al crimine organizzato. Pertanto, la Confederazione legifera nell'ambito delle sue competenze; non vi è spazio per disciplinamenti alternativi.

3.3.5 Aspetti pratici dell'esecuzione

Il progetto è attuato sulla base delle attuali strutture collaudate delle autorità di sicurezza. Non cambia tuttavia il principio della responsabilità congiunta della Confederazione e dei Cantoni in materia di protezione dello Stato.

3.4 Altre ripercussioni

3.4.1 Impatto sulla politica estera

L'immagine internazionale della Svizzera può trarre un profitto a lungo termine, in particolare per quanto concerne la volontà di combattere efficacemente il terrorismo internazionale. Inoltre le attività in Svizzera dei gruppi estremisti violenti provenienti dall'estero possono essere individuate prima ed essere maggiormente controllate. Questa richiesta era già stata avanzata molto tempo fa dalla Giunta del Consiglio federale in materia di sicurezza.

3.4.2 Impatto sulle relazioni internazionali

Sul piano formale, la revisione della legge non mette in atto alcun impegno internazionale. L'adeguamento degli standard invece porterà probabilmente a un netto miglioramento della collaborazione internazionale.

4 Programma di legislatura

Il disegno non è stato annunciato nel programma di legislatura 2003–2007 (FF *2004* 969).

Tuttavia fa parte del nostro obiettivo 19 per il 2007: «Ottimizzare la cooperazione internazionale, la prevenzione e le strutture interne nei settori di giustizia e polizia».

L'urgenza e la necessità del disegno sono dettate dalla sempre più grave situazione in cui versa la Svizzera in materia di sicurezza e di minaccia, che si è notevolmente acuita a causa degli attentati compiuti da terroristi islamici. L'Europa occidentale quindi non è più soltanto un'area di rifugio e di preparazione e la Svizzera ormai fa parte dei Paesi a rischio. La legge oggi in vigore tollera nell'ambito della sicurezza rischi che non sono compatibili con il cambiamento della situazione di minaccia. A rischio risulta essere anche la capacità di offrire solidarietà a livello internazionale (soprattutto con l'ONU e gli Stati europei).

5 Aspetti giuridici

5.1 Costituzionalità

La LMSI si fonda sulla competenza non scritta della Confederazione di salvaguardare la sicurezza interna ed esterna e sui compiti della Confederazione per la tutela della sicurezza interna (art. 173 Cost.). In questo ambito s'inserisce anche la presente revisione di legge, che non va oltre i compiti attuali descritti nell'articolo 2 capoversi 1 e 2 LMSI, ma si limita ad applicare singole misure ad atti di terrorismo, di spionaggio politico o militare, di commercio illecito di armi o materiale radioattivo oppure al trasferimento illegale di tecnologia. Né lo spionaggio economico, né la criminalità organizzata sono oggetto delle misure speciali per la ricerca di informazioni della presente revisione.

Le misure proposte nell'ambito della presente revisione possono ledere i diritti fondamentali, più in particolare la sfera privata (art. 13 Cost.), la libertà d'associazione (art. 23 Cost.), la libertà di credo e di coscienza (art. 15 cpv. 3 Cost.), la libertà di riunione (art. 22 Cost.) e la garanzia della proprietà (art. 26 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 dev'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.

Gli strumenti e le misure proposti vanno sanciti in una legge formale, la LMSI. L'interesse pubblico consiste nel salvaguardare la sicurezza interna o esterna e nell'individuare tempestivamente le minacce derivanti da attività di terrorismo, di spionaggio politico o militare, di commercio illecito di armi o materiale radioattivo oppure dal trasferimento illegale di tecnologia. È inconfutabile l'esistenza di un interesse pubblico legittimo. Per l'analisi della proporzionalità delle nuove misure, si rimanda alle spiegazioni dei singoli articoli. A questo proposito va anche ricordato che, nell'accertare la proporzionalità di un intervento statale, vanno prese in considerazione anche le circostanze connesse con le misure in questione (come nel parere espresso dal Tribunale federale nella procedura di consultazione). Del resto, le condizioni per ordinare l'impiego di mezzi speciali per la ricerca di informazioni di cui all'articolo 18*b*, e in particolare alla lettera c, evidenziano inequivocabilmente la natura sussidiaria delle misure suscettibili di ledere i diritti fondamentali. Vanno insomma adottate soltanto qualora altre misure di ricerca di informazioni risultino insufficienti per accertare un sospetto concreto di minaccia alla sicurezza interna o esterna.

I singoli strumenti e le misure contenuti nel progetto sono conformi alla Costituzione. I principi dello Stato di diritto sono pienamente salvaguardati.

5.2 Compatibilità con gli impegni internazionali della Svizzera

In veste di Parte contraente di vari trattati e convenzioni internazionali dei diritti dell'uomo, la Svizzera è tenuta a informare regolarmente gli organi di controllo internazionali sull'attuazione dei suoi impegni di diritto pubblico internazionale. Anche sotto questo profilo, l'approvazione degli strumenti e delle misure qui proposti costituisce un contributo importante alla lotta contro il terrorismo e altre gravi minacce per la sicurezza internazionale. L'immagine internazionale della Svizzera non può che trarne vantaggio.

Sia lo scopo generale sia le singole disposizioni del presente disegno di legge sono conformi alla CEDU e al Patto internazionale del 16 dicembre 1966[69] relativo ai diritti civili e politici (Patto II).

Secondo la CEDU, l'esercizio dei diritti fondamentali (quali il rispetto della vita privata e familiare di cui all'art. 8 o la libertà di riunione ed associazione secondo l'art. 11 CEDU) può essere limitato, se tale restrizione è prevista dalla legge, perse-

69 RS **0.103.2**

gue uno scopo legittimo ed è necessaria in una società democratica. La presente revisione soddisfa le esigenze di una legge in senso materiale secondo la CEDU. In particolare, le nuove disposizioni specificano, con sufficiente precisione, le persone interessate dalle misure (cfr. art. 18*k*–18*n*), le condizioni (cfr. art. 18*a* e 18*b*) e le garanzie procedurali (cfr. art. 18*d*, 18*e*, 18*f* e 18*i*). La verifica delle altre due condizioni (scopo legittimo, necessità in una società democratica) corrisponde a quella dell'interesse pubblico e della proporzionalità (cfr. quanto illustrato sopra).

Il Patto II (art. 17 e 22) non offre – rispetto alla CEDU o alla Costituzione – una tutela più marcata dei diritti fondamentali in questione.

Per il resto, le misure proposte sono senz'altro conformi agli accordi e alle convenzioni specifiche in materia di terrorismo.

5.3 Forma dell'atto

5.3.1 Forma legislativa

Le disposizioni importanti che contengono norme di diritto in materia di restrizioni dei diritti costituzionali devono essere emanate sotto forma di legge federale (art. 36 cpv. 1, art. 163 cpv. 1 e art. 164 cpv. 1 Cost.). Questi requisiti sono adempiuti.

5.3.2 Revisione parziale

Anche se per motivi di chiarezza sarebbe stata auspicabile una revisione totale, si è optato per una revisione parziale per i motivi seguenti:

- al momento non è ancora stato deciso il futuro delle norme limitate nel tempo contenute nel progetto LMSI I (lotta alla violenza in occasione di manifestazioni sportive) dopo la decorrenza della loro validità (2009);
- pur contenendo relativamente numerosi articoli, le modifiche auspicate nel quadro della presente revisione di legge sono nella sostanza limitate a poche tematiche e incentrate chiaramente sulla ricerca di informazioni con l'ausilio di mezzi speciali;
- il collocamento delle modifiche auspicate nella sistematica della legge è giustificabile, anche se non ottimale.

5.4 Subordinazione al freno alle spese

Conformemente all'articolo 159 capoverso 3 lettera b della Costituzione il presente disegno di legge dev'essere approvato dalla maggioranza dei membri di entrambe le Camere, se le nuove spese ricorrenti superano i 2 milioni di franchi. Nel disegno questa condizione è soddisfatta, ma il fabbisogno di personale e di mezzi finanziari sarà coperto facendo ricorso a risorse all'interno del Dipartimento.

5.5 Conformità alla legge sui sussidi

Nella procedura di consultazione i Cantoni chiedono unanimemente che la Confederazione rimborsi loro le eventuali spese supplementari per la protezione dello Stato.

L'articolo 28 capoverso 1 LMSI disciplina le prestazioni finanziarie ai Cantoni come segue: «La Confederazione rimborsa ai Cantoni le prestazioni fornite dietro suo mandato ai sensi della sezione 3. Il Consiglio federale fissa l'indennità forfettaria sulla base del numero di persone che svolgono essenzialmente compiti federali».

Nel relativo rapporto esplicativo è stato esposto che nel caso del trattamento delle informazioni, un mancato rimborso dei costi potrebbe avere conseguenze gravi. Questo giustifica una deroga al principio secondo cui i Cantoni debbano sostenere i costi per l'esecuzione del diritto federale. Le spiegazioni in questione mantengono la loro validità.

5.6 Delega di competenze legislative

Secondo l'articolo 10*a* del presente disegno il Consiglio federale disciplina nei particolari i diritti d'accesso e i principi validi per la conservazione e la cancellazione dei dati applicabili al sistema d'informazione elettronico della situazione e della gestione. Inoltre stabilisce all'interno di un'ordinanza le organizzazioni che secondo l'articolo 13*a* del disegno sono tenute a informare le autorità e conformemente all'articolo 14*a* del disegno disciplina nei particolari le attività, l'organizzazione e la procedura dell'esplorazione radio. Ai sensi dell'articolo 99*a* LM disciplina la composizione dell'Autorità di controllo indipendente, l'indennizzo dei suoi membri e l'organizzazione della sua segreteria.

Diritto comparato (Germania, Austria, Francia, Italia, Lussemburgo, Paesi Bassi, UE)

1. Germania

La Repubblica federale di Germania è uno Stato federale con un sistema federalista. L'ordinamento costituzionale federalista conferisce di principio alle regioni (Länder) la sovranità in materia di polizia sui loro rispettivi territori.

Il compito principale dei servizi di sicurezza dello Stato federale e delle regioni consiste nel raccogliere e analizzare le informazioni sui tentativi di attentare all'assetto istituzionale democratico e liberale, come pure su attività e manovre di spionaggio o di minaccia alla sicurezza nel campo d'applicazione della legge sull'Ufficio federale di tutela della Costituzione[70].

Lo Stato federale e le regioni sono tenuti a collaborare per tutelare la Costituzione. Lo Stato federale gestisce l'Ufficio federale di tutela della costituzione (Bundesamt für Verfassungsschutz, BfV), subordinato al ministro dell'interno. Il BfV è autorizzato a trattare e utilizzare le informazioni necessarie all'adempimento dei propri compiti, compresi i dati personali, purché non vi si oppongano le disposizioni pertinenti della legge tedesca sulla protezione dei dati o norme particolari della BVerfSchG. Può inoltre richiedere dati e informazioni alle autorità di repressione[71]. Viceversa, il Servizio federale di informazione (Bundesnachrichtendienst, BND) può trasmettere informazioni ad autorità nazionali se l'adempimento dei suoi compiti lo richiede o se i dati sono necessari ai fini della sicurezza pubblica[72]. Tali dati possono essere utilizzati per il perseguimento penale.

L'attività del BfV è sorvegliata da un comitato parlamentare di controllo (PKGr), che va regolarmente aggiornato sulle attività generali del BfV e sugli eventi di particolare rilevanza[73]. Se il PKGr lo richiede, il governo federale deve consentirgli di consultare gli atti e i dati e interrogare i propri collaboratori. Su domanda, il BfV comunica gratuitamente a una persona interessata i dati memorizzati che la riguardano, purché essa indichi fatti concreti e faccia valere un interesse particolare per l'informazione[74]. I dati memorizzati vanno rettificati se risultano errati. Dopo cinque anni al massimo, il BfV deve verificare se, nel caso specifico, i dati vanno rettificati o cancellati. Trascorsi 15 anni dall'ultima memorizzazione, le informazioni devono essere cancellate, a meno che i vertici delle autorità non decidano altrimenti[75].

Qui di seguito è illustrata la normativa federale.

70 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz; BVerfSchG).
71 § 18 BVerfSchG.
72 § 9 Gesetz über den Bundesnachrichtendienst del 20 dicembre 1990 (BNDG).
73 § 2 Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes.
74 § 15 BVerfSchG.
75 § 12 BVerfSchG.

Per adempiere i propri compiti, il BfV è autorizzato in singoli casi a servirsi tra l'altro di dati e servizi di telecomunicazione[76]. L'istanza motivata va presentata per iscritto dal presidente del BfV o dal suo rappresentante. La decisione in merito spetta al ministero federale incaricato dal cancelliere. Prima di autorizzare il BfV a procedere, il ministero designato informa, a scadenza mensile, la commissione G 10 sulle istanze approvate. In caso di pericolo nel ritardo, il ministero può disporre l'esecuzione della decisione prima di informare la commissione[77]. Il ministero competente informa, a intervalli di sei mesi al massimo, il PKGr sulle ricerche di informazioni effettuate. Il BfV è inoltre autorizzato a servirsi di informatori, a procedere a osservazioni e registrazioni di suoni e immagini e a utilizzare documenti fittizi e targhe false[78]. Queste misure vanno indicate in una norma di servizio, che dev'essere approvata dal Ministero degli interni, che a sua volta ne mette al corrente il PKGr. Se si raccolgono informazioni direttamente presso gli interessati, occorre indicare lo scopo del rilevamento.

Il BfV è inoltre autorizzato, a determinate condizioni, a richiedere informazioni alle banche[79]. Nelle indagini sui canali di comunicazione di gruppi terroristici, il BfV può inoltre chiedere ai fornitori di servizi postali di rivelare taluni dati, quali nomi, indirizzi e indicazioni sulle caselle postali, e di comunicare i dati su collegamenti, quali identificazioni, numeri di chiamata e dati di posizione[80]. Il BfV può infine servirsi di dispositivi d'intercettazione per individuare i numeri degli apparecchi e delle carte di telefonia mobile[81]. Vigono le stesse condizioni applicabili alle intercettazioni telefoniche.

I servizi tedeschi preposti alla tutela della Costituzione non hanno, per contro, alcuna competenza in materia di polizia, in particolare non sono autorizzati a effettuare perquisizioni e sequestri.

In seguito agli attentati dell'11 settembre 2001, la legge limitata nel tempo sulla lotta al terrorismo (Terrorismusbekämpfungsgesetz, TBGE)[82] è stata rivista il 12 luglio 2006 e la revisione è stata approvata dal gabinetto della Repubblica federale sotto forma di un emendamento alla legge sulla lotta al terrorismo (Terrorismusbekämpfungsergänzungsgesetz, TBEG)[83]. I servizi d'informazione sono ora autorizzati a consultare online le informazioni contenute nella banca dati sui veicoli. Per prevenire gravi minacce è possibile anche segnalare a livello europeo persone sospette senza comunicarlo ai diretti interessati. Così, quando le persone segnalate sono controllate dalla polizia, i servizi d'informazione ne vengono informati. Le richieste d'informazione possono ora riguardare anche le attività che violano la Costituzione. Le norme critiche dei servizi d'informazione restano in vigore per cinque anni e prima della scadenza vengono riesaminate.

76 § 8 cpv. 8 BVerfSchG.
77 § 8 cpv. 9 BVerfSchG.
78 § 8 cpv. 2 BVerfSchG.
79 § 8 cpv. 5 BVerfSchG.
80 § 8 cpv. 6 BVerfSchG e § 8 cpv. 8 BVerfschG.
81 § 9 cpv. 4 BVerfSchG.
82 Terrorismusbekämpfungsgesetz del 9 gennaio 2002 (BGBI I 2002, pagg. 361, 3142).
83 Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes vom 5. Januar 2007 (BGBI I 2007, 2).

2. Austria

L'Austria ha un assetto istituzionale federalista. Il suo ordinamento giuridico distingue in linea di massima tra repressione e prevenzione. L'Ufficio federale per la tutela della costituzione e la lotta al terrorismo (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, BVT) funge da servizio d'informazione in ambito civile[84]. I compiti del BVT sono in sostanza la difesa dello Stato e delle sue istituzioni costituzionali e comprendono in particolare la lotta al terrorismo internazionale, all'estremismo, allo spionaggio, al traffico d'armi internazionale, al commercio di materiale nucleare e al crimine organizzato che opera in questi settori. Il BVT è integrato nella Direzione generale per la sicurezza pubblica (Generaldirektion für die öffentliche Sicherheit) del Ministero degli interni.

Per adempiere i propri compiti in materia di tutela della costituzione, ogni regione è dotata di un Ufficio regionale per la tutela della costituzione e la lotta al terrorismo (Landesamt für Verfassungsschutz und Terrorismusbekämpfung, LVT) integrato nella relativa direzione della sicurezza. Il BVT decide, coordina e applica per il tramite dei LVT, le misure a tutela delle persone e degli oggetti e a protezione dei rappresentanti di Stati stranieri, di organizzazioni internazionali e di altre persone protette dal diritto internazionale.

I servizi di protezione dello Stato possono accedere ai dati raccolti dalle autorità di repressione, che trasmettono loro le proprie informazioni. Le persone interessate hanno il diritto di essere informate, di chiedere la rettifica o la cancellazione dei dati personali che le riguardano e di ricorrere dinanzi alla Commissione per la protezione dei dati. Qualora gli interessi di protezione dello Stato lo esigano, in casi eccezionali il diritto di essere informati non è concesso.

Le autorità di sicurezza che indagano più a fondo sulle minacce devono comunicare senza indugio al ministro dell'interno le misure adottate. Le indagini nel settore sono consentite soltanto dopo aver consultato il garante dei rimedi giuridici o dopo un periodo di tre giorni, salvo se è necessario indagare immediatamente per prevenire una grave minaccia[85].

Se il garante dei rimedi giuridici riscontra che l'utilizzo dei dati personali lede i diritti di persone ignare di tale uso, egli è autorizzato a informarle o, se ciò non è possibile, a ricorrere dinanzi alla Commissione per la protezione dei dati.

Il garante dei rimedi giuridici stila un rapporto annuale relativo alle indagini approfondite sulle minacce (sorveglianza di gruppi) e lo sottopone al ministro dell'interno[86]. Il sottocomitato permanente del Consiglio nazionale può chiedere di prendere visione di tale rapporto.

A determinate condizioni, i servizi di protezione dello Stato sono autorizzati a richiedere informazioni ai fornitori di servizi di telecomunicazione. Tuttavia, la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni è permessa soltanto alle autorità di repressione. Sono altresì ammesse l'inchiesta mascherata e la registrazione di suoni sotto copertura[87]. La registrazione di suoni in assenza dell'agente infiltrato non è ammessa. Il garante dei rimedi giuridici vigila

84 Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei del 31 ottobre 1992 (Sicherheitspolizeigesetz; SPG).
85 § 62a cpv. 7 SPG (SPG Novelle 2005).
86 § 21 cpv. 3 SPG.
87 § 54 SPG.

costantemente sull'inchiesta mascherata e sull'impiego sotto copertura di apparecchi di registrazione di immagini e suoni[88]. Egli va messo al corrente delle inchieste e dei motivi principali che vi hanno dato adito, nella misura in cui l'identità degli interessati sia nota. I servizi di protezione dello Stato possono inoltre mettere al sicuro, sequestrare e confiscare oggetti[89], sorvegliare locali privati[90] e accedervi[91], come pure ordinare ed effettuare interrogatori[92]. In determinati casi, gli intermediari finanziari devono fornire informazioni alle autorità competenti[93].

L'attività del BTV è soggetta al controllo parlamentare in virtù dell'articolo 52*a* della costituzione austriaca. Una volta esauriti tutti gli altri rimedi giuridici amministrativi, è possibile ricorrere dinanzi al Tribunale amministrativo o alla Corte costituzionale.

L'11 settembre 2001 ha lasciato il segno anche in Austria. Le strutture sono state snellite, le disposizioni di legge inasprite e i servizi di protezione dello Stato godono ora di competenze più ampie.

Le nuove disposizioni della SPG del 2002 estendono ai familiari la protezione offerta a persone in grado di fornire informazioni su un attacco pericoloso o un gruppo criminale. Sono altresì state modificate le basi legali per dissimulare i provvedimenti di sostegno in occasione di osservazioni o inchieste mascherate. Per combattere l'avanzata dell'estremismo, il 1° ottobre 2000 sono state inserite nella SPG le disposizioni in materia di indagini approfondite sulle minacce e i rimedi giuridici pertinenti[94]. Tali disposizioni permettono alle autorità di sicurezza di sorvegliare gruppi di persone, qualora si possa presumere che commetteranno reati in grado di mettere gravemente a repentaglio la sicurezza pubblica. Prima della modifica di legge, le autorità di sicurezza potevano sorvegliare i gruppi estremisti soltanto se questi avevano già perpetrato un reato.

Mediante una nuova disposizione della SPG del dicembre 2003 è stata introdotta un'attestazione con cui si può certificare il potenziale di rischio a cui sono esposte determinate imprese e impianti[95].

Il 1° dicembre 2002, in seno al Ministero degli interni è stato istituito il BVT[96] che è subordinato direttamente al direttore generale per la sicurezza pubblica.

Il BVT svolge la sua attività nel campo d'applicazione della SPG e, quando agisce al servizio della giustizia penale, si attiene alle disposizioni del codice di procedura penale (Strafprozessordnung, StPO).

88 § 62a cpv. 7 SPG.
89 § 42 SPG.
90 § 54 cpv. 2 SPG.
91 § 39 SPG.
92 § 28*a* SPG.
93 § 38 Bankwesengesetz (BWG).
94 §§ 21 cpv. 3, 53 cpv. 1 Z. 2a, 54 cpv. 2 e 62*a* SPG.
95 § 55-55b SPG.
96 § 7 cpv. 1 e 9 Bundesministeriengesetz.

3. Francia

La Francia è una democrazia ad assetto centralizzato. Al contrario dei Cantoni svizzeri, le 26 regioni non godono di una vera e propria autonomia.

La sicurezza interna compete direttamente al primo ministro, che è assistito dal segretariato generale per la difesa nazionale (SGDN)[97] e da un gabinetto militare. Della sicurezza interna si occupano vari servizi statali, ragion per cui non vi è un'effettiva separazione tra prevenzione e repressione.

La Francia possiede due servizi di sicurezza indipendenti: la polizia e la gendarmeria nazionale (Gendarmerie Nationale). La prima opera nelle città, la seconda in campagna. Alla gendarmeria mobile competono la salvaguardia dell'ordine pubblico e la lotta al terrorismo, al crimine organizzato e alle sette. La polizia nazionale, subordinata al Ministero degli interni e diretta dalla Direzione generale della polizia nazionale (DGPN)[98], comprende varie subdirezioni, tra cui la Direzione della sorveglianza del territorio (D.S.T.)[99], la Direzione generale dei servizi d'informazione (DCRG)[100] e l'Unità di coordinamento per la lotta al terrorismo[101].

La D.S.T. funge da servizio d'informazione incaricato di combattere i crimini che minacciano la sicurezza dello Stato[102]. La sua organizzazione e il suo ruolo sono disciplinati in un decreto segreto dell'8 marzo 1993. La D.S.T. è l'ufficio centrale che raccoglie, tratta e smista tutte le informazioni che le sono trasmesse dalla DCRG e contribuisce alla protezione di settori sensibili e di segreti della difesa nazionale. La DCRG gestisce un sistema d'informazione a cui ha accesso anche la D.S.T[103].

L'Unità di coordinamento per la lotta al terrorismo coordina i lavori di tutti i servizi nazionali che operano in Francia e all'estero.

Il SGDN è un'autorità interministeriale cui competono tra l'altro la sicurezza dei sistemi d'informazione, la prevenzione e la difesa dal terrorismo, la protezione delle strutture di gestione e di comunicazione del Governo e la lotta alla proliferazione nucleare; inoltre sorveglia l'esportazione di materiale bellico.

La direzione generale della sicurezza esterna (DGSE)[104] funge per contro da servizio segreto operante all'estero e responsabile della sicurezza esterna della Francia. La DGSE è subordinata al primo ministro e i suoi compiti comprendono la ricerca di informazioni e gli interventi.

Il diritto di consultare i sistemi d'informazione della DCRG è di norma conferito mediante una procedura cosiddetta indiretta[105]. La relativa richiesta va presentata alla Commissione nazionale dell'informazione e delle libertà (Commission nationale de l'information et des libértés, CNIL). Questa commissione indipendente verifica le informazioni e informa il richiedente di eventuali rettifiche. Se la sicurezza interna non è minacciata, i dati possono essere comunicati al richiedente. Se la banca dati

97 Secrétariat Générale de la Défense Nationale.
98 Direction Générale de la Police Nationale.
99 Direction de la surveillance du territoire.
100 Direction Centrale des Renseignements généraux.
101 Unité de coordination de la lutte antiterroriste.
102 Decreto n. 82-1100 del 22 dicembre 1982, aggiornato il 15 settembre 2004.
103 Decreti n. 91-1052 e 91-1051.
104 Direction Générale de la Sécurité Extérieure.
105 Loi pour la sécurité intérieure (LOI nº 2003-239 del 18 marzo 2003), qui di seguito denominata legge del 18 marzo 2003).

contiene informazioni la cui comunicazione al diretto interessato non mette a repentaglio lo scopo stesso della banca dati, il responsabile del sistema può informare direttamente l'interessato.

Nell'interesse della sicurezza interna possono essere disposte intercettazioni telefoniche preventive per tutelare l'economia della Francia, prevenire il terrorismo, combattere il crimine organizzato e sorvegliare i gruppi illegali[106]. Secondo l'articolo 4 della legge del 10 luglio 1991, l'autorizzazione è conferita per ordine del primo ministro o di due persone da lui designate su istanza del ministro della difesa, del ministro dell'interno, del ministro delle dogane o dei loro supplenti. Il primo ministro stabilisce contingenti per limitare il numero delle misure disposte eseguibili contemporaneamente; il relativo controllo è affidato alla Commissione nazionale di controllo delle intercettazioni per la salvaguardia della sicurezza (Commission nationale de contrôle des interceptions de sécurité)[107], esterna all'amministrazione e composta di un presidente designato dal presidente della Repubblica per una durata di sei anni e da altre persone. L'autorizzazione è accordata per quattro mesi al massimo e può essere prorogata alle medesime condizioni per altri quattro mesi al massimo. Le informazioni ottenute durante la sorveglianza devono essere distrutte sotto la supervisione del primo ministro, al più tardi entro dieci giorni dalla loro raccolta.

La commissione ha stabilito che tutti i dati inerenti alle intercettazioni preventive vanno classificati come segreti riguardanti la difesa nazionale (Secret-Défense). Questo significa, tra l'altro, che le persone sorvegliate a titolo preventivo non vanno informate perché tale informazione potrebbe compromettere gravemente la difesa nazionale (défense nationale). I servizi francesi di protezione dello Stato non sono tuttavia autorizzati a sorvegliare la corrispondenza postale.

In casi eccezionali è possibile, in virtù di una decisione motivata, confiscare e trattenere oggetti di valore se la sicurezza interna lo richiede[108]. Sono previsti interrogatori. Inoltre sono consentite perquisizioni di vetture e abitazioni senza l'autorizzazione di un giudice[109]. In caso di criminalità organizzata, sono altresì ammessi interventi notturni.

Per quanto attiene alle registrazioni di suoni e immagini sotto copertura, ai documenti fittizi e alle targhe false, la legge del 18 marzo 2003 ha istituito varie competenze: sono ad esempio ammessi l'accesso diretto a sistemi d'informazione e la richiesta d'informazioni presso banche e privati. In determinate circostanze possono essere vietate talune attività, in particolare nel caso di manifestazioni armate e di organizzazioni che potrebbero mettere in pericolo la sicurezza della Francia[110]. Nell'ambito del crimine organizzato è consentito l'impiego di informatori con notifica al pubblico ministero in un secondo tempo. Gli informatori vengono rimborsati attingendo a fondi speciali[111].

106 Art. 3 della legge n. 91-646 del 10 luglio 1991 (Loi relative au secret des correspondances émises par la voie des télécommunications), qui di seguito denominata legge del 10 luglio 1991.
107 Art. 5 della legge del 10 luglio 1991.
108 Art. 3 della legge del 18 marzo 2003 e legge n. 2005–750 del 4 luglio 2005 (Loi nº 2005–750).
109 Legge n. 2004–204 del 9 marzo 2004, qui di seguito denominata legge del 9 marzo 2004.
110 Legge del 10 gennaio 1936.
111 Legge del 9 marzo 2004.

Una legge del 19 gennaio 2006 consente fra l'altro una sorveglianza video più ampia in luoghi pubblici e installazioni a rischio in caso di eventuali minacce di attentati terroristici, autorizza la polizia o la gendarmeria nazionale ad accedere ai dati elettronici in possesso dei fornitori di servizi di telecomunicazione e delle compagnie aeree, permette di prorogare il fermo di polizia e introduce controlli a bordo dei treni internazionali[112].

La Francia non conosce alcun sistema di controllo parlamentare, ma sta elaborando vari progetti di legge in tal senso. Il Governo deve comunque rendere conto al Parlamento.

4. Italia

Contrariamente alla Svizzera, alla Germania e all'Austria, che sono Stati federali, l'Italia è uno Stato unitario decentralizzato.

La salvaguardia della sicurezza interna ed esterna poggia su tre pilastri: il SISMI (Servizio per le informazioni e la sicurezza militare), il SISDE (Servizio per le informazioni e la sicurezza democratica) e la D.I.A. (Direzione investigativa antimafia).

La salvaguardia della sicurezza interna compete al Ministero degli interni, cui è subordinata la Direzione centrale per la polizia di prevenzione (DCPP)[113].

La DCPP ha il compito di combattere le organizzazioni terroristiche interne ed esterne e i gruppi paramilitari e violenti. L'articolo 6 della legge 121 permette infatti di classificare, analizzare e valutare dati per garantire la sicurezza.

Mentre il SISMI è competente per quanto avviene all'estero, il SISDE sorveglia le attività in Italia. Il SISDE è incaricato di combattere il terrorismo, l'immigrazione illegale, la criminalità informatica, lo spionaggio economico, le nuove minacce e il crimine organizzato.

Il SISDE raccoglie dati per tutelare la sicurezza interna. Esiste un diritto di consultazione generale[114], ma tutti i documenti e gli atti la cui pubblicazione potrebbe compromettere la sicurezza nazionale sono soggetti al segreto di Stato[115]. Il Garante per la protezione dei dati personali controlla quali dati vengono raccolti. Nell'ambito della sicurezza informatica, i servizi di protezione dello Stato collaborano con la polizia giudiziaria.

Una commissione parlamentare sorveglia le attività del SISMI e del SISDE. Il Governo presenta al Parlamento un resoconto semestrale delle attività dei servizi. Le attività dei servizi d'informazione sono inoltre controllate da organi giudiziari.

112 Legge n. 2005-532 del 19 gennaio 2006 (Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers), qui di seguito denominata legge del 19 gennaio 2006.
113 Legge n. 121 del 1981 Nuovo ordinamento dell'Amministrazione della pubblica sicurezza, qui di seguito denominata legge 121.
114 Decreto legislativo del 30 giugno 2003, n. 196, qui di seguito denominato decreto 196.
115 Art. 12 della legge del 24 ottobre 1997.

La D.I.A. adotta misure contro il crimine organizzato, quali la sorveglianza e le intercettazioni telefoniche, e svolge indagini antimafia[116]. Può raccogliere informazioni sulla situazione finanziaria delle persone sospettate di appartenere a un'organizzazione criminale. La D.I.A. trasmette le informazioni ottenute al SISDE e al SISMI e collabora con le forze di polizia.

In linea di massima i dati possono essere trattati soltanto con il consenso degli interessati, a meno che il trattamento non rientri nell'adempimento di un compito legale[117].

Con il decreto legge del 17 luglio 2005 è stata introdotta una serie di nuove competenze e misure a disposizione dei servizi di protezione dello Stato[118]. Ora è ad esempio consentito intercettare le telefonate a titolo preventivo se sussiste un sospetto fondato di terrorismo o una minaccia all'ordinamento statale. Di norma, la richiesta va prima motivata dal presidente del Consiglio dei ministri, che può delegare le sue competenze ai servizi d'informazione. L'ordine è emanato dalla procura di Stato, previa approvazione del giudice. Se vi è pericolo nel ritardo, l'ordine può essere emanato senza l'approvazione del giudice. Questa va tuttavia richiesta per via ordinaria entro 24 ore e il giudice deve decidere in merito entro 48 ore. Se tale scadenza non viene rispettata, le informazioni raccolte non possono essere utilizzate in tribunale.

La legge 675, che scade alla fine di dicembre del 2007, obbliga inoltre le società telefoniche e i provider a conservare i dati telefonici e quelli relativi a Internet. Ora anche i servizi di protezione dello Stato possono interrogare i detenuti in assenza di un avvocato difensore (colloquio investigativo), prassi finora riservata ai reati di stampo mafioso.

È poi stata introdotta la possibilità di agevolare l'espulsione di persone sospette che minacciano la sicurezza pubblica o appoggiano in qualche maniera un'organizzazione terroristica. L'espulsione è eseguita senza indugio, ma può essere impugnata dinanzi al tribunale amministrativo. Se la decisione di espulsione poggia su fonti dei servizi segreti, l'udienza può essere aggiornata di due anni. La decisione di espulsione può essere sospesa se l'interessato coopera con le autorità. Se la cooperazione è determinante ai fini delle indagini sul terrorismo, l'interessato può ottenere il permesso di residenza, revocabile in caso di abuso.

La legge del 27 luglio 2005 autorizza infine il Ministero degli interni a istituire unità investigative interforze per combattere il terrorismo.

116 Legge n. 410 del 1991, qui di seguito denominata legge 410.

117 Art. 12 comma 1 della legge n. 675 del 31 dicembre 1996 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, qui di seguito denominata legge 675.

118 Testo del decreto legge del 27 luglio 2005 n. 144, coordinato con la legge di conversione del 31 luglio 2005, qui di seguito denominata legge del 27 luglio 2005.

5. Lussemburgo

Il Lussemburgo è una monarchia costituzionale retta da una democrazia parlamentare ed è suddiviso in tre distretti comprendenti dodici cantoni e 118 comuni.

In Lussemburgo la protezione preventiva dello Stato è affidata a tre organizzazioni: il Servizio d'informazione per la sicurezza interna (SRDE)[119], il Servizio d'informazione per la sicurezza esterna (HCSE)[120] e il Servizio d'informazione militare[121]. Il SRDE è subordinato al Ministero dell'interno.

Il SRDE è incaricato di combattere il terrorismo, lo spionaggio, la proliferazione di armi non convenzionali e le tecnologie connesse e il crimine organizzato che opera in questi settori. Sono inoltre di sua competenza tutte le attività che possono compromettere l'integrità, la sovranità e l'indipendenza del Paese, la sicurezza delle istituzioni e della popolazione oppure il funzionamento dello Stato[122]. Nell'ambito delle sue competenze, il SRDE coopera sia con gli organi di polizia, le autorità giudiziarie e l'amministrazione, sia con il HCSE. La polizia, le autorità giudiziarie e l'amministrazione sono tenute a trasmettere al SRDE le informazioni che rientrano nel campo d'applicazione dell'articolo 2 della legge sull'organizzazione del 15 giugno 2004.

Il trattamento dei dati personali da parte del SRDE è retto dalle disposizioni della legge del 2 agosto 2002[123]. Il SRDE può accedere a un numero limitato di banche dati, in particolare a quella generale della polizia, a quella della polizia degli stranieri e a quella sui veicoli[124]. La vigilanza è affidata al procuratore generale dello Stato, o un suo rappresentante, e a due membri di una commissione ad hoc designati dal ministro dell'interno. Essi hanno accesso ai dati trattati dal SRDE, ordinano le rettifiche necessarie e informano le persone interessate del trattamento, conforme alla legge, di dati che le riguardano.

Per le questioni riguardanti la criminalità organizzata o la sicurezza esterna[125], il capo del Governo può, su richiesta del SRDE e previa approvazione di una commissione ad hoc, ordinare la sorveglianza telefonica preventiva[126]. La sorveglianza va sospesa dopo tre mesi, ma può essere prorogata per altri tre mesi. Le informazioni raccolte grazie alle intercettazioni telefoniche non possono essere utilizzate in tribunale se la persona coinvolta è vincolata dal segreto professionale ai sensi dell'articolo 458 del codice penale e non è sospettata di aver commesso o di pianificare un reato. In tal caso, il capo del SRDE deve distruggere senza indugio i relativi documenti. Le decisioni della commissione vanno trasmesse al direttore dei servizi di telecomunicazione competente in materia, che quindi incarica un apposito servizio di effettuare e controllare le intercettazioni. Una volta portato a termine il provvedimento, gli interessati ricevono copia delle informazioni raccolte, purché non siano state classificate come segrete. Se le misure non hanno dato alcun esito nel

119 Service de Renseignement de l'Etat.
120 Haute Commissariat de la Sécurité Extérieure.
121 2e Bureau de l'Armée.
122 Loi du 15 juin portant l'organisation du Service de Renseignement de l'Etat, qui di seguito denominata legge sull'organizzazione del 15 giugno 2004.
123 Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qui di seguito denominata legge del 2 agosto 2002.
124 Art. 4 della legge sull'organizzazione del 15 giugno 2004.
125 Sécurité exterieure de l'Etat.
126 Art. 88-3 del codice penale (Code Pénal) e legge del 26 novembre 1982 (Loi du 26 novembre1982).

periodo in questione, tutti i documenti vanno distrutti senza indugio e altrimenti alla fine del procedimento.

Le attività del SRDE sono controllate da una commissione, composta dai presidenti dei gruppi politici rappresentati nella Camera dei deputati (Chambre des Députés). Il direttore del servizio d'informazione rende conto delle attività generali del suo servizio. La commissione può chiedere di consultare gli atti e di interrogare gli agenti che se ne occupano. Approva un rapporto finale confidenziale, che contiene osservazioni, conclusioni e raccomandazioni e che è indirizzato al primo ministro, al capo del servizio d'informazione e ai deputati della commissione di controllo. La commissione parlamentare di controllo viene informata ogni sei mesi delle intercettazioni telefoniche preventive effettuate.

Non sono consentite né confische e perquisizioni né audizioni di testimoni. Il primo ministro può ordinare la sorveglianza di ogni tipo di comunicazione con l'ausilio di strumenti tecnici appropriati, qualora sussista il sospetto che la sicurezza dello Stato sia minacciata[127]. Soltanto una parte delle informazioni così raccolte possono essere trasmesse agli uffici competenti, segnatamente i cognomi, i nomi e, se sono noti, gli indirizzi IP[128]. Non è consentito vietare determinate attività.

Sono in fase di elaborazione diversi progetti di legge, ad esempio modifiche del codice penale concernenti le osservazioni, le inchieste mascherate e il trattamento delle informazioni di carattere generale da parte della polizia (traitement d'informations de police générale POLIS)[129].

6. Paesi Bassi

I Paesi Bassi sono una monarchia costituzionale; la regina è membro del governo e nomina i ministri.

L'insieme dei servizi d'informazione olandesi si compone degli istituti seguenti: il Servizio d'informazione civile (AIVD)[130], il Servizio d'informazione militare, comprendente i servizi segreti veri e propri (MIVD)[131], il Servizio militare speciale (BD)[132] e il Servizio antiterrorismo[133]. Dopo gli attentati dell'11 settembre 2001, la cooperazione tra l'AIVD e la polizia è stata notevolmente intensificata.

La lotta al terrorismo è uno degli obiettivi primari dell'AIVD.

L'AIVD e il MIVD svolgono indagini, effettuano controlli di sicurezza e adottano misure nei confronti di organizzazioni e persone sospettate di minacciare la sicurezza, l'ordine democratico o altri interessi essenziali dello Stato[134]. Cooperano con le autorità di polizia e di perseguimento penale trasmettendo le informazioni sotto

127 Art. 88-3 del codice di procedura criminale (Code de procédure criminelle).
128 Loi du 30 mai 2005 relative à la protection de la personne à l'égard du traitement de données à caractère personnel dans le secteur de communications électroniques.
129 Modifiche del 17 marzo e del 26 maggio 2006.
130 Algemene Inlichtingen- en Veiligheidsdienst (General Intelligence and Security Service).
131 Inlichtingen- en Veiligheidsdienst (Military Intelligence and Security Service).
132 Koninklijke Marechaussee, Bijzondere Dienst en Veiligheid» (Military policeSpecial section for intelligence and security).
133 Bijzondere Bijstands Eenheid (Special Help Union Anti-Terrorist Service).
134 Act of 7 February 2002, providing for rule s relating to the intelligence and security services and amendment of several acts (Intelligence and Security Services Act 2002).

forma di rapporti al pubblico ministero. L'AIVD può conferire mandati ai servizi d'informazione regionali (RID) e al Servizio di sicurezza speciale della polizia militare reale. Una revisione del codice di procedura penale (Code of Criminal Procedure) consentirà di utilizzare le informazioni dell'AIVD anche in tribunale[135].

In linea di massima, gli interessati possono chiedere di consultare i dati raccolti nell'ambito delle misure adottate nei loro confronti; la protezione delle fonti è comunque garantita. I diritti di consultazione vengono limitati se la pubblicazione dei dati potrebbe mettere a repentaglio la sicurezza interna. In questi casi bisogna informare la competente commissione di vigilanza[136], che sorveglia l'attività dei servizi e informa i ministri responsabili.

L'AIVD e il MIVD sono autorizzati a sorvegliare a titolo preventivo la corrispondenza postale e il traffico delle telecomunicazioni. I capi dell'AIVD e del MIVD presentano in anticipo la richiesta dopo aver ottenuto l'approvazione del ministro della difesa e del ministro dell'interno. Se vi è pericolo nel ritardo, è ammessa l'approvazione *ex post*, a condizione che venga richiesta quanto prima.

È inoltre ammessa l'osservazione con l'ausilio di strumenti tecnici, previa approvazione scritta del ministro competente. Se il ministro dell'interno o il capo dei servizi vi acconsentono, i servizi possono osservare e perquisire luoghi privati. Sono altresì previsti interventi sotto copertura ed è inoltre consentito aprire lettere di terzi se il tribunale distrettuale dell'Aja approva una richiesta in tal senso del capo dei servizi. È permesso anche accedere a sistemi informatici di terzi, previa autorizzazione del ministro dell'interno o del capo dei servizi. Non esiste per contro alcuna norma esplicita in materia di sequestro, confisca e messa al sicuro di oggetti né la possibilità di vietare determinate attività svolte da persone singole o da organizzazioni.

Il garante dei diritti civili, indipendente dal governo, sorveglia tra l'altro le attività dei servizi. Le sue competenze nei loro confronti sono tuttavia state ridotte nell'ambito di una revisione della legge[137]. I documenti dei servizi possono essere consultati, ma non copiati.

Il ministro competente informa regolarmente la commissione parlamentare di vigilanza sulle attività dei servizi.

7. UE

La lotta al terrorismo è un obiettivo dell'UE sin da quando il 26 luglio 1995 è stato istituito l'Ufficio europeo di polizia (Europol) che ha fra l'altro lo scopo di prevenire e combattere il terrorismo.

Dagli attentati dell'11 settembre 2001 negli Stati Uniti, l'Unione Europea sta attuando una politica antiterrorismo mirata. In occasione di un vertice straordinario dei ministri europei degli interni e della giustizia svoltosi a Bruxelles in seguito agli attacchi terroristici di Londra, l'Unione Europea si è detta favorevole a una cooperazione più stretta fra i 25 Stati membri per combattere il terrorismo e ha invocato una maggiore collaborazione transfrontaliera fra la polizia e i servizi di sicurezza.

135 Parliamentary documents II, 29 743.
136 Supervisory committee.
137 Act of 3 February 2005.

Il 21 settembre 2005, la commissione UE ha presentato un pacchetto di iniziative, comprendente quattro misure.

1. È stata proposta una direttiva sulla conservazione dei dati relativi al traffico delle comunicazioni che prevede per tutti i fornitori di comunicazioni elettroniche accessibili al pubblico o di una rete pubblica di telecomunicazioni, l'obbligo di conservare per un anno i dati relativi alla telefonia mobile e fissa e per sei mesi quelli sulle comunicazioni via Internet.
2. Sono stati stanziati 7 milioni di euro per un progetto pilota nel settore della prevenzione e della risposta immediata agli attentati terroristici. I fondi servono per incentivare i contatti fra le autorità che partecipano al perseguimento penale al fine di agevolare lo scambio di informazioni e la gestione delle crisi e per sostenere il prossimo programma europeo per la protezione delle infrastrutture a rischio.
3. È stata presentata una decisione da sottoporre al Consiglio che autorizza la firma della convenzione numero 198 del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reati e sul finanziamento del terrorismo. La Commissione esorta i 46 Stati membri del Consiglio d'Europa ad adottare norme contro il riciclaggio dei proventi del crimine altrettanto severe di quelle attualmente applicabili nell'UE e a costituire un fronte unico nella lotta contro il finanziamento del terrorismo.
4. È stata diramata la comunicazione intitolata «Il reclutamento dei terroristi: studio dei fattori che contribuiscono alla radicalizzazione violenta» che costituisce il contributo della Commissione, come richiesto dal Programma dell'Aja, alla strategia in materia che deve essere messa a punto dal Consiglio entro la fine di quest'anno. Il documento propone una serie di possibili metodologie di lavoro di cui servirsi per affrontare il tema in diversi ambiti come Internet, la cooperazione tra le autorità che partecipano al perseguimento penale e i servizi segreti degli Stati membri e le relazioni esterne.

Il 20 settembre 2005 l'UE ha emanato una decisione sullo scambio d'informazioni e la cooperazione per combattere i reati legati al terrorismo (2005/671/JI). Infine, la Commissione UE ha elaborato, nel contesto del programma dell'Aja, dieci priorità per i prossimi cinque anni (COM(2005), fra cui un progetto per la lotta al terrorismo.