Progetto del 05.07.2006

Legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI)

Modifica del ….

Rapporto esplicativo

Indice

1. Parte generale

1.1 Situazione di partenza in virtù del diritto vigente

1.1.1 Mandato della politica di sicurezza

La protezione dello Stato e la polizia costituiscono gli strumenti per la salvaguardia della sicurezza interna. Essi sono oggetto della politica di sicurezza nella misura in cui servono per combattere la violenza che può minacciare vaste aree del Paese e una parte consistente della popolazione. La lotta contro la violenza civile fa parte della politica di sicurezza dei Cantoni. Sono innanzitutto i Cantoni a far fronte ai turbamenti esistenti.

I compiti in materia di politica di sicurezza della protezione dello Stato e della polizia sono i seguenti:

- La protezione dello Stato prevede misure preventive per riconoscere tempestivamente i pericoli dovuti al terrorismo, all'estremismo violento e allo spionaggio nonché al commercio illecito di armi e materiale radioattivo e al trasferimento illegale di tecnologie. Gli organi di protezione dello Stato assistono inoltre le competenti autorità di polizia e di perseguimento penale, fornendo loro informazioni sulla criminalità organizzata.
- La polizia, sottoposta prevalentemente alla sovranità cantonale, salvaguarda la sicurezza, la tranquillità e l'ordine pubblico e combatte la criminalità. 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 assume la direzione.

1.1.2 I servizi d'informazione interno ed esterno della Confederazione

È ormai quasi impossibile distinguere chiaramente la sicurezza interna da quella esterna. La sicurezza è inscindibile. Le minacce e i rischi tendono ad assumere un carattere sempre più transfrontaliero, e l'instabilità e i conflitti, persino in regioni molto lontane, possono ripercuotersi direttamente e immediatamente sulla sicurezza interna della Svizzera.

Come la quasi totalità degli Stati democratici del mondo, la Svizzera gestisce un servizio d'informazione interno e uno esterno. Il Servizio informazioni strategico (SIS) in seno al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) è il servizio segreto per l'estero.

Il Servizio di analisi e prevenzione (SAP) dell'Ufficio federale di polizia (fedpol) è il servizio segreto interno. Esso ha il compito di fornire tempestivamente agli organi dirigenti della Confederazione e ai Cantoni informazioni su minacce per la sicurezza interna, affinché sia possibile prendere misure preventive in tempo utile. I compiti del servizio d'informazione interno sono disciplinati dalla legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI; RS *120*) e dalle relative disposizioni esecutive.

Se le minacce si manifestano a livello internazionale e non possono essere affrontate separatamente in base al criterio che distingue fra minacce interne ed esterne, i servizi segreti operano in stretta collaborazione, attualmente in base a un cosiddetto

schema di gruppi comuni contro il terrorismo, la criminalità organizzata e la proliferazione.

1.1.3 Attività del servizio d'informazione interno

a) Dimensione preventiva della protezione

La ricerca, l'esame e la distribuzione permanente di informazioni da parte del SAP ha lo scopo di informare gli organi direttivi dello Stato sulle minacce in grado di mettere a repentaglio l'esistenza del Paese, il suo libero ordinamento sociale e 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.

b) Compiti del servizio d'informazione interno

Per mettere seriamente a repentaglio l'esistenza di un'intera società e la sicurezza di un gran numero di cittadini occorrono persone che condividono le stesse idee e sono animate da una forte volontà di distruzione. La storia dimostra che le minacce rilevanti nell'ottica della protezione dello Stato si basano pertanto solitamente su motivazioni politiche e ideologiche. Il perseguimento della criminalità motivata principalmente dalla ricerca di profitti compete invece tradizionalmente alle autorità di perseguimento penale.

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 autorità di sicurezza estere.

c) Scopo preventivo

Le ricerche del SAP hanno lo scopo di fornire tempestivamente alle autorità competenti, in particolare agli organi dirigenti della Confederazione e ai Cantoni, informazioni sulla situazione in materia di sicurezza, onde consentire di riconoscere per tempo le minacce (p. es. mediante la valutazione periodica della situazione di minaccia da parte delle autorità politiche) e prendere provvedimenti (p. es. pronunciando divieti d'entrata nei confronti di cittadini stranieri in grado di mettere a repentaglio la sicurezza interna della Svizzera oppure proteggendo persone e installazioni). L'attività mira pertanto innanzi tutto a scoprire eventuali minacce per la sicurezza della Svizzera (scopo preventivo della verifica di un sospetto) ed eventualmente a prevenirle.

d) Ricerca di informazioni

Tutte le analisi delle minacce e 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 di un servizio segreto consiste pertanto nel raccogliere informazioni su fatti riservati. Non possono tuttavia procurarsi informazioni più numerose e più approfondite rispetto a quelle che la legge consente di raccogliere e analizzare.

Quando il servizio segreto scopre minacce e pericoli rilevanti nell'ottica della protezione dello Stato, le autorità competenti della Confederazione e dei Cantoni prendono le misure di polizia o di diritto amministrativo in virtù dell'articolo 2 capoverso 1 LMSI necessarie per prevenire le minacce o i turbamenti già esistenti.

L'articolo 14 capoverso 2 LMSI elenca esaustivamente gli strumenti 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 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 esclude l'impiego da parte del servizio d'informazione di misure coercitive ammissibili nel quadro di un procedimento penale e l'osservazione di fatti in ambienti privati. Di conseguenza non è consentito operare per scopi preventivi nel settore della comunicazione (posta, telefono, telefax, posta elettronica).

e) Servizio informazioni strategico

Il Servizio informazioni strategico (SIS) è il servizio segreto esterno della Svizzera che, conformemente all'articolo 99 capoverso 1 della legge federale del 3 febbraio 1995[1] sull'esercito e sull'amministrazione militare (Legge militare; 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'articolo 99 capoverso 5 LM, il SIS è direttamente subordinato al capo del DDPS. Al SIS è assegnata una missione fondamentale, sottoscritta dai tre Consiglieri federali che fanno parte della 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 anche 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[2] sui servizi d'informazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport (OSINF).

1.1.4 Distinzione fra attività di protezione dello Stato (prevenzione) e prevenzione generale delle minacce da parte della polizia

L'attività del SAP è circoscritta ai compiti legali di cui all'articolo 2 LMSI, nell'ambito dei quali le analisi e le informazioni del servizio segreto possono basarsi su notizie concernenti turbamenti della sicurezza imminenti o preesistenti.

---

1 RS **510.10**
2 RS **510.291**

In previsione di imminenti turbamenti della sicurezza, i servizi segreti si concentrano sulla scoperta e sulla tempestiva segnalazione di minacce che rischiano di compromettere la sicurezza e l'ordine pubblico. Intervengono ad esempio per prevenire attacchi terroristici individuando per tempo le organizzazioni coinvolte e impedendo loro di agire. La segnalazione tempestiva presuppone che i servizi segreti possano effettuare le loro ricerche prima che le minacce siano concrete e incombenti o che sorga addirittura il sospetto di un atto criminale.

L'individuazione tempestiva e la prevenzione della violenza a livello locale (violenza urbana) compete invece ai corpi cantonali di polizia che, nel quadro della prevenzione generale delle minacce, possono intervenire soltanto quando queste sono concrete e incombenti. Eliminare i disturbi della quiete pubblica rientra nei compiti generali dei corpi cantonali di polizia.

1.1.5 Distinzione fra attività di protezione dello Stato (prevenzione) e repressione penale

Questa distinzione dipende fondamentalmente dallo scopo che le autorità perseguono con le loro attività (scopo preventivo o repressivo).

Le attività di prevenzione e repressione nascono entrambe da un sospetto.

La protezione preventiva dello Stato consiste nel verificare un sospetto concernente una minaccia per la sicurezza della Svizzera o dei suoi abitanti dovuta a terrorismo, estremismo violento, spionaggio, commercio illecito di armi o materiale radioattivo oppure al trasferimento illegale di tecnologie (scopo preventivo).

La repressione consiste nel verificare un sospetto concernente un reato concreto perseguibile in virtù della legislazione federale o cantonale (scopo repressivo).

L'attività di protezione dello Stato si prefigge di scoprire il maggior numero possibile di organizzazioni che mettono in pericolo lo Stato e la società e di prevenirne e ostacolarne i propositi antidemocratici. A questo scopo le autorità competenti raccolgono e trattano dati e informazioni su possibili minacce per la sicurezza e attuano o propongono misure preventive adeguate.

Le ricerche in ambito preventivo necessitano solitamente di una procedura pianificata, con effetto a lungo termine.

La situazione è diversa per quanto riguarda la repressione penale. In questo caso lo Stato interviene per chiarire giuridicamente un sospetto di reato e valutare la colpevolezza dei singoli autori. La repressione (giustizia e polizia giudiziaria) implica la risoluzione del conflitto fra la comunità giuridica e il singolo individuo che viola le norme fondamentali della società. In altri termini, essa accerta d'ufficio il comportamento umano in relazione a un reato s o a un atto preparatorio punibile (e quindi si riferisce a un caso specifico).

Il diritto penale ha il compito di proteggere in modo particolare determinati beni tutelati dalla legge. Tale protezione particolare consiste nel dissuadere i potenziali autori di reati comminando pene inflitte ed eseguite rigorosamente. D'altro canto, se il fatto sussiste, il diritto penale prevede obbligatoriamente l'ingerenza nei beni giuridici

dell'autore del reato (p. es. privazione della libertà). In questo caso l'obiettivo consiste nel recuperare e, se del caso, nel rinchiudere l'autore del reato.

In virtù del principio della legalità, è punibile chiunque commette un reato per il quale la legge commina espressamente una pena. Sebbene la *nuda cogitatio* non possa essere punita, in seguito all'impressione suscitata dagli attacchi terroristici degli anni Settanta, sono stati dichiarati singolarmente punibili anche gli atti preparatori di determinati reati capitali (omicidio intenzionale, assassinio, lesioni gravi, rapina, sequestro di persona e rapimento, presa d'ostaggio e incendio intenzionale; cfr. art. 260bis CP; RS *311.0*:), estendendo pertanto la punibilità alla fase di pianificazione e di preparazione di un reato. Analogamente, per combattere la criminalità organizzata, è stata in seguito resa punibile anche la «semplice» partecipazione a un'organizzazione criminale (art. 260ter CP). La punibilità degli antefatti rende sempre più difficile tracciare il confine tra prevenzione e repressione penale.

Il perseguimento penale verte su una suddivisione dei compiti fra la Confederazione e i Cantoni. Il Ministero pubblico della Confederazione (MPC) e la Polizia giudiziaria federale (PGF), che durante gli ultimi anni sono stati notevolmente rafforzati e sviluppati (cosiddetto Progetto Efficienza), eseguono le indagini di polizia giudiziaria e perseguono i reati di competenza della Confederazione.

1.1.6 Distinzione fra attività di protezione dello Stato (prevenzione) e accertamenti preliminari di polizia giudiziaria

Gli accertamenti nell'ambito dei compiti di cui all'articolo 2 LMSI sono effettuati per ottenere informazioni utili ai fini della prevenzione, in particolare per valutare la minaccia e adottare misure preventive (scopo preventivo).

La situazione è diversa per quanto riguarda gli accertamenti preliminari di polizia giudiziaria che servono per decidere della necessità di un procedimento penale. La legge federale sugli Uffici centrali di polizia giudiziaria della Confederazione (LUC; RS *360*) prescrive di scoprire e combattere le gravi forme di criminalità ai sensi degli articoli 260ter e 340bis CP e di gestire a tale scopo un sistema d'informazione. Questo compito compete attualmente alla PGF. I provvedimenti consentiti per la ricerca delle informazioni necessarie corrispondono in larga misura a quelli previsti dalla LMSI. Gli accertamenti specifici della PGF si basano tuttavia su un fondato sospetto di reato e sono finalizzati all'applicazione del diritto penale. Il loro scopo è quindi repressivo e non sussiste un conflitto di competenza con le autorità preposte alla prevenzione. Ciò vale anche se la PGF esegue di propria iniziativa ricerche più approfondite su informazioni e indizi di un sospetto di reato.
Vi sono tuttavia dei 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 anche se da prospettive completamente 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. Nella prassi, in Svizzera e all'estero si constata che, a breve termine, gli accertamenti di lunga durata dei servizi segreti passano in secondo piano rispetto ai procedimenti giudiziari. Se lo scambio di informazioni funziona, questa concomitanza di prevenzione e repressione produce effetti positivi e non comporta svantaggi.

Per quanto riguarda il diritto d'essere informati, per il settore della prevenzione e per gli accertamenti preliminari di polizia giudiziaria, valgono regole simili. In virtù dell'articolo 14 capoverso 4 LUC e dell'articolo 18 capoverso 6 LMSI, le persone registrate che hanno inoltrato una domanda d'informazione e che, conformemente alle disposizioni di cui agli articoli 14 capoverso 2 LUC e 18 capoverso 1 LMSI, hanno dapprima ottenuto informazioni indirette da parte dell'Incaricato federale della protezione dei dati (IFPD), hanno diritto di essere poi informate anche direttamente non appena l'interesse a mantenere il segreto viene a cadere, al più tardi però quando scade il periodo di trattamento da parte delle autorità. Questo rimedio giuridico *ex post* contempla anche la comunicazione di informazioni raccolte sotto copertura.

1.1.7 Collaborazione fra il SAP e la PGF

L'attività di protezione dello Stato, incentrata sulla prevenzione, non esclude la trasmissione di dati dei servizi segreti ad autorità di perseguimento penale svizzere e straniere, se questi dati sono utili per il perseguimento penale. L'articolo 17 capoverso 1 LMSI sancisce persino l'obbligo di trasmettere alle autorità svizzere di perseguimento penale le informazioni rilevanti per perseguire i reati.

Non appena il SAP, nel corso della sua attività di servizio segreto, scopre indizi che potrebbero giustificare un sospetto di reato, li trasmette alle competenti autorità di perseguimento penale federali o cantonali. A seconda della consistenza degli indizi trasmessi, le autorità di perseguimento penale aprono direttamente un'inchiesta oppure effettuano ulteriori accertamenti per corroborare ulteriormente o delimitare il fondato sospetto di reato.

D'altro canto, l'articolo 13 LMSI impone a tutti i servizi di polizia e gli organi di perseguimento penale di fornire informazioni e di comunicare spontaneamente al SAP le minacce concrete per la sicurezza interna o esterna di cui giungono a conoscenza. Detti servizi informano inoltre in virtù dei mandati generali di informazione ai sensi dell'articolo 11 LMSI o di mandati conferiti nel caso specifico.

1.1.8 Raffronto schematico

La repressione e la prevenzione comportano entrambe compiti rilevanti per la sicurezza. Tuttavia, analizzano problematiche diverse da prospettive diverse. Per la distinzione è fondamentale lo scopo («preventivo» o «repressivo») degli accertamenti.

Sospetto di	
Una minaccia per la sicurezza della Svizzera dovuta a terrorismo, estremismo violento, spionaggio e proliferazione	**Un reato concreto o un atto preparatorio ai sensi del diritto penale federale o cantonale.**
Competenza	
Prevenzione Servizio di analisi e prevenzione / servizi cantonali d'informazione	**Repressione** Polizia giudiziaria federale, Ministero pubblico della Confederazione, autorità cantonali di perseguimento penale
Attività	
Accertamenti del servizio d'informazione / ricerca d'informazioni Analisi nel settore della sicurezza interna	Indagini giudiziarie e di polizia giudiziaria (eventualmente con l'ausilio di misure coercitive)
Oggetto	
Tutte le attività che mettono a repentaglio la sicurezza, indipendentemente dalla loro qualifica come reato	Atti punibili e sospetti sufficienti per l'apertura di un'inchiesta
Scopo	
Scopo preventivo: accertamenti finalizzati a verificare una possibile minaccia per i fondamenti democratici e costituzionali della Svizzera o la libertà della sua popolazione.	Scopo repressivo: accertamenti finalizzati a verificare l'effettivo compimento di un reato o di un atto preparatorio.
Strategico (osservazione a lungo termine)	Focalizzato sul singolo caso (reato specifico)
Risultato	
Rapporto destinato alle autorità politiche, eventualmente misure a livello politico o amministrativo	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 servizi d'informazione e di sicurezza stranieri sotto la vigilanza degli organi di protezione dei dati	Scambio formale d'informazioni con autorità giudiziarie e di polizia straniere
Vigilanza	
Organi di protezione dei dati e autorità politiche	Organi di protezione dei dati e autorità di giustizia penale
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

1.2. Situazione e rischi in materia di sicurezza in Svizzera

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 al trattamento dei dati. Si è sostanzialmente rinunciato alla ricerca di informazioni che interferiscono nella sfera privata. L'accento è posto sui limiti posti alla 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 legge federale sulle misure per la salvaguardia della sicurezza interna e sull'iniziativa popolare «S.o.S. – per una Svizzera senza polizia ficcanaso»; FF *1994* II 1007). In linea di principio, la legge si prefigge di salvaguardare la sicurezza interna facendo capo all'insieme delle misure repressive e delle direttive vigenti e contempla misure preventive soltanto negli ambiti in cui è necessario sventare pericoli considerevoli per beni giuridici essenziali. La legge tollera quindi che determinate minacce per la sicurezza interna possano essere affrontate soltanto *a posteriori*.

Dopo che la LMSI è stata approvata, la situazione di minaccia si è tuttavia notevolmente aggravata. Occorre pertanto adeguare la legge alla nuova situazione.

1.2.1 Terrorismo

Attualmente non esiste una definizione di terrorismo riconosciuta ovunque a livello nazionale o internazionale. In Svizzera, nel 2003, il Parlamento ha bocciato l'introduzione di una disposizione penale sul terrorismo. Una definizione legale indiretta è tuttavia contenuta nell'articolo 260^{quinquies} CP (Finanziamento del terrorismo), entrato in vigore nel 2003. L'articolo prevede una pena per chi raccoglie o mette a disposizione valori patrimoniali con l'intenzione di finanziare atti di violenza tesi a intimidire la popolazione o a costringere uno Stato o un'organizzazione internazionale a fare o ad omettere un atto.

Questa definizione corrisponde sostanzialmente a quella contenuta all'articolo 8 capoverso 1 lettera a dell'ordinanza del 27 giugno 2001 sulle misure per la salvaguardia della sicurezza interna (OMSI; RS *120.2*), che definisce le attività terroristiche «*mene tendenti a influire o a modificare Stato e società, da attuare o favorire commettendo o minacciando di commettere gravi reati nonché propagando paura e timore*». La definizione si basa sulle direttive del DFGP del 1992 sulla protezione dello Stato che riprendono a loro volta la definizione di attacchi terroristici proposta per finalità di ordine assicurativo dall'Organizzazione per la cooperazione e lo sviluppo in Europa (OCSE): «*l'uso o la minaccia della violenza dettata da motivazioni politiche, ideologiche, religiose o di altra natura tendenti a influire o a destabilizzare Stati o a suscitare timore fra la popolazione*»[3].

La presente revisione non mira a modificare questa situazione giuridica o la prassi consolidata sin dal 1992. La definizione contenuta nell'OMSI rimarrà in vigore, mentre, a causa della mancanza di un'intesa a livello internazionale, non è opportuno inserire una definizione nella legge formale.

[3] Si tratta di una traduzione della citazione letterale in tedesco, n.d.t.

Nel corso degli ultimi anni, la situazione della sicurezza in Svizzera si è costantemente aggravata, in particolare per quanto riguarda la minaccia terroristica. In base alle valutazioni attuali la Svizzera non è un obiettivo prioritario del terrorismo di matrice islamista. Tuttavia, il pericolo di attacchi terroristici è elevato in tutta l'Europa e quindi anche la Svizzera risulta coinvolta alla pari degli altri Stati dell'Europa occidentale. Il Consiglio federale è giunto a questa conclusione nell'«Analisi della situazione attuale e dei rischi per la Svizzera dopo gli attacchi terroristici dell'11 settembre 2001» presentata al Parlamento il 26 giugno 2002. A causa della situazione della sicurezza tuttora tesa in Iraq e nel Medioriente, le minacce permangono gravi, in particolare per le installazioni e i cittadini degli Stati Uniti e dei loro alleati, quali la Gran Bretagna, l'Italia, la Spagna e la Polonia, ma anche Israele e, a causa delle loro forti minoranze musulmane, la Germania e la Francia.

Con gli attentati di Istambul (15 e 20 novembre 2003), Madrid (11 marzo 2004) e Londra (7 e 21 luglio 2005) il terrorismo islamico ha colpito anche l'Europa. Gli attentati suicidi del 7 luglio 2005 a Londra sono stati i primi di questo genere in Europa occidentale che non è quindi più soltanto un area di rifugio e di preparazione. Le minacce terroristiche in genere non prendono più di mira soltanto gli interessi angloamericani e israeliani, bensì gli interessi occidentali nel complesso, di cui, secondo i fondamentalisti islamici, fanno parte anche l'ONU o il CICR che hanno sede in Svizzera. Per diffondere il loro messaggio di terrore, i terroristi hanno bisogno di pubblicità. Un mezzo consiste in attentati con esplosivi compiuti a sorpresa in mezzo alla folla. Più gli obiettivi abituali sono protetti, più aumenta la possibilità di un ripiego su obiettivi meno protetti (i cosiddetti «*soft targets*» o «obiettivi morbidi»). Infine è necessario tenere conto in misura sempre maggiore dell'intensificazione delle indagini effettuate dai Paesi limitrofi nei confronti delle organizzazioni terroristiche (aumento del personale e dei mezzi a disposizione).

I terroristi del giorno d'oggi sfruttano ogni possibilità. Per attirare l'attenzione della comunità internazionale, commettono attentati sempre più efferati e atti di violenza sempre più sanguinosi. Mentre l'efferatezza di attacchi sferrati con mezzi convenzionali appare quasi impareggiabile (New York: oltre 3000 morti e migliaia di feriti; Madrid: 191 morti e ca. 1500 feriti), cresce il timore di attentati nucleari, biologici o chimici.

Gli attentati terroristici dell'11 settembre 2001 hanno anche confermato che le moderne società industriali sono tuttora esposte a una vasta gamma di possibili minacce, anche del terrorismo tradizionale. Questo ha messo in discussione le procedure adottate finora nell'ambito della politica di sicurezza, soprattutto se si considera l'influenza di protagonisti estranei ai Governi, la crescente importanza della guerra combattuta senza un nemico preciso e la ricerca di informazioni da parte dei servizi segreti.

Gli esperti, fra cui il direttore generale dell'Agenzia internazionale per l'energia atomica, giudicano concreto e attuale il pericolo rappresentato dal terrorismo nucleare che riguarda prevalentemente le cosiddette «*dirty bombs*» o «bombe sporche» (bombe contenenti sostanze esplosive convenzionali cui viene aggiunto del materiale radioattivo). Anche se il numero di morti e feriti è limitato, in questi casi le conseguenze sul

piano politico, psicologico ed economico possono essere funeste. Può causare danni analoghi anche il terrorismo biologico, che consiste ad esempio nel propagare agenti patogeni altamente contagiosi quali il virus del vaiolo o la peste bubbonica. Un'«arma» di questo genere risulterebbe impossibile da controllare e potrebbe causare uno sterminio di massa a livello mondiale. Le armi chimiche, infine, sembrano meno adatte per i terroristi, poiché, anche se il loro potenziale di distruzione a livello locale è paragonabile a quello delle armi nucleari o biologiche, il loro effetto rimane circoscritto a un determinato territorio.

In seguito agli attentati terroristici di Madrid e di Londra, l'Europa occidentale, da rifugio e base d'appoggio, si è trasformata in area operativa del terrorismo islamista. 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. Alcuni terroristi si distinguono per la loro predisposizione a sacrificarsi come martiri dell'Islam in un attentato suicida, come accaduto a Londra il 7 luglio 2005. 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. Oltretutto si comportano come occidentali e utilizzano lingue extra-europee, il che rende molto difficile scoprire le loro intenzioni. Infine dispongono ormai di notevoli conoscenze per evitare di essere scoperti dai servizi segreti. Senza violare la sfera privata non è possibile né individuare tempestivamente gruppi come quelli descritti né sorvegliarli o controllarli sufficientemente in altro modo. Le conclusioni tratte dai procedimenti penali in Svizzera e le informazioni provenienti dai Paesi limitrofi dimostrano chiaramente che taluni sostenitori di Al Qaïda si servono della Svizzera.

1.2.2 Spionaggio

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

Il Consiglio federale ritiene che occorre 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, suscitata dalla mancanza di inchieste in materia, che la Svizzera non sia più interessata da questo fenomeno o lo sia soltanto marginalmente, non è corretta. Infatti, in base alle informazioni del SAP, in Svizzera sono presenti, sotto copertura diplomatica, numerosi agenti dei servizi segreti di determinati Paesi. A ciò si aggiungono le ricerche effettuate da agenzie investigative private attive su scala internazionale che agiscono frequentemente (sotto copertura) per conto di un Governo.

Sarebbe illusorio ritenere che lo spionaggio politico e militare ad opera di servizi segreti stranieri sia cessato insieme alla guerra fredda. Il numero elevato di agenti (presunti o identificati con certezza) dei servizi segreti che determinati Paesi inviano in Svizzera, conferma effettivamente il proseguimento di questo genere di attività. Non potendo accedere ai luoghi privati (con l'ausilio di apparecchi tecnici di sorveglianza, ecc.), le autorità preventive svizzere hanno tuttavia scarse possibilità d'intervenire, poiché le persone in questione sono professionisti specializzati e ottimamente equipaggiati per dissimulare e celare le loro attività. Nella prevenzione dello spionaggio, la mancanza di competenze in materia di ricerca di informazioni è sempre più evidente.

1.2.3 Estremismo violento

Per estremismo violento s'intendono 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 (cfr. art. 8 cpv. 1 lett. c LMSI).

Le attività degli estremisti sono potenzialmente violente e possono eventualmente 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 molti piccoli gruppi, in parte collegati fra loro. Si stima che attualmente vi siano in Svizzera circa 1000 estremisti di destra, mentre gli ambienti di estrema sinistra contano circa 2000 militanti. Anche i gruppi estremisti stranieri sfruttano il margine di manovra relativamente ampio offerto in Svizzera dai diritti fondamentali.

Il Consiglio federale ritiene che l'insieme delle leggi vigenti è sufficiente per affrontare l'attuale situazione di minaccia.

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

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

Di solito non è possibile acquistare sul mercato internazionale armi nucleari, chimiche e biologiche già confezionate. Le cerchie interessate sono pertanto costrette a costruire impianti propri per la ricerca, la progettazione e la produzione. A tal fine necessitano di macchinari reperibili sul mercato, apparecchi di misurazione e materiali che possono essere adoperati anche in numerosi settori civili (i cosiddetti beni «*dual-use*» o a duplice impiego). Tanto per fare un esempio: la fornitura di pezzi di ricambio di perforatrici per gallerie non costituisce di norma un problema. La situazione è diversa se il macchinario viene utilizzato per costruire un'installazione sotterranea per la fabbricazione di armi chimiche o di missili.

La progettazione e la produzione di armi chimiche e biologiche è più semplice e meno costosa rispetto a quella delle armi nucleari.

Per acquisire le conoscenze necessarie è possibile avvalersi di diversi mezzi (reclutare specialisti, fondare società di facciata, acquistare società che producono la tecnologia di cui si ha bisogno, importare tecnologie, non rivelandone l'utilizzazione e il destinatario finale, ecc.).

La Svizzera è 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.

La scoperta dell'organizzazione, specializzata in tecnologia nucleare, del «padre» della bomba atomica pakistana, il dottor Abdul Qadeer Khan, non soltanto ha dimostrato chiaramente che questo genere di organizzazione presenta una struttura altamente complessa e professionale, ma anche che la Svizzera può e potrà essere coinvolta senza difficoltà in simili attività criminali e che la sua infrastruttura può essere utilizzata in modo mirato a scopo di acquisizioni. Ciò comporta notevoli rischi per l'immagine del nostro Paese.

Nel settore del commercio illecito di armi e materiale radioattivo operano 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 luoghi 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. Se non può sorvegliare la sfera segreta o privata, nel settore della proliferazione il servizio segreto ha pochissime possibilità di verificare il sospetto, basato su determinate circostanze attuali, che le persone e le organizzazioni coinvolte costituiscano una grave minaccia per la sicurezza interna o esterna della Svizzera. La summenzionata scoperta di parte dell'organizzazione di Khan, specializzata nel trasferimento di tecnologia nucleare, dimostra l'utilizzazione mirata di conoscenze svizzere (sia per quanto riguarda le infrastrutture sia sotto il profilo tecnico).

1.2.5 Criminalità organizzata (CO)

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. Se il riciclaggio di denaro, la corruzione e l'incetta di società e immobili si insinuano nel regolare mondo degli affari, ciò può minacciare la stabilità economica e politica. Tuttavia anche gli Stati, la loro politica economica, la polizia e le autorità giudiziarie sono spesso infiltrati direttamente dalla 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 preoccupazioni 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.

Il Consiglio federale ritiene che potenziando il MPC e la PGF negli scorsi anni (Progetto Efficienza), si sia tenuto sufficientemente conto dell'attuale minaccia.

1.3 Valutazione degli strumenti mancanti per fronteggiare la situazione di minaccia

Come già constatato dal Consiglio federale nell'analisi della situazione e dei rischi del 2002, negli ultimi anni la situazione in materia di sicurezza e di minaccia per la Svizzera si è costantemente aggravata. I rischi sono notevolmente aumentati, in particolare a causa degli efferati attentati compiuti dai terroristi islamici. Gli autori dei reati non intendono colpire determinate personalità, bensì uccidere il maggior numero possibile di persone sferrando attacchi spietati contro installazioni civili. Secondo il Consiglio federale è indispensabile sventare questi atti di violenza scoprendo i preparativi e impedendone la commissione. A questo scopo sono necessarie la sorveglianza di persone e gruppi pericolosi e un'ottima cooperazione internazionale.

Le possibilità di prevenzione, notoriamente molto limitate, previste dalle leggi vigenti, non sono sufficienti per fronteggiare l'attuale situazione di minaccia. Vi sono evidenti lacune soprattutto per quanto riguarda la possibilità di raccogliere e trattare informazioni.

È generalmente vietato sorvegliare la sfera segreta e privata, indipendentemente dalla situazione di minaccia. Non è possibile scoprire gli incontri e le discussioni che si svolgono in luoghi privati. Attualmente non è consentito nemmeno sorvegliare i contatti elettronici fra diversi gruppi terroristici o determinate persone. Ciò ha sempre più spesso conseguenze negative, poiché le diverse persone e i differenti gruppi non sono più organizzati in strutture gerarchiche di comando, ma agiscono in maniera più o meno indipendente e mantengono i contatti servendosi soltanto di corrieri o di mezzi di comunicazione elettronici. La comunicazione avviene soprattutto con l'ausilio di tecnologie basate su Internet che attualmente sfuggono alla prevenzione.

Laddove manca anche questo tipo di comunicazione, le autorità di protezione dello Stato devono cercare di entrare in contatto sotto copertura con i gruppi e le persone in questione, onde poter individuare tempestivamente progetti pericolosi e minacce. A questo scopo occorrono identità fittizie, che la legge attualmente non consente.

Inoltre, al momento, le basi legali formali presentano delle lacune in materia di esplorazione radio (LMSI e LM). Negli scorsi anni, il Consiglio federale ha dovuto ricorrere più volte alle competenze conferitegli dalla Costituzione, per impedire a determinate persone di esercitare attività che minacciavano la sicurezza della Svizzera o le sue relazioni con l'estero. Se si rende necessario adottare regolarmente provvedimenti di questo genere, allora si impone un disciplinamento a livello di legge per permettere che le competenze costituzionali vengano fatte valere soltanto in casi eccezionali.

1.4 Possibilità d'intervenire

In considerazione della recrudescenza della situazione di minaccia, in particolare nel settore del terrorismo e della proliferazione, è necessario intervenire. Nemmeno lo spionaggio politico e militare ai danni della Svizzera è ammissibile. È indispensabile ridurre i rischi per la sicurezza in tali ambiti.

Di conseguenza occorre verificare in che modo è possibile tenere conto di questa necessità d'intervenire. Entrano in linea di conto:

- lo sfruttamento sistematico di tutte le possibilità offerte dal diritto penale e dalla protezione preventiva dello Stato;
- la migliore circolazione delle informazioni e un migliore coordinamento fra le autorità preventive e repressive;
- il rafforzamento del diritto penale formale e materiale;
- il rafforzamento della protezione preventiva dello Stato (modifica della LMSI).

1.4.1 Sfruttamento sistematico di tutte le possibilità offerte dal diritto penale e della protezione preventiva dello Stato

Se da un lato non vi sono indizi concreti di scorrettezze vasti e sistematiche nello sfruttare le attuali competenze legislative, dall'altro non è possibile raccogliere le informazioni necessarie a colmare le lacune nell'ambito della sicurezza, nemmeno interpretando e applicando il diritto vigente in modo alquanto estensivo. Sarebbe di per sé auspicabile applicare sistematicamente il diritto penale a vantaggio della LMSI, ad esempio riducendo i presupposti necessari per l'apertura di un procedimento penale oppure impiegando maggiori risorse. Misure di questo genere non sono tuttavia sufficienti per colmare da sole le lacune esistenti.

1.4.2 Migliore circolazione delle informazioni e coordinamento fra autorità preventive e repressive

Il SAP è al corrente di tutte le ricerche in ambito preventivo condotte dalla Confederazione e dai Cantoni nel settore della sicurezza interna. La situazione è diversa per quanto riguarda le autorità di perseguimento penale, per i quali il SAP dispone soltanto delle informazioni che tali autorità gli hanno trasmesso.

Si pone pertanto il quesito se le informazioni che mancano attualmente in ambito preventivo possano essere ottenute garantendone l'ottimale circolazione fra autorità preventive e repressive. Ciò non è tuttavia possibile, già per motivi strutturali. Infatti le informazioni che servono per la repressione sono raccolte caso per caso e si limitano a indagini effettuate su determinate fattispecie durante procedure penali concrete. Le informazioni di cui necessitano le autorità di prevenzione per valutare dettagliatamente la situazione di minaccia e prendere le opportune misure preventive, sono invece non soltanto più ampie e approfondite, bensì anche di natura strategica e quindi finalizzate a un'attività di sorveglianza permanente.

Migliorare lo scambio di informazioni fra il MPC, la PGF e il SAP è un compito permanente. La collaborazione è disciplinata dettagliatamente con leggi, ordinanze e direttive, e le procedure interne sono stabilite e verificate regolarmente. Ulteriori provvedimenti sono in fase di realizzazione. Attualmente si può tuttavia già affermare che anche le possibili migliorie elencate qui di seguito sono largamente insufficienti per colmare le lacune nel settore delle ricerche interne.

1.4.3 Rafforzamento del diritto penale formale e materiale

Va verificato se rafforzando il diritto penale materiale (p.es. norma penale contro chi fomenta l'odio) o formale (p. es. programma di protezione dei testimoni), si consente al SAP di ottenere le informazioni supplementari che gli mancano.

Il vantaggio consiste nella possibilità di basarsi su strutture esistenti e su procedure con collaudati rimedi giuridici per ordinare ed eseguire misure coercitive processuali.

Inoltre per molte questioni esistono una dottrina e una giurisprudenza consolidate. In altri termini è disponibile che funziona.

Vi sono tuttavia anche i seguenti dubbi:

- I servizi segreti eseguono un'attività di sorveglianza permanente, concentrandosi soprattutto sulla scoperta di eventi e organizzazioni. In linea di massima non vi è motivo d'intervenire direttamente fino alla loro identificazione completa.
- Gli accertamenti in ambito repressivo concernenti un reato e l'insieme dei mezzi a disposizione per effettuarli hanno uno scopo diverso rispetto alle ricerche in ambito preventivo effettuate dai servizi segreti per raccogliere informazioni nel quadro di una valutazione della situazione in materia di politica di sicurezza o per adottare le eventuali misure preventive.
- Varando la LMSI, il legislatore ha volutamente separato la repressione dalla prevenzione e il Consiglio federale ha poi applicato sistematicamente questa suddivisione anche sul piano strutturale durante la riorganizzazione dell'Ufficio federale di polizia. Questo principio va mantenuto.
- La ricerca di informazioni con strumenti repressivi in ambito preventivo reintrodurrebbe sostanzialmente il metodo di lavoro dell'ex Polizia federale e metterebbe in dubbio la suddivisione delle competenze.
- La ricerca di informazioni con l'ausilio di strumenti repressivi presuppone perlomeno l'avvio di un'indagine di polizia giudiziaria. Se questa indagine non produce alcun risultato la persona coinvolta subisce ugualmente un reale danno d'immagine. Questo vale soprattutto se il caso giunge a conoscenza dell'opinione pubblica. Ciò può comportare per lo Stato ulteriori conseguenze e possibili responsabilità, ad esempio se il danno d'immagine influenza del tutto o parzialmente l'esistenza economica di una persona o la compromette definitivamente.
- Un'estensione della punibilità alla fase preparatoria di un reato, che va oltre gli atti preparatori singolarmente punibili ai sensi degli articoli 260^{bis} e 260^{ter} CP, è in contraddizione con la sistematica del Codice penale e, dato che persegue scopi diversi, non è neppure in grado di colmare le lacune della ricerca d'informazioni in ambito preventivo.
- L'attività di repressione si basa su una norma penale che descrive dettagliatamente il comportamento punibile. Per consentire un'azione investigativa finalizzata a ottenere informazioni per scopi preventivi, una norma penale deve formulare una fattispecie in modo molto generico. In tal caso la norma perde tuttavia la propria prevedibilità, ossia la singola persona non può più prevedere con certezza come comportarsi per non violare la legge.
- In base al diritto vigente un'azione repressiva presuppone un sospetto fondato che venga commesso un reato. Tuttavia sono esattamente questi sospetti che mancano all'inizio delle ricerche dei servizi segreti. Durante una prima fase vi sono unicamente supposizioni e vaghi indizi. Inoltre le minacce per la sicurezza interna spesso non sono immediatamente riconoscibili come tali e le relative attività non sono (inizialmente) contemplate dal diritto penale. Per istituire una fattispecie che consente ricerche anticipate in ambito preventivo, è praticamente necessario rinunciare a un sospetto iniziale o prevederne uno molto meno fondato. I procedimenti penali che non si fondano su indizi sono tuttavia contrari al principio della precisione.

Complessivamente gli svantaggi che scaturirebbero da un ampliamento del Codice penale superano i vantaggi di una tale soluzione.

1.4.4 Rafforzamento della protezione preventiva dello Stato (modifica della LMSI)

Le lacune riscontrate influenzano la prevenzione da minacce e quindi soprattutto la protezione preventiva dello Stato. Poiché la LMSI disciplina i compiti e i mezzi della protezione preventiva dello Stato, essa costituisce l'atto normativo appropriato. Inoltre anche in questo caso è possibile basarsi su un sistema collaudato con strutture esistenti.

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, ne formula le esigenze 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 del potere politico, le lacune riscontrate nel dispositivo di difesa preventiva.
- Per combattere il terrorismo e minacce analoghe, occorre utilizzare tutti i mezzi disponibili, ossia applicare l'insieme degli strumenti sia repressivi sia preventivi. Per individuare tempestivamente le minacce ed evitarle, ossia sventare attacchi terroristici o simili, è necessaria innanzitutto la prevenzione, e quindi l'attività dei servizi segreti.
- Le differenze fra gli strumenti di sicurezza dei vari servizi segreti nazionali comportano livelli di qualità differenti. Adeguando le competenze dei servizi segreti a quelle di diversi Paesi limitrofi, si intende evitare che la Svizzera divenga un territorio meno sicuro.
- Ampliare la LMSI rafforza notevolmente la cooperazione internazionale.
- Ampliare LMSI non mette in discussione i principi di diritto processuale che presuppongono un sospetto sufficientemente fondato per avviare indagini penali e la possibilità, per chi è soggetto alla legge, di prevedere con sufficiente certezza quali sono i comportamenti punibili.
- Rafforzare la prevenzione consente di ottenere costantemente informazioni dettagliate su forme gravi di criminalità. Queste informazioni sono utili agli organi preposti alla repressione che procedono in modo mirato, consentendo loro di impiegare con efficacia le loro risorse.
- Le ricerche mirate dei servizi segreti e le misure tempestive del caso consentono di prevenire gravi reati, e spesso evitano anche l'apertura di un procedimento penale lungo e dispendioso sgravando quindi efficacemente le autorità di perseguimento penale.

1.4.5 Revisione totale o parziale?

Rimane da stabilire se per i lavori legislativi imminenti sia necessario sottoporre la LMSI a una revisione totale oppure se sia possibile effettuarli nel quadro di una revisione parziale. Una revisione parziale è preferibile 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 di LMSI II sono nella sostanza limitate a poche tematiche e incentrate chiaramente sulla ricerca di informazioni con l'ausilio di strumenti specifici.
- Il collocamento delle modifiche auspicate nella sistematica della legge è giustificabile, anche se non ottimale.
- Anche dopo i progetti di legge LMSI I e LMSI II, la LMSI necessita di ulteriori adeguamenti, soprattutto nel settore dei controlli di sicurezza delle persone.
- Nel complesso sembra molto più vantaggioso rimandare, per il momento, una revisione totale ed effettuarla più tardi.

1.5 Progetti di legge in corso nel settore della sicurezza interna

La legislazione sulla sicurezza interna viene costantemente adeguata e rinnovata. Attualmente numerosi accordi internazionali, leggi e ordinanze sono in fase di realizzazione o di revisione. È tuttavia accertato che tali progetti e il presente avamprogetto di legge non presentano punti di contatto rilevanti (cfr. allegato 1).

La presente revisione ha soprattutto lo scopo di migliorare la ricerca delle informazioni necessarie per valutare la situazione in materia di politica di sicurezza e le misure che ne scaturiscono. Tale revisione influenza in modo decisivo la gestione della prevenzione da minacce nel suo complesso e comporta conseguenze indirette per il diritto penale formale e materiale.

È in corso la verifica degli adeguamenti delle basi legali del SIS.

1.6 Diritto comparato e rapporto con il contesto 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 promulgate in seguito, poiché le situazioni di minaccia, i sistemi giuridici (ruoli del potere esecutivo, giudiziario e legislativo) e le esperienze dei singoli Paesi in relazione al terrorismo (p. es. ETA in Spagna) sono diverse.
La recrudescenza della minaccia terroristica ha indotto in generale i servizi segreti 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 «Gruppo anti-terrorismo (GAT, *Counter Terrorist Group*)» istituito dal «Club di Berna» 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 legali sulla sicurezza interna degli Stati europei più importanti.
La legislazione di tutti i Paesi elencati qui di seguito è stata influenzata dagli attentati dell'11 settembre 2001 negli Stati Uniti.

Le strutture statali e le possibilità d'intervento consentite dalla legge 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 rimedi giuridici e i sistemi di controllo. Le spiegazioni dettagliate sono contenute nell'allegato. La mancanza di

un'esplicita norma di legge non significa necessariamente che il Paese in questione non applichi una determinata misura. È probabile che il disciplinamento non sia ritenuto necessario oppure che la misura sia parte integrante di altre norme.

1.6.2 Diritto comparato

Confronto con l'estero

Misura	Repressione/perseguimento penale	Prevenzione
Esplorazione radio, art. 14*a* AP		Germania, Francia, Italia, Paesi Bassi
Compenso degli informatori, art. 14*b* AP	Francia, Italia	Italia, Francia
Protezione degli informatori, art. 14*c* AP	Austria, Germania, Francia, Italia	Austria, Germania, Francia, Paesi Bassi
Identità fittizie, art. 14*d* AP	Austria, Germania, Francia, Italia, Paesi Bassi	Austria, Germania, Francia, Paesi Bassi
Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, art. 18*k* AP	Austria, Germania, Francia, Italia, Lussemburgo, Paesi Bassi	Germania, Francia (esclusa la corrispondenza postale), Italia, Lussemburgo, Paesi Bassi
Osservazione in un luogo non liberamente accessibile, art. 18*l* AP	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* AP	Germania, Francia, Lussemburgo, Paesi Bassi	Francia, Paesi Bassi
Divieto per una persona o organizzazione di compiere determinate attività, art. 18*n* AP	Austria, Germania, Italia, Lussemburgo, Paesi Bassi	Francia, Germania, Austria

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 dei rimedi giuridici, controllo parlamentare, le autorità di sicurezza informano senza indugio il ministro dell'interno. **Inchieste mascherate e impiego sotto copertura di apparecchi di registrazione di immagini e suoni**: sotto la vigilanza dell'incaricato per i rimedi giuridici.
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 e richiesta per via ordinaria entro 24 ore dell'approvazione del giudice, che deve decidere entro 48 ore.
Lussemburgo	Commissione parlamentare di controllo, il procuratore generale dello Stato o un suo rappresentante e due membri di una commissione *ad hoc* 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 SRDE previa approvazione di una commissione *ad hoc*, 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 delle misure di sorveglianza delle telecomunicazioni eseguite.
Paesi Bassi	Commissione di vigilanza, difensore indipendente dei diritti civili, 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 richiesta il più presto possibile. **Osservazione:** in generale consentita l'osservazione previa approvazione scritta del ministro competente. Consentita l'osservazione in luoghi non liberamente accessibili, previa approvazione del ministro dell'interno o del direttore dei servizi.

1.6.3 Paragone con la Svizzera

Le strutture in materia di sicurezza e le possibilità d'intervento delle autorità di sicurezza previste dalla legge sono diverse in ogni Stato. Eppure, dal paragone risulta che le misure preventive e gli strumenti attualmente disponibili in Svizzera sono notevolmente ridotti rispetto alle risorse di numerosi Paesi dell'Europa occidentale.

Questa situazione può causare lacune pericolose, percettibili anche all'estero. È possibile che autorità straniere raccolgano illegalmente informazioni in territorio svizzero. Questo è già avvenuto in diversi casi.

Una capacità insufficiente di cooperare a livello internazionale può inoltre ripercuotersi sulla Svizzera, poiché riduce la predisposizione allo scambio di informazioni, da cui potrebbe scaturire un ulteriore indebolimento della prevenzione del terrorismo in Svizzera.

I recenti attentati dimostrano che le organizzazioni terroristiche vengono individuate troppo tardi se lo scambio di informazioni viene interrotto. Gli strumenti 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 a Monaco di Baviera fu impedito l'attentato progettato dal gruppo neonazista «Kame*radschaft Süd*» in occasione dell'inaugurazione del centro culturale ebreo.

La Svizzera deve essere in grado di raggiungere *de facto* almeno il livello degli Stati europei. Per il momento, si propone di rinunciare a ulteriori misure.

1.7 Le nuove norme proposte

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

A tale fine, gli strumenti di cui dispongono i servizi segreti per raccogliere informazioni vanno ottimizzati e adeguati agli standard europei. Le autorità e le unità amministrative della Confederazione e dei Cantoni saranno tenute, in casi specifici, a fornire informazioni circostanziate – allo scopo esclusivo di prevenire il terrorismo, lo spionaggio politico o militare e la proliferazione (diffusione di armi di distruzione di massa). Alle medesime condizioni saranno soggetti all'obbligo di comunicazione anche i trasportatori commerciali, purché le informazioni siano già state raccolte comunque. È inoltre previsto l'impiego di strumenti specifici per la ricerca di informazioni – a condizioni severissime e come *ultima ratio*. Sempre limitatamente ai settori del terrorismo, della proliferazione e dello spionaggio militare e politico, in presenza di un sospetto fondato saranno ammessi 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, nonché l'accesso segreto a sistemi di elaborazione di dati.

L'impiego degli strumenti specifici per la ricerca di informazioni è sottoposto a un doppio controllo. L'Ufficio federale di polizia avvia la procedura presentando un'istanza la cui legittimità viene in seguito verificata dal Tribunale amministrativo federale. Se la verifica ha esito positivo, l'istanza è esaminata dal punto di vista politico dal capo del DFGP. Questi consulta il capo del DDPS in quanto presidente della Giunta del Consiglio federale in materia di sicurezza. In caso di accordo il capo del DFGP decide definitivamente in merito all'istanza. In caso di disaccordo decide il Consiglio federale.

Al termine dell'operazione, la persona in questione deve essere informata della sorveglianza, a meno che prevalga un interesse pubblico preponderante o un interesse di protezione di terzi. Le deroghe all'obbligo di comunicazione sono decise dal capo del DFGP.

Viene delegata al capo del DFGP e disciplinata nella legge la competenza del Consiglio federale di vietare a determinate persone, organizzazioni o fazioni di svolgere attività finalizzate, direttamente o indirettamente, a propugnare, appoggiare o sostenere in altro modo operazioni terroristiche o di estremismo violento e a minacciare *de facto* la sicurezza interna o esterna (ad es. raccolta di fondi). La facoltà di vietare intere organizzazioni resta di competenza del Consiglio federale.

È altresì 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 possono essere create anche i-

dentità fittizie. 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.

1.8 Realizzazione

Le misure saranno attuate facendo ampio ricorso alle strutture federali e cantonali esistenti (TAF, SAP e servizi segreti dei Cantoni). Per il TAF, il SCS (Servizio per compiti speciali del DATEC, cui compete la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni), l'attuazione giuridica, operativa e amministrativa dei nuovi strumenti di ricerca e l'analisi dei risultati presso fedpol occorreranno complessivamente una quarantina di posti, che tuttavia non richiederanno l'assunzione di personale esterno.

Il fabbisogno di personale supplementare è in primo luogo riconducibile al potenziamento:

- delle strutture operative, in particolare le unità di polizia incaricate di raccogliere e trattare le informazioni (agenti di polizia, interpreti, tecnici, analisti operativi);
- delle strutture di elaborazione dei dati, in particolare la registrazione dei dati, l'assicurazione di qualità e lo scambio con l'estero;
- delle strutture estranee ai servizi d'informazione, quali il SCS (tecnica e amministrazione) o il TAF (segreteria).

Pertanto le nuove competenze delle autorità di sicurezza potranno essere introdotte utilizzando poche risorse supplementari.

2. Parte specifica

2.1 Struttura sistematica

L'introduzione di strumenti specifici per la ricerca di informazioni richiede un disciplinamento diverso da quello applicato agli strumenti semplici impiegati finora. Occorre pertanto modificare la struttura sistematica della legge, aggiungendo un capitolo composto da due sezioni. Nella prima sezione sono definite le regole generali applicabili ai nuovi strumenti per la ricerca specifica di informazioni, mentre la seconda sezione è dedicata ai singoli strumenti specifici e al loro impiego. L'inserimento del nuovo capitolo comporta una modifica della struttura generale del testo di legge.

2.2 Articolo 2 capoverso 4 lettere b^{bis} e b^{ter}

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

2.3 Articolo 7 capoverso 2 terzo periodo

In base 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 può assumere la direzione. Tale competenza verrà ampliata: l'Ufficio federale può coordinare lo scambio di informazioni se il lavoro della Confederazione e dei Cantoni ne risulta considerevolmente agevolato. L'Ufficio federale dovrà quindi garantire uno scambio coordinato di informazioni tra le unità amministrative (cantonali) competenti. L'idea del «coordinare» pone l'accento sul carattere cooperativo dell'intervento, mentre il qualificativo «considerevole» specifica che dallo scambio reciproco di informazioni deve risultare un netto vantaggio. La cooperazione assicurata dall'Ufficio federale mira quindi a ottimizzare la resa informativa di tutti gli uffici coinvolti. Si tratta di una disposizione potestativa; l'Ufficio federale non è in alcun modo obbligato a coordinare i lavori, ma dispone di un certo margine discrezionale.

Interesse pubblico e proporzionalità

La crescente internazionalizzazione del terrorismo e dell'estremismo violento e dei loro militanti rende sempre più difficile prevenire i rischi. È pertanto opportuno adeguare la funzione coordinatrice dell'Ufficio federale nello svolgimento delle funzioni attribuitegli dalla legge. Per riconoscere 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. In genere è altrettanto importante l'intenso scambio di informazioni con le autorità omologhe straniere. Il coordinamento proposto rispetta inoltre 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 e che dovrebbe entrare in vigore il 1° gennaio 2008).

2.4 Capitolo 3 Ricerca e trattamento generale delle informazioni

La nuova struttura sistematica della legge comporta la trasformazione della vecchia sezione 3 in un nuovo capitolo 3.

Il titolo del nuovo capitolo 3 è modificato per mettere in maggior risalto la differenza tra ricerca generale e ricerca specifica di informazioni (capitolo 3*a*). La ricerca generale corrisponde a quella attualmente ammessa, che non lede quasi per nulla i diritti fondamentali e rispecchia la concezione liberale di polizia preventiva su cui il legislatore si basava nel 1997 (ad es. valutazione delle fonti accessibili al pubblico oppure osservazione dei fatti in luoghi pubblici e liberamente accessibili). Di conseguenza, le misure ammissibili si situano in primo luogo nell'ambito dell'assistenza amministrativa tra autorità (cfr. gli obblighi d'informazione delle autorità cantonali o di determinate autorità federali).

Il fulcro dell'attuale LMSI è costituito dalla sezione che disciplina il trattamento delle informazioni. La presente revisione non cambia nulla in proposito: le norme pertinenti continuano a valere e si applicano anche ai dati raccolti con l'ausilio di strumenti specifici per la ricerca di informazioni, purché il capitolo 3*a* non preveda espressamente altrimenti.

2.5 Articolo 10*a* Situazione in materia di sicurezza interna

La disposizione disciplina un compito affidato agli organi di sicurezza della Confederazione (cfr. l'ordinanza sull'organizzazione del Dipartimento federale di giustizia e polizia; RS *172.213.1;* in particolare art. 9 cpv. 2 lett. a n. 2).

Capoverso 1

A fedpol incombe la descrizione permanente della situazione in materia di sicurezza interna. A tale scopo dirige il Centro federale di situazione, che traccia la situazione rilevante, integrando i settori della sicurezza interna (Cantoni, altri servizi federali). In occasione di eventi particolari (ad es. grandi manifestazioni), il Centro federale di situazione fornisce inoltre un contributo decisivo alla gestione della rete dei servizi d'informazione nazionali. L'adempimento di tali compiti comporta un continuo flusso di informazioni, che va disciplinato.

Capoverso 2

Per comunicare le informazioni raccolte, il Centro federale di situazione si serve tra l'altro di una rappresentazione elettronica della situazione (RES). Tale sistema d'informazione elettronico non costituisce una collezione di dati ai sensi della legge federale del 19 giugno 1992 sulla protezione dei dati (LPD; RS *235.1*) e non comporta il trattamento sistematico di dati personali. Si tratta piuttosto di un sistema d'informazione nel quale i servizi autorizzati possono richiamare informazioni costantemente aggiornate sulla situazione in materia di sicurezza interna. In caso di avvenimenti concreti (ad es. rete informativa durante una grande manifestazione, attacco terroristico), la RES è impiegata per comunicare informazioni aggiuntive relative agli eventi.

Non esiste alcun collegamento tecnico tra ISIS e RES. I dati personali di pubblico dominio sono quelli già resi noti dai media, gli altri sono quelli indissolubilmente legati a un evento rilevante ai fini della situazione in materia di sicurezza. La LMSI autorizza i destinatari ad accedere a questo tipo di informazione.

Capoverso 3
In conformità con l'articolo 17 (Comunicazione di dati personali), la descrizione periodica della situazione nella RES è accessibile ai servizi che necessitano delle informazioni che vi sono inserite per adempiere i propri compiti. L'Ufficio federale disciplina l'accesso ai contenuti che sono accessibili soltanto temporaneamente (descrizione della situazione in relazione a determinati eventi) e alle informazioni che non contengono dati personali degni di particolare protezione.

Capoverso 4
Il capoverso 4 colma una lacuna permettendo la comunicazione di dati a enti privati, purché tale comunicazione sia limitata nel tempo e si limiti alla descrizione della situazione in relazione a un dato evento (ad es. società di sicurezza private operanti nell'ambito di una grande manifestazione). È determinante a tale proposito che la comunicazione dei dati sia necessaria ai fini della sicurezza interna o esterna.

2.6 Articolo 13 titolo e capoversi 3 e 4 Obbligo generale d'informazione delle autorità

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

Titolo
Nel titolo dell'articolo 13 è inserito l'aggettivo «generale» per indicare che l'obbligo comprende l'intero campo d'applicazione della LMSI.

Capoverso 3
Le informazioni in merito a una minaccia derivante da terrorismo, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo oppure trasferimento illegale di tecnologia sono comunicate in continuazione, ragion per cui al Consiglio federale possono essere delegati soltanto i settori rimanenti, ossia l'estremismo violento e lo spionaggio economico.

Capoverso 4
La disposizione finora contenuta in questo capoverso è abrogata e inserita in un articolo separato (cfr. art. 13*b*). La nuova disposizione è applicabile a eventuali divergenze tra tutte le autorità vincolate all'obbligo d'informazione, sia secondo l'articolo 13 sia secondo l'articolo 13*a*. La modifica si impone anche dal momento che in futuro non saranno soltanto le autorità penali e amministrative a essere soggette all'obbligo d'informazione.

2.7 Articolo 13*a* Obbligo d'informazione specifico delle autorità

Al termine della procedura di consultazione, il progetto normativo verrà accordato alla revisione parziale della LMSI approvata dal Parlamento, ma non ancora entrata in vigore (modifica del 24 marzo 2006; LMSI I; propaganda violenta e violenza nel corso di manifestazioni sportive).

Come specificato poc'anzi, la disposizione introduce una nuova tipologia di obbligo d'informazione. Rispetto all'articolo 13, si tratta di una norma speciale che, da un lato, si limita a un settore dei compiti previsti dalla legge, ma dall'altro risulta più incisiva in quanto si applica a tutte le autorità federali e cantonali, e alle organizzazioni che esercitano funzioni pubbliche.

Capoverso 1
Questo capoverso istituisce un obbligo d'informazione in presenza di determinate minacce (cfr. lettere 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, aumenta il senso di insicurezza e lo Stato rischia l'erosione del suo sistema democratico. Pericoli di questo tipo derivano dal terrorismo, dallo spionaggio politico o militare, dal commercio illecito di armi o materiale radioattivo e dal trasferimento illegale di tecnologia.

In linea di massima, la disposizione sottopone a obbligo d'informazione tutte le autorità e le unità amministrative della Confederazione e dei Cantoni. È ad esempio un'unità amministrativa della Confederazione anche l'Ufficio centrale di comunicazione in materia di riciclaggio di denaro (MROS). Le unità amministrative dei Cantoni comprendono anche quelle dei Comuni; il concetto di «Cantone» si riferisce anche ad esse. Secondo l'articolo 2 capoverso 4 della legge federale sull'organizzazione del Governo e dell'Amministrazione (LOGA; RS *172.010*), si tratta di organizzazioni di diritto pubblico o privato al di fuori dell'Amministrazione federale cui sono stati attribuiti compiti amministrativi. Come nel diritto in vigore, il concetto di «organizzazione» va inteso in senso lato e comprende gli enti pubblici. 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. 2).

L'espressione «in casi specifici» evidenzia che le autorità vincolate dall'obbligo d'informazione devono sì comunicare costantemente le informazioni, ma soltanto quelle riguardanti determinati casi specifici e soltanto dietro speciale richiesta dell'Ufficio federale o di organi di sicurezza cantonali da esso incaricati.

Le informazioni raccolte presso le autorità e le organizzazioni sono indirizzate all'Ufficio federale, 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. Tale modo di procedere è conforme alla legge (cfr. art. 7 cpv. 1, art. 13 cpv. 1, art. 14 cpv. 1). 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, e non già l'autorità cantonale che, su mandato dell'Ufficio federale, 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 per i diritti dell'uomo. Eventuali clausole di riservatezza, codici di condotta particolari o procedure operative permanenti (SOP) vanno inoltre rispettati nel modo dovuto. Fanno stato le circostanze specifiche del caso.

Capoverso 2
Per motivi di legalità, gli organi di sicurezza non possono decidere autonomamente sull'obbligo d'informazione cui è sottoposta un'organizzazione. Il Consiglio federale deve quindi definire in un'ordinanza l'elenco esaustivo delle organizzazioni soggette a tale obbligo.

Capoverso 3
I servizi di cui ai capoversi 1 e 2 sono altresì autorizzati a informare, di propria iniziativa, le autorità federali e cantonali incaricate della protezione dello Stato in merito a fatti che ritengono legati ad attività di terrorismo, di 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 2 venga mossa l'accusa di violare il segreto d'ufficio. Tanto per fare un esempio, in futuro il MROS potrebbe spontaneamente fornire informazioni agli organi di sicurezza (cfr. quanto esposto *supra* in merito al cpv. 1). Tuttavia, non sussiste alcun obbligo di comunicazione sistematico.

Interesse pubblico e proporzionalità
Il nuovo articolo 13*a* sancisce nella legge il contenuto dell'attuale articolo 13 capoverso 3, che conferisce al Consiglio federale la facoltà di estendere, per un periodo limitato, l'obbligo d'informazione anche ad autorità diverse da quelle indicate all'articolo 13 capoverso 1. Il Consiglio federale si avvalse di tale facoltà emanando l'ordinanza del 7 novembre 2001 concernente l'estensione degli obblighi di informazione e del diritto di comunicazione di autorità, servizi e organizzazioni a tutela della sicurezza interna ed esterna («ordinanza»). L'ordinanza, prorogata due volte, è valida fino al 31 dicembre 2008 (cfr. RU *2005* 5423).

Dall'entrata in vigore dell'ordinanza, la minaccia terroristica è rimasta pressoché invariata. Non è mutata nemmeno la valutazione della situazione: certo, la Svizzera non è un obiettivo diretto e primario del terrorismo, ma il rischio generale di atti terroristici resta elevato in tutto il mondo, coinvolgendo anche la Svizzera – alla stregua di altri Paesi. Il bacino del Mediterraneo e l'Europa continentale non fungono più soltanto da rifugio e base d'appoggio di cellule dormienti. Tutto considerato, si può presumere che, alla prima occasione, le organizzazioni terroristiche saranno disposte a sferrare attacchi tesi a ledere gli interessi occidentali. Il conflitto si prospetta di lunga durata; al momento attuale non è possibile prevedere quando la minaccia rientrerà.

Nel dicembre del 2002, il Consiglio federale incaricò il DFGP di valutare l'efficacia dell'ordinanza e di stilare un rapporto alla sua attenzione. L'inchiesta svolta a tale proposito tra i corpi di polizia cantonali e quelli delle Città di Zurigo e di Berna non poneva l'accento tanto sul numero di comunicazioni di per sé (quantità), quanto piuttosto sulla loro valenza in termini di contenuto (qualità).

In un primo tempo, si pensò 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. Tale proposito si rivelò tuttavia (troppo) oneroso, per cui si ritenne opportuno rinunciarvi. Inoltre risultò che contrassegnare le comunicazioni non era sufficiente a rilevare gli effetti dell'ordinanza nei Cantoni, in particolare laddove l'ampliamento delle competenze rendeva meno dispendioso verificare le informazioni comunicate nei Cantoni, senza comunicazione specifica 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 circolari ad ampio raggio.

Nel complesso, il numero di comunicazioni è aumentato di poco, mentre il loro contenuto è nettamente migliorato. Taluni giudicano l'esistenza stessa di tale diritto, o di tale obbligo, più importante della sua utilità pratica. Gli organi esecutivi cantonali si sono nondimeno detti fermamente contrari all'abrogazione della disposizione. La mera esistenza dell'ordinanza è considerata fondamentale. I suoi effetti concreti sono però difficili da comprovare nel dettaglio, dal momento che soltanto un numero molto esiguo di comunicazioni è riconducibile esclusivamente all'ampliamento delle competenze. In compenso, i costi derivanti dall'ordinanza risultano alquanto contenuti.

Tutto sommato, l'ordinanza si è dimostrata di importanza non trascurabile sul piano politico interno ed esterno (interno: metro per la volontà del Consiglio federale di combattere il terrorismo; esterno: segnale per la disponibilità della Svizzera ad assumere il proprio ruolo internazionale nella lotta al terrorismo). Altrimenti detto, 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.

2.8 Articolo 13*b* Controversie in merito all'obbligo d'informazione

L'articolo 13*b* si applica quando l'Ufficio federale o un organo di sicurezza cantonale operante dietro suo mandato richiede un'informazione sulla base dell'articolo 13 o 13*a*, ma il servizio interpellato non è disposto a fornire l'informazione desiderata.

Capoverso 1
Le divergenze d'opinione tra unità amministrative dell'Amministrazione federale centrale (cfr. art. 7 OLOGA; RS *172.010.1*) 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 PA; RS *172.021*). Se, ad esempio, sorge una controversia in merito a un'informazione che fedpol richiede all'UFM, la decisione spetta al capo del DFGP.

Capoverso 2
In tutti gli altri casi, l'Ufficio federale può adire il Tribunale amministrativo federale (TAF) chiedendo una decisione definitiva (cfr. art. 83 lett. a LTAF[4]). L'Ufficio federale 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 TAF sia riservata all'Ufficio federale e non all'organo di sicurezza.

La procedura dinanzi al TAF sostituisce la procedura dinanzi al Tribunale penale federale secondo l'attuale articolo 13 capoverso 4; in base al nuovo articolo 29*a*, al

[4] FF **2005** 3689. La legge del 17 giugno 2005 sul Tribunale amministrativo federale dovrebbe entrare in vigore il 1° gennaio 2007.

TAF 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, ad es. MPC).

2.9 Articolo 13*c* Obbligo d'informazione dei trasportatori commerciali

Il nuovo obbligo d'informazione è analogo a quello di cui all'articolo 13*a*, ma non si rivolge ad autorità o organizzazioni che esercitano funzioni pubbliche, bensì a trasportatori commerciali che forniscono prestazioni in tale settore. Proprio come l'obbligo d'informazione secondo l'articolo 13*a*, anche quello dei trasportatori commerciali sussiste in relazione a determinate minacce (terrorismo, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo e trasferimento illegale di tecnologia).

La disposizione si applica a ditte quali le imprese di taxi, le compagnie aeree, le società ferroviarie, i trasportatori su strada, ecc.

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

L'espressione «in casi specifici» evidenzia che l'obbligo d'informazione sussiste soltanto quando l'Ufficio federale o un organo di sicurezza operante dietro suo mandato si rivolge al trasportatore in un dato caso specifico richiedendo un'informazione.

Interesse pubblico e proporzionalità

Secondo l'articolo 14 capoverso 2 lettera b LMSI, gli organi di sicurezza possono richiedere informazioni per l'adempimento dei propri compiti. Spesso 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, i trasportatori vengono obbligati 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 che, alla luce dell'interesse pubblico minacciato, l'ingerenza sia proporzionata. Da notare che le informazioni dei trasportatori commerciali possono essere determinanti nel valutare una potenziale minaccia. Non di rado sono proprio gli spostamenti di determinate merci o persone oppure le informazioni sulla frequenza di tali spostamenti a permettere di verificare l'esattezza di certe segnalazioni. È indubbio che l'accesso a questo tipo di informazioni costituisce uno strumento adeguato quanto necessario per prevenire con successo le minacce.

Sebbene la proporzionalità sia difficile da valutare sul piano puramente astratto, occorre tener conto degli aspetti seguenti: il trasportatore non è tenuto a ricercare attivamente le informazioni, ma deve soltanto comunicare quelle che già gli sono note. L'obbligo d'informazione non costituisce pertanto *a priori* un'ingerenza sproporzionata nella sua sfera professionale. Inoltre, il trasportatore non può far valere un segreto

professionale degno di particolare protezione, ragion per cui i suoi clienti non possono invocare un rapporto di fiducia particolare insito nel contratto di trasporto.

Se i dati in questione risultano da osservazioni in luoghi liberamente accessibili, l'ingerenza nella sfera privata non può dirsi sproporzionata alla luce dell'interesse pubblico da tutelare. Nel caso specifico occorrerà tuttavia verificare che l'interesse pubblico da proteggere prevalga sull'interesse personale egualmente degno di protezione.

2.10 Articolo 13*d* Segreto professionale

L'esercizio di talune «*professioni può svolgersi normalmente e correttamente solo ispirando nel pubblico, mediante una seria garanzia di discrezione, la indispensabile fiducia nel professionista*» (DTF *87* IV 108). Tale condizione è garantita sia dal fatto che le violazioni del segreto professionale sono passibili di pena (ad es. art. 321 CP; RS *311.0*; oppure art. 5 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 non occorre tener conto soltanto nei procedimenti giuridici, ma ogniqualvolta un privato sia tenuto a fornire informazioni alle autorità. Di conseguenza, le persone tenute a mantenere il segreto professionale potranno rifiutarsi di fornire l'informazione richiesta dall'Ufficio federale, proprio come nei procedimenti penali condotti dalla Confederazione. L'informazione non può per contro essere negata in presenza di semplici obblighi di segretezza contrattuali, anche se materialmente fondati sull'attività professionale della persona tenuta a mantenere il segreto.

2.11 Articolo 14 capoverso 3

L'articolo 14 LMSI elenca in maniera esaustiva gli strumenti cui gli organi di sicurezza possono attualmente ricorrere per adempire i loro compiti. L'impiego di tali strumenti non arreca grave pregiudizio ai diritti fondamentali, ragion per cui conserveranno la loro importanza e continueranno a essere impiegati dagli organi di sicurezza, mentre la ricerca di informazioni con l'ausilio di strumenti specifici secondo il capitolo 3*a* entra in linea di conto soltanto in determinate circostanze e a titolo sussidiario.

Capoverso 3

La disposizione riveste grande importanza nella legge in vigore. In linea di massima, vieta agli organi di sicurezza incaricati della prevenzione di adottare misure coercitive processuali o di osservare fatti in ambienti privati. La revisione introduce l'impiego preventivo di misure coercitive – la ricerca di informazioni con l'ausilio di strumenti specifici – a condizioni restrittive. Se finora vigeva un divieto generalizzato, la revisione prevede ora un sistema di deroghe soggette ad autorizzazione. La disposizione del capoverso 3 risulta pertanto caduca ed è abrogata, sebbene i nuovi strumenti specifici non siano misure coercitive ai sensi della procedura penale, ma piuttosto strumenti per raccogliere informazioni segrete.

Gli strumenti specifici per la ricerca di informazioni possono essere impiegati soltanto qualora siano soddisfatte le condizioni indicate all'articolo 18*a* segg. All'atto concreto significa soprattutto che l'impiego di strumenti specifici è riservato ai settori per i quali sono previsti, ossia terrorismo, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo e trasferimento illegale di tecnologia. Per contro, non è possibile servirsene per raccogliere informazioni in merito a una minaccia derivante da estremismo violento o spionaggio economico (cfr. quanto esposto ad art. 13 cpv.

3). Inoltre, l'impiego di strumenti specifici per la ricerca di informazioni non è ammesso se la minaccia non appare considerevole e sufficientemente plausibile o se poggia su fatti non abbastanza precisi o attuali.

2.12 Articolo 14*a* Esplorazione radio

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

Negli ultimi anni, il DDPS ha portato avanti il progetto ONYX e potenziato le capacità di esplorazione delle comunicazioni internazionali trasmesse via satellite. Il sistema capta e valuta le emissioni dei satelliti trasmesse alla terra, dove in genere vengono anche captate e ritrasmesse dai fornitori commerciali di servizi di telecomunicazione. Dall'aprile del 2001, anche il SAP utilizza il sistema ONYX nell'ambito di una fase operativa di prova. La base giuridica è stata creata introducendo l'articolo 9*a* OMSI, che nell'ambito della presente revisione verrà integrato nella LMSI. Così si esaudisce inoltre 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 servirsi di ONYX (cfr. cifra II n. 3 AP-LMSI, art. 99 cpv. 1 e 1^{bis} e art. 99*a* LM).

Il nuovo articolo 14*a* LMSI corrisponde in larga misura alle attuali disposizioni dell'OMSI. In aggiunta contempla la possibilità di sorvegliare obiettivi nazionali, opzione ammessa alle condizioni e secondo la procedura prevista dai nuovi articoli 18*d* segg. Sarebbe un controsenso non poter considerare alla stregua di un obiettivo (temporaneo) dell'esplorazione le persone i cui collegamenti di telecomunicazione nazionali possono essere sorvegliati.

Capoverso 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 conviene né in termini materiali né sul piano giuridico.

Capoverso 2
Il primo periodo si riferisce alla ricerca di informazioni tecniche, quali frequenze, potenza e orari di trasmissione, relative a emissioni provenienti dalla Svizzera. Riguarda quindi dati che non soggiacciono al segreto delle telecomunicazioni ai sensi dell'articolo 13 capoverso 1 Cost. e della legge sulle telecomunicazioni (LTC; RS *784.10*). Se tuttavia l'esplorazione radio è usata per intercettare comunicazioni soggette al segreto delle telecomunicazioni (ad es. chiamate sul cellulare), il secondo periodo mette in chiaro che questo genere di esplorazione costituisce una misura specifica di ricerca di informazioni, alla stregua della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, per cui si applicano le disposizioni del capitolo 3*a* (cfr. art. 18*a* segg., in particolare l'art. 18*k*). Pertanto, le disposizioni più severe si applicano anche ai casi in cui la sorveglianza è compiuta senza l'appoggio tecnico dei fornitori di servizi di telecomunicazione.

Capoverso 3
La disposizione sancisce la prassi attuale della cooperazione tecnica tra i servizi federali, autorizzando il Consiglio federale a cooperare con altre unità amministrative della Confederazione e dei Cantoni ai fini dell'esplorazione radio. Fedpol gestisce in proprio soltanto pochi impianti d'intercettazione di onde corte e in sostanza funge da mandante autonomo della sezione Divisione della guerra elettronica del DDPS. Ai sensi della presente disposizione, resta comunque esclusa l'integrazione in una rete di ascolto straniera (ad es. ECHELON).

Capoverso 4
Questo capoverso garantisce che l'esplorazione radio permanente venga in ogni caso controllata secondo quanto disposto agli articoli 99 segg. della legge militare (cfr. cifra II n. 3 AP-LMSI, in particolare art. 99*a* LM). Per evitare discrepanze rispetto all'esplorazione radio a favore dei servizi d'informazione del DDPS, molto più importante in termini di quantità, l'esplorazione di obiettivi collocati all'estero continuerà ad essere controllata dalla stessa autorità di vigilanza (finora «Istanza di controllo indipendente», ICI; nel presente progetto «autorità di vigilanza indipendente»). Nel caso di eventuali obiettivi nazionali va tuttavia seguita la procedura di cui agli articoli 18*d* e 18*e* (cfr. quanto esposto qui di seguito), purché la misura o l'esplorazione radio riguardi telecomunicazioni soggette a segreto.

Interesse pubblico e proporzionalità
L'esplorazione radio è uno strumento per raccogliere informazioni provenienti da fonti in genere accessibili al pubblico. Il suo impiego non costituisce pertanto né una grave ingerenza nella sfera privata né segnatamente una grave violazione del segreto delle telecomunicazioni. Talune forme di radiocomunicazione sorvegliate 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 specifica di informazioni, segnatamente l'articolo 18*k* (Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni). Per altre considerazioni in merito si veda quanto illustrato all'articolo 18*k*.

2.13 Articolo 14*b* Informatori

Per poter adempire i propri compiti, i servizi d'informazione necessitano della cooperazione di persone che hanno accesso a informazioni rilevanti. In conformità al principio della legalità sancito nella Costituzione federale, tutte le disposizioni importanti che contengono norme di diritto sono emanate sotto forma di legge federale (art. 164 cpv. 1 Cost.). Pur ammettendo implicitamente l'impiego di informatori, l'attuale LMSI non contiene tuttavia disposizioni specifiche in merito al loro intervento, ai loro diritti o doveri o alle prestazioni da parte dello Stato (cfr. in part. art. 14 cpv. 2 lett. b e d; richiesta di informazioni e ricezione di comunicazioni). Tale situazione giuridica frammentaria va chiarita.

Capoverso 1
La disposizione autorizza esplicitamente l'Ufficio federale a servirsi di informatori e ne definisce la funzione. La collaborazione con i servizi d'informazione avviene su base volontaria e non dà origine a un contratto di lavoro ai sensi dell'articolo 319 del

Codice delle obbligazioni (CO; RS *220*). La possibilità di ricompensare tali persone o di rimborsare loro le spese di volta in volta (cfr. cpv. 2) non giustifica in alcun modo la qualifica di tale rapporto come contratto di lavoro. La costituzione di 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 sotto il profilo del diritto del personale, dell'organizzazione e dell'orario di lavoro. All'atto pratico, tale presupposto è lungi dall'essere adempito.

Capoverso 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 in materia di AVS. Sono considerate spese ai sensi di questo capoverso quelle cagionate all'informatore nello svolgimento della sua attività.

È inoltre possibile ricompensare, se del caso, le informazioni particolarmente utili. Nella prassi corrente, le ricompense si situano già a livelli alquanto modesti (al massimo qualche migliaio di franchi all'anno) e sono ben lungi dal raggiungere il minimo vitale. Per evitare una male intesa corsa al successo, l'incentivo finanziario non deve determinare la decisione di fungere da informatore. Le ricompense vengono concesse a chi sia in grado di fornire informazioni che agevolano in maniera considerevole l'ulteriore ricerca di informazioni o la valutazione della situazione di minaccia.

Capoverso 3
Il rapporto tra i servizi d'informazione e gli informatori poggia sulla reciproca fiducia e sulla confidenzialità. Nelle aree d'intervento rilevanti ai fini della protezione dello Stato, gli informatori potrebbero correre gravi rischi se gli indagati venissero a conoscenza della loro attività per i servizi d'informazione. Ecco perché gli informatori non dovranno né figurare negli incarti del personale dell'Ufficio né essere annunciati alle assicurazioni sociali, nemmeno per indicare l'esonero dall'obbligo d'assicurazione. Per contro, il DFGP e la Delegazione delle Commissioni della gestione vegliano, in qualità di organi di controllo ordinari della LMSI, sulla legalità e l'opportunità del loro impiego. Il capoverso 3 specifica che eventuali indennità non sono soggette ad alcun obbligo d'imposizione o di contribuzione se 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.

2.14 Articolo 14*c* Protezione degli informatori

Tale disposizione è finalizzata a proteggere chi si espone a rischi per raccogliere informazioni utili allo scopo della LMSI. Vi sono due tipologie di informatori: coloro che devono temere rappresaglie perché cooperano con i servizi d'informazione di propria iniziativa e coloro che sono disposti a cooperare purché venga loro garantita un'adeguata protezione. Tale garanzia permetterebbe o agevolerebbe la ricerca delle informazioni necessarie ed eviterebbe il ripetersi di quanto accaduto in passato, ovvero che informatori di grosso calibro disposti a cooperare debbano essere «affidati» a servizi segreti stranieri in grado di assicurarne la protezione perché la Svizzera non ne ha la possibilità.

Chi coopera con i servizi d'informazione di propria iniziativa si espone, in certi casi, a rischi notevoli e deve temere ritorsioni, sia da parte dell'*entourage* (ad es. informatori

inseriti in gruppi estremisti violenti), sia da parte di Stati esteri (ad es. persone che in apparenza si sono messe al servizio di uno Stato estero, ma in realtà operano per le autorità svizzere). Il pericolo cui si espongono tali persone è paragonabile a quello corso dagli agenti infiltrati, che godono di ampia protezione. Di conseguenza appare giustificato, se non addirittura doveroso, creare i presupposti per garantire una protezione efficace anche agli informatori.

La normativa a protezione degli informatori va chiaramente distinta da quella a protezione dei pentiti, originaria del diritto penale anglo-americano. I pentiti hanno in genere preso parte al reato in questione, ma sono disposti a testimoniare contro i coimputati, ottenendo in cambio l'impunità, la riduzione della pena o altri benefici processuali. In un rapporto dedicato all'unificazione della procedura penale, una commissione peritale della Confederazione giudicava inopportuno introdurre nella procedura penale svizzera una normativa a protezione dei pentiti. Lo stesso vale sul piano della prevenzione: è esclusa un'esenzione dalla pena sul modello di detta normativa. La prevenzione non pone l'accento sull'accertamento dei fatti, che può essere agevolato grazie a testimonianze particolari; prevale piuttosto la ricerca di informazioni rilevanti ai fini della sicurezza; lo scopo è di individuare e di disinnescare le minacce e, per quanto possibile, di prevenire reati futuri.

Del resto tale misura verrà verosimilmente impiegata soltanto in casi eccezionali alquanto rari dai quali si presume possano emergere informazioni di grande valore. È ad esempio ipotizzabile la protezione di persone in grado di fornire informazioni importanti per la prevenzione di gravi rischi alla sicurezza, quali notizie su attacchi terroristici progettati o in preparazione, 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 fanno seguito vari colloqui esplorativi e, se le condizioni sono adempite, viene stipulata una convenzione di protezione che stabilisce obblighi e diritti reciproci. Soltanto allora ha inizio la collaborazione vera e propria.

Capoverso 1
Questo capoverso crea le basi giuridiche per la protezione degli informatori da parte dell'Ufficio federale. Le misure necessarie a tutela della vita e dell'integrità personale degli informatori comprendono la protezione della persona e gli spostamenti fisici. La protezione della persona comprende misure quali l'impiego di guardie del corpo, di veicoli o impianti protetti oppure provvedimenti edili. Lo spostamento fisico può consistere nel trasferimento – previo 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 trasferimento di tale persona in un luogo 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 finanziamento limitato nel tempo.

L'Ufficio federale può attuare le misure di protezione o finanziarle. All'atto pratico, tali misure si renderanno necessarie e potranno essere attuate soltanto in numero ridotto. Dal momento che la Svizzera, considerate le sue dimensioni, non è in grado di adottare misure di protezione integrali per determinate minacce, il pacchetto di servizi del caso («*package*») dovrà essere acquistato all'estero, il che rende determinabile il costo. 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.

Capoverso 2
Le medesime considerazioni impongono che l'Ufficio federale possa altresì adottare misure a protezione di persone prossime a un informatore, se la loro sicurezza dipende da tali provvedimenti. Il carattere potestativo della disposizione garantisce all'Ufficio federale il potere discrezionale necessario ad attuare le misure adeguate al caso specifico.

Capoverso 3
La disposizione prevede la possibilità di proteggere l'informatore fornendogli un'identità fittizia. Tale misura, al contrario di quelle previste ai capoversi 1 e 2, viene adottata soltanto qualora l'Ufficio federale abbia interrotto i contatti con un informatore e non si serva più della fonte. Se la persona in questione è in grave pericolo a causa della propria collaborazione con l'Ufficio federale, quest'ultimo può proteggerla fornendole un'identità fittizia permanente. La persona è autorizzata a utilizzare tale identità seguendo le istruzioni dell'Ufficio federale.
La creazione di un'identità fittizia presuppone che il TAF abbia emesso un parere favorevole e che il capo del Dipartimento abbia dato il suo consenso (cfr. quanto illustrato qui di seguito).

Questa disposizione non disciplina tuttavia la ricerca di informazioni sotto identità fittizia. Infatti, l'identità fittizia può essere impiegata nella ricerca di informazioni soltanto a determinate condizioni e seguendo l'apposita procedura (cfr. quanto esposto ad art. 14*d*).

In base all'articolo 27 capoverso 1bis (nuovo), il Dipartimento è tenuto a informare regolarmente il Consiglio federale e i servizi di controllo del Parlamento sul numero di identità fittizie create, sullo scopo al quale sono state fornite e sul loro concreto utilizzo. Tale disposizione si applica anche alle identità fittizie di cui al capoverso 3 di questo articolo.

Capoverso 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 un limite temporale se una persona è manifestamente esposta a un rischio grave e permanente; in tale evenienza, le misure di protezione possono essere mantenute a tempo indeterminato.

2.15 Articolo 14*d* Identità fittizie

Per adempire i propri compiti e proteggere i propri collaboratori, i servizi d'informazione sono costretti a servirsi di identità fittizie quando cercano informazioni in determinati ambienti. Tali identità fittizie sono sempre predisposte a lunga scadenza e raramente possono essere assunte soltanto all'inizio di un determinato caso. Il disciplinamento delle identità fittizie non rientra quindi nel settore degli strumenti specifici per la ricerca di informazioni, per il quale vigono condizioni molto restrittive. Dal 1998 il SIS ha la facoltà, in base all'articolo 99 LM, di fornire identità fittizie ai suoi organi di ricerca (cfr. 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.

Nel caso specifico compete al capo del DFGP autorizzare l'Ufficio federale a fornire un'identità fittizia. Prima di tutto, il TAF (articolo 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 i risvolti politici e, se del caso, dare il suo benestare.

In teoria è ipotizzabile che in determinati settori operino sia collaboratori secondo la LMSI e informatori del SIS sia agenti infiltrati delle polizie giudiziarie della Confederazione o dei Cantoni, quest'ultimi a norma della legge federale del 20 giugno 2003 sull'inchiesta mascherata (LFIM; RS *312.8*). Situazioni del genere in seno a fedpol possono essere risolte dal servizio di controllo interno della direzione. Nella misura in cui le identità fittizie fornite dal SIS siano impiegate in Svizzera, eventuali conflitti tra i due servizi vanno evitati in conformità alla decisione del 22 giugno 2005 del Consiglio federale in merito alla cooperazione tra SIS e SAP.

Capoverso 1
Il presente capoverso pone le basi per l'impiego di identità fittizie allo scopo di raccogliere informazioni e garantire la sicurezza di collaboratori e informatori. Va segnalato che le identità fittizie sono di norma utilizzate nell'ambito della ricerca generale di informazioni (art. 14 cpv. 2). Se, per contro, l'uso di un'identità fittizia è richiesta nel corso di una ricerca di informazioni con l'ausilio di strumenti specifici (ad es. osservazione in luoghi non liberamente accessibili, anche ricorrendo a un'identità fittizia), si applicano le procedure di cui agli articoli 18*a* segg. Il capoverso 1 fornisce un elenco esaustivo delle persone cui può essere fornita un'identità fittizia.

Lettere a e b. Gli organi di sicurezza secondo la LMSI mantengono uno stretto legame con le forze di polizia svizzere e possono svolgere gran parte della loro attività di ricerca alla luce del sole. Talvolta è tuttavia necessario poter predisporre 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. Possono servirsi di identità fittizie anche terze persone (informatori) se la ricerca di informazioni lo richiede. Si tratta in particolare di persone che potranno infiltrare determinati ambienti rilevanti ai fini della protezione dello Stato con maggiore facilità rispetto ai collaboratori dell'Ufficio federale 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 andrebbe limitato nello spazio e nel tempo e andrebbe concesso soltanto per determinate operazioni.

L'uso dell'identità fittizia comprende il diritto di servirsene per concludere negozi giuridici e, in particolare, per costituire strutture fittizie. Le persone munite di identità fittizia hanno piena personalità giuridica e possono stipulare contratti (ad es. affitto di locali e veicoli o collegamenti di telecomunicazione, costituzione di strutture fittizie quali ditte o altre persone giuridiche).

Capoverso 2

Per meglio controllare i rischi inerenti all'uso di un'identità fittizia, conviene limitare il tempo in cui tale identità può essere impiegata. Tale precauzione si impone in particolar modo per gli informatori che non sono impiegati all'Ufficio federale e quindi sfuggono al suo potere disciplinare.

Capoverso 3
Il capoverso 3 precisa che l'identità fittizia può essere usata soltanto per gli scopi perseguiti dalla LMSI. Va inoltre rilevato che, giusta l'articolo 27 capoverso 1bis lettera a del presente avamprogetto, il conferimento e l'uso di identità fittizie sono oggetto di 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.

2.16 Articolo 15 capoverso 6
La disposizione affonda le sue radici nella normativa sulla vecchia Polizia federale, cui erano affidati compiti e di repressione e di prevenzione. La separazione di questi due compiti e della loro attuazione organizzativa 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 escluso.

2.17 Articolo 16 capoverso 3 secondo periodo
In base all'articolo 16 capoverso 3 periodo 1, gli organi di sicurezza cantonali che trattano dati secondo la LMSI sottostanno al diritto federale sulla protezione dei dati. Il secondo periodo stabilisce inoltre che sono fatti salvi i diritti di sorveglianza previsti dal diritto cantonale. In altre parole, al trattamento di dati provenienti dalla sfera di attività della LMSI (e quindi inerenti al diritto federale) da parte di organi cantonali si applica in linea di massima il diritto federale sulla protezione dei dati. In via eccezionale, il diritto cantonale, qualora preveda una sorveglianza particolare, prevale su quello federale.

All'atto pratico, la riserva del diritto di sorveglianza cantonale si è rivelata problematica perché un'autorità di vigilanza cantonale – ad esempio una commissione della gestione – può chiedere di accedere a documenti operativi della Confederazione, e questo addirittura se i documenti sono stati classificati a livello federale. Inoltre, il tenore della disposizione potrebbe indurre a ritenere (erroneamente) che i dati raccolti dal Cantone in maniera apparentemente «autonoma» nell'ambito di un mandato integrale (ad es. lista d'osservazione), prima di essere trasmessi all'autorità federale appartengano al Cantone. In entrambi i casi, comunque, interessi inerenti alla sicurezza possono imporre di escludere qualsivoglia diritto di consultazione. Pertanto, l'articolo 16 capoverso 3 LMSI statuisce ora la competenza del Consiglio federale di definire gli atti della Confederazione che possono essere consultati dalle autorità di controllo cantonali. È quindi il Consiglio federale a stabilire la portata del diritto di sorveglianza cantonale; anche in futuro sarà possibile tener conto di legittimi interessi cantonali.

2.18 Articolo 17 capoverso 3 lettera e nonché capoverso 7
Capoverso 3 lettera e
Il cosiddetto *clearing* è un compito tradizionale del SAP nelle relazioni con l'estero. Su richiesta di un servizio estero, il SAP effettua controlli di sicurezza relativi a Svizzeri o a stranieri residenti in Svizzera, allo scopo di permetterne la collaborazione a progetti (o impieghi) esteri classificati. A tal fine, lo Stato richiedente garantisce al SAP per scritto che le persone in questione acconsentono al *clearing*.

Da sempre, il SAP fonda le sue operazioni di *clearing* sull'articolo 17 capoverso 3 lettera c LMSI. In passato, tuttavia, tale base giuridica è stata messa in questione più di una volta. Per tale motivo s'intende ora creare una base giuridica formale per il *clearing*. È un accorgimento necessario affinché anche i servizi fedpol che effettuano *clearing* possano essere presi in considerazione nell'ambito del progetto legislativo preparato dall'UFG per un nuovo disciplinamento dei diritti d'accesso di fedpol a VOSTRA (casellario giudiziale informatizzato). Infatti, sotto il profilo della protezione dei dati, l'accesso di fedpol a VOSTRA per scopi di *clearing* richiede anche un'esplicita base giuridica all'articolo 359 segg. CP. La presente modifica della LMSI crea soltanto le premesse per un futuro disciplinamento dell'accesso al casellario giudiziale informatizzato. Gli estratti del casellario giudiziale costituiscono un elemento importante per valutare il *clearing*. Senza di essi, il *clearing* effettuato dal SAP per conto di uno Stato estero risulterebbe di minor rilievo. Ne subirebbe le conseguenze la persona in questione, che probabilmente, quantunque il *clearing* dia esito positivo, non verrebbe ritenuta abbastanza fidata da poter cooperare a progetti segreti o confidenziali all'estero.

Capoverso 7
L'attività dei servizi segreti comprende innanzi tutto la ricerca e il trattamento di informazioni. Per procacciarsi le informazioni, i servizi segreti si servono di vari metodi di ricerca, tra cui la cosiddetta *Human Intelligence* (HUMINT), che consiste nel raccogliere informazioni sensibili con l'aiuto fattivo di persone (fonti). Molte informazioni importanti vengono comunicate soltanto quando le autorità competenti forniscono la garanzia vincolante che la fonte di un informazione non sarà rivelata a terzi (protezione delle fonti).

L'articolo 17 capoverso 7 LMSI prevede espressamente che nelle relazioni con l'estero la protezione delle fonti dev'essere garantita in ogni caso. Per quanto attiene alla Svizzera invece, il Consiglio federale determina per ordinanza i destinatari con funzioni pubbliche residenti in Svizzera ai quali, nel caso specifico, l'Ufficio federale è autorizzato a comunicare dati personali, nella misura necessaria per la salvaguardia della sicurezza interna ed esterna o il controllo dell'adempimento dei compiti (art. 17 cpv. 1 LMSI). Pertanto, sul piano nazionale, la questione della protezione delle fonti si pone in particolare in questi casi di comunicazione delle informazioni.

Secondo l'articolo 99 capoverso 4 LM, entrato in vigore il 1° gennaio 2004, alle fonti del SIS è accordata una protezione assoluta: «*La tutela delle fonti dev'essere in ogni caso garantita*».

Sorge pertanto la domanda se sia giustificato riservare un trattamento diverso alle fonti del servizio d'informazione interno rispetto a quelle del servizio d'informazione per l'estero. Sebbene vi siano argomenti a favore del mantenimento della normativa attuale, l'armonizzazione con la legge militare appare più opportuna. Per le riflessioni a favore dello *status quo*, si vedano le considerazioni che nel 1997 indussero il legislatore a rinunciare alla protezione assoluta per le fonti nazionali. Il Consiglio federale temeva che un'autorità si impegnasse, nei confronti di un informatore, a non rivelare la provenienza dell'informazione nemmeno se l'informatore fosse incorso in un reato.

Nel messaggio che accompagnava il disegno di legge, il Consiglio federale scriveva: «*se le fonti provengono dall'interno del Paese, non sarà per esempio possibile prendere in ogni caso un impegno a rispettare il carattere confidenziale, segnatamente se l'informatore stesso si è reso colpevole di un reato. Per contro una protezione assoluta delle fonti deve essere garantita nei confronti dei servizi esteri* [...]» (cfr. FF *1994* II 1004).

A favore dell'armonizzazione depone il fatto che la protezione assoluta delle fonti sancita per il SIS nella legge militare ha dato buona prova di sé. Soddisfa infatti sia le esigenze operative degli organi di sicurezza sia la concezione di protezione delle fonti prevalsa finora nel SAP. Alla luce delle esperienze maturate con il servizio d'informazione per l'estero, si è rivelato decisivo l'argomento delle esigenze operative in questo ambito alquanto particolare, ragion per cui va abbandonato il modello postulato nella legge del 1997. La protezione delle fonti nella LMSI va disciplinata analogamente a quanto fatto nella legge militare. Il testo della disposizione rispecchia quello dell'articolo 99 capoverso 4 LM.

Per il resto, la protezione delle fonti comprende il mantenimento del segreto sia in merito all'identità dell'informatore sia riguardo al contenuto dell'informazione.

2.19 Capitolo 3*a* Ricerca specifica di informazioni

Il capitolo 3*a* racchiude le disposizioni sostanziali della revisione, che autorizzano gli organi di sicurezza a impiegare strumenti specifici per raccogliere informazioni a titolo preventivo.

Il titolo del capitolo – ricerca specifica di informazioni – riflette il concetto fondamentale alla base di questo tipo di ricerca, che si distingue da quella effettuata con gli strumenti generali indicati al capitolo 3. La ricerca specifica di informazioni richiede strumenti specifici. Il concetto di «misura coercitiva» secondo il testo in vigore non si estende a tutti gli strumenti specifici previsti nell'avamprogetto, ma è comunque destinato a essere stralciato dalla legge in seguito all'abrogazione dell'articolo 14 capoverso 3.

Il capitolo 3*a* si suddivide in due sezioni: la prima è dedicata alle disposizioni generali che disciplinano l'impiego della ricerca specifica di informazioni, la seconda illustra gli strumenti specifici da utilizzare allo scopo.

2.20 Articolo 18*a* Principio

Questo articolo pone le basi per la ricerca specifica di informazioni elencando gli strumenti ammessi e determinandone gli ambiti d'impiego.

Capoverso 1

La disposizione precisa lo scopo della ricerca specifica di informazioni, ossia la scoperta o la soppressione di una minaccia concreta per la sicurezza interna o esterna, e richiama quanto disposto all'articolo 18*b*: prima di impiegare strumenti specifici per la ricerca di informazioni per individuare o sventare una minaccia, gli organi di sicurezza devono nutrire il sospetto che una determinata persona, organizzazione o fazione minacci la sicurezza (cfr. DTF *109* Ia 273, secondo cui la sorveglianza non deve servire a confermare un sospetto).

Le minacce la cui soppressione giustifica l'impiego di strumenti specifici per la ricerca di informazioni sono: terrorismo, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo oppure trasferimento illegale di tecnologia. Questi concetti sono specificati ai numeri 2.7 (ad art. 13*a* cpv. 1) e 1.2.1 (terrorismo).

Capoverso 2

Il capoverso 2 propone un elenco esaustivo degli strumenti della ricerca specifica di informazioni. Per ulteriori ragguagli si vedano i commenti dei singoli strumenti.

2.21 Articolo 18*b* Condizioni

L'impiego di strumenti specifici per la ricerca di informazioni presuppone l'adempimento cumulativo di cinque condizioni.

Capoverso 1

Le prime quattro condizioni sono di tipo materiale; adempiono quanto previsto all'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, come pure la protezione di collaboratori dell'Ufficio federale da persone, organizzazioni o fazioni sospettate di costituire una minaccia (presunti autori della minaccia; cfr. lett. a).

In fatto di proporzionalità, occorre – per quanto possibile – fare la distinzione tra le componenti di fondo: adeguatezza dello strumento impiegato per raggiungere lo scopo perseguito nell'interesse pubblico (lett. d *in initio*); necessità (lett. c e d *in fine*), in quanto tutti gli strumenti convenzionali si sono rivelati inefficaci; proporzionalità *stricto sensu* (lett. b), allorché prevale l'interesse pubblico e giustifica l'ingerenza nei diritti della persona in questione.

2.22 Articolo 18*c* Sorveglianza di terzi e tutela del segreto professionale

L'articolo disciplina due particolari forme di sorveglianza: quella di terzi coinvolti in un'operazione di sorveglianza di cui non sono l'obiettivo designato, e quella di persone vincolate dal segreto professionale ai sensi dell'articolo 321 CP; questi casi richiedono determinate misure di protezione specifiche.

Capoverso 1

La disposizione disciplina il coinvolgimento indiretto di terzi. È ipotizzabile che il presunto autore della minaccia, controllato con l'ausilio di strumenti specifici per la ricerca di informazioni, si serva di strumenti di comunicazione o di luoghi che non gli appartengono, ma rientrano nella disponibilità di un terzo (ad es. un apparecchio telefonico o un sistema informatico locale privato). È senz'altro possibile che il terzo sia all'oscuro dell'uso fatto dei suoi strumenti 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 considerato una minaccia.

Capoverso 2

Questa disposizione non si applica esclusivamente ai terzi, ma disciplina qualsiasi coinvolgimento diretto o indiretto di una persona vincolata dal segreto professionale, quale ad esempio un avvocato. La disposizione punta alla massima tutela possibile del segreto professionale, per cui si applica sia a terzi il cui ambiente è sorvegliato secondo il capoverso 1, sia a persone controllate con l'ausilio di strumenti specifici per la ricerca di informazioni. Il testo richiama l'articolo 4 capoverso 6 della legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT; RS *780.1*). Secondo la giurisprudenza della Corte europea dei diritti dell'uomo (decisione Kopp vs Confederazione Svizzera, 25 marzo 1998), la selezione dev'essere controllata da un'autorità giudiziaria. Tale decisione verte su un procedimento penale, ma può essere applicata per analogia. Appare pertanto opportuno affidare tale compito al TAF (cfr. 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).

2.23 Articolo 18*d* Tribunale amministrativo federale

L'impiego di strumenti specifici per la ricerca di informazioni lede i diritti fondamentali, in particolare quello al rispetto della sfera privata garantito dagli articoli 8 CEDU e 13 Cost. Inoltre, la natura della ricerca specifica fa sì che una persona sorvegliata non possa opporsi alla misura finché questa dura. È quindi indispensabile che l'applicazione delle pertinenti disposizioni normative venga disciplinata con la massima precisione possibile e che il loro rispetto venga controllato rigorosamente.

Il controllo è duplice e scaglionato nel tempo. Le persone sottoposte a una ricerca di informazioni con l'ausilio di strumenti specifici devono esserne informate una volta portato a termine l'incarico; possono impugnare tale misura mediante ricorso dinanzi al TAF (verifica *ex post*). L'obbligo di rivelare *ex post* l'avvenuta ricerca specifica di informazioni è disciplinato all'articolo 18*i*, i rimedi giuridici all'articolo 29*a*.

Ma ciò 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). Alla verifica *ex post* va pertanto abbinata una verifica *ex ante* tale da garantire un severo controllo già nel momento in cui viene richiesto l'impiego di strumenti specifici per la ricerca di informazioni.

Per le misure in ambito penale, la legge prevede di norma una duplice verifica, affidata a un'autorità giudiziaria (procuratore, giudice istruttore, giudice di merito). Dal momento che la ricerca specifica di informazioni a titolo preventivo costituisce una lesione analoga dei diritti fondamentali, non si giustifica la rinuncia alla duplice verifica. Nella sua decisione principale del 1983 (DTF *109* Ia 273), il Tribunale federale stabiliva 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 prevista vada considerata un appannaggio delle autorità giudiziarie o se possa essere affidata a un ente paragiudiziale che, come minimo, sia indipendente dall'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 senza mezzi termini che basta una verifica paragiudiziale, ma il Tribunale federale sembra dedurne la necessità di una verifica giudiziale.

Nella decisione Klass vs Repubblica Federale di Germania del 6 settembre 1978, la Corte eur. DU stabilì che, per quanto attiene alla sorveglianza preventiva, la legge tedesca soddisfa i requisiti dell'articolo 8 capoverso 2 della convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (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 conformità della legge alla CEDU presuppone tuttavia che le ingerenze nella sfera privata siano ammesse soltanto se l'intervento è giustificato dall'interesse pubblico (ad es. per motivi di sicurezza nazionale o pubblica), è necessario in una società democratica (cfr. in particolare decisione Klass, § 21, 53 e 60) ed è giustificato dallo scopo, alla luce dell'articolo 13 CEDU (Diritto ad un ricorso effettivo).

La corte ritenne di per sé auspicabile che, in un ambito in cui vi è il rischio di gravi abusi a detrimento di una società democratica, la verifica fosse affidata a un giudice. Giunse tuttavia alla conclusione che il sistema tedesco di un comitato indipendente, anche se soltanto paragiudiziale, soddisfaceva il criterio della necessità, com'è inteso in una società democratica (op. cit., § 56).

Nelle sue considerazioni (DTF *109* Ia 273), il Tribunale federale fornisce un'interpretazione leggermente diversa in materia. Si trattava di 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 vecchia Cost., che tutelava il segreto epistolare. Secondo i giudici federali, 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 tutelava a sufficienza gli interessati (DTF *109* Ia 273). Dodici anni dopo, il Tribunale federale, richiamandosi a tale decisione, ribadì 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 nelle procedure penali formali.

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

Alla luce di tale incertezza, il presente avamprogetto privilegia la «soluzione Tribunale federale», prevedendo che il TAF verifichi la legalità dell'impiego di strumenti specifici per la ricerca di informazioni.

Capoverso 1

Il primo capoverso 1 istituisce le basi per l'impiego di strumenti specifici per la ricerca di informazioni: le istanze sono presentate dall'Ufficio federale, mentre al TAF compete la verifica giuridica di queste e altre istanze; le sue attribuzioni sono definite come segue:

Lettera a
Il compito principale del TAF consiste nell'esaminare la legalità degli strumenti specifici disposti dall'Ufficio federale. Vanno verificati in particolare l'esistenza di un interesse pubblico, la proporzionalità ai sensi dell'articolo 18*b* e il rispetto delle disposizioni di legge in materia. Sono pertanto oggetto di verifica la legittimità e la proporzionalità dell'impiego previsto di strumenti specifici per la ricerca di informazioni.

Lettera b
Il TAF deve inoltre verificare se sono adempite le condizioni previste dalla legge per procedere o rinunciare a una comunicazione secondo l'articolo 18*i*. Anche in questo caso si tratta di una verifica giuridica e non già di un esame dell'opportunità politica, fattore di stretta competenza del capo del Dipartimento DFGP.

Lettera c
In terzo luogo, il TAF 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*). Ancora una volta si tratta di un controllo della legalità, vale a dire che il TAF deve accertare l'adempimento delle condizioni previste all'articolo 14*c* capoverso 3 e all'articolo 14*d* capoversi 1 e 2. Per contro non si esprime sull'opportunità di creare tali identità fittizie; è una competenza che spetta al capo del Dipartimento. Anche per le identità fittizie è quindi indispensabile l'autorizzazione: la creazione di un'identità fittizia presuppone un parere favorevole del TAF (cfr. art. 14*c* cpv. 3 e 14*d* cpv. 1).

Capoverso 2
Il secondo capoverso specifica che il TAF dispone le misure previste al capoverso 1 soltanto se è a conoscenza di tutti i fatti rilevanti. Quando chiede l'impiego di strumenti specifici per la ricerca d'informazioni, l'Ufficio federale deve pertanto indicare i principi di cui all'articolo 18*a*, le condizioni di cui all'articolo 18*b* e i particolari procedurali di cui all'articolo 18*f* capoverso 2; per chiedere deroghe all'obbligo di comunicazione, deve comprovare l'esistenza di motivi secondo l'articolo 18*i* capoverso 2, mentre per creare identità fittizie secondo gli articoli *14c* e 14*d*, deve specificare i motivi e le modalità d'impiego.

Capoverso 3
Il TAF verifica la legalità dell'istanza presentata dall'Ufficio federale. Comunica entro 72 ore la sua decisione scritta e motivata all'Ufficio federale, cui può comunque chiedere delucidazioni o ulteriori informazioni prima di decidere. Allo stesso modo, il TAF può accogliere l'istanza in parte o vincolarla a oneri.

Il parere favorevole, in tutto o in parte, costituisce la prima, seppure non unica, condizione per l'impiego di strumenti specifici per la ricerca di informazioni (art. 18*e*). Il parere favorevole dà il via libera al seguito della procedura di autorizzazione; la decisione definitiva in merito all'istanza compete al Consiglio federale.

L'ultimo periodo del capoverso 3 stabilisce che il TAF deve comunicare al Dipartimento tutti i pareri sfavorevoli. La disposizione mira a offrire ai vertici del Dipartimento una panoramica delle istanze proposte dall'Ufficio federale (e non solo dei pareri favorevoli).

Capoverso 4
Questo capoverso attribuisce al TAF il margine di manovra dovuto per l'organizzazione interna e si limita a statuire che la continuità della giurisprudenza va garantita designando un'apposita corte cui sono attribuite regolarmente questioni inerenti alla protezione dello Stato. La disposizione specifica inoltre le necessarie esigenze di segretezza, che giustificano in particolare l'istituzione di una segreteria propria.

Sebbene non esista una base legale specifica, alla luce degli interessi e dei beni giuridici in gioco, si presuppone inoltre che i casi vengano trattati esclusivamente dai giudici competenti (senza la collaborazione di segretari giuridici, cancellieri, ecc.).

2.24 Articolo 18*e* Decisione in merito all'impiego di strumenti specifici per la ricerca di informazioni

Capoverso 1
La disposizione stabilisce che l'Ufficio federale può sottoporre al Dipartimento o, se del caso, al Consiglio federale l'istanza di approvazione degli strumenti specifici per la ricerca di informazioni soltanto se il TAF ha, in precedenza, espresso un parere favorevole.

Capoversi 2 e 3
Se il TAF ha emesso un parere giuridico favorevole in merito all'impiego di strumenti specifici, in seguito è effettuato un esame secondo criteri politici. L'incarto è trasmesso, insieme al parere positivo del TAF, al capo del DFGP. Questi è tenuto a consultare il capo del DDPS in quanto presidente della Giunta del Consiglio federale in materia di sicurezza. Se vi è accordo sull'impiego di strumenti specifici per la ricerca di informazioni, il capo del DFGP decide definitivamente. In caso di disaccordo decide il Consiglio federale. Anche in caso di parere positivo del TAF, il capo del DFGP o il Consiglio federale possono comunque rinunciare, in tutto o parzialmente, ad adottare le misure richieste.

Il capo del DFGP o il Consiglio federale è vincolato dagli oneri previsti nel parere favorevole del TAF (cfr. art. 18*d* cpv. 3).

Capoverso 4
Se il capo del DFGP o il Consiglio federale ritengono opportuno l'impiego di strumenti specifici per la ricerca di informazioni, ne specificano le modalità (lett. a-e), e in particolare

- l'obiettivo perseguito;
- il bersaglio (ossia il presunto autore della minaccia);
- gli strumenti ammessi secondo l'articolo *18a* capoverso 2;
- la durata dell'impiego. La legge prevede una prima scadenza dopo sei mesi al massimo (cfr. cpv. 4). Determinate operazioni, ad esempio l'accesso a un sistema informatico, non richiedono prolungati lassi di tempo, ma possono talvolta essere effettuati nell'ambito di un unico intervento. In questi casi l'avamprogetto prevede che venga fissata una scadenza. Nella fattispecie si tratta di fissare una data entro la quale l'intervento debba essere portato a

termine. Non è quindi la ricerca specifica di informazioni a essere limitata nel tempo, ma la validità dell'autorizzazione; e
- gli oneri cui è vincolata l'esecuzione (rendiconti periodici).

Capoverso 5
Il termine autorizzato dal capo del DFGP o dal Consiglio federale può essere prorogato due volte di tre mesi in caso di parere favorevole del TAF. Ciò significa che uno strumento specifico può essere impiegato per dodici mesi al massimo (6 + 3 + 3). Per impieghi più prolungati, l'Ufficio federale o il Dipartimento deve presentare una nuova istanza.

Capoverso 6
Il capoverso 6 descrive il rapporto con le competenze costituzionali del Consiglio federale ed è di natura dichiarativa. La procedura prevista dalla LMSI non sostituisce le competenze costituzionali del Consiglio federale. La procedura secondo la LMSI ha piuttosto funzione integrativa, in quanto istituisce le basi legali per il caso ordinario. In casi eccezionali, il Consiglio federale potrà continuare a procedere in particolare a norma dell'articolo 184 capoverso 3 Cost., a condizione che siano adempite le condizioni per sventare un'imminente minaccia alla sicurezza interna o esterna. A titolo puramente teorico, è pertanto ipotizzabile la situazione seguente: sebbene l'Ufficio federale rinunci a presentare istanza o il TAF emetta un parere sfavorevole perché non vi sono le premesse legali per disporre strumenti specifici per la ricerca di informazioni, è ammesso e doveroso che il Consiglio federale adotti misure costituzionali a motivo di una minaccia di altro tipo non contemplata dalla LMSI ossia in ragione della particolare gravità del caso. Se, insomma, le particolari circostanze rendessero necessario un atto di governo, compete al Consiglio federale assumere la responsabilità politica in particolare secondo quanto disposto all'articolo 184 capoverso 3 Cost. e ordinare l'impiego di uno strumento specifico.

2.25 Articolo 18*f* Procedura d'urgenza
L'articolo 18*f* definisce, a titolo di deroga, il caso in cui vi sia un pericolo imminente. Se la decisione tardiva del TAF, del capo del DFGP o del Consiglio federale compromette o rende impossibile riuscire nella ricerca specifica di informazioni, dev'essere possibile agire senza indugio. È quanto succede ad esempio quando un obiettivo di spicco entra di sorpresa in Svizzera e va subito posto sotto controllo (ad es. anche sorvegliandone le telecomunicazioni).

Capoverso 1
In casi urgenti, l'impiego di strumenti specifici è disposto direttamente dal direttore dell'Ufficio federale; l'esecuzione è immediata. Le condizioni materiali per l'impiego di uno strumento specifico (art. *18b* cpv. 1 lett. a-d) devono essere adempite anche nei casi urgenti. Incombe al direttore dell'Ufficio federale assicurare che le condizioni siano effettivamente adempite. Il Dipartimento è informato in contemporanea.

Capoverso 2
Il direttore dell'Ufficio federale è tenuto a presentare al TAF l'istanza ordinaria entro 24 ore; l'urgenza va motivata in sede separata. La procedura segue poi il suo corso abituale. Il TAF deve decidere entro 72 ore come nella procedura «ordinaria».

Capoverso 3
L'istanza dell'Ufficio federale per autorizzare *ex post* l'impiego di strumenti specifici per la ricerca di informazioni presuppone un parere favorevole del TAF. L'istanza dev'essere presentata senza indugio, ossia rapidamente.

Capoverso 4
Se l'impiego di strumenti specifici disposto d'urgenza non ottiene il parere favorevole del TAF o l'autorizzazione *ex po*st del capo del DFGP o del Consiglio federale, l'Ufficio federale deve distruggere senza indugio i dati tratti da tale ricerca e raccolti fino ad allora (cfr. la disposizione analoga inserita all'art. 7 cpv. 4 LSCPT).

2.26 Articolo 18*g* Sospensione dell'intervento
L'Ufficio federale interrompe senza indugio la ricerca di informazioni se questa non è più necessaria (lett. a), risulta infruttuosa (lett. b), non viene prorogata (lett. c) o, nella procedura d'urgenza, non è considerata legale dal TAF o non viene autorizzata dal capo del DFGP o dal Consiglio federale (lett. d-e). Se una misura la cui esecuzione è in corso non ottiene l'autorizzazione necessaria, le informazioni ricavate non possono essere utilizzate. Se le informazioni ottenute con tale misura sono già state trasmesse ad altri organi o autorità, l'Ufficio federale deve chiederne la distruzione. Tali disposizioni riflettono i principi generali in materia di protezione dei dati personali.

2.27 Articolo 18*h* Trattamento dei dati personali raccolti impiegando strumenti specifici
L'articolo disciplina il trattamento dei dati personali raccolti impiegando strumenti specifici per la ricerca di informazioni.

Capoverso 1
La disposizione disciplina le condizioni generali per la conservazione dei dati elencati all'articolo 15 LMSI. I dati raccolti vanno distrutti entro trenta giorni dalla fine dell'intervento, purché non abbiano alcuna relazione con la minaccia che ha dato adito all'impiego di strumenti specifici per la ricerca di informazioni.

Capoverso 2
Questo capoverso stabilisce che il trattamento dei dati personali raccolti impiegando strumenti specifici per la ricerca d'informazioni è retta dall'articolo 3 capoversi 1-3 e dagli articoli 15, 16 e 17 LMSI.

2.28 Articolo 18*i* Obbligo di comunicazione
Questa disposizione è un elemento cardine dell'avamprogetto e si rivela determinante ai fini della verifica *ex post* (cfr. quanto esposto ad art. 18*d in initio*). Se, 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 strumenti specifici, essa di norma non ha alcuna possibilità di difendersi a fatto avvenuto, a meno che non ne sia venuta a conoscenza per altri canali. La comunicazione permette pertanto all'interessato di interporre ricorso (cfr. art. 29*a*).

L'obbligo di informare gli interessati è di natura costituzionale e deriva implicitamente dalla garanzia di rispettare la sfera privata e la corrispondenza epistolare. Tale garanzia si fonda sugli articoli 8 CEDU e 13 Cost. In un procedimento penale, il diritto di essere informati e quello di essere sentiti (art. 29 Cost.) si sovrappongono. Nell'ambito di un'operazione preventiva dalla quale non scaturisce alcun procedimento penale, può tuttavia accadere che la legge su cui si basa l'operazione non contempli alcun obbligo di comunicazione. Era il caso della legge del Cantone di Basilea Città, oggetto della citata decisione del novembre 1983. La legge recitava seccamente che la procedura è segreta nei confronti dell'interessato (DTF *109* Ia 273). I giudici federali replicarono che la Costituzione vietava di rinunciare in modo generalizzato e indistinto alla comunicazione *ex post*. A loro parere, gli interessati devono di regola venire a conoscenza delle misure di sorveglianza effettuate – che si tratti di sorveglianza preventiva o repressiva, di imputati e sospettati o di terzi. In linea di massima, si può quindi partire dal presupposto che le misure di sorveglianza vadano comunicate agli interessati (DTF *109* Ia 273).

Capoverso 1

In osservanza di tale giurisprudenza, il presente avamprogetto sancisce l'obbligo di comunicazione. Al termine di un'operazione, l'Ufficio di federale è tenuto, in linea di massima, a mettere al corrente gli interessati della ricerca specifica di informazioni (per il concetto di «operazione», cfr. art. 14 OMSI).

Capoverso 2

Nella citata decisione Klass (§§ 57 – 59; cfr. quanto esposto all'art. 18*d*), la Corte europea dei diritti dell'uomo constatò che la comunicazione *ex post* poteva senz'altro mettere in questione lo scopo a lungo termine di una sorveglianza. Riconobbe inoltre che sussisteva il rischio di rivelare i metodi di lavoro dei servizi segreti, i settori sorvegliati ed eventualmente addirittura l'identità degli inquirenti. Furono pertanto giudicate lecite le deroghe all'obbligo di comunicazione previste dalla legge tedesca.

Nella sua decisione del 1983, il Tribunale federale accolse 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 relativizzato dalle esigenze inerenti alle indagini di polizia. Le deroghe elencate alle lettere a-d del capoverso 2 riflettono ampiamente l'articolo 10 capoverso 3 LSCPT e l'articolo 22 capoverso 2 LFIM.

Le lettere a-d riportano l'elenco esaustivo dei motivi che giustificano di rimandare la comunicazione o di rinunciarvi.

Del resto, la decisione di procrastinare la comunicazione o di rinunciarvi non è di competenza dell'Ufficio federale. 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 di strumenti specifici per la ricerca di informazioni. È pertanto opportuno prevedere regole severe: se del caso, l'Ufficio federale presenta istanza motivata chiedendo una deroga all'obbligo di comunicazione. Il TAF

verifica la legalità della richiesta e, qualora emetta un parere favorevole, il capo del DFGP prende una decisione definitiva in merito.

Con la consultazione del capo del DDPS prevista dall'articolo 18e capoverso 2 del presente avamprogetto, si garantisce anche che eventuali necessità di tutela del segreto del Servizio informazioni strategico (SIS) siano tempestivamente incluse negli atti e che il TAF oppure il capo del DFGP ne possano tenere conto in occasione della loro decisione.

Il diritto d'essere informati ai sensi degli articoli 8 segg. LPD è retto dall'articolo 18 LMSI.

2.29 Articolo 18*j* Esecuzione da parte dei Cantoni

Questo articolo stabilisce che la ricerca specifica di informazioni da parte degli organi di sicurezza cantonali su mandato della Confederazione è retta dalle disposizioni della LMSI. Se pertanto gli organi di sicurezza cantonali osservano luoghi non liberamente accessibili o vi installano apparecchi di sorveglianza operando su mandato della Confederazione, si applicano gli articolo *18a* segg. del presente avamprogetto e non le disposizioni del diritto cantonale.

2.30 Sezione 2 Strumenti specifici 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 previste dalla legge medesima. Tuttavia, non basta elencare i vari strumenti che potrebbero limitare i diritti fondamentali. Occorre piuttosto esporre nel dettaglio la portata delle limitazioni, specificare i punti su cui vertono e disciplinare nei particolari le azioni ammesse. Tali normative sono tanto più essenziali, quanto la loro applicazione varia a seconda dell'impiego di tali strumenti in un procedimento penale o nell'ambito di una ricerca di informazioni da parte dei servizi segreti. Tanto per fare un esempio: nel corso di un'istruttoria, si accede a un sistema informatico in presenza del sospettato o di una persona che lo sostituisce, a meno che sussistano circostanze ben definite sancite nella legge. Nella sfera d'attività dei servizi d'informazione, per contro, va offerta la possibilità di svolgere la medesima operazione all'insaputa degli interessati.

2.31 Articolo 18*k* 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 si inserisce tuttavia nell'ambito del procedimento penale, ma mira a riconoscere minacce concrete derivanti da terrorismo, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo oppure trasferimento illegale di tecnologia. Per tale motivo è necessario un disciplinamento speciale nella LMSI.

Comunque, la LMSI istituisce regole speciali soltanto laddove occorrono varianti o precisazioni rispetto alla LSCPT. Nelle questioni tecniche e organizzative, la LMSI rimanda quindi alla LSCPT, poiché il legislatore non si prefigge di definire altre procedure e altri requisiti tecnici per la sorveglianza preventiva, ma intende piuttosto far capo alle strutture collaudate.

Capoverso 1
Questo capoverso specifica lo scopo perseguito sorvegliando la corrispondenza postale e il traffico delle telecomunicazioni: si parla di «mezzi di comunicazione» in genere. Come nella legge sulle telecomunicazioni e nella LSCPT, si rinuncia ad indicare strumenti tecnici specifici, per garantire il necessario margine di manovra in questo settore, in cui il progresso tecnico procede a velocità particolarmente sostenuta. Occorrono inoltre indizi concreti per fondare il sospetto che il presunto autore della minaccia si serva di tali strumenti per scambiare informazioni o commettere atti direttamente connessi alla concreta minaccia alla sicurezza interna o esterna. Per giustificare la sorveglianza in un determinato momento, tali indizi devono essere sufficientemente specifici e attuali.

Capoverso 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 soltanto in determinate occasioni, una certa cabina telefonica pubblica.

Capoverso 3
Se una persona sospetta cambia in rapida successione i collegamenti di telecomunicazione, ad esempio utilizzando carte prepagate, 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).

Capoverso 4
Non si intende creare strutture parallele alla LSCPT per la sorveglianza preventiva della corrispondenza postale e del traffico delle telecomunicazioni. Per tale motivo, le varie forme di sorveglianza, la loro attuazione tecnica e le indennità sono rette per analogia dalla LSCPT e dalle 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 strumenti specifici, possono essere impiegati unicamente nei tre ambiti da cui può scaturire una minaccia che rischia di minare i fondamenti della nostra società (cfr. quanto esposto all'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, *stricto sensu*, 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, allora questa forma di sorveglianza è lo strumento adatto per ottenere informazioni che permettono di meglio giudicare e prevenire la minaccia.

Gli organi di sicurezza non sono tuttavia autorizzati a effettuare sorveglianze a titolo puramente «esplorativo», vale a dire muovendosi a caso, soltanto perché hanno motivo di sospettare che una persona possa minacciare la sicurezza interna. Occorrono

in ogni caso indizi concreti che corroborino il sospetto che la persona in questione si serve di determinati mezzi di telecomunicazione per le sue attività. La sorveglianza è considerata adeguata se può essere reso verosimile che le attività pericolose vengono compiute con l'ausilio dei mezzi di telecomunicazione.

Quanto alla necessità di adottare tale misura, appare evidente che soltanto la sorveglianza delle telecomunicazioni permette di individuare i contatti di una persona sospettata di costituire una minaccia o di scoprire il contenuto di messaggi scambiati con i mezzi di telecomunicazione. È pressoché impossibile procurarsi tali informazioni necessarie 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 *stricto sensu*, ossia se l'interesse pubblico prevale al punto da giustificare la lesione dei diritti fondamentali dell'individuo. Gli organi competenti possono ponderare l'interesse pubblico e la tutela dei diritti fondamentali del singolo, giungendo a una decisione fondata soltanto se sono a conoscenza delle circostanze specifiche. È importante che gli aspetti giuridici non vengano valutati soltanto dagli organi di sicurezza, ma anche da un'autorità giudiziaria indipendente, che è in grado di meglio ponderare 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 conto tenuto delle restrizioni e dei provvedimenti previsti dall'avamprogetto, la sorveglianza preventiva della corrispondenza postale e del traffico delle telecomunicazioni costituisce uno strumento proporzionato alla tutela dell'interesse pubblico, che può essere impiegato in conformità con le richieste della Costituzione e della CEDU.

2.32 Articolo 18*l* Osservazione in un luogo non liberamente accessibile, anche ricorrendo ad 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 in luoghi non liberamente accessibili (ad es. locali adibiti a uso commerciale, sale di riunione, appartamenti, camere d'albergo; cfr. cpv. 1). A tal fine è anche previsto l'impiego di apparecchi tecnici di sorveglianza (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 riservata di una persona (art. 179^{quater} CP), se essa lo tiene intenzionalmente segreto benché avvenga in un luogo liberamente accessibile. Non sono per contro tutelati fatti privati di natura generale che avvengono in pubblico.

Capoverso 1
La disposizione fissa i particolari e le condizioni dell'osservazione. Devono sussistere fatti concreti e attuali che facciano 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.

Capoverso 2
L'impiego di apparecchi tecnici di sorveglianza corrisponde, per contenuto e portata, alla disposizione dell'articolo 66 capoverso 2 della legge federale sulla procedura

penale (PP; RS *312.0*). Si tratta di apparecchi per la ripresa di suoni e immagini, che possono essere impiegati anche nella sfera privata, 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 strumento specifico alla luce dell'interesse pubblico, rimandiamo a quanto illustrato agli articoli 13*a* e 18*k*. Per quanto attiene alla proporzionalità, si impongono le seguenti considerazioni: se vi sono fatti sufficienti ad accertare che il presunto autore della minaccia si serva di un determinato luogo per le sue attività, allora l'osservazione è lo strumento adatto per ottenere informazioni che permettono di meglio giudicare e prevenire la minaccia. Gli organi di sicurezza non sono tuttavia 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 costituisca un elemento chiave degli atti del presunto autore della minaccia. La misura è considerata adeguata a condizione che venga 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 nei luoghi privati. Tali situazioni però non consentono sempre di trovare o impiegare informatori. Come spiegato in precedenza, soltanto gli organi competenti possono giudicare se la misura è proporzionata *stricto sensu*, 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 TAF.

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.

2.33 Articolo 18*m* Accesso segreto a un sistema per l'elaborazione di dati

Le moderne infrastrutture EEP rivestono un'importanza crescente nella vita di tutti i giorni. Internet in particolare è assurto a importante strumento per lo scambio di informazioni. Dal momento che le autorità preposte alla sicurezza stanno già conducendo intense ricerche di informazioni nella rete pubblica, i gruppi in questione (ad es. organizzazioni terroriste) stanno relegando la diffusione di contenuti delicati in settori riservati protetti 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).

La disposizione definisce tale strumento di ricerca specifica 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 a dati registrati elettronicamente o secondo un modo simile e specialmente protetti contro l'accesso di terzi. Al contrario della perquisizione effettuata nell'ambito di un'istruzione penale, questo tipo di accesso è ammesso anche 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 nel portatile del presunto autore della minaccia o la decodifica di un messaggio elettronico cifrato.

Interesse pubblico e proporzionalità
L'introduzione in 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 strumento specifico alla luce dell'interesse pubblico, rimandiamo a quanto illustrato agli 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 o una rete di dati per 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 indispensabile per procurare le informazioni necessarie a valutare la minaccia. Per accedere a tali dati non vi è altro modo che introdursi nel sistema informatico. La disposizione si applica soltanto ai sistemi informatici, non ai locali o ai veicoli, che non potranno essere perquisiti, ma soltanto sottoposti ad altre ricerche di informazioni, quali l'osservazione fisica o l'uso di apparecchi tecnici di sorveglianza. La revisione propone una gamma ristretta di strumenti, al fine di preservare la proporzionalità già a livello di legge. Come spiegato in precedenza, soltanto gli organi competenti possono giudicare se la misura è proporzionata *stricto sensu*, 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 TAF.

2.34 Capitolo 3*b* Divieto di determinate attività

Il divieto di determinate attività costituisce una nuova misura. La legge in vigore si limita a disciplinare il trattamento dei dati personali da parte degli organi di sicurezza e a proporre norme basate sull'assistenza amministrativa. Non contiene alcuna disposizione atta a influenzare il comportamento delle persone. La revisione della LMSI, sottoposta al Parlamento il 24 marzo 2006 (propaganda violenta, violenza nel corso di manifestazioni sportive), fa un primo passo in questa direzione. Prevede misure contro la violenza in occasione di manifestazioni sportive, e in particolare disposizioni atte a indurre i privati a mutare il proprio comportamento: aree interdette, divieto limitato di lasciare la Svizzera, obbligo di presentarsi alla polizia e fermo preventivo di polizia. La presente revisione costituisce un ulteriore passo in questa direzione. Si intende rafforzare la prevenzione dei pericoli creando la possibilità di reagire senza indugio alla condotta seguita da privati.

2.35 Articolo 18*n*

La disposizione autorizza il capo del Dipartimento a pronunciare divieti amministrativi nei confronti di determinate attività, purché connesse a una concreta minaccia alla sicurezza interna o esterna. Nel diritto vigente, l'emanazione di divieti del genere deve fondarsi sulla Costituzione federale. Il Consiglio federale è autorizzato 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 minare la Costituzione. Ecco perché si intende creare la possibilità, a livello di legge, 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., competenze che continuano a sussistere in parallelo (cfr. anche quanto esposto in merito agli 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[5], altrimenti sono definitive. Per contro, le disposizioni emesse in base alla LMSI sono impugnabili mediante ricorso al TAF, la cui decisione può essere impugnata dinanzi al Tribunale federale.

Capoverso 1

La disposizione permette di vietare determinate attività. Vi sono ad esempio comportamenti che a prima vista possono sembrare innocui o addirittura degni 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 (ad es. si avvicinano i membri di una comunità straniera residente nel nostro Paese lasciando intendere che, se si rifiutano di fare una donazione, i loro familiari rimasti in patria ne pagheranno lo scotto). 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: i donatori involontari in Svizzera tacciono per paura di nuocere a sé stessi e ai loro familiari, amici e conoscenti rimasti in patria; le tracce del denaro si perdono nei meandri dei trasferimenti di capitali, dell'uso dei fondi attestato da certificati stranieri lacunosi o contraffatti (o autentici, ma fasulli sotto il profilo del contenuto) e via dicendo.

Il capo del Dipartimento deve definire il contenuto del divieto con la massima precisione possibile. Le sanzioni penali per chi viola il divieto sono fissate all'articolo 292

[5] Cfr. DTF **125** II 417; tale giurisprudenza è esplicitamente sancita all'art. 83 lett. a della legge federale sul Tribunale federale (FF **2005** 3643) e all'art. 32 cpv. 1 lett. a della legge sul Tribunale amministrativo federale (FF **2005** 3689). L'entrata in vigore di entrambe le leggi è prevista per il 1° gennaio 2007.

CP. Non occorre che la legge rimandi alla norma penale, in quanto tale rinvio avrebbe carattere puramente dichiarativo.

Capoverso 2

È indispensabile che tali divieti vengano limitati nel tempo dato che incidono sulla possibilità degli interessati di far valere i propri diritti fondamentali. Una volta scaduto il divieto, le autorità devono quindi verificare se continuano ad essere soddisfatte le condizioni per un divieto.

All'occorrenza, la durata di un divieto può essere prorogata fintantoché le circostanze lo esigono. In questo caso, lo scopo del limite temporale è diverso da quello contenuto nelle disposizioni degli articoli 184 capoverso 3 e 185 capoverso 3 Cost. Il limite temporale sancito nella Costituzione federale è teso a garantire che tali misure vengano trasposte nel diritto ordinario se la minaccia persiste. Lo scopo primario è quindi di rispettare il principio della separazione dei poteri e la procedura legislativa ordinaria. Il limite temporale proposto per la LMSI, per contro, si giustifica per motivi materiali, ossia per la gravità dell'ingerenza nei diritti fondamentali. Ecco perché la LMSI impone esplicitamente al Dipartimento di verificare, a intervalli regolari, se le condizioni all'origine della disposizione continuano a essere soddisfatte e, eventualmente, di revocare senza indugio il divieto. Il Dipartimento è quindi tenuto ad attivarsi 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 il divieto di una determinata attività alle condizioni indicate nella legge non è *a priori* sproporzionato, ma che vanno piuttosto ponderati gli interessi in causa nel caso specifico.

2.36 Articolo 27 capoverso 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 degli strumenti introdotti con la presente revisione. Alla luce delle eventuali restrizioni dei diritti fondamentali, appare indispensabile informare sull'uso delle identità fittizie, sull'impiego di strumenti specifici per la ricerca di informazioni e sul divieto di determinate attività. Del resto, il Dipartimento riceve già oggi rendiconti completi senza che esista un espresso obbligo legale (rapporti sulle operazioni).

2.37 Articolo 29*a*

La LMSI in vigore non contiene disposizioni in materia di procedura e di rimedi giuridici, ad eccezione dell'articolo 18, che disciplina il diritto d'essere informati dei dati personali trattati nel sistema d'informazione dell'Ufficio federale. L'introduzione della

ricerca di informazioni impiegando strumenti specifici richiede un adeguamento ai principi della Costituzione e della CEDU. Appaiono particolarmente rilevanti a tal proposito il futuro articolo 29*a* Cost. (Garanzia della via giudiziaria) e l'articolo 13 CEDU (Diritto ad un ricorso effettivo); cfr. anche quanto esposto in merito all'articolo 18*j*.

Capoverso 1
La disposizione sancisce il diritto di ricorrere dinanzi al TAF contro le decisioni di cui all'articolo 18*i* capoverso 1 e all'articolo 18*n*. La disposizione esplicita inoltre l'articolo 32 capoverso 1 lettera a della legge sul Tribunale amministrativo federale (LTAF; FF *2005* 3689), 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 TAF (cfr. quanto esposto in merito all'articolo18*n*).

L'attribuzione al Consiglio federale della competenza decisionale in materia di strumenti specifici per la ricerca di informazioni non incide sulla procedura ricorsuale perché, nel caso dell'articolo 18*i* capoverso 1, l'atto impugnabile dinanzi al TAF è la comunicazione *ex post* dell'Ufficio federale.

Capoverso 2
Nei ricorsi contro l'impiego di strumenti specifici comunicato secondo l'articolo 18*i* capoverso 1, la natura delle misure in questione e i problemi inerenti alla ricostruzione successiva degli atti giustificano una disposizione più severa rispetto all'articolo 49 della legge federale sulla procedura amministrativa (PA; RS *172.021*). Il presente capoverso stabilisce infatti che può essere fatta valere soltanto la presunta violazione del diritto federale. Negli altri casi il ricorrente può far valere anche l'accertamento inesatto o incompleto di fatti giuridicamente rilevanti e l'inadeguatezza (cfr. art. 49 cpv. 2 PA).

Capoverso 3
Alla stregua di altre leggi federali, la LMSI, per motivi di chiarezza, rimanda alle disposizioni generali in materia di organizzazione giudiziaria.

2.38 Legge sul Tribunale amministrativo federale[6]
L'introduzione dell'articolo 13*b* LMSI richiede l'adeguamento della LTAF. Infatti, l'articolo stabilisce che il TAF è competente per comporre le controversie tra l'Ufficio federale e le autorità, le unità amministrative dei Cantoni, le organizzazioni che esercitano funzioni pubbliche e le unità amministrative dell'Amministrazione federale decentralizzata (cfr. quanto esposto ad art. 13*b*).

2.39 Codice penale svizzero[7]
Articoli 179^{octies} e 317bis
Articolo 179^{octies}
L'impiego, nella sfera segreta, di apparecchi tecnici di sorveglianza, quali registratori e macchine da presa, costituisce un reato ai sensi dell'articolo 179 CP segg. L'articolo 179^{octies} autorizza tuttavia la sorveglianza statale in base alla LSCPT.

La disposizione penale va modificata affinché la deroga comprenda anche le nuove misure di sorveglianza ammesse secondo la LMSI.

[6] RU ... (FF **2005** 3689)
[7] RS **311.0**

Articolo 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 atti a costituire o conservare un'identità fittizia nell'ambito di un'inchiesta mascherata approvata dal giudice. La norma penale va adeguata affinché la deroga comprenda anche l'utilizzo delle identità mascherate secondo la LMSI.

2.40 Legge federale sull'esercito e sull'amministrazione militare
Articolo 99 capoversi 1 secondo periodo, 1bis e 2 e articolo 99*a*
Articolo 99 capoverso 1 secondo periodo e articolo 2
Limitando (in linea di principio) l'esplorazione radio a obiettivi situati all'estero, come previsto all'articolo 99 capoverso 1 dell'avamprogetto, si intende mettere in atto quanto raccomandato dalla Delegazione delle Commissioni della gestione nel suo rapporto del 10 novembre 2003 sul progetto ONYX. Per esplorazione radio all'estero s'intende il rilevamento di emissioni elettromagnetiche di sistemi di telecomunicazione provenienti dall'estero. Oggi a tale scopo vengono impiegati sia il sistema ONYX per le comunicazioni trasmesse via satellite sia apparecchi riceventi capaci di captare le onde corte. Sarà lo sviluppo tecnico a determinare quali strumenti e sistemi verranno utilizzati in futuro per l'esplorazione radio all'estero. L'avamprogetto rinuncia volutamente a una definizione più specifica e utilizza l'espressione generica di «esplorazione radio».

Articolo 99 capoverso 1bis
Secondo il capoverso 1 secondo periodo, 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 al capoverso 1 secondo periodo, 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 seguenti.

Lettera a: sorveglianza delle frequenze. Nel corso dei suoi interventi, l'esercito deve poter controllare se eventuali civili si stanno servendo delle frequenze assegnate ai militari. Se del caso, identificherà e filtrerà tali utenti civili. Soltanto eliminando gli utenti civili indesiderati, l'esercito può garantire la capacità di comunicazione necessaria all'espletamento dei suoi compiti.

Lettera b: salvaguardia della sovranità sullo spazio aereo. Secondo l'ordinanza concernente la salvaguardia della sovranità sullo spazio aereo (OSS; RS *748.111.1*), tale compito spetta alle Forze aeree. A tale scopo devono potersi avvalere dell'esplorazione radio per intercettare le comunicazioni radio trasmesse tra aerei militari e civili e le loro stazioni terrene (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 vigilare sullo spazio aereo e descrivere la situazione aerea, come prescritto dall'articolo 5 OSS.

Inoltre, l'impiego dell'esplorazione radio da parte dell'esercito contro obiettivi civili in Svizzera (o all'estero) è ammessa anche nell'ambito della legittima difesa o di uno stato di necessità, ad esempio per proteggere i militari da un imminente attacco sfer-

rato da civili. Si tratta di un classico motivo giustificativo, che la legge militare non deve prevedere esplicitamente in quanto è già disciplinato agli articoli 25 e 26 del Codice penale militare (CPM; RS *321*).

*Articolo 99*a
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 del 15 ottobre 2003 concernente la condotta della guerra elettronica (OCGE; RS *510.292*) 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.

Capoverso 1
La disposizione prevede la designazione dell'Autorità di controllo indipendente, l'equivalente dell'istanza di controllo indipendente (ICI) attualmente retta dalle disposizioni degli articoli 14 segg. OCGE.

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 dei mandati di esplorazione radio permanente (ad es. del SIS DDPS). L'esplorazione radio all'estero (effettuata dall'esercito) può inserirsi anche negli interventi per il promovimento della pace. In questo caso, la decisione parlamentare in merito racchiude 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 accerta la legalità dell'esplorazione radio permanente, compresa la proporzionalità della misura, ma non si pronuncia in merito all'adeguatezza del controllo.

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

Capoverso 2
La disposizione delega al Consiglio federale il disciplinamento riguardante la composizione dell'Autorità di controllo indipendente.

2.41 Legge sulle telecomunicazioni[8]

Articolo 44
L'articolo 44 LTC va completato dal momento che d'ora in avanti la sorveglianza del traffico delle comunicazioni non è più retta soltanto dalla LSCPT (RS *780.1*), ma anche dalla LSMI (RS *120*).

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 secondo la legge federale del 20 marzo 1981 sull'assistenza internazionale in materia penale (AIMP; RS *351.1*). Lo scopo della sorveglianza in base alla LMSI è di individuare minacce derivanti da terrorismo, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo oppure trasferimento illegale di tecnologia.

[8] RS **784.10**

3. Ripercussioni

3.1 Ripercussioni per la Confederazione

3.1.1 Impatto finanziario
Dipende dalla tipologia e la configurazione delle singole misure e dal loro utilizzo.

3.1.2 Impatto sugli effettivi del personale
Le misure saranno attuate facendo ampio ricorso alle strutture federali e cantonali esistenti (TAF, SAP e servizi segreti dei Cantoni). Per il TAF, il SCS (Servizio per compiti speciali del DATEC, cui compete la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni), l'attuazione giuridica, operativa e amministrativa dei nuovi strumenti di ricerca e l'analisi dei risultati presso fedpol occorreranno complessivamente una quarantina di posti, che tuttavia non richiederanno l'assunzione di personale esterno.

Il fabbisogno di personale supplementare è in primo luogo riconducibile al potenziamento:

- delle strutture operative, in particolare le unità di polizia incaricate di raccogliere e trattare le informazioni (agenti di polizia, interpreti, tecnici, analisti operativi);
- delle strutture di elaborazione dei dati, in particolare la registrazione dei dati, l'assicurazione di qualità e lo scambio con l'estero;
- delle strutture estranee ai servizi d'informazione, quali il SCS (tecnica e amministrazione) o il TAF (segreteria).

Pertanto le nuove competenze delle autorità di sicurezza potranno essere introdotte utilizzando poche risorse supplementari.

3.1.3 Altre ripercussioni
Dipendono dalla tipologia e la configurazione delle singole misure.

3.2 Ripercussioni per i Cantoni e i Comuni
Cantoni e Comuni stanno innalzando il livello di sicurezza. All'eventuale inasprimento degli obblighi d'informazione e di comunicazione fanno da contraltare sgravi a media e lunga scadenza (accertamenti facilitati, parziale sostituzione delle osservazioni – costose per il loro fabbisogno di effettivi – con gli strumenti specifici per la ricerca di informazioni, ecc.), non ancora quantificabili allo stato attuale delle cose. A seconda della tipologia e della configurazione delle nuove misure, sono ipotizzabili oneri di lavoro supplementari nei Cantoni, che dovranno quindi decidere se aumentare gli effettivi del personale.

3.3 Impatto economico
In base alle direttive del 15 settembre 1999 del Consiglio federale 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
Il progetto mira tra l'altro all'attuazione degli interventi parlamentari. Il Consiglio federale ha incaricato il DFGP di presentare le proposte di revisione necessarie. Per il resto è competente la Confederazione.

3.3.2 Conseguenze per i singoli gruppi della società
Le disposizioni proposte rafforzano la sicurezza interna e quindi migliorano la protezione della popolazione.

3.3.3 Conseguenze per l'insieme dell'economia
Non si prevedono ripercussioni dirette sull'economia globale. Indirettamente, invece, un contesto sicuro migliora le condizioni generali.

3.3.4 Disciplinamenti alternativi
Della sicurezza interna del proprio territorio è responsabile in primo luogo ogni singolo Cantone. Se in virtù della Costituzione e della legge la Confederazione è responsabile della sicurezza interna, i Cantoni l'assistono sul piano dell'amministrazione e dell'esecuzione. Secondo la legge in vigore, alla Confederazione compete in particolare individuare tempestivamente le minacce derivanti da terrorismo, spionaggio politico o militare, commercio illecito di armi o materiale radioattivo oppure trasferimento illegale di tecnologia (non proliferazione). La Confederazione appoggia 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 e 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 muta 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 sulle relazioni internazionali
Sul piano formale, la revisione della legge non mette in atto alcun impegno internazionale. L'adeguamento degli standard migliora comunque la cooperazione internazionale.

3.4.2 Impatto per l'immagine della Svizzera
L'immagine internazionale della Svizzera ne trae grande profitto, in particolare vista la volontà di combattere efficacemente il terrorismo internazionale.

4. Aspetti giuridici

4.1 Base costituzionale

La LMSI si fonda sulla competenza non scritta della Confederazione di salvaguardare la sicurezza interna ed esterna. In questo ambito si inserisce anche la presente revisione di legge, che non va oltre i compiti descritti all'articolo 2 capoversi 1 e 2 LMSI. La revisione resta entro i limiti di tali compiti nella misura in cui singoli interventi si applicano esclusivamente ad atti di terrorismo, di spionaggio politico o militare, di commercio illecito di armi o materiale radioattivo oppure al trasferimento illegale di tecnologia. Né l'estremismo violento né lo spionaggio economico o la criminalità organizzata sono oggetto della presente revisione.

4.2 Compatibilità con i diritti fondamentali

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), la libertà di riunione (art. 22) e la garanzia della proprietà (art. 26).

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 la 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 proposte si fondano su una legge formale, la LMSI. L'interesse pubblico consiste nel salvaguardare la sicurezza interna o esterna e nell'individuare tempestivamente le minacce, segnatamente quelle 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 ai commenti ai singoli articoli (in part. ad art. 13*a*, 13*c*, 13*d*, 18*k*, 18*l*, 18*m*, 18*n*). 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 (in particolare le condizioni impostate come *ultima ratio*, il previo esame delle condizioni giuridiche e politiche, la garanzia dell'accesso a un esame giudiziale, ecc.). Del resto, le condizioni 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 risultano insufficienti per accertare un sospetto concreto di minaccia alla sicurezza interna o esterna («*ultima ratio*»).

La LMSI intende rafforzare la sicurezza della Svizzera e dei suoi abitanti. I singoli strumenti e le misure contenuti nel progetto sono conformi alla Costituzione.

4.3 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. Anche sotto questo profilo, l'approvazione degli strumenti e delle misure qui proposti costituisce un'importante contributo alla lotta contro il terrorismo e altri gravi minacce alla sicurezza internazionale. L'immagine internazionale della Svizzera non può che trarne vantaggio.

Sia lo scopo generale sia le singole disposizioni del presente progetto di legge sono conformi alla CEDU e al Patto internazionale relativo ai diritti civili e politici (Patto II; RS *0.103.2*).

Secondo la CEDU, l'esercizio dei diritti fondamentali (quali il rispetto della vita privata e familiare [art. 8 CEDU] o la libertà di riunione ed associazione [art. 11 CEDU]) può essere limitato, se tale restrizione è prevista dalla legge, persegue 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*c*, 18*d* 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 *supra*).

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. Allegati

5.1 Progetti legislativi in corso in materia di sicurezza interna

Trattati internazionali

Titolo	Contenuto	Stato dell'affare	Punti di contatto rilevanti con la presente revisione
Accordi bilaterali per l'applicazione dell'accordo di Schengen	Accordi bilaterali per l'attuazione dell'acquis di Schengen	Esame della necessità	No
Europol: dichiarazione d'intenti concernente l'estensione del mandato e modifica delle prescrizioni di classificazione	Estensione del campo d'applicazione di Europol ad altri reati	Progetto	No
Europol: accordo con i Paesi Bassi per il distacco di addetti di polizia	Distacco permanente di addetti di polizia nei Paesi Bassi	Progetto	No
Dichiarazione d'intenti CH-BRD per i mondiali 2006 (*Memorandum of understanding*)	Cooperazione nell'ambito dei mondiali 2006	Firma nel maggio del 2006	No
Accordo con la Slovenia sulla cooperazione transfrontaliera in materia di polizia	Cooperazione bilaterale in materia di polizia	Deliberazione al Consiglio degli Stati	No
Accordo con Lettonia / Repubblica Ceca sulla cooperazione transfrontaliera in materia di polizia	Cooperazione bilaterale in materia di polizia	Deliberazione al Consiglio nazionale	No
Accordo con Albania / Macedonia / Romania sulla cooperazione transfrontaliera in materia di polizia, ossia Modifica del trattato con Francia / Italia ossia Cooperazione con il Liechtenstein ossia Trattato con Bosnia ed Erzegovina / Lettonia / Montenegro / Serbia / Slovenia / Repubblica Ceca / Turchia / Ucraina / USA	Cooperazione bilaterale in materia di polizia	Documento interlocutorio sulla strategia per la cooperazione internazionale in materia di polizia sottoposto al Consiglio federale	No

Leggi

Titolo	Contenuto	Stato dell'affare	Punti di contatto rilevanti con la presente revisione
Codice di procedura penale svizzero	Unificazione del diritto procedurale svizzero	Messaggio	Disciplinamento delle indagini preliminari e della comunicazione di informazioni emersi dal procedimento penale
Legge sulla polizia	Istituzione delle basi legali per organi federali con compiti di polizia	Avamprogetto	In un secondo tempo: ev. inserimento della LMSI nella LPol
Legge federale sulle misure per la salvaguardia della sicurezza interna (LMSI I)	Prevenzione della violenza, in particolare in occasione di manifestazioni sportive	Approvato dal Parlamento; entrata in vigore da definirsi	Sì (struttura della legge)
Legge federale sulle armi, gli accessori di armi e le munizioni (Legge sulle armi)	Migliore prevenzione degli abusi, ossia adeguamento a Schengen	In commissione (Consiglio degli Stati)	No
Legge federale sui sistemi d'informazione di polizia della Confederazione	Unificazione delle basi legali formali per i sistemi d'informazione di polizia gestiti dalla Confederazione	Analisi dei risultati della consultazione	No
Legge federale sull'impiego della coercizione nell'ambito del diritto degli stranieri e dei trasporti di persone su mandato delle autorità federali	Condizioni quadro uniformi per l'uso della forza fisica, di mezzi ausiliari e di manette e ceppi e l'uso di armi	Messaggio	No
Legge federale concernente le misure contro il razzismo	Divieto di simboli razzisti, ossia ammissibilità della sorveglianza delle comunicazioni nell'ambito di un procedimento penale secondo l'art. 261bis CP	Analisi dei risultati della consultazione	No

Ordinanze

Titolo	Contenuto	Stato dell'affare	Punti di contatto rilevanti con la presente revisione
Ordinanza sulle misure per la salvaguardia della sicurezza interna	Esecuzione LMSI I	Progetto	No
Ordinanza sul sistema per il trattamento dei dati relativi alla protezione dello Stato	Disciplinamento dello scambio di dati con Europol	Analisi dei risultati della consultazione degli Uffici	No
Ordinanza SIRENE	Disciplinamento dei compiti dell'ufficio SIRENE	Progetto	No
Ordinanza sul sistema d'informazione della Polizia giudiziaria federale	Adeguamento a Europol	Analisi dei risultati della consultazione degli Uffici	No
Ordinanza sulle armi, gli accessori di armi e le munizioni	Adeguamento alla revisione della legge	Progetto	No
Ordinanza SIS	Esecuzione dell'art. 351^{decies} CP e disciplinamento del trattamento dei dati	Progetto	No
Ordinanza sull'esportazione, l'importazione e il transito dei beni utilizzabili a fini civili e militari e dei beni militari speciali	Adeguamento a Schengen	Progetto	No
Ordinanza sul materiale bellico	Adeguamento alla revisione della legge	Progetto	No
Ordinanza concernente l'entrata e la notificazione degli stranieri	Adeguamento a Schengen	Progetto	Modulo analogo agli attuali «bollettini di notifica»
Ordinanza sul trattamento dei dati segnaletici	Adeguamento a Dublino (Eurodac)	Progetto	No
Ordinanza sul sistema informatizzato di gestione e indice informatizzato delle persone e dei fascicoli dell'Ufficio federale di polizia	Adeguamento a Europol	Progetto	No

Allegato 2

5.2 Diritto comparato (Germania, Austria, Francia, Italia, Lussemburgo, Paesi Bassi, Unione Europea)

1. Germania

La Repubblica Federale di Germania è uno Stato federale con un sistema federalista. L'ordinamento costituzionale federalistico conferisce ai *Länder* la sovranità in materia di polizia nei loro rispettivi territori. Al contempo, la costituzione tedesca attribuisce allo Stato centrale competenze prevalenti in settori di polizia fondamentali, quali in particolare la cooperazione tra *Bund* e *Länder* in materia di polizia giudiziaria e l'intera lotta al crimine internazionale. Inoltre, lo Stato centrale garantisce la sicurezza alle frontiere e nel traffico ferroviario e aereo; emana leggi per l'adempimento dei propri compiti e gestisce proprie autorità di polizia. Tale ripartizione delle competenze fa sì che alle 16 polizie dei *Länder* si affianchino le autorità di polizia federali, che sono l'Ufficio federale per la repressione della criminalità (BKA) e la polizia federale, entrambe integrate nel ministero degli interni.
Il compito primario dei servizi di sicurezza di *Bund* e *Länder* consiste nel raccogliere e analizzare informazioni su mene che attentano 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[9].
Bund e *Länder* sono tenuti a collaborare in materia di servizi di sicurezza. Il *Bund* gestisce l'Ufficio federale di tutela della Costituzione (BfV), sottoposto al ministro degli interni. 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 applicabili della legge tedesca sulla protezione dei dati o norme particolari della BVerfSchG. Può inoltre richiedere dati e informazioni alle autorità di repressione[10]. Viceversa, il Servizio federale di informazione (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[11]. Tali dati possono essere utilizzati a scopo di perseguimento penale.
Nel dicembre del 2004, il nuovo centro antiterrorismo ha iniziato la sua attività. Tale centro integra nelle proprie attività il BND, gli uffici per la repressione della criminalità e per la tutela della Costituzione dei *Länder*, la guardia federale di frontiera, il corpo federale di protezione delle frontiere e il servizio di controspionaggio militare (MAD).
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[12]. Il governo federale deve, dietro richiesta, consegnargli atti e dati per visione e deve permettere che i suoi collaboratori vengano interrogati. Su richiesta, il BfV comunica gratuitamente alla persona interessata i dati memorizzati che la ri-

[9] Legge sulla cooperazione del Bund e dei *Länder* in materia di tutela costituzionale e sull'Ufficio federale di tutela della Costituzione (*Bundesverfassungsschutzgesetz*; BVerfSchG)
[10] § 18 BVerfSchG
[11] § 9 della legge del 20 dicembre 1990 sul BND (BNDG)
[12] § 2 della legge sul controllo parlamentare dell'attività d'informazione del *Bund* (*Kontrollgremiumgesetz; PKGrG*)

guardano, purché essa si riferisca a fatti concreti e faccia valere un interesse particolare per l'informazione[13]. I dati memorizzati vanno rettificati se risultano errati. Dopo cinque anni al più tardi, il BfV deve verificare se, nel caso specifico, i dati vanno rettificati o cancellati. Trascorsi 15 anni dall'ultima memorizzazione, le informazioni vanno cancellate, a meno che i vertici delle autorità non decidano altrimenti[14].
Qui di seguito verrà illustrata esclusivamente la normativa federale.
Nell'adempimento dei propri compiti, il BfV è autorizzato a servirsi tra l'altro di dati di telecomunicazione e di servizi a distanza[15]. L'istanza motivata va presentata per scritto dal presidente del BfV o dal suo rappresentante. La decisione in merito compete al ministero federale incaricato dal cancelliere. Tale ministero informa, a scadenza mensile, la commissione G 10 sulle istanze approvate e la loro esecuzione. In caso di pericolo nel ritardo, il ministero può disporre l'esecuzione della decisione prima che venga informata la commissione[16]. 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 (*Grosser Lauschangriff*) e a utilizzare documenti fittizi e targhe false[17]. Tali misure vanno indicate in una norma di servizio, da approvare dal ministero degli interni, che ne mette al corrente il PKGr. Se si raccolgono informazioni presso i diretti interessati, occorre indicare lo scopo del rilevamento.
Il BfV è inoltre autorizzato, a determinate condizioni, a richiedere informazioni alle banche[18]. Nelle indagini relative ai 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 relativi ai collegamenti, quali identificazioni, numeri di chiamata e dati di posizione[19]. Il BfV può infine servirsi di dispositivi d'intercettazione IMSI per individuare i numeri degli apparecchi e delle carte di telefonia mobile[20]. Vigono le stesse condizioni applicabili alle intercettazioni telefoniche.
I servizi di sicurezza tedeschi non hanno, per contro, alcuna competenza in materia di polizia, in particolare non sono autorizzati a effettuare perquisizioni e sequestri.

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 costituzionale e la lotta al terrorismo (BVT) funge da servizio d'informazione civile[21]. 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, a manifestazioni estremiste, allo spionaggio, al traffico d'armi internazionale, al commercio con materiale nucleare e al crimine organizzato in tali settori. Il BVT è integrato nella direzione generale per la sicurezza pubblica del ministero degli interni.

[13] § 15 BVerfSchG
[14] § 12 BVerfSchG
[15] § 8 cpv. 8 BVerfSchG.
[16] § 8 cpv. 9 BVerfSchG
[17] § 8 cpv. 2 BVerfSchG
[18] § 8 cpv. 5 BVerfSchG
[19] § 8 cpv. 6 BVerfSchG e § 8 cpv. 8 BVerfschG
[20] § 9 cpv. 4 BVerfSchG
[21] Legge del 31 ottobre 1992 sull'organizzazione della sicurezza e l'attività della polizia di sicurezza (*Sicherheitspolizeigesetz*; SPG)

Il BVT si compone di una sezione direttiva e di tre divisioni; la prima è responsabile del personale, della formazione, del preventivo e degli affari economici. Inoltre tratta tutti gli affari giuridici fondamentali in materia di difesa dello Stato.
L'unità organizzativa più vasta è la seconda divisione (ricerca d'informazioni, analisi e indagine), composta da cinque sezioni (estremismo, terrorismo e estremismo straniero, controspionaggio, proliferazione e commercio d'armi, analisi strategica e sostegno operativo). Il BVT coordina, sul piano nazionale, l'attività di difesa dello Stato dei nove uffici regionali per la tutela costituzionale e la lotta al terrorismo (LVT).
La terza divisione infine dispone e coordina le misure di protezione delle persone e degli oggetti sul piano nazionale, valuta costantemente le misure di sicurezza elaborate alla luce di eventuali situazioni di minaccia, ed effettua esami della sicurezza.

Per adempiere i propri compiti in materia, ogni regione è dotata di un LVT integrato nella relativa direzione della sicurezza. Al BVT competono la disposizione, il coordinamento e l'attuazione, mediante i LVT, delle misure a tutela delle persone e degli oggetti, come pure la protezione dei rappresentanti di Stati esteri, di organizzazioni internazionali e di altri soggetti di diritto internazionale.
I servizi di sicurezza possono accedere ai dati raccolti dalle autorità di repressione, che trasmettono loro le proprie informazioni. Gli interessati hanno il diritto di essere informati e di ottenere la rettificazione o la cancellazione dei propri dati personali; possono inoltre ricorrere dinanzi alla commissione per la protezione dei dati. Qualora gli interessi di difesa dello Stato lo esigano, il diritto di essere informati viene eccezionalmente a cadere.
Le autorità di sicurezza che indagano più a fondo sulle minacce devono, senza indugio, comunicare al ministro degli interni le misure adottate; questi inviterà l'incaricato per i rimedi giuridici ad esprimersi in merito purché egli abbia chiesto di essere sentito.
Se l'incaricato per i 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 fosse possibile, a ricorrere dinanzi alla commissione per la protezione dei dati.
L'incaricato per i rimedi giuridici stila un rapporto annuale relativo alle indagini approfondite sulle minacce (osservazione di raggruppamenti)[22] all'indirizzo del ministro degli interni; il sottocomitato permanente del consiglio nazionale può chiedere visione di tale rapporto.

A determinate condizioni, i servizi di sicurezza sono autorizzati a richiedere informazioni ai fornitori di prestazioni 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[23]. La registrazione di suoni in assenza dell'agente infiltrato non è ammessa. All'incaricato per i rimedi giuridici compete la vigilanza concomitante sull'inchiesta mascherata e l'impiego sotto copertura di apparecchi di registrazione di immagini e di suoni. Egli va messo al corrente di tali inchieste e dei motivi essenziali che vi hanno dato adito, nella misura in cui l'identità degli interessati sia nota. I servizi di sicurezza possono inoltre mettere al sicuro, sequestrare e confiscare oggetti[24], osservare locali privati[25] e accedervi[26], come pure ordinare ed effettuare in-

[22] § 21 cpv. 3 SPG
[23] § 54 SPG
[24] § 42 SPG
[25] § 54 cpv. 2 SPG
[26] § 39 SPG

terrogatori[27]. In determinati casi, gli intermediari finanziari devono passare informazioni alle autorità competenti[28].

L'attività del BTV è soggetta al controllo parlamentare secondo l'articolo 52*a* della costituzione austriaca. Percorsa la via gerarchica amministrativa, è possibile ricorrere dinanzi al tribunale amministrativo o alla corte costituzionale.

L'11 settembre ha lasciato il segno anche in Austria: le strutture sono state snellite e le disposizioni di legge inasprite, mentre i servizi di sicurezza godono ora di competenze più ampie.
La novella 2002 della SPG estende 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 la copertura dei provvedimenti di sostegno in occasione di osservazioni o inchieste mascherate. Sullo sfondo di un dilagante estremismo, il 1° ottobre 2000 sono state inserite nella SPG le disposizioni in materia di indagini approfondite sulle minacce e i rimedi giuridici pertinenti[29]. Tali disposizioni permettono alle autorità di sicurezza di osservare gruppi di persone, qualora si possa presumere che commetteranno reati minaccianti la sicurezza pubblica. Prima della modifica di legge, le autorità di sicurezza potevano osservare i gruppi estremisti soltanto se questi avevano già perpetrato un reato.

Il BVT[30], direttamente sottoposto al direttore generale per la sicurezza pubblica, è stato istituito il 1° dicembre 2002 nella sezione II del ministero degli interni.
Il BVT svolge la sua attività nell'ambito della SPG e, nella misura in cui agisce al servizio della giustizia penale, si attiene alle disposizioni del codice di procedura penale (StPO).

3. Francia

La Francia è una democrazia ad assetto centrale. Al contrario dei Cantoni svizzeri, le 26 regioni non godono di una vera e propria autonomia.
La sicurezza interna è di diretta competenza del primo ministro, appoggiato dal segretariato generale per la difesa nazionale (SGDN)[31] e da un gabinetto militare. Della sicurezza interna si occupano vari servizi dello Stato, 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; la prima opera nelle città, la seconda in campagna. Alla gendarmeria mobile competono il mantenimento dell'ordine pubblico e la lotta al terrorismo, al crimine organizzato e alle sette. La polizia nazionale, sottoposta al ministero degli interni e diretta dalla direzione generale della polizia nazionale (DGPN)[32], comprende varie subdirezioni, tra cui la direzione della sorveglianza del territorio (D.S.T.)[33], le informazioni generali (RG)[34] e l'unità di coordinamento per la lotta al terrorismo[35].

[27] § 28*a* SPG
[28] § 38 della legge bancaria (BWG)
[29] §§ 21 cpv. 3, 53 cpv. 1 n. *2a*, 54 cpv. 2 e 62*a* SPG
[30] § 7 cpv. 1 e 9 della legge sui ministeri federali (BMG)
[31] *Secrétariat Générale de la Défense Nationale*
[32] *Direction Générale de la Police Nationale*
[33] *Direction de la surveillance du territoire*
[34] *Renseignements généraux*

La D.S.T. funge da servizio d'informazione incaricato di combattere i crimini contro la sicurezza dello Stato[36]. La sua organizzazione e la funzione sono disciplinati in un decreto segreto dell'8 marzo 1993. La D.S.T. è l'ufficio centrale che raccoglie, tratta e ritrasmette tutte le informazioni che le sono trasmesse dalle RG e contribuisce alla protezione di settori sensibili e di segreti della difesa nazionale. Le RG gestiscono un sistema d'informazione cui ha accesso anche la D.S.T.[37].
L'unità di coordinamento per la lotta al terrorismo coordina i lavori di tutti i servizi mobilizzati in Francia e all'estero.
La 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)[38], per contro, funge da servizio segreto operante all'estero e responsabile della sicurezza esterna della Francia. La DGSE è sottoposta al primo ministro e i suoi compiti comprendono la ricerca di informazioni e gli interventi.
Il diritto di consultare i sistemi d'informazione delle RG è di norma conferito in una procedura cosiddetta «indiretta»[39]. La relativa richiesta va presentata alla «*Commission nationale de l'information et des libértés*» (CNIL). Questa commissione indipendente verifica le informazioni e informa il richiedente di eventuali rettificazioni. Se la sicurezza interna non è minacciata, i dati possono essere comunicati al richiedente. Se la banca dati comprende informazioni la cui comunicazione al diretto interessato non metta a repentaglio lo scopo stesso della banca dati, il responsabile 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 gruppi illegali[40]. 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 degli interni, del ministro delle dogane o dei loro supplenti. Il primo ministro stabilisce dei contingenti per limitare il numero delle misure disposte eseguibili allo stesso tempo; il relativo controllo è affidato alla «*Commission nationale de contrôle des interceptions de sécurité*», esterna all'amministrazione[41] e composta da 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 tratte dalla sorveglianza devono essere distrutte sotto la supervisione del primo ministro, al più tardi dieci giorni dopo l'avvenuta esecuzione.
Stando alla commissione, tutti i dati inerenti alle intercettazioni preventive vanno classificati come «*Secret-Défense*». Ciò significa, tra l'altro, che le persone sorvegliate a titolo preventivo non vanno informate perché tale informazione potrebbe compromettere la «*défense nationale*». I servizi di sicurezza francesi non possono tuttavia sorvegliare la corrispondenza postale.

[35] *Unité de coordination de la lutte antiterroriste*
[36] Decreto n° 82-1100 del 22 dicembre 1982, aggiornato il 15 settembre2004
[37] Decreti n° 91-1052 e n° 91-1051
[38] *Direction Générale de la Sécurité Extérieure*
[39] *Loi pour la sécurité intérieure* (Legge n° 2003-239 del 18 marzo 2003; Legge del 18 marzo 2003)
[40] Art. 3 della legge n° 91-646 del 10 luglio 1991 (*Loi relative au secret des correspondances émises par la voie des télécommunications*; Legge del 10 luglio 1991)
[41] Art. 5 della legge del 10 luglio 1991

In casi eccezionali è possibile, dietro ordine motivato, confiscare e bloccare oggetti di valore se la sicurezza interna lo richiede[42]. Sono inoltre previsti interrogatori e perquisizioni di vetture e abitazioni senza esame giudiziale[43]. 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 metterebbero in pericolo la sicurezza della Francia[44]. Nell'ambito del crimine organizzato è previsto l'impiego di informatori con notifica *ex post* al pubblico ministero. Tali informatori vengono rimborsati attingendo a fondi speciali[45].
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.
Dopo gli attacchi dell'11 settembre 2001, la lotta al terrorismo è prioritaria anche in Francia. Sebbene i Francesi abbiano maturato decenni di esperienza in tale ambito, è stata emanata tutta una serie di leggi e decreti nuovi.

4. Italia

Contrariamente alla Svizzera, alla Germania e all'Austria, che sono Stati federali, l'Italia è uno Stato unitario decentralizzato. Le regioni godono di ampie competenze in vari settori, tra cui l'agricoltura, la sanità e l'istruzione pubblica e il sistema di vigilanza in materia di polizia locale.
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 sottoposta la direzione centrale per la polizia di prevenzione (DCPP)[46].
La DCPP si prefigge di combattere le organizzazioni terroriste 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 debellare il terrorismo, l'immigrazione illegale, i reati informatici, lo spionaggio economico, le nuove minacce e il crimine organizzato.
Il SISDE raccoglie dati a tutela della sicurezza interna. Esiste un diritto di consultazione generale[47], ma tutti i documenti e gli atti la cui pubblicazione potrebbe compromettere la sicurezza nazionale sono soggette al segreto di Stato[48]. Il garante per la protezione dei dati personali vigila sui dati raccolti. Nell'ambito della sicurezza informatica, i servizi di sicurezza collaborano con la polizia giudiziaria.

[42] Art. 3 della legge del 18 marzo 2003 e legge n° 2005-750 del 4 luglio 2005 (Legge n° 2005-750)
[43] Legge n° 2004-204 del 9 marzo 2004 (Legge del 9 marzo 2004)
[44] Legge del 10 gennaio 1936
[45] Legge del 9 marzo 2004
[46] Legge n. 121 del 1981. Nuovo ordinamento dell'Amministrazione della pubblica sicurezza (Legge 121)
[47] Decreto legislativo del 30 giugno 2003, n. 196 (Decreto 196)
[48] Art. 12 della legge del 24 ottobre 1997

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.
La D.I.A. adotta misure contro il crimine organizzato, quali la sorveglianza e le intercettazioni telefoniche, e svolge indagini antimafia[49]. Può cercare informazioni relative alla situazione finanziaria delle persone sospettate di appartenere a un'organizzazione criminale. La D.I.A. trasmette le informazioni raccolte al SISDE e al SISMI e collabora con le forze di polizia.
I dati possono essere trattati soltanto con il consenso degli interessati, a meno che il trattamento non rientri nell'adempimento di un compito legale[50].
Con la legge del 17 luglio 2005[51] è stata introdotta una serie di nuove competenze e misure per i servizi di sicurezza. Ora è ad esempio ammesso 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; il giudice deve decidere in merito entro 48 ore. Se tale scadenza non viene rispettata, le informazioni raccolte non possono essere utilizzate in giudizio.
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 servizi di sicurezza 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 individui sospetti che minacciano la sicurezza pubblica o appoggiano in qualche maniera un'organizzazione terrorista. L'espulsione è eseguita senza indugio, ma può essere impugnata dinanzi al tribunale amministrativo. Se la decisione di espulsione poggia su fonti dei servizi di sicurezza, 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 d'abuso.
La legge del 27 luglio 2005 autorizza infine il ministero degli interni a istituire unità investigative interforze per combattere il terrorismo.

5. Lussemburgo

Il Lussemburgo è una monarchia costituzionale; ha forma di democrazia parlamentare ed è suddivisa in tre distretti comprendenti dodici cantoni e 118 comuni. Il potere esecutivo è esercitato dal granduca e dal governo, composto dal primo ministro e da dodici ministri, un ministro delegato e una segretaria di Stato.
La difesa preventiva dello Stato è affidata a tre organizzazioni: il servizio d'informazione per la sicurezza interna (SRDE)[52], il servizio d'informazione per la sicurezza esterna (HCSE)[53] e il servizio d'informazione militare[54].

[49] Legge n. 410 del 1991 (legge 410)
[50] Art. 12 cpv. 1 della legge n. 675 del 31 dicembre 1996. Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali (Legge 675)
[51] Testo del decreto-legge 27 luglio, n. 144, coordinato con la legge di conversione 31 luglio 2005 (Legge del 27 luglio 2005)
[52] *Service de Renseignement de l'Etat*

Il SRDE, sottoposto al ministero degli interni, è incaricato di combattere il terrorismo, lo spionaggio, la proliferazione di armi non convenzionali e le tecnologie che vi sono connesse e il crimine organizzato in questo ambito. 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[55]. 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 rientranti nel campo d'applicazione dell'articolo 2 della legge sull'organizzazione.
Il trattamento dei dati personali da parte del SRDE è retto dalle disposizioni della legge del 2 agosto 2002[56]. 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 sul traffico delle telecomunicazioni[57]. 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 degli interni. Questi hanno accesso ai dati trattati dal SRDE, dispongono le rettifiche necessarie e informano le persone interessate del trattamento, conforme alla legge, di dati che le riguardano.

Negli affari riguardanti la criminalità organizzata o la sicurezza esterna[58], il capo del governo può, dietro richiesta del SRDE e previa approvazione di una commissione *ad hoc*, ordinare la sorveglianza telefonica preventiva[59]. 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 giudizio se la persona in questione è vincolata dal segreto professionale ai sensi dell'articolo 458 del *Code pénale* e non è sospettata di aver commesso un reato o di progettarne uno. In tal caso, il capo del SRDE deve distruggere senza indugio i relativi documenti. Le decisioni della commissione vanno trasmesse al rispettivo direttore dei servizi di telecomunicazione, che quindi incarica un apposito servizio di effettuare e controllare le intercettazioni. Una volta terminata la misura, gli interessati ricevono copia delle informazioni raccolte, purché non siano state classificate come segrete. Se le misure non hanno dato alcun esito nel periodo in questione, tutti i documenti vanno distrutti senza indugio; altrimenti la distruzione avverrà alla fine del procedimento.

Le attività del SRDE sono controllate dalla commissione, composta da presidenti dei gruppi politici rappresentati nella «*Chambre des Députés*». Il direttore del servizio d'informazione rende conto delle attività generali del suo servizio. La commissione può chiedere di consultare le pratiche e di interrogare gli agenti addetti ai vari incarti. Approva un rapporto finale confidenziale, che contiene osservazioni, conclusioni e raccomandazioni ed 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 misure di intercettazione telefonica effettuate.

[53] *Haut Commissariat de la Sécurité Extérieure*
[54] *2ième Bureau de l'Armée*
[55] *Loi du 15 juin portant sur l'organisation du Service de Renseignement de l'Etat* (Legge sull'organizzazione)
[56] *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* (Legge del 2 agosto 2002)
[57] Art. 4 della legge sull'organizzazione
[58] *Sécurité exterieure de l'Etat*
[59] Art. 88-3 del *Code Pénal* e secondo la *loi du 26 novembre1982*

Non sono previsti né confische e perquisizioni né interrogatori. 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[60]. Soltanto parte delle informazioni così raccolte possono essere trasmesse agli uffici competenti, segnatamente il cognome, il nome e, semmai, l'indirizzo IP[61]. È escluso vietare determinate attività.

6. Paesi Bassi

I Paesi Bassi sono una monarchia costituzionale; la regina è membro del governo e nomina i ministri; il parlamento consta di due camere; la seconda camera è il parlamento *stricto sensu*, che rappresenta il popolo e controlla il governo.
La difesa dello Stato olandese è affidata agli istituti seguenti: il servizio d'informazione civile (AIVD)[62], il servizio d'informazione militare, comprendente i servizi segreti veri e propri (MIVD)[63], il servizio militare speciale (BD)[64] e il controspionaggio[65]. Dopo gli attacchi dell'11 settembre, la cooperazione tra l'AIVD e la polizia è stata 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[66]. Cooperano con le autorità di polizia e di perseguimento penale trasmettendo le informazioni sotto forma di rapporto al pubblico ministero. L'AIVD può chiedere ai servizi d'informazione regionali (RID) e al servizio di sicurezza speciale della polizia militare reale di procedere dietro suo incarico.
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 qualora la pubblicazione dei dati metterebbe a repentaglio la sicurezza interna. La non entrata nel merito va comunicata alla competente commissione di vigilanza[67], che sorveglia l'attività dei servizi e informa i ministri competenti.
L'AIVD e il MIVD possono sorvegliare a titolo preventivo la corrispondenza postale e il traffico delle telecomunicazioni. La richiesta va presentata *ex ante* dal capo dell'AIVD e del MIVD, previa approvazione del ministro della difesa e del ministro degli interni. 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 degli interni o il capo dei servizi vi acconsentono, i servizi possono osservare e perquisire luoghi privati. Sono altresì previsti interventi sotto copertura; è inoltre consentito aprire lettere di terzi se il tribu-

[60] Art. 88-3 del *Code de procédure criminelle*
[61] *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*
[62] *Algemene Inlichtingen- en Veiligheidsdienst* (Servizio d'informazione e di sicurezza generale)
[63] *Inlichtingen- en Veiligheidsdienst* (Servizio d'informazione e di sicurezza militare)
[64] *Koninklijke Marechaussee, Bijzondere Dienst en Veiligheid* (Polizia militare, sezione speciale per l'informazione e la sicurezza)
[65] *Bijzondere Bijstands Eenheid* (Unità di sostegno speciale per la lotta al terrorismo).
[66] *Act of 7 February 2002, providing for rules relating to the intelligence and security services and amendment of several acts* (*Intelligence and Security Services Act 2002*)
[67] *Supervisory committee*

nale distrettuale dell'Aja approva una richiesta in tal senso del capo dei servizi. È pure permesso accedere a sistemi informatici di terzi, previa autorizzazione del ministro degli interni 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 singoli o da organizzazioni.
Il difensore 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[68]. 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. Unione Europea

Dopo l'11 settembre 2001, l'Unione Europea sta attuando una politica antiterrorismo mirata. In occasione di un incontro *ad hoc* dei ministri europei degli interni e di giustizia svoltasi a Bruxelles in seguito agli attacchi terroristici di Londra, l'Unione Europea si è detta favorevole a una più stretta cooperazione dei Venticinque nella lotta al terrorismo e ha invocato una maggiore collaborazione transfrontaliera in materia di polizia e di servizi di sicurezza.
Il 21 settembre 2005, la commissione ha presentato un pacchetto di iniziative:

- la proposta di direttiva sulla conservazione dei dati relativi al traffico delle comunicazioni prevede l'armonizzazione degli obblighi dei fornitori di comunicazioni elettroniche disponibili al pubblico, o di una rete pubblica di telecomunicazioni, di conservare i dati relativi alla telefonia mobile e fissa e alle comunicazioni via Internet, per un periodo, rispettivamente, di un anno e di sei mesi;
- la decisione finanziaria relativa ad iniziative nel settore della prevenzione, preparazione e risposta agli attentati terroristici stanzia 7 milioni di euro. È finalizzata a mettere in connessione le autorità di contrasto al fine di agevolare lo scambio di informazioni e la gestione delle crisi e sosterrà il prossimo programma europeo per la protezione delle infrastrutture critiche;
- con la proposta di decisione del Consiglio che autorizza la firma della convenzione del Consiglio d'Europa n. 198 – sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato 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 dello stesso valore qualitativo di quelle attualmente applicabili nell'UE e a costituire un fronte unico nella lotta contro il finanziamento del terrorismo;
- la comunicazione intitolata «*Il reclutamento dei terroristi: studio dei fattori che contribuiscono alla radicalizzazione violenta*» costituisce il contributo della Commissione, come richiesto dal programma dell'Aia, 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 settori come Internet, la cooperazione tra le autorità di contrasto e i servizi segreti degli Stati membri e le relazioni esterne.

[68] *Act of 3 February 2005*