Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Servizio delle attività informative della Confederazione SIC

Settembre 2013

Legge sul servizio informazioni (LSI)

Rapporto sui risultati della procedura di consultazione

Indice

1. Contenuto dell'avamprogetto

Il presente avamprogetto intende creare una base legale formale unitaria che disciplini l'attività, i mandati e il controllo del Servizio delle attività informative della Confederazione (SIC).

Nel 2009 il Consiglio federale ha incaricato il DDPS di elaborare entro la fine del 2013 un messaggio per una nuova legge sul servizio informazioni (decisione del Consiglio federale del 27 novembre 2009). Il mandato impartito dal Consiglio federale prevede quanto segue:

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

Il presente avamprogetto è stato sottoposto a consultazione degli uffici la prima volta nell'aprile 2012 e, siccome se ne presentava la necessità, una seconda volta nell'ottobre.

I tratti essenziali del progetto sono i seguenti:

<u>Codificazione</u>
Le disposizioni relative al servizio informazioni concernente la Svizzera e l'estero, sinora contenute in due leggi separate, vengono riunite in un unico atto legislativo.

Nuova impostazione dell'acquisizione di informazioni
Per quanto riguarda l'acquisizione di informazioni, a differenza di prima l'avamprogetto non distingue più in primo luogo tra minacce provenienti dalla Svizzera e dall'estero, bensì tra, da un lato, l'estremismo violento con riferimento alla Svizzera e, dall'altro, i rimanenti ambiti di minacce e compiti. Il nuovo concetto prevede che nel caso dell'estremismo violento le misure di acquisizione soggette ad autorizzazione, che comportano ingerenze particolarmente gravi nei diritti fondamentali, non possono essere applicate e che i dati sull'estremismo violento devono essere gestiti in base a criteri particolarmente severi. Questi dati hanno spesso legami più forti con la Svizzera rispetto ai dati di altri settori di attività del SIC. Altrettanto spesso sono anche più delicati, poiché toccano più da vicino attività prettamente politiche, che in Svizzera in virtù dell'articolo 3 capoverso 5 non possono essere oggetto di attività informative.

Introduzione di nuove misure di acquisizione
Le disposizioni riguardanti i mezzi speciali per la ricerca di informazioni previste nell'originario progetto LMSI II e rinviate dal Parlamento ai fini di una rielaborazione, sono state rimaneggiate e adeguate alle nuove condizioni e vengono ora riproposte come misure di acquisizione in Svizzera soggette ad autorizzazione.
Per l'impiego di queste misure è necessaria un'autorizzazione giudiziaria preliminare del presidente della corte competente del Tribunale amministrativo federale, seguita da una verifica basata su considerazioni politiche da parte del capo del DDPS e quindi dal nullaosta di quest'ultimo.
Le nuove misure di acquisizione di informazioni vengono proposte in quanto gli attuali strumenti (art. 14 LMSI) non bastano più per consentire al servizio informazioni di svolgere i suoi compiti preventivi nell'ambito della sicurezza interna. Attori sempre più aggressivi e forme di minaccia sempre più complesse gravano sulla sicurezza interna ed esterna della Svizzera e impongono l'introduzione di misure di acquisizione nuove e più efficaci. Questo riscontro coincide con le constatazioni già effettuate dal Consiglio federale in rapporto con l'originario progetto LMSI II.

Ampliamento delle misure di acquisizione non soggette ad autorizzazione
Anche le misure di acquisizione non soggette ad autorizzazione vengono moderatamente ampliate: la possibilità di segnalare persone e veicoli a titolo preventivo ai fini della loro localizzazione, già oggi tacitamente ammessa, è ora espressamente contemplata nell'avamprogetto.

Elaborazione differenziata dei dati
L'avamprogetto prevede che le informazioni acquisite dal SIC o da esso ricevute siano archiviate, in funzione della tematica, della fonte e del grado di sensibilità dei dati, in una rete di sistemi d'informazione specializzati. Questa soluzione consente di prevedere prescrizioni ottimali per l'elaborazione e la protezione dei diversi tipi di dati (intervalli di verifica e periodi di conservazione, autorizzazioni d'accesso differenziate per il personale del SIC ecc.). Prima di trasmettere dati, il SIC è inoltre espressamente tenuto in ogni singolo caso ad accertarsi che la loro elaborazione sia stata effettuata in modo corretto e la loro trasmissione sia permessa.

2. Svolgimento della procedura di consultazione

La procedura di consultazione relativa all'avamprogetto di legge sul servizio informazioni è stata avviata dal Consiglio federale l'8 marzo 2013 e si è conclusa il 30 giugno 2013. Sono stati interpellati 72 destinatari, tra cui i Cantoni, i partiti politici, le associazioni mantello nazionali di Comuni, città e regioni di montagna, le associazioni mantello nazionali dell'economia e altri ambienti interessati nel singolo caso.

3. Partecipanti alla consultazione

Si sono pronunciati 68 partecipanti, mentre 8 interpellati hanno espressamente rinunciato a esprimere un parere.

Cantoni
Hanno espresso un parere tutti i Cantoni, la Conferenza dei comandanti delle polizie cantonali della Svizzera CCPCS, la Conferenza legislativa intercantonale CLI (AG, AI, BL, BS, BE, JU, LU, SG, SO, TI, VD, ZH), l'Organo di controllo per la protezione dello Stato del Cantone di BS e l'Organo di vigilanza in materia di protezione dei dati del Cantone di Turgovia OVPD TG. (30)

Partiti politici rappresentati nell'Assemblea federale
Hanno espresso un parere il Partito borghese democratico PBD, il Partito popolare democratico PPD, il Partito liberale radicale PLR, i Verdi, il Partito verde liberale PVL, il Partito Pirata, il Partito socialista svizzero PS e l'Unione democratica di centro UDC. (8)

Associazioni mantello nazionali dell'economia
Hanno espresso un parere economiesuisse, l'Unione svizzera delle arti e mestieri USAM e SwissBanking. (3)

Altri ambienti interessati nel singolo caso
Hanno espresso un parere il Tribunale federale svizzero TF, il Tribunale amministrativo federale TAF, Amnesty International AInt, i Giuristi democratici svizzeri GDS, il Gruppo per una Svizzera senza esercito GSsE, la Conferenza delle autorità inquirenti svizzere CAIS, la Conferenza delle direttrici e dei direttori di sicurezza delle città svizzere KSSD, la Società Svizzera degli Ufficiali SSU, l'Associazione svizzera degli ufficiali informatori ASUI e la Federazione Svizzera Funzionari di Polizia FSFP. (10)

Partecipanti non previsti nell'elenco degli interpellati
Hanno espresso un parere l'Associazione svizzera delle telecomunicazioni asut, l'Azione per una Svizzera neutrale e indipendente ASNI, il Chaos Computer Club di Zurigo CCCZH, il Centre Patronal, la Chambre vaudoise des arts et métiers CVAM, la Digitale Gesellschaft DigGes**,** la Delegazione delle finanze delle Camere federali DelFin, dirittifondamentali.ch, l'associazione degli incaricati svizzeri per la protezione dei dati Privatim, Referendum LMSI RefLMSI, la Federazione svizzera delle comunità israelitiche SIG, die Swiss Privacy Foundation SPF, l'Associazione economica svizzera della tecnica d'informazione Swico, Swisscom, l'Università di Ginevra e due persone private (PP1/PP2). (17)

Rinuncia a esprimere un parere
Hanno espressamente rinunciato a esprimere un parere il Tribunale penale federale, l'Unione svizzera degli imprenditori, l'Associazione dei Comuni Svizzeri, l'Unione sindacale svizzera, la Croce Rossa Svizzera, l'Unione delle città svizzere, la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia e la Società svizzera degli impiegati di commercio. (8)

4. Valutazione generale del progetto legislativo

CCPCS, AR, BE, BL, BS, GE, GL, GR, JU, LU, NE, NW, SO, SZ, TI, UR, VD, ZH, OVPD TG e *CAIS* approvano la creazione di una base legale formale unitaria per le attività informative a favore della sicurezza interna della Svizzera, poiché essa migliora la certezza del diritto per i cittadini in un ambito politicamente delicato e nel complesso rappresenta per le attività informative un fondamento idoneo tanto sul piano materiale quanto su quello formale.

CCPCS, AR, BE, GR, NW, SO e *UR* reputano sensata la distinzione fondamentale operata dalla legge tra estremismo violento in rapporto con la Svizzera e gli altri ambiti di minacce e compiti.

CCPCS, AR, GR e *SZ* ritengono che le misure proposte siano urgentemente necessarie per proteggere la popolazione dagli atti di violenza e tengano inoltre sufficientemente conto dei mutati rischi e delle moderne forme di minaccia.

AI sostiene il progetto legislativo ma presuppone chiaramente che nell'applicazione delle misure di acquisizione delle informazioni debba essere sempre rispettato scrupolosamente il principio dello Stato di diritto. Si aspetta anche che si tenga conto delle risorse e dei mezzi tecnici limitati di cui dispone.

BS è del parere che la base legale proposta nell'avamprogetto tenga fondamentalmente conto del principio costituzionale della legalità. Tanto maggiore è la gravità di un'ingerenza nei diritti costituzionali delle persone interessate, tanto più severe saranno le esigenze cui soggiace la corrispondente base legale. L'avamprogetto è caratterizzato da un'elevata densità normativa e quindi soddisfa sostanzialmente i presupposti di diritto costituzionale.

FR approva fondamentalmente le proposte presentate nell'avamprogetto.

GE giudica positivamente la stretta collaborazione tra Confederazione e Cantoni, il sostegno previsto sotto forma di mezzi tecnici e corsi di formazione, la possibilità di assegnare identità fittizie e l'introduzione della sorveglianza delle comunicazioni. Considera invece insoddisfacenti soprattutto il limite di un anno previsto per la conservazione dei dati, la necessità del consenso della Confederazione per i contatti con partner esteri, la procedura di approvazione prevista per le misure di acquisizione e il disciplinamento dei diritti di accesso ai dati della Confederazione.

GR ritiene che il meccanismo di controllo istituito per le nuove misure di acquisizione soggette ad autorizzazione sia senz'altro atto a garantire la legalità e la proporzionalità delle attività del SIC. Ritiene anche che dal punto di vista della protezione dei dati il progetto soddisfi le esigenze di densità normativa da rispettare per procedure di elaborazione dei dati che implicano un tale potenziale di rischio. In particolare la conservazione e il rilevamento differenziati dei dati contribuiscono a proteggere le persone interessate dalle ingerenze nei diritti fondamentali loro garantiti dalla Costituzione e dal diritto internazionale.

LU constata che i punti criticati nei precedenti progetti di revisione sono stati migliorati e che le disposizioni previste dal nuovo avamprogetto sono ora di maggiore qualità dal punto di vista dello Stato di diritto.
LU approva in particolare gli strumenti di controllo della qualità, la direzione e il controllo politici esercitati sul SIC, le disposizioni differenziate in materia di protezione dei dati e la procedura di autorizzazione a più stadi.

NE si chiede se con le misure e i controlli previsti il SIC sarà ancora in grado di adempiere i propri compiti.

SH approva il progetto e ritiene che si fondi su un'adeguata ponderazione dei beni giuridici nella dicotomia esistente tra salvaguardia della sicurezza interna ed esterna della Svizzera e tutela della libertà personale.

TI intravvede nel progetto cinque sostanziali novità:
- una base legale unitaria per il SIC;
- la reimpostazione dell'acquisizione di informazioni, senza la distinzione tra minacce alla sicurezza interna e minacce alla sicurezza esterna;

- l'introduzione di nuove misure di acquisizione negli ambiti del terrorismo, dello spionaggio, della proliferazione e degli attacchi a infrastrutture critiche o per la tutela di altri interessi nazionali essenziali;
- un sistema differenziato per la conservazione dei dati;
- un sistema di vigilanza a più livelli.

Per *ZH* occorre tener presente che la legge tocca un ambito politicamente e giuridicamente delicato e il difficile equilibrio tra sicurezza e libertà, ossia tra sicurezza e tutela dei diritti fondamentali del cittadino. Chiede dunque di fare in modo che i meccanismi di approvazione e controllo previsti nell'avamprogetto non vengano erosi nel corso dei lavori di legiferazione.

L'OVPD TG deplora che con l'avamprogetto proposto gli organi preposti alla politica di sicurezza si siano dotati di mezzi talmente estesi per la ricerca di informazioni al punto da mettere in pericolo il conseguimento dello scopo sinora perseguito dal servizio informazioni interno (tutelare i fondamenti democratici e istituzionali della Svizzera e soprattutto le libertà riconosciute alla sua popolazione). Auspica pertanto che si rinunci a dette ingerenze eccessive nei diritti della personalità del cittadino.

Il PBD esprime sostanzialmente un giudizio favorevole sulla LSI. Considera positivamente l'indispensabile aggiornamento dell'acquisizione di informazioni, ma manifesta in particolare le seguenti preoccupazioni:
la diatriba tra l'aumentato bisogno di sicurezza della popolazione e il bisogno di protezione della sfera privata (a dispetto del fatto che oggi gli individui rendano più che mai spontaneamente pubblica in Internet una parte sempre maggiore della loro vita) lascia evidentemente il segno anche sul progetto in discussione. Definizioni, compiti e restrizioni sono stati disciplinati con acribia a livello di legge. In un'era frenetica come la nostra, caratterizzata da una fulminea evoluzione della tecnica e da minacce in continuo mutamento, il SIC si frena con le proprie mani imponendosi regolamentazioni troppo strette e procedure complicate.

Per il PPD è chiaro che, considerata l'evoluzione della situazione di minaccia, lo Stato necessiti di strumenti incisivi per proteggere se stesso e la propria popolazione, ciò che rientra tra i suoi compiti fondamentali. Il PPD considera cruciale che nell'insieme della legge venga rispettato il principio secondo cui le competenze del servizio informazioni non devono oltrepassare quelle delle autorità inquirenti, e che la sfera privata del cittadino sia senz'altro toccata tanto quanto necessario ma comunque il meno possibile.

Il *PLR* si dice soddisfatto della direzione imboccata con l'avamprogetto e approva la creazione di una base legale unitaria per il SIC, la reimpostazione dell'acquisizione di informazioni, nuove misure di acquisizione comprese, il rafforzamento delle disposizioni applicabili alla conservazione ed elaborazione dei dati, il triplice controllo delle attività del servizio e l'introduzione di nuovi strumenti di sorveglianza resi necessari dall'evoluzione tecnologica.
Per il *PLR*, la tutela della sfera privata rimane comunque fondamentale. Chiede di non dimenticare che i mezzi del SIC, in particolare le nuove misure di acquisizione proposte, possono comportare una profonda ingerenza della sfera privata. Pertanto dovrebbero essere rigidamente disciplinati vegliando costantemente al rispetto del principio di proporzionalità. Il duplice controllo è il minimo indispensabile per garantire lo Stato di diritto. Il rischio di abusi parrebbe essere stato gestito in modo corretto. Occorre preoccuparsi anche di una collaborazione ottimale e di un equilibrio tra Confederazione e Cantoni per quanto riguarda l'esecuzione e il controllo delle misure di sorveglianza.

I *Verdi* respingono l'avamprogetto nella misura in cui comporta ulteriori ingerenze nella libertà personale.
A priori non vi è nulla da eccepire alla creazione di una nuova legge sul servizio informazioni. I *Verdi* hanno però assunto sin dall'inizio un atteggiamento critico riguardo alla LMSI a motivo di talune competenze in materia di protezione dello Stato. È ovvio che queste critiche val-

gono a maggior ragione nei riguardi della LSIC, dato che questa prevede un'ulteriore estensione di tali competenze.
Non si contesta che lo Stato debba provvedere in sostanza anche preventivamente alla sicurezza della popolazione svizzera. Tuttavia, questo compito pubblico prescritto dalla Costituzione non deve incidere in modo inammissibile sui diritti fondamentali del singolo cittadino. I mezzi da impiegare dovrebbero dunque essere sempre proporzionali.
Per le minacce concrete menzionate nell'avamprogetto, il Codice penale svizzero prevedrebbe già fattispecie che in caso di sospetto impongono alle autorità inquirenti di intervenire d'ufficio con possibilità di richiedere provvedimenti coercitivi previsti dalla procedura penale o di far approvare siffatti provvedimenti dal competente giudice dei provvedimenti coercitivi.
Per il resto i *Verdi* rimandano al parere espresso da dirittifondamentali.ch.

Il *PVL* accoglie di principio positivamente il progetto legislativo, anche se ritiene che presenti alcuni eccessi in certi ambiti. Ammette che in materia di attività informative, per lottare contro il terrorismo, la proliferazione e gli attacchi alle infrastrutture critiche, sono necessarie in casi particolari nuove misure di acquisizione delle informazioni che toccano anche la sfera privata. In tale contesto è però anche espressamente favorevole, per questo tipo di misure, a considerare necessaria una procedura di autorizzazione a più stadi con il coinvolgimento del Tribunale amministrativo federale.

Il *Partito Pirata* è risolutamente contrario all'avamprogetto, di cui si dichiara deluso, poiché non sarebbero stati tratti insegnamenti dalla bocciatura della LMSI II. Il progetto sopprimerebbe i diritti fondamentali in assenza di fondati sospetti e senza approfondito esame.

Il *PS* approva la creazione di una base legale al passo con i tempi per il servizio informazioni civile.
Anzitutto, l'estensione delle competenze del servizio informazioni è giustificata da ragioni di politica di sicurezza. Secondariamente, l'avamprogetto rafforza i diritti di consultazione degli interessati e sviluppa l'alta vigilanza istituzionale e politica sul servizio introducendo un sistema di autorizzazione e vigilanza a tre livelli. L'avamprogetto prevede il rafforzamento dei controlli interni indipendenti, l'estensione degli obblighi di autorizzazione da parte delle autorità giudiziarie e provvede affinché le autorità politiche possano esercitare le proprie responsabilità.
Per il *PS* l'estensione dei diritti di consultazione e del sistema di autorizzazione e vigilanza riveste un'importanza primaria. Al servizio infromazioni possono essere attribuite ulteriori competenze soltanto a patto che agisca effettivamente entro un quadro istituzionale e politico inattaccabile e che sia garantita l'imprescindibile tutela dei diritti costituzionali.
Il *PS* chiede pertanto che l'alta vigilanza politica e istituzionale sul servizio informazioni sia ulteriormente rafforzata ed estesa in diversi punti.

L'*UDC* accoglie essenzialmente con favore il progetto legislativo. La Svizzera ha bisogno di un servizio informazioni efficiente come elemento del proprio apparato di sicurezza. La ponderazione dei beni in gioco operata nell'avamprogetto – tra protezione dei cittadini e un inutile sorveglianza di persone incensurate – appare ampiamente adeguata.
L'*UDC* approva che con la LSI si istituisca una base legale formale unitaria, e che le misure di acquisizione esistenti vengano completate.

AInt esprime preoccupazione per il fatto che nell'avamprogetto non vengano integralmente considerate le raccomandazioni formulate nella perizia presentata dal professor Biaggini nel 2009 riguardo alla costituzionalità del progetto LMSI II.

L'*ASNI* respinge il progetto integralmente e per principio. La legge non ha sufficientemente riguardo per la tutela della libertà e della sfera privata dei cittadini e si scontra con le libertà fondamentali del popolo svizzero.

Il *CCCZH* respinge il progetto in toto e non vi ravvisa alcunché di positivo.

Considera la ricodificazione della legislazione in materia di servizio informazioni civile, rappresentato dal SIC, una vera e propria farsa e un pericolo per l'ordinamento liberale della Svizzera. Vista l'incapacità del SIC di districarsi già nel vigente regime, non vi sarebbe ragione di riconoscergli ulteriori competenze. Il *CCCZH* consiglia pertanto nella migliore delle ipotesi di procedere a una ristrutturazione della LMSI (la LSIC andrebbe in ogni caso abrogata al più presto).

Pur ritenendo sensata la creazione di una base legale formale unitaria per il servizio informazioni civile, il *Centre Patronal* e la *CVAM* auspicano però che la questione della base costituzionale sia correttamente risolta e che la distinzione tra estremismo violento e terrorismo venga ancora una volta verificata o perlomeno motivata con serietà.

La *DigGes* si dichiara sconcertata dall'avamprogetto. Benché l'articolo sullo scopo specifichi con piena ragione che la nuova legge contribuisce «a garantire i fondamenti democratici e costituzionali della Svizzera», a tal fine occorrerebbe però dapprima garantire che questi fondamenti non vengano sovvertiti da questa stessa legge. In particolare, la *DigGes* chiede pertanto che siano rispettati i seguenti principi:
- comprovata proporzionalità;
- tutela dei diritti dell'uomo anche per quanto riguarda l'estero;
- tutela della libertà di opinione e di espressione;
- limitazione dell'impiego delle informazioni di intelligence;
- rispetto dei limiti previsti per le ingerenze nella sfera privata ai fini del perseguimento penale;
- impedimento di sanzioni indirette per chi esprime opinioni politiche critiche;
- tutela dei diritti dell'uomo dei richiedenti l'asilo;
- protezione dei dati in caso di controversie tra ditte e movimenti critici nei loro confronti;
- sorveglianza soltanto in presenza di indizi di reato;
- equità delle procedure di autorizzazione;
- riconoscimento del diritto di consultazione e rettifica dei dati;
- riconoscimento del diritto di essere informati sulle misure di sorveglianza adottate e in caso di trasmissione di dati personali all'estero;
- le deroghe ai due principi appena menzionati devono essere rare e il loro numero deve essere reso pubblico;
- controllo indipendente del rispetto dei suddetti principi e pubblicazione di un rapporto al riguardo;
- regole dettagliate sul tipo di informazioni ricercate, sulle modalità di acquisizione e sull'uso successivo delle informazioni;
- informazione particolareggiata del pubblico in merito alle misure adottate e alle informazioni acquisite.

economiesuisse approva fondamentalmente la creazione di una base legale formale unitaria per il SIC. Un regime moderno per l'acquisizione delle informazioni a favore della sicurezza del Paese è anche nell'interesse dell'economia e di conseguenza della piazza economica svizzera. Ma devono essere tenuti in considerazione anche i legittimi interessi dei privati e delle imprese. In tal senso, le nuove misure di acquisizione delle informazioni si rivelano eccessive. Competenze attribuite in buona fede presterebbero il fianco ad abusi che causerebbero danni considerevoli, e inoltre l'onere delle nuove misure non dovrebbe essere semplicemente scaricato su terzi (non coinvolti) o intermediari. Pertanto, devono essere posti severi limiti alle autorità e le competenze vanno descritte con precisione. L'avamprogetto contiene troppe circonlocuzioni generiche e vaghe. La sicurezza assoluta non può essere garantita e quindi vi saranno sempre rischi residui. In caso di dubbio, occorre pertanto optare a favore della libertà e contro poteri di ingerenza generalizzati.

dirittifondamentali.ch, i *GDS* e la *SPF* si dichiarano totalmente contrari al progetto legislativo e non vi intravvedono alcunché di positivo. Si tratta di un elenco di desiderata della protezione dello Stato che si vuole trasformare in normativa legale. Tanto gli evidenti punti deboli

della protezione dello Stato quanto le riserve espresse dal Parlamento sarebbero stati ignorati o volutamente sminuiti.
Il diritto penale e i codici di procedura penale offrirebbero già strumenti sufficienti e molto ampi per indagini anche di carattere preventivo. Le ingerenze nella sfera privata previste dall'avamprogetto violerebbero il principio di proporzionalità. I nuovi provvedimenti coercitivi messi a disposizione del SIC rappresenterebbero il perno del progetto legislativo, pur essendovi inseriti in modo da passare quasi inosservati.

Il *GSsE* respinge il progetto in blocco. L'avamprogetto affosserebbe quasi completamente le condizioni poste dal Parlamento al Consiglio federale con il rinvio della LMSI II. Il *GSsE* critica inoltre di principio il fatto che l'ex servizio informazioni civile, dopo la sua fusione con il servizio informazioni militare per dare vita al SIC, sia stato accorpato al DDPS e non a un Dipartimento civile.
Il vigente Codice di procedura penale e il vigente Codice penale fornirebbero strumenti sufficienti e alquanto ampi per indagini anche di carattere preventivo.
Le ingerenze nella sfera privata previste dalla LSI violerebbero il principio di proporzionalità e il pericolo che si ricominci a costituire banche dati incontrollate sarebbe grande. Le ingerenze nella sfera privata di persone impegnate politicamente comporterebbero al di là di ogni dubbio non solo un pericolo per la democrazia, ma anche uno spreco enorme di risorse statali.
Il *GSsE* teme inoltre che senza una sorveglianza efficace e senza trasparenza la protezione dello Stato non si orienti alle minacce concrete per il Paese, bensì in funzione delle simpatie politiche personali dei suoi collaboratori. Non vi sarebbero motivi di credere che oggi le cose possano andare diversamente rispetto all'epoca dello scandalo delle schedature.

La *PP1* constata con riconoscenza che l'avamprogetto prevede una serie completa di importanti garanzie per il controllo delle attività degli organi del SIC e per la protezione contro ingerenze sproporzionate: principio della proporzionalità, tutela della vita privata e della sfera privata, intervento di un'istanza giudiziaria indipendente per le ingerenze gravi, responsabilità personale e politica dei titolari dei mandati per le misure di sorveglianza ordinate, protezione dei depositari legali di segreti, attuazione della trasparenza (a posteriori), disposizioni a garanzia della protezione dei dati, alta vigilanza parlamentare, protezione giuridica e responsabilità dello Stato per attività illegali degli organi di intelligence della Confederazione o dei Cantoni secondo le pertinenti leggi sulla responsabilità.

L'associazione *RefLMSI* dichiara di poter benissimo rinunciare alle schedature e alla sorveglianza delle comunicazioni telefoniche e di posta elettronica. Il SIC acquisirà e tratterà anche in avvenire informazioni concernenti l'attività politica e l'esercizio della libertà di opinione, di riunione o della libertà sindacale, salvo nel caso in cui lo si sciolga o si limiti drasticamente il suo entusiasmo per la raccolta di dati. La LSI conterrebbe ancora tutte le insidie della LMSI. Se oltretutto si concedesse al SIC addirittura la facoltà di adottare anche misure soggette ad autorizzazione, l'insensata marea di dati senza la minima utilità crescerà a dismisura. Per evitare che in avvenire si produca un simile risultato, la soluzione più semplice consisterebbe nell'eliminare del tutto il servizio informazioni interno. In questo senso, *RefLMSI* chiede di mantenere le disposizioni transitorie che abrogano la LMSI e di stralciare definitivamente il resto dell'avamprogetto.

L'*USAM* respinge il presente avamprogetto. Non sarebbero importune le attività di intelligence in quanto tali ma l'assenza di tutela per la sfera privata del cittadino. In particolare, le difficoltà risiederebbero nell'impiego dei dati, rispettivamente nella carente distinzione tra Svizzera ed estero. Ci si deve domandare dove viene situato il confine tra queste due categorie e qual è il significato di tale differenziazione per il diritto alla protezione della sfera privata. Altri problemi risiederebbero nelle indagini in assenza di sospetti, nei provvedimenti coercitivi e nella concezione del SIC come «polizia federale».
Un servizio informazioni solido sarebbe caratterizzato dai seguenti elementi: difesa contro i pericoli in Svizzera e all'estero, monitoraggio delle tendenze geostrategiche compresi i rapporti di scambio nelle catene di produzione e nei movimenti finanziari globali, analisi dei nes-

si importanti per la politica di sicurezza che potrebbero esercitare un influsso sulla Svizzera. In un simile quadro l'*USAM* sarebbe favorevole a un servizio informazioni ben strutturato ed efficiente sul piano operativo.
D'altra parte occorre assolutamente tener conto delle esigenze di sicurezza della popolazione. Il cittadino ha infatti il diritto non solo di essere protetto dalle minacce che incombono sulla sua sicurezza, ma anche al rispetto incondizionato della propria sfera privata. Questo diritto ingloba un diritto di autodeterminazione riguardo alle informazioni e ai dati personali e il diritto di proteggersi dalle ingerenze eccessive dello Stato.

La *SIG* spera che l'avamprogetto venga approvato possibilmente senza modifiche o quantomeno che non venga indebolito, poiché auspicherebbe che le misure di acquisizione soggette ad autorizzazione potessero essere adottate anche nell'ambito dell'estremismo violento. Ritiene che si tratti di un progetto legislativo equilibrato, che non compromette né il diritto alla protezione della sfera privata né la libertà personale.

La *SSU* e l'*ASUI* approvano la nuova base legale unitaria per il SIC, compresa la reimpostazione dell'acquisizione di informazioni e le misure previste a tal fine, l'introduzione di una base legale per la registrazione, il trattamento e la memorizzazione differenziati dei dati necessari nonché il sistema di controllo proposto.
Gli strumenti previsti dall'avamprogetto sono necessari per difendersi dalle minacce odierne e per individuare tempestivamente le minacce future. La procedura destinata a garantire un equilibrio tra la tutela delle libertà individuali del cittadino e l'interesse pubblico alla salvaguardia della sicurezza interna ed esterna del nostro Paese appare adeguata.
La distinzione tra attività terroristiche ed estremismo violento è considerata impraticabile e inoltre il rischio risultante dalle attività illecite di entrambe le categorie per lo Stato e i cittadini è ugualmente grave. *SSU* e *ASUI* deplorano pertanto l'esclusione dell'estremismo violento dal campo di applicazione delle misure soggette ad autorizzazione.
Le due associazioni approvano invece espressamente la facoltà concessa al Consiglio federale di far capo al SIC, informando contemporaneamente la competente Delegazione delle Camere federali, per salvaguardare altri interessi nazionali essenziali.

La *Swico* approva sostanzialmente la creazione di una base legale formale unitaria per le attività informative e dei relativi sistemi d'informazione, ma si dichiara contraria a un'estensione verso una sorveglianza totale.

SwissBanking ritiene che l'avamprogetto fornisca una soluzione molto equilibrata alla dicotomia tra gli interessi del nostro Paese in materia di sicurezza e quelli delle persone vittime di ingerenze nei propri diritti fondamentali. La creazione di una base legale universale consente di imporre uniformemente collaudati principi di legge e meccanismi di protezione per tutti i settori interconnessi del servizio informazioni.

Swisscom condivide pienamente il parere e le proposte della propria associazione di categoria asut.

La *FSFP* appoggia l'avamprogetto, che considera una soluzione politica senza fronzoli. In Svizzera la vigente legislazione sul servizio informazioni (LMSI) sarebbe estremamente indulgente. Rispetto ad altri Stati, si può affermare senza timore che in Svizzera la sfera privata è protetta come massimo principio. Oggi, tuttavia, la situazione di minaccia sarebbe ben diversa rispetto a qualche anno fa.

5. Pareri sulle singole disposizioni dell'avamprogetto

Articolo 1

Capoverso 1:
CCCZH considera assurdo il modo in cui il SIC può interagire a piacimento con i privati o con l'estero. Desidera evitare che il SIC interagisca per i propri fini con contesti criminali o con Paesi che non rispettano né la morale né la legge.

Capoverso 2:
Per il *PS,* le attività informative ai sensi del capoverso 2 sono chiaramente prioritarie. Attività più estese che non avessero nulla a che fare con i tradizionali compiti di un servizio informazioni dovrebbero pertanto essere svolte soltanto in via eccezionale, per decisione del Consiglio federale, entro limiti temporali e territoriali strettamente circoscritti e unicamente in singoli casi (art. 62).

Per quanto concerne le lettere a e b, per il *CCCZH* rimane irrisolta la questione di sapere fino a che punto il SIC non contribuisca esso stesso a provocare incertezza e arbitrarietà ponendosi al di sopra della legge e invadendo illegalmente la sfera privata delle persone.

Secondo la *SSU* e l'*ASUI*, l'individuazione precoce dei segni di potenziali rischi e il relativo preallarme in situazioni di minaccia costituiscono un punto critico. Le due associazioni propongono pertanto di completare lo scopo della legge di cui all'articolo 1 capoverso 2 con le seguenti lettere a e e:
a. contribuire a garantire l'indipendenza e la sicurezza della Svizzera di fronte a minacce esterne;
le lettere a–c diventano le lettere b–d;
e. avviare l'adeguamento tempestivo degli strumenti di politica di sicurezza della Confederazione, segnatamente dell'esercito, all'evoluzione della minaccia;
la lettera d diventa la lettera f.

Capoverso 3:
Per il *PS*, il rapporto non fornisce indicazioni che chiariscano la formulazione scelta: che cosa significa «sostegno alla politica estera svizzera»? E «protezione della piazza industriale, economica e finanziaria svizzera»? Nel messaggio bisognerà rendere convincenti queste espressioni.

Per *CCCZH* il capoverso 3 spiana la strada allo spionaggio industriale ed economico, rischiando di compromettere la neutralità della Svizzera.

SSU e ASUI apprezzano la possibilità data al Consiglio federale di impiegare il SIC, informandone il competente organo delle Camere federali, per tutelare altri interessi nazionali essenziali. Le due associazioni suggeriscono però di precisare che questi interessi nazionali devono rientrare nell'ambito delle competenze che la Costituzione federale assegna alla Confederazione, salvo nel caso in cui uno o più Cantoni chiedano di impiegare il SIC per tutelare interessi nazionali essenziali che per la Costituzione federale (Cost.) rientrano nell'ambito delle competenze cantonali.

Per *PP1* l'attribuzione dei settori di attività e di competenza è complicata dal fatto che l'elenco dei compiti previsto all'articolo 4 non combacia perfettamente con quanto previsto all'articolo 1 capoverso 2 e capoverso 3. Per giunta, l'articolo 17 capoverso 2 contiene un elenco di fattispecie, dedotto dall'articolo 4, il quale definisce che cosa sia «una minaccia concreta nei confronti della sicurezza interna o esterna» del nostro Paese. A questo proposito va osservato che i settori di attività del SIC secondo il capoverso 2 lettera a e il capoverso 3 sono difficilmente delimitabili gli uni dagli altri, e che da questa difficoltà potrebbero na-

scere determinati rischi per le attività e l'influenza del SIC nel dibattito politico democratico interno.
PP1 consiglia pertanto di impostare con maggiore precisione i capoversi 2 e 3 sul campo di attività fondamentale del SIC, inserendo:
al capoverso 2 i compiti del SIC che secondo la LSI esso può esercitare senza altra autorizzazione, chiaramente destinati – ed espressamente limitati – alla protezione della popolazione svizzera (includendovi eventualmente gli Svizzeri all'estero), alla protezione della libertà del popolo e alla sicurezza e indipendenza del Paese secondo la descrizione di cui all'articolo 2 capoverso 1 Cost.; si tratta dei compiti descritti all'articolo 4 capoverso 1 lettera a; e
al capoverso 3 la tutela di «altri interessi nazionali» quali gli interessi della sicurezza internazionale, il sostegno alla politica estera e la protezione della piazza industriale, economica e finanziaria svizzera sulla base di mandati chiaramente delimitati impartiti dal Consiglio federale nell'ambito della propria responsabilità politica, sia sulla base di un mandato da descrivere in maniera generale ma concretizzando la nozione nella legislazione d'esecuzione secondo l'articolo 72, come l'emanazione della «lista d'osservazione» ai sensi dell'articolo 63, sia sulla base di un mandato particolare impartito caso per caso con la procedura prevista all'articolo 62.

L'*USAM* suggerisce di impiegare nel capoverso 3, la cui formulazione considera di principio abbastanza precisa, l'espressione «piazza economica svizzera» («Wirtschaftsstandort Schweiz»), a suo dire migliore e più precisa. Con l'attuale enumerazione non si capisce infatti in che cosa consistano le rispettive differenze e se l'elencazione considera soltanto le esigenze di protezione dei settori menzionati.

Articolo 2

CCCZH segnala un'incoerenza tra le lettere b e c. Alla lettera b non è specificato che le informazioni possono essere acquisite, direttamente o indirettamente (per mezzo di intermediari), soltanto secondo la legge.

SSU e *ASUI* giudicano infelice la formulazione di questo articolo, poiché può essere interpretato nel senso che la legge sviluppa soltanto un effetto interno sugli attori in esso menzionati. Le due associazioni propongono pertanto di assoggettare all'obbligo di collaborazione anche le altre autorità della Confederazione, non direttamente incaricate dell'esecuzione, nella misura in cui dispongano di informazioni rilevanti per il servizio informazioni:

Art. 2 *Autorità e persone soggette alla presente legge*
La presente legge si applica:

a. *[nessuna modifica]*
b. *alle altre autorità della Confederazione e dei Cantoni nonché ad altre persone giuridiche di diritto pubblico o privato, nella misura in cui adempiano compiti pubblici e dispongano di informazioni rilevanti per il servizio informazioni;*
c. *alle persone fisiche o giuridiche nella misura in cui siano tenute a trasmettere o trasmettano spontaneamente informazioni rilevanti per il servizio informazioni.*

Articolo 3

GE critica il termine di un anno, dal momento che l'accertamento di importanti fattispecie richiede ovviamente tempi più lunghi.

Il *Partito Pirata* lamenta la mancanza di un accenno al principio di proporzionalità.

Per il *CCCZH* i capoversi 1 e 4 dimostra chiaramente che l'ingerenza nella sfera privata delle persone diventerebbe la norma.

SSU e *ASUI* considerano eccellente la formulazione dei capoversi 1 a 5.

Capoverso 3:
Secondo il *Partito Pirata* la scelta dovrebbe essere compiuta da un'autorità indipendente.

DigGes ravvisa un possibile conflitto tra le lettere a e b e auspica la creazione di un servizio responsabile nei confronti del Parlamento per la gestione di tale conflitto (nella prassi la lett. b rimarrebbe altrimenti lettera morta).

Capoverso 4:
Secondo l'*Università di Ginevra* questa disposizione viola l'articolo 4 capoverso 4 LPD. Dato che incide sull'autodeterminazione riguardo ai dati personali, occorre una base legale precisa. Il capoverso 4 non dovrebbe essere formulato in modo tanto vago, e in particolare dovrebbe menzionare non solo l'acquisizione ma anche il trattamento di questi dati, fatto salvo l'articolo 29 e nel rispetto dell'articolo 22.

Capoverso 5:
Il *Partito Pirata* indica che anche le organizzazioni estremiste dispongono per lo più di un braccio politico moderato.

CCCZH esprime diffidenza riguardo a questo capoverso.

Per *DigGes* un divieto di principio non è sufficiente se non si prevede anche che le deroghe richiedono l'autorizzazione oggettiva e indipendente da parte di un'autorità giudiziaria.

Capoverso 6:
AG ribadisce l'importanza del principio previsto al capoverso 6.

Secondo il *CCCZH*, in virtù di questo capoverso il SIC potrebbe osservare le attività che gli sembrano connesse all'estremismo violento o al terrorismo già nella fase preparatoria.

Per *SSU* e *ASUI*, le eccezioni sarebbero troppo limitate. Le due associazioni propongono la formulazione seguente:
[6] Tuttavia, può eccezionalmente acquisire informazioni su un'organizzazione o una persona e registrarle con i relativi riferimenti alle persone se sussistono indizi fondati secondo cui tale organizzazione o persona esercitando i diritti previsti al capoverso 5 mette in pericolo la sicurezza interna o esterna della Svizzera.
eventualmente completata dal seguente passaggio:
..in particolare per la preparazione o l'esecuzione di attività terroristiche, spionistiche o di estremismo violento.

I capoversi 6 e seguenti disciplinerebbero le competenze del SIC per l'acquisizione di informazioni in un ambito sensibile dal profilo della politica giuridica e oltretutto delicato in quanto legato all'esercizio dei diritti democratici dei cittadini (attività politica ed esercizio della libertà di opinione, della libertà di riunione e della libertà sindacale). Secondo *PP1* non bisognerebbe istituire una competenza del SIC per l'acquisizione di informazioni con una disposizione derogatoria genericamente descritta come quella qui prevista, poiché essa concede agli organi direttivi del SIC tutto l'agio per operare in base a decisioni di opportunità. Occorrerebbe piuttosto prevedere la necessità di richiedere di caso in caso un'autorizzazione del Consiglio federale o della sua Delegazione Sicurezza.
L'attuale capoverso 8 dovrebbe essere sostituito con un nuovo capoverso 7 che descriva la procedura per l'ottenimento di questo nullaosta. L'attuale capoverso 7, concernente la cancellazione delle informazioni acquisite in questo ambito, dovrebbe essere aggiunto come capoverso 8 alla fine dell'articolo 3.

Capoverso 7:
Secondo *PP2* la cancellazione non dovrebbe impedire né alla persona interessata di consultare i propri dati né ai tribunali di trattare un'eventuale opposizione.

Per il *Partito Pirata* questo capoverso sarebbe l'unica proposta progredita di tutto l'atto normativo, ma ciò nonostante se si procedesse ad accurati accertamenti preliminari dovrebbe essere possibile evitare già la registrazione di simili dati. Il Partito Pirata si domanda come farebbe il SIC per garantire che i dati siano cancellati da tutte le sue banche e che anche gli Stati terzi provvedano alle cancellazioni necessarie.

Per la *DigGes* questo principio è fondamentalmente giusto, ma richiede misure di accompagnamento supplementari, quali ad esempio la cancellazione di copie in altre banche dati, la correzione di informazioni errate trasmesse ad altre autorità o la possibilità di richiedere l'accertamento giudiziario dell'illiceità dell'acquisizione di informazioni. Inoltre occorrerebbe introdurre meccanismi che consentano al SIC di trarre insegnamento da eventuali errori.

In questo capoverso si pongono accresciute esigenze quanto al grado della prova che l'autorità è chiamata a fornire («trovato conferme»). Dato che il breve periodo di un anno spesso non basta per accertare sufficientemente una fattispecie, occorrerebbe porre esigenze minori in materia di prova. *SSU* e *ASUI* propongono pertanto la seguente formulazione:
[7] Cancella i dati registrati con i riferimenti alle persone senza indugio, ma al più tardi entro un anno da quando gli indizi si sono dimostrati infondati.

Capoverso 8:
Il *PS* considera troppo ampia questa formulazione e propone di limitarla sostituendo il termine «adeguate» con «necessarie»:
[8] … necessarie per la valutazione della minaccia proveniente… ».

dirittifondamentali.ch, *Verdi*, *GDS* e *SPF* sottolineano che il SIC ha regolarmente mancato di attenersi ai limiti previsti al capoverso 5, che vieta l'acquisizione e il trattamento di informazioni concernenti l'attività politica e l'esercizio della libertà di opinione, della libertà di riunione o della libertà sindacale.
Di conseguenza il capoverso 8 dovrebbe essere soppresso oppure assoggettare alla riserva di un'autorità giudiziaria quantomeno la lista di osservazione e la lista dei gruppi da classificare nella categoria dell'estremismo violento nonché qualsiasi ingerenza compresa nel tenore del capoverso 5.
Ancora meglio sarebbe se si pubblicassero in futuro tutte queste liste o se non altro si indicasse nel rapporto annuale del SIC quali gruppi e quante persone sono stati sottoposti a sorveglianza. Anche *DigGes* è dello stesso parere.

SSU e *ASUI* vorrebbero che si evitasse di fare riferimento a una prescrizione situata più avanti nella legge:
[8] Può inoltre acquisire informazioni su organizzazioni e persone di cui è giustificatamente possibile supporre che rappresentino una minaccia per la sicurezza interna o esterna e registrarle con i relativi riferimenti alle persone.

Articolo 4

GE riconosce l'opportunità dell'enumerazione dei settori di attività del SIC. In particolar modo la menzione degli attacchi a infrastrutture critiche completa adeguatamente il ventaglio di compiti del SIC.

SG suggerisce di prevedere il principio secondo cui i riscontri del SIC circa possibili reati devono essere comunicati ai pubblici ministeri e di introdurre tale principio nella legge. Se si fa obbligo alle autorità penali di informare il SIC, quest'obbligo deve valere anche in senso inverso. Non si capisce in che modo le autorità inquirenti possano venire a sapere che il SIC

possiede dati con valore probatorio che nell'ambito di procedimenti penali esse possono richiedere in virtù dell'articolo 55.

Per la *CAIS* il catalogo di compiti è sufficientemente chiaro, ma il capoverso 1 lettera d assomiglia troppo a una clausola generale.

Per il *PBD* la limitazione relativa alle sostanze radioattive di cui al numero 4 è formulata in modo eccessivamente restrittivo.
A causa dell'imprevedibilità di determinate minacce, il Consiglio federale dovrebbe poter impartire un mandato ai sensi della lettera d anche a posteriori.

Il *PLR* reputa confacente la distinzione tra terrorismo ed estremismo violento. I recenti avvenimenti avrebbero peraltro dimostrato che la guerra elettronica e i pericoli legati ai mezzi informatici dovrebbero essere presi molto sul serio. Occorre dunque che il SIC disponga degli strumenti per anticipare e contrastare questo tipo di minacce. Il *PLR* propone pertanto di completare il numero 5 o farlo seguire da un ulteriore numero dal seguente tenore:
«gli attacchi o i preparativi di attacchi informatici intesi a penetrare, indebolire, distruggere o disturbare i sistemi civili, militari o di organizzazioni internazionali presenti in Svizzera o direttamente legati agli interessi della Svizzera».

Il *Partito Pirata* vorrebbe che il capoverso 1 lettera a numero 5 fosse formulato esaustivamente; vorrebbe inoltre, come la *DigGes*, che il capoverso 7 fosse soppresso, poiché disciplina ancora una volta un tema già trattato all'articolo 5.

L'acquisizione di informazioni nel settore dei cosiddetti beni a duplice impiego («dual use») persegue uno scopo legittimo, ma dischiude al SIC un campo d'azione molto vasto. La *PP1* vi scorge pertanto anche un certo rischio che nelle proprie raccolte di dati il SIC accumuli preziose informazioni sulle attività dell'industria riguardanti la «piazza industriale e finanziaria svizzera», appartenenti alla sfera delle imprese interessate protetta dal segreto e che potrebbero costituire un pegno interessante per la collaborazione con i servizi informazioni esteri ma anche un accattivante bersaglio di tentativi di accesso da parte di questi servizi.
Di conseguenza la legislazione d'esecuzione dovrebbe concretizzare maggiormente l'attività del SIC in questo settore, ispirandosi eventualmente alla legislazione federale sul materiale bellico e alla legge sul controllo dei beni a duplice impiego. Per le informazioni raccolte nel campo della proliferazione si dovrebbero prevedere, nell'ambito dell'articolo 5, misure di protezione e di sicurezza particolari.

La separazione dei poteri è un requisito fondamentale per un ordinamento democratico. Perciò l'*ASNI* chiede che il Consiglio federale elenchi situazioni concrete in cui è lecito intraprendere attività informative. Il coinvolgimento del Tribunale amministrativo federale, previsto sotto forma di presentazione di una domanda (art. 25) costituirebbe un errore. Inoltre, il Consiglio federale dovrebbe definire esaustivamente le fattispecie concrete che giustificano lo svolgimento di attività informative. La responsabilità sarebbe così disciplinata esaustivamente. L'avamprogetto presentato violerebbe il principio della separazione dei poteri.

Il *CCCZH* si chiede quali siano per l'esattezza i tratti che distinguono il terrorismo dall'estremismo violento. Gradirebbe inoltre che il numero 4 fosse messo in relazione con il numero 1. Si chiede anche se il ruolo del SIC per la sicurezza del WEF non sia in contraddizione con l'articolo 3 capoverso 5.

DigGes teme che a causa della sua ambiguità il numero 5 possa rivelarsi una norma elastica che con l'andar del tempo consentirà di estendere le ingerenze.

SSU e *ASUI* ritengono che la formulazione proposta escluda il fabbisogno informativo generale. Il periodo introduttivo dell'articolo 4 capoverso 1 lettera a dovrebbe pertanto essere formulato come segue:

a. *individuare tempestivamente e sventare minacce nei confronti della sicurezza interna ed esterna risultanti in particolare:*

Il capoverso 7 dovrebbe essere formulato in modo da chiarire che tutti i compiti esercitati dal SIC sottostanno alle condizioni poste:
[7] *Nell'esercizio dei propri compiti protegge i suoi collaboratori, le sue installazioni, le sue fonti e i dati da esso elaborati.*

La *Swico* ravvisa nell'esteso e vago catalogo di compiti una licenza quasi illimitata ad acquisire e trattare informazioni e sostiene che debba per questa ragione essere circoscritto ai compiti e alle attività fondamentali e assolutamente indispensabili del SIC.

Articolo 5

DigGes chiede di specificare che le misure di protezione e di sicurezza possono servire unicamente a garantire il mandato legale del SIC e non a nascondere alla popolazione le modalità o la portata delle attività del SIC o a coprire irregolarità.

Secondo *dirittifondamentali.ch*, i *Verdi*, i *GDS* e *SPF*, il posto di queste disposizioni non è nella legge, bensì dovrebbero essere sottintese, per un servizio che opera in un contesto tanto delicato. Disposizioni di questo tipo potrebbero trovare collocazione in un'ordinanza o addirittura in un regolamento. In virtù dell'articolo 34 capoverso 1*ter* LTC, il Consiglio federale stabilisce le condizioni in cui la polizia e le autorità incaricate dell'esecuzione delle pene possono, nell'interesse della sicurezza pubblica, installare, mettere in servizio o esercitare un impianto di telecomunicazione che provoca interferenze. Questa norma andrebbe eventualmente completata con l'aggiunta dell'espressione «le autorità incaricate della protezione dello Stato» («Staatsschutzbehörden»). Al massimo ha un senso il capoverso 2 dell'articolo 5 (altrettanto dicasi riguardo all'art. 4 cpv. 7).

Per il *CCCZH*, il commento relativo a questa disposizione induce a chiedersi quanto siano già vaghi oggi i confini tra servizio informazioni civile e militare e quali persone abbiano accesso a schede sensibili sulle persone, visto che a quanto pare potrebbe darsi che i controlli di sicurezza siano delegati a terzi e che alla sede del SIC si registri un andirivieni di militari. La cerchia delle persone che hanno virtualmente accesso a dati personali sensibili sembra troppo vasta, e il SIC non è nemmeno in grado di escludere che «collaboratori frustrati» si impossessino di consistenti raccolte di dati.
Il SIC prevede anche di utilizzare impianti di telecomunicazione che provocano interferenze. Il *CCCZH* ritiene che l'uso di questo tipo di impianti da parte del SIC debba essere vietato, poiché questa soluzione potrebbe essere anteposta per tenere appositamente «conversazioni» nei luoghi in cui si intende disturbare la comunicazione interpersonale.

Secondo la *PP1*, l'accesso alla rete gestita dal SIC deve essere consentito soltanto, analogamente a quanto previsto all'articolo 42 capoverso 2 lettera b, ai collaboratori del SIC che sono stati debitamente autorizzati all'accesso secondo le regole della «information security». Questo punto dovrebbe essere concretizzato nella normativa di esecuzione.

Articolo 6

Il *CCCZH* è dell'idea che armare un servizio informazioni civile sia uno sbaglio e si chiede in quali contesti il SIC abbia assolutamente bisogno di essere armato per svolgere le proprie attività. Ritiene inoltre che occorrerebbe definire sommariamente il tipo di armi, ma che disciplinare questo aspetto per via di ordinanza sarebbe delicato, tanto più che altrimenti in definitiva proprio all'estero tutto sarebbe legittimabile.

Articolo 7

Capoverso 2:
Il *Partito Pirata* e la *DigGes* sostengono entrambi che grazie ai mezzi tecnici di cui disponiamo oggi non vi siano più problemi per trasmettere senza ritardi mandati scritti, magari confermando per sicurezza successivamente per telefono i mandati impartiti,. La formulazione dei mandati per iscritto serve anche a garantire che vengano eseguiti in modo preciso e verificabile. Questo capoverso dovrebbe pertanto essere soppresso.

Il *PBD* vorrebbe invece che si stabilisse un termine concreto entro cui poter confermare i mandati per iscritto a posteriori.

Articolo 8

GE approva questa disposizione.

CCPCS, AR, BE, SG, SO, SZ, TG, UR e *ZG* segnalano che in situazioni straordinarie in cui devono svolgere compiti di polizia di sicurezza i corpi di polizia hanno bisogno di informazioni complete sugli imminenti avvenimenti. Questa esigenza si manifesta parimenti per eventi di portata cantonale o anche solo locale (quali le manifestazioni Reclaim the Street a Zurigo, le azioni organizzate attorno alla Reithalle di Berna ecc.). Rappresentanti delle autorità d'esecuzione cantonali partecipano regolarmente alle relative valutazioni della situazione e con le loro conoscenze contribuiscono alla definizione di un quadro completo delle circostanze senza per questo dover rivelare informazioni delicate quali dati personali, indicazioni sulle operazioni o altre informazioni non necessarie per la gestione immediata degli eventi. Tuttavia, dato che si tratta di informazioni qualificate, converrebbe che la legge prevedesse un'autorizzazione per questo impiego delle informazioni derivanti dalle attività informative su incarico della Confederazione. Benché l'articolo 48 menzioni il sistema d'informazione per la presentazione elettronica della situazione, l'uso di informazioni di intelligence per il pilotaggio e l'attuazione di misure di polizia di sicurezza (dei Cantoni) dovrebbe già figurare come compito al capitolo 2 della legge, e quindi l'articolo 8 dovrebbe essere completato di conseguenza.

Articolo 9

Il *CCCZH* vede la collaborazione del SIC con l'esercito come legittimazione di fatto a scambiare informazioni con i servizi informazioni militari, con conseguente dissolvimento dei confini tra sicurezza civile e militare. Inoltre, teme che il SIC possa servirsi dell'articolo 9 come «varco» per procurarsi informazioni attraverso tutti i canali possibili, le norme del servizio informazioni militare essendo maggiormente «lasche».

Capoverso 2:
La *PP1* teme un possibile conflitto di competenze con le autorità gerarchiche degli organi militari interessati nell'ambito dell'assegnazione del mandato.

Articolo 10

La *PP1* pensa che, analogamente a quanto previsto all'articolo 9 capoverso 3, il Consiglio federale dovrebbe essere incaricato e abilitato a emanare ulteriori disposizioni per l'ambito delicato della collaborazione del SIC con servizi informazioni e autorità di sicurezza esteri. Il controllo di questa collaborazione dovrebbe essere inserito nel piano dei controlli dell'autorità di vigilanza indipendente di cui agli articoli 66 e seguenti.

Capoverso 1:
Lettera e:
SZ e *ZG* chiedono che, contrariamente a quanto previsto all'articolo 61 capoverso 3, i relativi trattati internazionali non possano essere conclusi dal solo Consiglio federale ma debbano

essere anche approvati dal Parlamento. Questo garantirebbe un sufficiente dibattito politico sui dati destinati a essere scambiati.

Il *Partito Pirata* vuole che vengano condivise informazioni soltanto con Stati che rispettano i diritti dell'uomo e dati personali soltanto con Stati che secondo il giudizio dell'IFPDT soddisfano un determinato standard minimo in materia di protezione dei dati.

Il *CCCZH* vede con preoccupazione la collaborazione del SIC con i servizi informazioni esteri prevista dalla legge.

DigGes vorrebbe che si completasse questa disposizione con un rimando a un articolo che andrebbe aggiunto e che dovrebbe prevedere:
- che i dati messi a disposizione a livello internazionale attraverso questi sistemi d'informazione possono essere utilizzati soltanto nel rispetto delle leggi svizzere, anche da parte delle autorità di altri Paesi;
- che l'effettiva attuazione di tale principio può essere verificata da un organismo indipendente;
- che gli interessati possono esercitare sul piano internazionale i diritti loro spettanti in materia di protezione dei dati;
- l'informazione degli interessati in merito alla trasmissione di dati personali all'estero;
- i tipi di dati che possono essere inseriti in simili sistemi d'informazione e le condizioni dell'inserimento.

Un simile articolo potrebbe ad esempio trovare una collocazione adeguata dopo l'articolo 56.

Capoverso 2:
Il *PVL* vede con occhio critico la competenza istituita in questa disposizione. Invita il Consiglio federale a sottoporre l'impiego di collaboratori all'estero a un'analisi costi-benefici e se del caso a rinunciarvi.

Capoverso 3:
BS auspica che si definisca a livello di legge se la trasmissione di dati da un'autorità cantonale a un'autorità di sicurezza estera è ammessa e a quali condizioni.

GE è preoccupata dal fatto che questa disposizione introduce una restrizione suscettibile di causare problemi. Questi potrebbero sorgere particolarmente per *GE*, che in quanto Cantone di confine deve occuparsi di molte questioni riguardanti i frontalieri. Inoltre vorrebbe che lo scambio preventivo di informazioni con i competenti servizi dei Paesi limitrofi venisse ulteriormente esteso, poiché ciò corrisponde attualmente a una prassi dettata dalla necessità. La prevista restrizione comprometterebbe questo importante aspetto.

PP1 suggerisce di verificare quali mezzi la Confederazione potrebbe chiedere che le venissero concessi affinché possa imporre il rispetto di questa disposizione.

Capitolo 3: Acquisizione di informazioni (art. 11 – 38)

AG considera opportuna l'estensione delle misure non soggette ad autorizzazione (per es. l'impiego di droni), mentre le nuove possibilità soggette ad autorizzazione previste per la ricerca di informazioni sarebbero lodevoli da un punto di vista di polizia.
La necessità di un'autorizzazione da parte del Tribunale amministrativo federale e inoltre del nullaosta del capo del DDPS garantisce una verifica politica dell'ammissibilità di queste ultime misure nel singolo caso.
AG e *Privatim* esprimono apprensioni riguardo alle reti sociali, ma anche ai gestori di motori di ricerca quali Google o a società di commercio elettronico quali Amazon, che possiedono non solo quantità immense di informazioni sulla personalità, i luoghi di dimora, il materiale informatico utilizzato, i contatti ecc. dei loro utenti ma persino profili ombra di persone che non sono utenti registrati dei siti in questione. Questi dati potrebbero avere enorme interesse per i servizi informazioni.

Non si capirebbe se non vengano affatto prese in considerazione misure di questo tipo o se invece le disposizioni al riguardo previste dall'avamprogetto siano sufficientemente precise. La questione si porrebbe per i server ubicati in Svizzera e all'estero. Data la complessità del contesto giuridico, i beni giuridici in gioco e la quantità di informazioni ottenibili, la questione dovrebbe essere necessariamente analizzata nel messaggio.

SG osserva che, inesplicabilmente, le misure di acquisizione di informazioni previste nell'avamprogetto di legge sul servizio informazioni non sono armonizzate con le misure previste dal CPP. Il problema sorgerebbe nel caso in cui si trasmettessero alle autorità inquirenti informazioni in merito a reati, poiché in sede di procedimento penale l'imputato potrebbe obiettare che le prove sono state acquisite con misure non previste dal CPP.

Sezioni 1 – 3 (art. 11 – 21)

GE ritiene che i Cantoni dovrebbero beneficiare dei medesimi diritti di precedenza riconosciuti al SIC e di conseguenza sostiene le proposte della CCPCS.

Articolo 11

La *PP1* suggerisce di esaminare, e se del caso di disciplinare nelle disposizioni d'esecuzione, se i «social media» (Facebook, Twitter, XING e simili) debbano essere considerati nella categoria dei «media pubblicamente accessibili» qualora il SIC potesse liberamente accedervi in virtù di una registrazione. Occorrerebbe tuttavia chiedersi se dal punto di vista della politica giuridica la libera analisi delle informazioni raccolte in tale contesto da parte del SIC debba essere permessa senza restrizioni.
Quanto alle registrazioni liberamente accessibili quali quelle di Google Earth, Google Maps o Street View, che in parte verrebbero già oggi utilizzate ad esempio dalle autorità fiscali, la *PP1* si chiede inoltre se e a quali condizioni, in quale misura e per quali scopi il SIC sia autorizzato a farne un uso sistematico per i propri fini, giungendo alla conclusione che sarebbe necessaria perlomeno una giustificazione fondata su considerazioni di politica istituzionale e giuridica.

Lettera b:

CCCZH ravvisa in questa disposizione un nullaosta all'accettazione di dati sotto qualsiasi forma e persino all'impiego di collezioni di dati acquisite al di fuori della legalità. Potrebbe addirittura darsi che vengano ingaggiati privati da impiegare per la raccolta di dati.

Secondo la *PP2*, l'impiego di dati acquisiti illegalmente da privati non deve essere ammesso.

Articolo 12

Capoverso 1:
La *CCPCS* da un lato e *AR, BE, SG, SO, TG* e *ZG* dall'altro segnalano che nel CPP e nelle leggi cantonali sulla polizia più recenti l'osservazione è assoggettata a condizioni e restrizioni ben precise (poiché le attività di osservazione comportano una restrizione dei diritti fondamentali, quantunque anche secondo il Tribunale federale tale restrizione sarebbe soltanto di minima entità se l'osservazione si limita ai luoghi pubblici). Alla luce di questa evoluzione, si dovrebbero ben porre determinate esigenze anche per l'osservazione di intelligence. Alla stregua di quanto previsto dalle leggi sulla polizia (applicate anche nell'ambito della prevenzione delle minacce) un'operazione che dura oltre un certo tempo dovrebbe essere soggetta all'approvazione di un organo superiore. Quest'organo dovrebbe imperativamente essere incluso nel SIC a livello di capodivisione.
BE auspicherebbe inoltre un disciplinamento analogo per le autorità d'esecuzione cantonali.

CCPCS, AR, SG, SO, SZ, TG e *ZG* suggeriscono di inserire nella legge l'impiego di mezzi tecnici per l'osservazione (localizzazione mediante radiogoniometro).

Il *PLR* ritiene che la questione dei droni dovrebbe essere disciplinata in modo distinto, a causa delle possibilità ma anche dei rischi che si celano nelle relative tecnologie.

Per il *PVL*, l'impiego di aeromobili e satelliti va inserito tra le misure soggette ad autorizzazione.

La *PP2* auspica che le attività di osservazione che si protraggono oltre i 30 giorni siano sottoposte ad autorizzazione e che vengano inoltre comunicate agli interessati. Dovrebbe essere sottoposto ad autorizzazione anche l'impiego di droni avente per oggetto persone precise.

Il *Partito Pirata* esprime perplessità riguardo all'espressione «aeromobili», poiché essa ingloba tutto il possibile e l'immaginabile, dagli aviogetti ai droni. Per questo aspetto occorre operare una distinzione tra Svizzera ed estero, poiché l'impiego ad esempio di droni all'estero può essere senz'altro ragionevole, mentre non lo sarebbe in Svizzera (i sequestri di persona rientrano nelle competenze dei Cantoni).

CCCZH sostiene che ci si deve accontentare dell'impiego di strumenti terrestri e che il contribuente non deve comprare giocattoli al SIC.

Capoverso 2:
Secondo la *PP2*, la nozione di sfera privata protetta deve essere precisata.

Per il *Partito Pirata* occorrerebbe sopprimere il secondo periodo: i mezzi la cui applicazione impedisce di proteggere la sfera privata protetta non sono adatti per l'osservazione.

CCCZH chiede che si rinunci in generale a osservazioni nell'ambito della sfera privata, poiché altrimenti il SIC interpreterebbe a modo suo la distinzione tra sfera privata protetta e non protetta.

Articolo 13

Il *Partito Pirata* considera opportune regole più severe in questo campo. L'impiego di fonti umane deve essere assolutamente menzionato all'articolo 22.

La *PP1* suggerisce di esaminare, considerata l'importanza delle informazioni acquisite dal SIC per la sicurezza della Svizzera, se per i collaboratori del SIC e le loro fonti non sia il caso di introdurre a livello di legge un obbligo del segreto particolarmente severo.
Sostiene inoltre che le fonti umane che procurano o comunicano informazioni al SIC devono essere tenute, a loro protezione ma anche come presupposto per l'attività del SIC, al segreto assoluto sui loro contatti con quest'ultimo, come previsto all'articolo 17 capoverso 3 per i servizi della Confederazione e dei Cantoni tenuti a fornire informazioni.

DigGes considera assolutamente necessario prevedere le disposizioni sinora mancanti per garantire che
- ammesso e non concesso che questa misura sia proprio necessaria, che venga impiegata soltanto in caso di gravi minacce;
- la corretta attuazione di questa emanazione del principio della proporzionalità possa essere verificata da un'autorità indipendente;
- l'opinione pubblica sia informata in merito alla frequenza d'impiego di questa misura e degli obiettivi con essa perseguiti nel caso concreto.

In questo punto la legge dovrebbe assolutamente prescrivere una valutazione da parte di un'autorità giudiziaria, in particolare per la concessione dell'esenzione dalle imposte e dai contributi AVS.

Capoverso 1:
Lettera b:
Secondo la *PP2* le prestazioni in questione non devono comprendere attività che al SIC sarebbero vietate.

Capoverso 2:
Il *Partito Pirata* chiede che i mezzi impiegati a questo scopo vengano specialmente menzionati nel budget e ritiene che il SIC debba corrispondere i contributi AVS in forma anonima.

Per quanto possano essere giustificabili, secondo il *PS* le indennità dovrebbero tuttavia rappresentare l'eccezione, essere di modesta entità e non essere mai versate con l'intenzione di esercitare un influsso (corruzione). Inoltre, dovrebbero essere sottoposte annualmente a una verifica da parte della Delegazione delle Commissioni della gestione delle Camere federali DelCG. Il *PS* propone perciò una formulazione restrittiva:
[2] In via eccezionale e in casi ben giustificati, il SIC può indennizzare adeguatamente le fonti umane per la loro attività. …

Secondo *dirittifondamentali.ch*, i *Verdi*, i *GDS* e *SPF* vi sarebbe il rischio che, per scopo di lucro, le fonti possano vendere al SIC indicazioni inventate, o perlomeno gonfiate in contrasto con i fatti. Qualora si volesse comunque prevedere il pagamento, la decisione al riguardo dovrebbe essere riservata a un'autorità giudiziaria. I pagamenti dovrebbero almeno essere assoggettati ai contributi AVS e alle imposte e la DelCG dovrebbe essere informata annualmente in merito ai singoli pagamenti.

GE considera perfettamente giustificati i capoversi 3 e 4.

Articolo 14

NE è del parere che la possibilità di applicare questa misura dovrebbe essere concessa anche ai Cantoni.

Il *Partito Pirata* esige la soppressione di questa disposizione, poiché comporta una grave ingerenza nei diritti della personalità degli interessati. Per lo stesso motivo *DigGes* chiede che si prevedano disposizioni identiche a quelle già contemplate all'articolo 13.

Per evitare che il SIC abusi di questa misura e quindi per impedire una marea di segnalazioni, *dirittifondamentali.ch*, i *Verdi*, i *GDS* e *SPF* esigono una riduzione del catalogo di minacce suscettibili di giustificare l'accertamento della dimora. Tutte le segnalazioni devono inoltre essere sottoposte alla riserva di un'autorità giudiziaria.

La PP1 presume che le situazioni menzionate costituiscano un'enumerazione alternativa e sostiene che l'emanazione di segnalazioni da parte del SIC al fine di tutelare interessi nazionali essenziali debba essere subordinata al rispetto della procedura prevista all'articolo 62.

La PP2 chiede che siano adottate misure affinché chi dovesse consultare il sistema d'informazione non abbia l'impressione che la persona segnalata è sospettata di aver commesso un crimine o un delitto.

Sezione 2: Coperture e identità fittizie (art. 15 – 16)

GE accoglie con favore la possibilità di dotare i collaboratori di una copertura o un'identità fittizia.

Gli articoli 15 e 16 prevedono entrambi l'impiego di collaboratori delle autorità d'esecuzione cantonali sotto copertura per ordine della Confederazione. *CCPCS, AR, SG, SO, SZ, ZG* e

ZH suggeriscono di prevedere in quest'ambito come condizione la necessità del consenso del superiore cantonale del collaboratore interessato, il quale non deve essere esposto a un rischio, che può essere non indifferente, scavalcando completamente il direttore dell'ufficio che ne è responsabile (comandante della polizia).

Articolo 15

A proposito del consenso del superiore cantonale, *ZG* propone il seguente complemento: *«[1] ....L'impiego di collaboratori di un'autorità d'esecuzione cantonale presuppone il consenso del capo dell'autorità cantonale interessata.»*

Il *Partito Pirata* auspica che le identità fittizie possano essere assegnate soltanto ai collaboratori del SIC e non ai collaboratori delle autorità d'esecuzione cantonali.

Articolo 16

Considerata la grave violazione dei diritti della personalità che le identità fittizie comportano, il *Partito Pirata* chiede che esse siano assoggettate all'obbligo dell'autorizzazione e che il numero di identità fittizie assegnate sia pubblicato in un rapporto.

dirittifondamentali.ch, i *Verdi*, i *GDS* e *SPF* si domandano come mai sia già necessaria dopo un tempo così breve (l'entrata in vigore è avvenuta nel luglio 2012) un'estensione di questa disposizione (per es. proroga dopo 5 anni di volta in volta per ulteriori 3 anni, impiego per tutte le concrete «minacce nei confronti della sicurezza interna ed esterna» ai sensi dell'art. 4 cpv. 1, identità fittizie di durata fino a 12 mesi nel contesto di una determinata operazione). In special modo le fonti umane cui si fa capo nel contesto di una determinata operazione tendono a sfuggire rapidamente al controllo se sono provviste di un'identità fittizia. Prima di pensare a un'estensione di questa disposizione, il SIC deve iniziare col rendere conto al Parlamento in merito alla prassi sinora seguita.

Capoverso 2:
CCPCS, *AR*, *SZ*, *UR* e *ZG* approvano che in questa disposizione non sia stata prevista una scadenza assoluta. Al riguardo il testo è però poco chiaro, poiché nonostante l'espressione «di volta in volta» la disposizione può essere compresa nel senso che un'identità fittizia deve essere cancellata al massimo entro otto anni. Il testo del capoverso 2 dovrebbe essere adeguato di conseguenza.

Sezione 3: Diritti e obblighi d'informazione (art. 17 – 21)

CCPCS, AR, BE, SG, SO, SZ, TG, UR e *ZG* fanno osservare che, come già esposto in precedenza, l'avamprogetto non menziona quasi mai esplicitamente le autorità d'esecuzione cantonali tra gli aventi diritto. Nell'ambito dell'obbligo di informazione e comunicazione previsto agli articoli 17 e seguenti, questa circostanza assume un rilievo particolare. Per i collaboratori delle autorità d'esecuzione cantonali, la richiesta di informazioni ad altre autorità fa parte del lavoro quotidiano. Negli ultimi anni, i servizi interpellati hanno chiesto sempre più spesso ai collaboratori in questione di indicare la base legale per il rilascio dei dati richiesti. Occorre pertanto introdurre in tal senso una norma esplicita attributiva di competenza.

Articolo 17

Il *Partito Pirata* chiede che gli obblighi d'informazione siano sottoposti all'approvazione di un'autorità indipendente che si occupi anche di valutare le informazioni pervenute.

CCCZH ritiene che l'effetto destabilizzante esercitato dal SIC sulla pubblica collettività superi quello proveniente dalle gravi minacce menzionate nel rapporto esplicativo.

dirittifondamentali.ch, i *Verdi*, i *GDS* e *SPF* ravvisano in questo articolo un automatismo che sfocia unicamente nell'accumulo di una quantità esorbitante di dati irrilevanti, senza recare alcun vantaggio. Di questo fenomeno si è già avuta più volte dimostrazione in passato.

Capoverso 1:
Per molti Cantoni, la necessità di una richiesta motivata per il rilascio di informazioni manca di pragmatismo. *CCPCS, AR, BE, SO, SG, SO, SZ, TG, UR* e *ZG* chiedono che venga aggiunto un complemento secondo cui le richieste di informazioni devono essere motivate soltanto a posteriori, poiché altrimenti si corre il rischio che la misura fallisca. Inoltre, riguardo alla motivazione non si devono porre esigenze elevate, in particolare poiché spesso i servizi d'esecuzione cantonali non hanno una conoscenza completa dei casi e la rivelazione di informazioni su concrete minacce nei confronti della sicurezza interna o esterna della Svizzera ad autorità terze può rivelarsi un compito estremamente delicato.

SwissBanking chiede di specificare che le banche cantonali non sono considerate servizi del Cantone ai sensi dell'articolo 17 capoverso 1 e quindi non sono assoggettate, o meglio sono escluse, dall'obbligo d'informazione previsto da questa disposizione.

Capoverso 2:
Il *Partito Pirata* vuole che in questo capoverso si rimandi ai compiti di cui all'articolo 4, poiché le lettere a, d ed e se ne discosterebbero a causa della scarsa chiarezza dei termini utilizzati.

dirittifondamentali.ch, i *Verdi*, i *GDS* e *SPF* chiedono la soppressione della lettera e, poiché l'espressione «approvano atti violenti» coprirebbe praticamente qualsiasi cosa possa venir detta anche solo in un'accesa discussione.

Capoverso 3:
AG considera importante che pur prevedendo che i servizi interessati sono tenuti al segreto nei confronti di terzi in merito alla richiesta e alle eventuali informazioni, sia però fatta espressamente salva l'informazione degli organi gerarchici e di vigilanza.

Il *Partito Pirata* chiede che il numero di richieste sia pubblicato in un rapporto annuale.

Articolo 18

Capoverso 1:
La *CCPCS, i Cantoni di AR, BE, SG, SO, SZ, TG, UR* e il *PLR* aggiungerebbero al catalogo delle autorità assoggettate all'obbligo d'informazione e di comunicazione anche i servizi sociali e le autorità fiscali.

CCPCS, BE, SO e *TG* approvano l'inserimento delle autorità competenti per la vigilanza sul mercato finanziario e degli uffici competenti per ricevere comunicazioni concernenti il sospetto riciclaggio di denaro nel catalogo delle autorità assoggettate all'obbligo d'informazione e di comunicazione, poiché tali autorità hanno grande importanza nella lotta al terrorismo.

TG propone di sostituire l'espressione «autorità di polizia, di perseguimento penale e penali» con l'espressione «autorità di polizia, altre autorità penali e autorità inquirenti», poiché secondo il CPP la polizia fa generalmente parte delle autorità penali.

Il *Partito Pirata* desidera che gli obblighi d'informazione siano approvati e valutati da un'autorità indipendente, sia sul piano cantonale quanto su quello nazionale. La cooperazione con le «autorità competenti per l'esercizio di sistemi informatici» deve essere disciplinata in modo specifico.

CCCZH si domanda per quale ragione il SIC debba avere un accesso agevolato ai dati dell'UFM e per quanto concerne gli obblighi d'informazione ritiene che non si debba lasciare mano libera al SIC, a causa dell'enorme rischio di abuso che ne deriva.

DigGes considera indispensabile precisare che nel caso della lettera i l'obbligo d'informazione riguarda soltanto il settore di compiti legato all'esercizio di sistemi informatici, a completa esclusione delle informazioni memorizzate nei sistemi stessi.

dirittifondamentali.ch, i *Verdi*, i *GDS* e *SPF* ravvisano anche in questo articolo un automatismo che sfocia unicamente nell'accumulo di una quantità esorbitante di dati irrilevanti, senza recare alcun vantaggio. La lettera i conferisce al SIC un diritto di consultazione illimitato per tutti gli affari, procedimenti e dati delle autorità comunali, cantonali e nazionali.

Capoverso 2:
Il *Partito Pirata* chiede che il numero di richieste sia pubblicato in un rapporto annuale.

Per *DigGes* l'obbligo generale di serbare il segreto sulle richieste d'informazione e le informazioni rilasciate viola il principio di proporzionalità: dovrebbe valere soltanto nel singolo caso in funzione della situazione concreta e soltanto per un periodo di tempo limitato, ed essere anche ordinato dal giudice. Eventualmente la legge potrebbe prevedere un obbligo del segreto che si estingue automaticamente dopo due settimane salvo decisione del giudice.

Capoverso 3:
Secondo *dirittifondamentali.ch*, i *Verdi*, i *GDS* e *SPF*, questa disposizione costituisce un'ulteriore lettera di franchigia per la denuncia d'ufficio ed essendovi ragione di temere che le autorità messe in tal modo sotto pressione fornirebbero dati personali in modo sconsiderato, la disposizione deve essere soppressa.

Capoverso 4:
Secondo il *Partito Pirata*, giacché l'elenco non è nemmeno pubblico, dovrebbe come minimo essere sottoposto al controllo di un'autorità indipendente.

Secondo *DigGes* il previsto elenco non pubblico viola il principio di trasparenza.

Articolo 19

Capoverso 2:
Il *TAF* espone che, contrariamente al progetto LMSI II, il presente avamprogetto non precisa se la sua decisione sia definitiva. Di conseguenza, non si capisce se si tratta di un caso d'applicazione dell'articolo 36*a* LTAF (nel qual caso la decisione non sarebbe impugnabile) o se si tratta comunque di una decisione in materia di sicurezza interna o esterna (ma anche in questo caso la decisione non sarebbe impugnabile).
Dovendo poi decidere il più rapidamente possibile nell'ambito di una procedura sommaria che dovrebbe essere ancora precisata nelle disposizioni d'esecuzione, il TAF auspica che questo punto sia precisato, nella legge e nel messaggio.

Articolo 20

La *PP1* è dell'opinione che i terzi o le organizzazioni che forniscono informazioni dovrebbero essere tenuti al segreto (analogamente a quanto previsto agli art. 17 e 18). Per loro dovrebbero poter essere adottate anche misure per la protezione delle fonti (nel senso degli art. 13 e 31).

Articolo 21

DigGes suggerisce di esplicitare meglio nel testo di legge che in questo articolo si pensa in primo luogo ai trasporti viaggiatori effettuati a titolo commerciale. In tutti i casi la richiesta dovrebbe essere subordinata al presupposto di un'autorizzazione giudiziaria. Il testo della

legge deve essere completato con una precisa delimitazione della categoria di infrastrutture di sicurezza alle quali si pensa, altrimenti la disposizione sarebbe troppo elastica.
La legge dovrebbe prevedere che prima di richiedere informazioni si debba ottenere un'autorizzazione del giudice. Le persone che fossero sicuramente o molto probabilmente toccate nella loro sfera privata dovrebbero esserne informate perlomeno a posteriori. Il giudice dovrebbe in particolare valutare se i dati auspicati riguardano o in qualche modo interessano manifestazioni di carattere politico o religioso, ed eventualmente se l'accesso alle registrazioni debba essere vincolato a determinate condizioni o del tutto negato. Gli organizzatori delle manifestazioni interessate dovrebbero esserne informati perlomeno a posteriori.

CCCZH vedrebbe volentieri che il debordante catalogo di desiderata del SIC fosse completamente circoscritto.

Capoverso 1:
Il *Partito Pirata* chiede che qualsiasi obbligo d'informazione debba essere confermato da un'autorità indipendente e che vengano indennizzate le spese almeno ai privati. Inoltre, i diritti della personalità di terzi devono essere tutelati e devono essere vietate le registrazioni di manifestazioni a carattere politico.

dirittifondamentali.ch, i *Verdi*, i *GDS* e *SPF* chiedono la soppressione di questa disposizione.

La *PP1* fa notare che il SIC deve essere in grado anche in questo caso di comprovare o rendere verosimile la specifica minaccia concreta alle persone o alle organizzazioni interpellate. Le persone chiamate a informare dovrebbero essere tenute al segreto analogamente a quanto previsto dagli articoli 17 capoverso 3 e 18 capoverso 2, eventualmente per mezzo di una decisione emanata con la comminatoria di una pena ai sensi dell'articolo 292 CP, e dovrebbero poter essere ordinate anche misure per la protezione delle fonti ai sensi dell'articolo 13 capoversi 3–5 e dell'articolo 31.

Lettera b:
La *Swico* deplora che la decisione impugnabile non sia provvista di effetto sospensivo (art. 71 cpv. 3) senza il quale un ricorso del gestore in questo caso interessato sarebbe privo di senso.

La *PP2* teme che la consegna e l'analisi di materiale proveniente da privati possano essere utilizzate per eludere la LSI. I sistemi di videosorveglianza dovrebbero essere installati legalmente e al SIC dovrebbe essere permesso di utilizzare soltanto materiale che avrebbe potuto acquisire anche direttamente. La disposizione andrebbe pertanto precisata in tal senso.

Capoverso 2:
Il *Partito Pirata* chiede che le disposizioni del CPP, più severe, valgano anche per il SIC.

DigGes chiede che vengano escluse le indicazioni di cui all'articolo 14 capoverso 4 LSCPT, altrimenti si precluderebbe ogni possibilità di comunicare in forma riservata mediante Internet. Simili ingerenze nei diritti fondamentali dovrebbero essere ammesse tutt'al più in via eccezionale nel quadro di misure di acquisizione soggette ad autorizzazione.

dirittifondamentali.ch, i *Verdi*, i *GDS* e *SPF* ritengono che non si debba permettere di principio un'ingerenza nel segreto delle telecomunicazioni senza la riserva della decisione di un giudice.

Sezione 4: Misure di acquisizione soggette ad autorizzazione (art. 22 – 38)

La *CCPCS* e i Cantoni di *AR, BE, FR, SO, TG* e *ZG* ritengono che le nuove misure di acquisizione soggette ad autorizzazione siano necessarie e confacenti. Dal punto di vista delle autorità d'esecuzione cantonali emerge un'esigenza di chiarimento da un lato per quanto

riguarda la competenza a ordinare queste misure e dall'altro per quanto riguarda la partecipazione dei Cantoni all'attuazione delle misure ordinate dal SIC.

Procedendo dagli sviluppi geopolitici e tecnici recenti, l'avamprogetto tenta di istituire la possibilità di individuare tempestivamente e se del caso anche di combattere gli sviluppi pericolosi con misure di sorveglianza segrete ma anche con misure di prevenzione. Per *BS* questo tentativo equivale a negare l'affermazione ripetuta a più riprese secondo cui gli strumenti rilevanti sarebbero già forniti dalla procedura penale, poiché i riscontri necessari per un procedimento penale in termini di urgente sospetto giungerebbero spesso troppo tardi e poiché le misure previste nei procedimenti penali non sono destinate primariamente alla limitazione dei danni o alla prevenzione, bensì all'identificazione dei colpevoli e al loro perseguimento.

GE sostiene che tanto la procedura di approvazione a più stadi quanto la procedura in caso di urgenza siano caratterizzate da una sorprendente macchinosità che nuoce all'efficienza. L'avamprogetto dovrebbe essere nuovamente rimaneggiato con l'intento di semplificare ulteriormente le diverse procedure.

SO fa dipendere il consenso alle nuove misure (soggette ad autorizzazione) di acquisizione di informazioni da tre condizioni, già previste nell'attuale progetto legislativo, che ritiene essenziali:
- la considerazione differenziata delle diverse forme di minaccia e dei diversi settori di attività del SIC;
- un elevato grado di specificazione delle norme concernenti i processi di elaborazione dei dati;
- una procedura di approvazione a più stadi.

UR è preoccupato dal fatto che le autorità d'esecuzione più piccole non siano affatto in grado di eseguire le misure di acquisizione soggette ad autorizzazione che verrebbero ordinate.

La *CCPCS* e i Cantoni di *TG* e *ZG* auspicano che le disposizioni degli articoli 22 e seguenti vengano completate concedendo anche alle autorità d'esecuzione cantonali la facoltà di ordinare misure di acquisizione soggette ad autorizzazione.

VD approva l'introduzione delle misure soggette ad autorizzazione a patto che si applichino soltanto in casi particolari e straordinari, ed è lieto di constatare che queste non possano essere applicate a esponenti di partiti politici riconosciuti, quand'anche le loro idee assumessero talvolta tratti già estremistici.

I mezzi di acquisizione oggi disponibili si basano in sostanza sull'acquisizione da fonti pubbliche, sulla richiesta di informazioni e sull'osservazione in luoghi pubblici. Tuttavia, essi non corrispondono più alla realtà attuale e per questa ragione il PPD è d'accordo che, per i settori del terrorismo, dello spionaggio, della proliferazione e degli attacchi a infrastrutture critiche ma anche per la salvaguardia di altri interessi nazionali essenziali, venga introdotta la possibilità di adottare in Svizzera nuove misure per l'acquisizione di informazioni.
La legge dovrebbe comunque essere completata prevedendo che il ricorso a misure di acquisizione soggette ad autorizzazione sia possibile anche nei casi di estremismo violento. In questo campo né la polizia né i servizi informazioni della Confederazione avrebbero allo stato attuale la possibilità di effettuare intercettazioni della corrispondenza telefonica o di posta elettronica a scopo preventivo o in seguito a un'escalation della violenza.
Queste misure rappresentano indiscutibilmente un'ingerenza nei diritti fondamentali. Il PPD approva pertanto che esse soggiacciano a un duplice obbligo di autorizzazione, da parte del Tribunale amministrativo federale e del capo del DDPS, e a severe direttive in materia di protezione dei dati.

L'*UDC* accoglie con soddisfazione l'introduzione di misure di acquisizione soggette ad autorizzazione. Le attività fondamentali oggetto della valutazione delle minacce non si svolgerebbero in luogo pubblico e le nuove misure entrerebbero in considerazione soltanto di rado.

Anzitutto, sorprende che la competenza per l'autorizzazione delle misure non sia attribuita al Tribunale penale federale, che essendo specializzato nel settore sarebbe l'autorità più idonea, ma il fatto che si tratti in primo luogo di un atto amministrativo compiuto da un'autorità federale giustifica comunque la competenza del Tribunale amministrativo federale.

Secondo *AInt*, chi non esercita una funzione pubblica non dovrebbe essere costretto ad accettare che gli organi dello Stato registrino parole, immagini o suoni riguardanti la sua persona. Anche il diritto di agire in luoghi pubblici senza essere sorvegliato dallo Stato rientrerebbe di principio tra i diritti fondamentali garantiti dalla Costituzione. Le misure di acquisizione soggette ad autorizzazione che prevedono l'acquisizione e l'elaborazione di dati in luoghi non pubblici sarebbero ancora più gravose di quelle previste per i luoghi pubblici e andrebbero pertanto qualificate come gravi ingerenze nei diritti riconosciuti dall'articolo 13 Cost. e dall'articolo 8 CEDU.
AInt chiede pertanto che le misure di acquisizione soggette ad autorizzazione siano espunte dall'avamprogetto.

L'*asut* formula in sintesi le seguenti considerazioni:
il potenziamento delle misure soggette ad autorizzazione previste agli articoli 22 e seguenti rappresenta una novità sostanziale. Tra le misure previste, un elemento cardine è costituito dalle misure di sorveglianza nel campo delle telecomunicazioni. Oltre alle misure di sorveglianza previste nell'ambito del perseguimento penale, ora gli offerenti di prestazioni di telecomunicazione sarebbero anche tenuti a eseguire gli ordini di sorveglianza del SIC.
Per l'*asut* è essenziale che l'onere rappresentato da questi ordini di sorveglianza supplementari si mantenga entro limiti ragionevoli e sostenibili. Al riguardo si fa osservare che la Confederazione non rifonde integralmente agli offerenti di prestazioni di telecomunicazioni le spese da loro incorse per le misure di sorveglianza, ma corrisponde loro soltanto un'indennità appropriata. Il Consiglio federale intende mantenere questo principio anche nell'ambito della revisione della LSCPT.
Nel rapporto si ipotizza che le misure di sorveglianza ordinate dal SIC saranno applicate soltanto in un numero esiguo di casi, stimato attorno alla decina di casi l'anno, ossia una percentuale di poco conto rispetto alle misure di sorveglianza ordinate nell'ambito del perseguimento penale.
Accanto al discorso puramente quantitativo, è però essenziale che nella LSI non si prevedano misure che vadano al di là di quelle previste dalla LSCPT. Riguardo alle possibilità di sorveglianza, la LSI dovrebbe attenersi totalmente alla LSCPT, o meglio rimandare semplicemente a quest'ultima. Non si vedono del resto ragioni oggettive che giustifichino una deroga a questo principio. Altrimenti si rischia che fondandosi sul testo divergente della LSI il SIC possa pretendere dal Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT), e quindi dagli offerenti di prestazioni di telecomunicazione**,** prestazioni diverse o addirittura più estese rispetto a quelle previste nella LSCPT. Occorre evitare che gli obblighi cui sottostanno gli offerenti di prestazioni di telecomunicazione nel campo della sorveglianza del traffico delle telecomunicazioni vengano estesi attraverso la LSI.
Con queste premesse, l'*asut* chiede che nella LSI si rinunci a una formulazione autonoma delle possibili misure di sorveglianza del traffico delle telecomunicazioni e che l'articolo 22 capoverso 1 lettere a-d sia depennato e sostituito esclusivamente con un rimando esplicito alle misure di acquisizione e di sorveglianza previste dalla LSCPT. Nella sezione 4 dell'avamprogetto, inoltre, occorrerebbe introdurre un'indicazione di ordine generale secondo cui le misure di sorveglianza nel campo del traffico delle telecomunicazioni vengono eseguite per il tramite del Servizio SCPT e conformandosi alle direttive e ai processi previsti dalla LSCPT.
L'*asut* rileva infine che anche la misura di acquisizione contemplata alla lettera g è molto vaga e quindi in definitiva formulata in modo oscuro. Le espressioni «sistema di ordinatori» e «rete di ordinatori» potrebbero ad esempio comprendere, se interpretate in senso lato, anche interi sistemi di posta elettronica, interi servizi Cloud o interi sistemi di trasferimento connessi a Internet. Tuttavia, sarebbe esagerato consentire al SIC di introdursi in simili sistemi e reti. Pertanto la disposizione va precisata nel senso che le possibilità di intervento previste ai

numeri 1 e 2 si limitano all'ambito strettamente privato (vale a dire a sistemi e reti di ordinatori di precisi «utenti finali»). Occorrerebbe inoltre garantire e stabilire che queste misure non devono disturbare gli utenti estranei. Per simili perturbazioni delle prestazioni, gli offerenti di prestazioni di telecomunicazione non potrebbero fornire spiegazioni soddisfacenti ai clienti interessati.

Per il *CCCZH*, in questa sezione si evidenzia la smania di controllo che caratterizza il SIC. Gli organi competenti per il rilascio dell'autorizzazione non sarebbero difficili da convincere e mancando delle conoscenze indispensabili non sarebbero comunque in grado di valutare la necessità di una misura.

Centre Patronal e *CVAM* non riescono a immaginare che un servizio informazioni possa adempiere i propri compiti senza disporre di mezzi di intelligence e sono convinti che tutti gli Stati ricorrano a simili mezzi. Pertanto non vi sarebbe nulla da eccepire al loro disciplinamento nella legge, dato che il controllo giudiziario e politico al quale soggiacciono garantisce sufficiente protezione da un abuso.
Centre Patronal e *CVAM* capiscono e accolgono con soddisfazione la soppressione della distinzione tra minacce per la sicurezza interna ed esterna. Ritengono invece dubbia la differenziazione introdotta tra estremismo violento e altre minacce. L'unico motivo che potrebbe giustificare tale differenziazione può essere colto nell'intenzione di proteggere meglio la sfera privata nel campo dell'estremismo violento per evitare di riaccendere la polemica sull'affare delle schedature. Per le due organizzazioni, si tratta di una motivazione piuttosto debole, soprattutto in considerazione della crescente difficoltà che la distinzione tra estremismo violento e terrorismo comporta.

economiesuisse constata che le definizioni non combaciano con quelle previste dalle basi legali determinanti in materia di polizia, ma si spingono oltre. Questo aspetto costituirebbe un errore. Tanto le competenze quanto le procedure dovrebbero essere strutturate come nella LSCPT. I costi che le misure di sorveglianza occasionano a terzi dovrebbero essere integralmente rifusi, ad inclusione dei costi di apprestamento. Ma lo Stato dovrebbe assumersi integralmente anche le conseguenze in caso di eventuali danni. Tali conseguenze comprendono in particolare i costi indiretti della perturbazione o del rallentamento di sistemi informatici. Potrebbe certamente trattarsi di una necessità in caso di pericolo nel ritardo, ad esempio per proteggere infrastrutture critiche, ma potrebbero comunque verificarsi anche errori di valutazione.

La *PP1* fa osservare che le misure di cui all'articolo 22 capoverso 1 lettera g numero 1 possono rischiare di perturbare l'esercizio dei sistemi e delle reti interessati o causare l'alterazione o la cancellazione di dati e provocare altre conseguenze analoghe. La LSI dovrebbe prevedere per questi rischi, come del resto per tutti gli altri casi in cui l'attività di organi del SIC provoca danni a terze persone, una norma speciale che disciplini la responsabilità della Confederazione.
La *PP1* lamenta inoltre la mancanza, nel rapporto esplicativo, di un commento che spieghi l'esclusione dell'estremismo violento dal novero dei motivi che consentono l'adozione di misure di acquisizione soggette ad autorizzazione.
Dato che tra i casi d'applicazione giustificanti l'adozione di misure soggette ad autorizzazione e nella definizione alquanto generica e non esaustiva di cui all'articolo 1 capoverso 3 figura anche la «tutela di altri interessi nazionali essenziali», e che tali misure comportano un'ingerenza particolarmente profonda nella posizione giuridica costituzionalmente protetta degli interessati, è importante in questi casi che il Consiglio federale conceda anticipatamente l'autorizzazione prevista all'articolo 62. L'iscrizione di un'organizzazione nella «lista d'osservazione» di cui all'articolo 63 non deve bastare per ordinare una misura di acquisizione soggetta ad autorizzazione.
La *PP1* fa inoltre presente che nei casi in cui deve essere rispettata la procedura di autorizzazione, la decisione concernente lo svolgimento della procedura è presa a entrambi i livelli da singoli individui, i quali dipendono dalla documentazione e dalle informazioni presentate dal SIC. Una verifica perfettamente sicura della richiesta non è dunque garantita, ma consi-

derata la necessità di rispettare la natura confidenziale della procedura, non sarebbe appunto possibile emanare ordini qualificati. In pratica, a causa del principio del segreto, il rimedio del ricorso al TAF è offerto soltanto alle terze persone.
Se un terzo ai sensi dell'articolo 24 viene sottoposto a una misura di acquisizione soggetta ad autorizzazione, occorre la garanzia che tutti i documenti e le informazioni che non hanno alcun nesso con lo scopo della misura vengano subito separati e quanto prima distrutti. Tale garanzia potrebbe essere data introducendo una disposizione analoga a quella già prevista all'articolo 33 capoverso 6 per quanto concerne l'esplorazione radio.
La *PP1* è sorpresa dal fatto che per la procedura di autorizzazione prevista all'articolo 25 capoverso 1 non si esiga espressamente che la richiesta al TAF contenga indicazioni sull'esistenza di una concreta situazione di minaccia che giustifichi la misura soggetta ad autorizzazione.
La *PP1* constata con soddisfazione che, grazie alla proposta aggiunta all'articolo 3 capoverso 1 lettera a numero 7 (nuovo) LTras, i documenti relativi alla procedura di autorizzazione sono esclusi dal diritto di accesso a documenti ufficiali. A suo parere, l'articolo 29 dovrebbe essere completato con l'aggiunta di una disposizione secondo cui, in particolare nei confronti di terze persone coinvolte nelle misure di acquisizione, la comunicazione in caso di differimento autorizzato in virtù dell'articolo 29 capoverso 3 debba seguire senza indugio quando i motivi addotti per giustificare il differimento della comunicazione o la rinuncia alla medesima fossero venuti a cadere. A tal fine, sui dati provenienti da misure di acquisizione soggette ad autorizzazione e memorizzati separatamente secondo l'articolo 53 dovrebbe essere effettuata annualmente una verifica concernente l'adempimento dell'obbligo di comunicazione, ad esempio nell'ambito di un controllo della qualità ai sensi dell'articolo 40 capoverso 4.

Secondo la *PP2*, l'avamprogetto non deve introdurre misure di sorveglianza preventive, alle quali il legislatore si è già opposto in occasione della revisione della LMSI. Nel commento non si attesta il motivo per cui queste misure sarebbero ora maggiormente necessarie, e la *PP2* ritiene anzi che dovrebbero piuttosto essere applicate soltanto molto di rado. Nonostante tutte le garanzie teoriche, il rischio di abusi è molto elevato. Concretamente, le persone interessate non verrebbero mai informate sulle misure eseguite, poiché sarebbe praticamente impossibile verificare a posteriori se la rinuncia alla comunicazione fosse davvero giustificata. La nozione di minaccia concreta è molto difficile da valutare ed è sempre condizionata anche da influssi esterni che il SIC potrebbe successivamente comunicare oppure no, a seconda della convenienza.
La *PP2* fa presente che il CP contiene una lista dei reati per i quali è prevista la punibilità anche a livello di atti preparatori. In uno Stato democratico, dovrebbero essere perseguiti soltanto per atti precedentemente definiti, e soltanto questi atti dovrebbero poter comportare una misura di sorveglianza. Oltretutto queste misure dovrebbero essere applicate soltanto nei confronti di persone alle quali viene addebitato un reato. Altrimenti non vi sarebbero più ostacoli a una sorveglianza totale e permanente dei cittadini. Del resto, una competenza cantonale in questa materia sarebbe problematica, poiché altrimenti i Cantoni potrebbero applicare disposizioni che derogano al diritto federale.

Privatim si chiede se la legalizzazione di un «software di governo» a scopo preventivo possa mai essere proporzionale, data l'enorme ingerenza che esso comporta nelle libertà dei cittadini. Sembra difficile immaginare quali sospetti che non siano già coperti dalle procedure preliminari previste nell'ambito del perseguimento penale possano giustificare il ricorso a simili strumenti. Se la necessità di questi strumenti fosse comunque ammessa, occorrerebbe garantire ai cittadini la certezza del diritto e che l'essenza delle libertà in questione non venga intaccata nell'ambito dell'impiego di simili strumenti.
Questo problema si rende particolarmente evidente in rapporto con l'intrusione in sistemi e reti di ordinatori. Dato che secondo l'articolo 24 si possono concepire misure di acquisizione anche nei confronti di terze persone, potrebbero essere esposte a un «operazione di hacking statale» persino persone che non hanno la minima velleità terroristica. Corrispondentemente elevate dovrebbero essere le esigenze poste, non solo per quanto riguarda la base legale ma anche per quanto attiene alla procedura di autorizzazione. Le pertinenti disposizioni sono

formulate con sufficiente concretezza, ma il rapporto esplicativo manca in quest'ambito della necessaria nitidezza.
Dal punto di vista dello Stato di diritto, è imperativamente necessario che la richiesta presentata al TAF contenga non solo indicazioni particolareggiate sullo scopo della misura di acquisizione e sulle persone da essa toccate, ma deve specificare con la massima precisione possibile anche le informazioni che si vogliono ottenere con l'intrusione, rispettivamente a quali informazioni si vuole impedire, rallentare o disturbare l'accesso.

RefLMSI si oppone decisamente a una sorveglianza preventiva in assenza di motivi di sospetto.

L'*USAM* deplora che al SIC si intenda ora permettere tutto quanto è già permesso alle autorità inquirenti in caso di fondato sospetto e con l'approvazione del giudice. Le competenze del SIC verrebbero comunque estese e non obbligatoriamente collegate a una decisione dell'autorità giudiziaria.
Riguardo alla sorveglianza del traffico delle telecomunicazioni, l'*USAM* osserva che la «conservazione dei dati relativi alle telecomunicazioni» è stata sinora considerata anticostituzionale da tutte le corti costituzionali dei Paesi europei che sono state chiamate a giudicare la questione. Ad aggravare ulteriormente la situazione concorre il fatto che con la revisione della LSCPT è prevista l'estensione da sei a dodici mesi della durata prevista per l'obbligo di conservazione dei dati relativi alla fatturazione e ai collegamenti. Il Tribunale federale permette inoltre l'accesso a dati che risalgono a un periodo di gran lunga anteriore ai sei mesi previsti dalla legge.
I privati che gestiscono infrastrutture di sicurezza potrebbero ora essere obbligati a produrre registrazioni. In tal modo si ingloba anche un numero imprecisato di terzi estranei ai fatti, che personalmente non dispongono di alcun rimedio giuridico per difendersi.
Alcune delle misure di sorveglianza previste invadono in misura davvero eccessiva la sfera intima delle persone, per poterle concedere a un servizio informazioni clandestino che agisce preventivamente.
Con la revisione della LSCPT, l'intrusione in sistemi e reti di ordinatori sarà consentita anche alle autorità inquirenti, ma soltanto per intercettare e desumere il contenuto di una comunicazione e i dati marginali del traffico delle telecomunicazioni in forma decifrata. Il presente avamprogetto prevede però che il SIC può introdursi in un sistema di ordinatori e acquisire e utilizzare tutte le informazioni in esso disponibili. In teoria, questa facoltà permette anche di manipolare i dati. Per installare via Internet un «cavallo di Troia» (trojan) su un computer, il SIC deve collaborare con il fornitore di servizi Internet della persona intercettata. Una simile abilitazione a perpetrare attacchi informatici è incomprensibile e pericolosa.
Contrariamente alle perquisizioni operate dalle autorità inquirenti, le perquisizioni di locali da parte di collaboratori del SIC sarebbero eseguite di nascosto. Le persone interessate non avrebbero la possibilità di esigere l'apposizione di sigilli o di assistere al visionamento della documentazione sequestrata.
Per queste ragioni, per il fatto che i compiti di polizia devono essere di principio separati dai compiti del servizio informazioni e a causa del previsto amalgama tra attività di protezione dello Stato e procedura penale, l'*USAM* si oppone categoricamente a questa misura di acquisizione.
L'*USAM* è contrario anche alla procedura a due stadi, poiché è impossibile concepire il Consiglio federale come ostacolo, dato che il SIC è appunto uno dei suoi strumenti.

SwissBanking approva con soddisfazione in particolare il fatto che rispetto al vigente ordinamento giuridico l'arsenale a disposizione nel campo delle misure di acquisizione soggette ad autorizzazione venga ampliato. Le competenze in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, le misure tecniche di sorveglianza in generale e in particolare anche l'esplicita menzione dell'intrusione in sistemi e reti di ordinatori sarebbero l'imperativo del momento. Considerata la crescente aggressività degli attori statali e dei loro gregari, constatata negli ultimi anni nella ricerca di informazioni finanziarie, e il pericolo al quale sono esposti gli interessi economici nazionali a causa degli attacchi mossi alla piazza finanziaria, è necessario adottare con urgenza e determinazione contromisure nel

campo dello spionaggio non solo a livello di perseguimento penale, bensì già anticipatamente e a titolo preventivo.

Swisscom chiede una correzione dell'obbligo di indennizzo, che giudica gravemente insufficiente, per gli oneri assunti dagli offerenti di prestazioni di telecomunicazione. Secondo il rapporto del Consiglio federale, le misure di sorveglianza attuate per il servizio informazioni forniscono un contributo sostanziale alla sicurezza della Svizzera e quindi alla protezione della collettività, la quale è pertanto tenuta anche ad assumersene i costi.

Articolo 22

SG si interroga sul senso delle divergenze del testo rispetto alle disposizioni del CPP sulla sorveglianza del traffico delle telecomunicazioni.

I *Verdi* lamentano il fatto che il Consiglio federale non fornisce alcuna spiegazione plausibile sul motivo che impedisce di comprendere la decina di casi l'anno previsti nelle facoltà d'indagine sinora esercitate.

DigGes ravvisa in questa disposizione una palese violazione dei principi fondamentali dello Stato di diritto:
- nella misura in cui non sono strettamente necessarie per il mantenimento dell'ordinamento democratico della Svizzera, le misure proposte vanno respinte, non fosse che per ragioni legate al rispetto dei diritti dell'uomo;
- se però queste misure fossero davvero necessarie, le persone interessate dovrebbero perlomeno essere informate a posteriori non solo in merito alla sorveglianza esercitata, ma anche sulle misure concretamente applicate. Qualora le misure risultassero ingiustificate, le persone interessate dovrebbero aver diritto a un indennizzo.

Secondo *dirittifondamentali.ch*, i *Verdi*, i *GDS* e *SPF*, è assolutamente esagerato che al SIC si intenda ora permettere tutto quanto è già permesso alle autorità inquirenti in caso di fondato sospetto e con l'approvazione del giudice, oltretutto con competenze più estese. Essi fanno presente che la «conservazione dei dati relativi alle telecomunicazioni» è stata sinora considerata anticostituzionale da tutte le corti costituzionali dei Paesi europei che sono state chiamate a giudicare la questione.
Volendo a tutti i costi discutere di questo punto, occorrerebbe piuttosto porre dei limiti alle autorità inquirenti, e certamente non estendere i diritti del SIC.
Per queste ragioni in particolare, per il fatto che polizia e servizi segreti vanno tenuti separati e a causa del previsto amalgama tra attività di protezione dello Stato e procedura penale, queste misure di acquisizione a favore del SIC vengono categoricamente respinte.

La *Swico* considera enorme il rischio di abusi legato ai «cavalli di Troia statali». Sarebbe altamente improbabile che la procedura di autorizzazione possa svolgere una «funzione di filtro». Questo genere di ingerenza nelle comunicazioni tra privati non avrebbe alcuna giustificazione.

La *PP2* e *Swisscom* lamentano che la terminologia del SIC diverga senza alcun motivo da quella del CPP, mentre una corrispondenza tra i due atti normativi sarebbe più importante che mai dal momento che entrambi fanno riferimento alla LSCPT.

<u>Capoverso 1:</u>
Lettera g:
BS è del parere che nel messaggio dovranno essere discusse le gravi ingerenze nei diritti fondamentali che questa misura di acquisizione comporta, si dovranno porre esigenze più elevate all'obbligo di motivazione della richiesta di adozione di misure di acquisizione e dovrà essere definito un criterio più severo per l'esame nell'ambito della procedura di autorizzazione. Occorrerà inoltre menzionare che la maggior parte dei Cantoni non sarà praticamente in

grado, con le risorse di personale e i mezzi tecnici di cui dispone, di eseguire anche solo in parte i relativi ordini del SIC.

TI auspica, viste le gravi ingerenze nei diritti fondamentali che questa misura di acquisizione comporta, che nel messaggio si precisi che essa può essere applicata soltanto per gravi e importanti ragioni; ammette tuttavia che questo strumento di acquisizione di informazioni è fondamentale per la lotta alle moderne forme di criminalità e in tal senso il suo impiego non deve essere ostacolato da eccessive formalità.

ZH non può dare il suo avallo al fatto che alla lettera g si attribuisca al SIC la competenza di manipolare computer e copiare dati memorizzati, neppure se tale competenza è subordinata alla necessità di un'autorizzazione da parte del TAF e del capo del DDPS. In tal modo si conferirebbero al SIC maggiori diritti, e al di fuori di qualsiasi procedimento penale, di quanti ne abbiano la polizia e il pubblico ministero nell'ambito di un'inchiesta.

Per l'*OVPD TG* questa disposizione sarebbe problematica dal punto di vista della legislazione sulla protezione dei dati. Sotto il profilo dello Stato di diritto, l'impiego di trojan sarebbe fonte di gravi preoccupazioni, poiché non consentirebbe più di garantire la necessaria stretta separazione tra comunicazioni intercettabili e la cosiddetta sfera privata digitale.
Oggi esistono già trojan in grado addirittura di essere telecomandati, per mezzo dei quali è possibile caricare ed eseguire altro software dannoso. Un trojan è ad esempio in grado non solo di cercare i dati disponibili nei supporti di memoria, ma addirittura di manipolare qualsiasi tipo di dati personali o persino di infiltrarvi altri dati, e di accedere al microfono, alla telecamera o alla tastiera di un computer, di un tablet o di un cellulare.
Questo spazio giuridico si sottrae di fatto a qualsiasi limitazione e controllo. Se viene impiegato su un sistema altrui, un trojan è necessariamente incapace di distinguere quali dati appartengono alla sfera protetta dei diritti della personalità della persona interessata e quali elementi possano giuridicamente essere oggetto di sorveglianza. Di conseguenza, l'impiego di trojan rende impossibile un controllo effettivo della sorveglianza e in definitiva la sorveglianza onnicomprensiva incide in modo estremamente pesante sui diritti fondamentali degli interessati.
L'impiego di trojan renderebbe completamente illusorie le seguenti disposizioni:
articolo 3 capoverso 5, articolo 1 capoverso 2 lettera a, articolo 3 capoverso 2 lettera b, articolo 3 capoverso 7, articolo 10 capoverso 1 lettera e, articolo 20 capoverso 3, articolo 24 capoverso 2, articolo 28, articolo 34 capoverso 2.
Pertanto, l'articolo 22 capoverso 1 lettera g deve essere necessariamente soppresso.

Il PPD si domanda come avverrebbe l'attuazione qualora il computer interessato risultasse ubicato all'estero.

Il *PS* accoglie favorevolmente il catalogo limitativo ed esaustivo delle operazioni soggette ad autorizzazione e reputa adeguata la procedura a più stadi con l'intervento del TAF e del capo del DDPS, la quale garantisce un doppio controllo, giudiziario e politico.
Solleva però qualche interrogativo l'articolo 22 capoverso 1 lettera g numero 2, in virtù del quale su richiesta motivata il SIC potrebbe essere autorizzato a introdursi in sistemi e reti di ordinatori altrui non solo per cercarvi informazioni ma anche per disturbare attivamente l'accesso a tali reti e sistemi. Per il *PS* è fondamentale che queste operazioni si limitino realmente ai casi in cui questi sistemi e reti di ordinatori «sono utilizzati per attacchi a infrastrutture critiche», come del resto precisato. Nella sua legge sul servizio informazioni la Svizzera non deve dare l'impressione di poter distruggere sistemi di ordinatori altrui sulla scorta di semplici sospetti. Queste operazioni dovrebbero dunque essere possibili soltanto nei casi in cui sia comprovata l'esistenza di un attacco. Il *PS* propone perciò di introdurre al numero 2 il seguente chiarimento:
[2] … se i sistemi e le reti di ordinatori sono <u>comprovatamente</u> utilizzati per attacchi a infrastrutture critiche.

Il *Partito Pirata* chiede la soppressione di questa disposizione.

Lettera h:
Il *Partito Pirata* chiede che la disposizione sia precisata, poiché sarebbe formulata in modo estremamente ampio.

Capoverso 2:
Il *Partito Pirata* chiede che le persone interessate vengano informate se i sospetti non trovano conferma.

Articolo 23

Secondo l'*asut*, il meccanismo decisionale deve distinguere tra la questione di sapere se in un determinato caso possono di per sé essere ordinate misure di sorveglianza e la questione delle misure o attività di sorveglianza concretamente possibili da chiedere all'offerente di prestazioni di telecomunicazioni. Detto meccanismo presenta le stesse pecche già osservabili nella LSCPT:
le autorità menzionate verificherebbero soltanto globalmente se nell'ottica della politica di sicurezza entra di principio in considerazione nella fattispecie una sorveglianza del traffico delle telecomunicazioni di una persona da sorvegliare. Non verificherebbero però se dal punto di vista del diritto amministrativo un offerente di prestazioni di telecomunicazioni può essere obbligato ad attuare una ben precisa misura tecnica di sorveglianza, magari addirittura una misura di nuovissima concezione. Quest'ultimo punto dovrebbe essere verificato di volta in volta perlomeno da un'autorità amministrativa, per esempio dal Servizio SCPT, su richiesta di un offerente di prestazioni di telecomunicazione tenuto ad attuare una misura. Ma è proprio questa verifica che il previsto articolo 13 lettera a D-LSCPT escluderebbe.
All'offerente di prestazioni di telecomunicazione verrebbe invece semplicemente imposto di eseguire la sorveglianza autorizzata, quindi anche nel caso in cui le corrispondenti forme di sorveglianza non corrispondono all'elenco degli obblighi definito per l'offerente dal diritto amministrativo. In tal modo l'offerente di prestazioni di telecomunicazioni rischia di trovarsi confrontato a sempre maggiori pretese e di essere oltretutto esposto unilateralmente ai costi che ne derivano.
Va inoltre segnalata la seguente incongruenza: secondo la LSI, il TAF entra in gioco due volte contemporaneamente, ma in ruoli completamente diversi. Anzitutto è chiamato a controllare se dal punto di vista della politica di sicurezza una misura di sorveglianza risulta indicata e proporzionale in una concreta fattispecie. In tale contesto non verifica se l'offerente di prestazioni di telecomunicazioni deve di principio eseguire una ben precisa misura. Come detto, tale verifica non può nemmeno essere effettuata dal Servizio SCPT, al quale spetterebbe oggettivamente questo compito. Se la misura autorizzata dal TAF, e ordinata «alla cieca» dal Servizio SCPT all'offerente, risulta per quest'ultimo insostenibile o addirittura inammissibile dal punto di vista del diritto amministrativo, all'offerente in questione rimarrà ormai soltanto la possibilità del ricorso al TAF. Ma evidentemente è estremamente incerto che a quel punto il TAF sia ancora disposto a riesaminare sotto altra luce una misura che aveva già direttamente autorizzato.
Infine, non è neppure chiaro se questa procedura di ricorso sarà retta dall'articolo 71 oppure dalle disposizioni della LSCPT (sinora l'OSCPT prevede un simile diritto di ricorso, in futuro all'art. 42 D-LSCPT verrebbe introdotta una disposizione analoga all'art. 71 LSI, ma non perfettamente identica).
In sostanza, i problemi evidenziati nel difettoso meccanismo decisionale dovrebbero essere nuovamente affrontati in modo coordinato con la revisione della LSCPT.

Il *Partito Pirata* chiede che il tipo e il numero delle misure autorizzate venga rilevato e pubblicato annualmente.

AInt esprime un giudizio favorevole, dal punto di vista del principio della proporzionalità, riguardo all'obbligo di duplice autorizzazione (da parte del TAF e del capo del DDPS) previsto per le misure nonché al criterio cumulativo della gravità della minaccia e della condizione secondo cui gli accertamenti informativi condotti fino a quel momento devono essere rimasti

senza esito oppure sarebbero comunque vani o sproporzionatamente difficili. In ultima analisi, tuttavia, le autorità di applicazione potrebbero comunque decidere in base al proprio apprezzamento se ordinare misure di acquisizione soggette ad autorizzazione e appunto questo esteso margine d'apprezzamento risulterebbe problematico sotto il profilo dei diritti fondamentali.
Quanto agli altri interessi nazionali essenziali (che in questa disposizione legittimano anch'essi gravi ingerenze nei diritti fondamentali), mancherebbe la definizione dei beni protetti preconizzata dal professor Biaggini nella propria perizia in nome del principio di determinazione.
Dal punto di vista dei diritti fondamentali, *AInt* critica inoltre la procedura in caso d'urgenza, poiché essa consente una sorveglianza senza autorizzazione giudiziaria. Non si capisce quando inizia a decorrere il termine di tre giorni, né quando ci si trova in un caso d'urgenza.

Capoverso 1:
Lettera a:
SZ, *UR* e *ZG* criticano l'esplicita esclusione dell'impiego di misure di acquisizione soggette ad autorizzazione nel caso dell'estremismo violento. Se l'esclusione può essere giustificata da considerazioni di natura politica, risulta però indifendibile dal punto di vista della polizia e del servizio informazioni. La ricerca di informazioni risulta estremamente difficile precisamente in questo campo. Il comportamento cospiratorio, da cui deriva l'impossibilità effettiva di gestire le fonti, impedisce l'acquisizione tempestiva e completa di informazioni. Per di più, negli ambienti dell'estremismo di destra si evidenzierebbero collegamenti internazionali. La radicalizzazione di alcune fazioni nel campo degli estremismi di destra e di sinistra o i movimenti islamici radicali implicherebbero un notevole potenziale di violenza. Se si vuole individuare precocemente tale potenziale e soffocarlo con misure preventive, si impone urgentemente il ricorso agli strumenti di intelligence soggetti ad autorizzazione anche in questo ambito tematico.
L'articolo 23 capoverso 1 lettera a deve pertanto essere modificato come segue:
*«sussiste una minaccia concreta ai sensi dell'articolo 17 capoverso 2 lettere a-**e** oppure lo richiede la tutela di altri interessi nazionali essenziali (art. 62);»*

Secondo il *CCCZH*, gli «interessi nazionali essenziali» sono soltanto un altro modo di esprimere la nozione di «spionaggio industriale o economico».

Lettera c:
Per il *Partito Pirata* questo presupposto non serve ad altro se non a semplificare il compito di giustificare le misure soggette ad autorizzazione.

Capoverso 2:
L'*Università di Ginevra* fa presenti i numerosi motivi a favore di una competenza del Tribunale penale federale: esso dispone già di esperienza nel campo in questione, e pertanto conviene approfittarne garantendo così oltretutto anche una certa coerenza nell'applicazione dei provvedimenti coercitivi. Spesso tali provvedimenti servono infatti a chiarire trame di rilevanza penale. Infine, il Tribunale penale federale interviene non di rado nella procedura amministrativa. Queste considerazioni si applicano anche all'articolo 71.

Il *CCCZH* si dichiara diffidente rispetto al fatto che le misure devono essere approvate dal Consiglio federale.

Capoverso 3:
La *PP2* auspica che la disposizione sia precisata nel senso che il capo del DDPS deve rilasciare personalmente il nullaosta (esclusione della delega).

Per il *CCCZH* questo approccio «dal vertice alla base» («top down») costringe altre autorità federali a collaborare mettendole così nei pasticci.

Articolo 24

AInt, il *Partito Pirata* e il *CCCZH* ravvisano in questo articolo un fondamento che consente al SIC di invadere la sfera privata di terzi (tra cui familiari, datori di lavoro, collaboratori) che non si sono resi colpevoli di alcun reato.

AInt fa presente che le misure adottate nei confronti di terze persone violano il principio della responsabilità del perturbatore, consacrato dal diritto in materia di polizia, ma riconosce nel contempo che con l'adeguamento al CPP le disposizioni concernenti i reperti casuali e il segreto professionale di terzi sono ora accettabili.

Il *Partito Pirata* propone di sopprimere l'articolo, che considera inaccettabile.

Capoverso 2:
SwissBanking esige che gli obblighi derivanti dal segreto professionale degli operatori finanziari vengano espressamente esclusi dal campo d'applicazione delle misure di acquisizione delle informazioni nei confronti di terze persone. Il rimando al CPP contemplato all'articolo 24 capoverso 2 non sarebbe sufficiente.

Articolo 25 e seguenti

SZ considera complicata la procedura di autorizzazione. Nella prassi occorre presumere che il capo del DDPS venga informato anticipatamente dal SIC già prima della presentazione della richiesta relativa alla misura di acquisizione. Se la richiesta non è politicamente condivisa, nemmeno dalla Delegazione Sicurezza, la procedura di autorizzazione deve concludersi già a questo stadio. Non ha senso far intervenire una decisione del TAF se poi manca la volontà politica necessaria per l'attuazione. In questo senso, il controllo politico deve essere effettuato a monte della procedura di autorizzazione dinanzi al TAF, per non causare a quest'ultimo un inutile lavoro supplementare.

Secondo la *CAIS* la procedura di autorizzazione è invece adeguata.

I *Verdi* criticano il mescolamento di valutazione giudiziaria e controllo politico e la mancanza di una norma che imponga al SIC di mettere gli atti a disposizione del TAF.

Il *TAF* auspica che le disposizioni concernenti la procedura di autorizzazione vengano precisati specificando se i termini sono intesi in giorni lavorativi o in giorni civili.
Peraltro, la LTAF non prevede sinora procedure di autorizzazione simili a quella introdotta dall'avamprogetto. Riguardo alla costituzionalità delle disposizioni processuali, il rapporto esplicativo non risponde agli interrogativi sollevati in proposito dal professor Biaggini. Sarebbe auspicabile che il commento fosse completato su questo punto.

DigGes lamenta la mancanza in questo sede di una garanzia che assicuri una difesa efficace dell'interesse alla tutela della sfera privata. Chiede inoltre la pubblicazione di statistiche che documentino perlomeno il numero di richieste, il numero di richieste integralmente approvate, parzialmente respinte o integralmente respinte, il numero di richieste ritirate e la media di ore di lavoro che la valutazione delle richieste ha comportato per i giudici.

Per *dirittifondamentali.ch*, i *Verdi*, i *GDS* e la *SPF* la disposizione proposta viola il principio della separazione dei poteri. L'autorità di ricorso del TAF non è il Consiglio federale bensì il Tribunale federale. Inoltre, per le misure di acquisizione soggette ad autorizzazione che avessero per oggetto un'organizzazione o una persona figurante nella lista d'osservazione, il Consiglio federale sarebbe al tempo stesso richiedente e autorità di approvazione. Oltretutto, i giudici tenderebbero ad accogliere tutte le richieste, supponendo eventualmente che il Con-

siglio federale effettui poi accuratamente i necessari controlli, e viceversa. In ogni caso, la disposizione non garantisce una protezione efficace contro le autorizzazioni di misure di acquisizione contrarie al principio di proporzionalità.
Per le misure di acquisizione soggette ad autorizzazione richieste dal SIC a prescindere dall'esistenza di sospetti occorre prevedere uno scoglio più elevato rispetto a misure comparabili previste dalla procedura penale: lo stesso articolo 197 capoverso 3 CPP esige che i provvedimenti coercitivi che incidono sui diritti fondamentali di chi non è imputato siano adottati con particolare cautela. *dirittifondamentali.ch*, i *Verdi*, i *GDS* e la *SPF* propongono una disposizione analoga al disciplinamento previsto per la cernita sotto la direzione di un giudice di documenti sigillati di persone legate dal segreto professionale. Al SIC possono essere forniti soltanto i dati che presentano un nesso con lo scopo indicato nella richiesta di autorizzazione della misura di acquisizione.

Articolo 25

Capoverso 1:
Lettera d:
NE auspica che il SIC dia prova di una certa discrezione nel designare altri servizi, evitando di esporre ad esempio gruppi di osservatori o squadre d'intervento.

Dato che né il testo della legge né il rapporto esplicativo indica in quale misura i Cantoni siano tenuti a eseguire direttamente le misure di acquisizione autorizzate, *SO* e *T*G gradirebbero che si precisasse in questa sede se l'esecuzione di tali misure è di principio riservata al SIC oppure se possono partecipare anche le autorità d'esecuzione cantonali. *SO* è senz'altro bendisposto nei confronti di questa possibilità, ma reputa tuttavia che si giustifichi di prevedere un ulteriore indennizzo finanziario per misure di acquisizione particolarmente onerose. *TG* vorrebbe veder precisato che le misure di acquisizione soggette ad autorizzazione devono di principio essere eseguite dal SIC (altrimenti bisognerebbe chiedere un indennizzo finanziario).

Il *Partito Pirata* auspica che le persone interessate siano rappresentate nella procedura da un organismo indipendente.

Articolo 27

CCCZH crede che in virtù della disposizione sui casi d'urgenza il SIC possa in ogni caso, e a suo libero arbitrio, curiosare nella vita privata delle persone e impiegare i dati acquisiti illegalmente per sostanziare ulteriori motivi di sospetto. L'autorizzazione a posteriori è inutile, poiché a quel punto il SIC disporrebbe già delle informazioni volute e il Consiglio federale non riuscirebbe ad accertarsi che i dati acquisiti illegalmente non siano stati memorizzati in un ambito sottratto all'ufficialità.

Articolo 28

Capoverso 2:
La *PP2* fa presente che se l'autorizzazione a posteriori viene negata i dati acquisiti nell'ambito della procedura prevista in caso d'urgenza oltre a dover essere distrutti non devono nemmeno poter essere utilizzati.

Articolo 29

Capoverso 2:
L'*UDC* accoglie con sostanziale favore il previsto obbligo di comunicazione. Desidera peraltro che il capoverso 2 lettera d venga completato indicando che il capo del DDPS ha la possibilità di rinunciare alla comunicazione se questa non presenta alcun interesse per la persona interessata.

Il *Partito Pirata* è contrario a questo articolo e vorrebbe che il capoverso 2 fosse integralmente soppresso, poiché dal punto di vista dello Stato di diritto non potrebbe esistere alcuna ragione per rinunciare alla comunicazione.

CCCZH considera questo articolo completamente insensato, poiché se dovesse fare una mossa sbagliata a livello di sorveglianza, il SIC troverebbe sempre, grazie al capoverso 2, un motivo per liberarsi dall'obbligo di informare la persona interessata.

DigGes ritiene che la pletora di eccezioni vanifichi quasi completamente il senso di questo articolo, ma considera legittime le lettere a (primo emistichio) e d. Considera però inquietante il secondo emistichio della lettera a, poiché un procedimento legale potrebbe essere compromesso soltanto se fossero impiegate per i fini del procedimento informazioni ottenute con misure di acquisizione illegali.

Il capoverso 2 priva le persone interessate di tutti i diritti di difesa. Perciò, secondo *dirittifondamentali.ch*, i *Verdi*, *GDS* e *SPF* è necessario specificare esplicitamente che le informazioni ottenute con misure di acquisizione soggette ad autorizzazione non possono assolutamente essere utilizzate penalmente, essendo state ricercate senza il minimo indizio iniziale.

La *PP2* ritiene che la comunicazione debba costituire la regola e chiede di specificare che essa può essere differita in via eccezionale. Inoltre, la comunicazione deve indicare la possibilità di controllo giudiziario della legalità della sorveglianza e il relativo rimedio giuridico.

Articolo 30

CCCZH chiede di impedire la generosa distribuzione di informazioni di intelligence, poiché altrimenti le collezioni di dati sfuggirebbero a qualsiasi controllo.

Secondo la *PP1* occorrerebbe prevedere a titolo complementare che la Confederazione è tenuta a rispondere dei danni cagionati a terzi da privati mandatari del SIC che violano le disposizioni della LSI o degli obblighi di diligenza.

Capoverso 2:
BS e *Privatim* possono capire che in determinate situazioni il SIC debba poter far capo alle conoscenze tecniche di privati, ma pensa che un simile scorporo accresca il rischio che siano commesse violazioni dei diritti fondamentali, poiché il destino dei dati personali in questione sfuggirebbe del tutto al controllo del SIC.
Il capoverso 2 tiene conto di questa difficoltà, ma *BS* e *Privatim* raccomandano comunque di disciplinare contrattualmente con i mandatari aspetti quali la tutela del segreto, i diritti di controllo del SIC e dell'IFPDT sull'impiego dei dati, il divieto di utilizzare i dati per fini diversi dal previsto, le misure sulla sicurezza delle informazioni e le sanzioni.

Il *PVL* suggerisce di esercitare estrema prudenza per quanto riguarda l'impiego di privati nel campo della sicurezza interna. Trattandosi di un ambito molto delicato, che tocca i diritti fondamentali, il capoverso 2 deve essere soppresso.

Il *Partito Pirata* chiede di sopprimere questo capoverso, poiché altrimenti il SIC perderebbe le conoscenze che possiede e finirebbe per dipendere per sempre dagli operatori privati.

Articolo 31

GE definisce imprescindibile la protezione delle fonti.

Capoverso 1:
L'eccezione prevista al capoverso 1 è troppo restrittiva secondo il *PS*, poiché prima che si giunga a una condanna definitiva possono trascorrere anche interi decenni. Propone pertanto di formulare in modo lievemente più ampio l'ultimo periodo del capoverso 1:
[1] … nei confronti delle quali sono stati promossi procedimenti per crimini gravi contro l'umanità.

Capoverso 2:
AG considera positivo che a determinate condizioni l'identità degli informatori domiciliati in Svizzera possa essere rivelata alle autorità inquirenti per far luce su un reato.

ZG sottolinea che il concetto di reato grave deve essere meglio definito (si rimanda alle lezioni tratte al riguardo nel caso dell'attentatore del Rütli, meglio noto come «Rütlibomber»).

Il *Partito Pirata* considera estremamente sfrontato che in una disposizione sulla protezione delle fonti si stabilisca che le fonti possono essere rivelate alle autorità inquirenti. Il capoverso 2 deve essere soppresso, poiché altrimenti le fonti potrebbero essere ricattate dal SIC.

La *PP1* propone di sopprimere la protezione delle fonti anche nei confronti delle persone segnalate, ricercate o condannate da un'autorità internazionale (Corte penale internazionale) per gravi crimini contro l'umanità.

Secondo la *PP2* l'identità delle fonti dovrebbe essere rivelata anche nel caso in cui queste informazioni fossero necessarie per un procedimento penale.

Capoverso 4:
Le osservazioni del *TAF* riguardo all'articolo 19 si applicano anche a questa disposizione. L'articolo 36*a* LTAF andrebbe logicamente adeguato, poiché copre anche questa controversia.

Articolo 32 e seguenti

Secondo la *PP2*, il fatto che i cittadini svizzeri all'estero non possano beneficiare della stessa protezione concessa ai cittadini svizzeri in Patria non avrebbe alcuna giustificazione. Le disposizioni della sezione 4 dovrebbero trovare applicazione tanto all'acquisizione di informazioni su fatti in Svizzera quanto ai casi in cui cittadini svizzeri vengono sorvegliati all'estero. Inoltre, l'esplorazione di segnali via cavo dovrebbe essere esclusa sia quando l'emittente o il ricevente si trovano in Svizzera, sia quando hanno per oggetto un cittadino svizzero all'estero. Le disposizioni della sezione 4 dovrebbero trovare applicazione anche in questi casi.

Articolo 32

FR approva l'applicazione delle misure, ma tiene comunque a sottolineare che nella legge occorrerebbe circoscriverle e precisarle meglio.

Il *PLR* accetta che in questo caso si rinunci a una procedura di autorizzazione e che ci si limiti invece alla documentazione. Un controllo giudiziario e politico sarebbe sicuramente auspicabile, ma anzitutto all'estero sarebbe sprovvisto di effetto (e potrebbe oltretutto essere interpretato come violazione della sovranità) e, secondariamente, si addosserebbe ai giudici incaricati di rilasciare l'autorizzazione un'inopportuna responsabilità politica, giuridica e diplomatica.

DigGes rammenta che la validità dei diritti dell'uomo, e quindi della tutela dei diritti fondamentali, non si ferma alla frontiera nazionale. Le accresciute difficoltà, peraltro incontestate, con cui si è confrontati nell'ambito degli impieghi all'estero non devono indurre ad abbassare la guardia per quanto riguarda la tutela dei diritti fondamentali. Se non fosse possibile preve-

dere un esame anticipato da parte di un giudice, occorrerebbe perlomeno prevedere un esame giudiziario a posteriori dell'acquisizione di informazioni.

L'*USAM* chiede di dichiarare nella legge che i dati su fatti all'estero e i dati su fatti in Svizzera non siano di principio collegati.

Capoverso 2:
Il *Partito Pirata* chiede la soppressione dell'eccezione prevista all'articolo 22 capoverso 1 lettera g, poiché l'intrusione in ordinatori di altri Stati potrebbe essere interpretata come atto di belligeranza.

DigGes vuole che si stabilisca chiaramente che il SIC non è autorizzato in nessun caso a sferrare attacchi (art. 22 cpv. 1 lett. g), poiché all'estero simili atti potrebbero essere interpretati come guerra elettronica e provocare un'escalation.

CCCZH vede nel capoverso 2 un'adesione del SIC alla guerra informatica e a operazioni di hacking condotti dallo Stato senza autorizzazione. Al SIC non si devono assolutamente attribuire competenze di questo genere.

Per la *PP1*, è senz'altro possibile riconoscere che l'articolo 22 capoverso 1 lettera g non può essere assoggettato in questo caso a una procedura di autorizzazione che all'estero non avrebbe alcun effetto. Considerata però la costellazione attuale del mondo dell'informatica (per es. il cosiddetto «Cloud Computing»), occorrerebbe stabilire in quali casi un sistema di ordinatori (e con ciò si intende sicuramente un «server») o una rete di ordinatori si trova in Svizzera e quando all'estero. Occorre inoltre presumere che i messaggi di posta elettronica scambiati tra partner che comunicano in Svizzera transitino in parte attraverso reti ubicate all'estero.

Capoverso 3:
Secondo il *PS* è essenziale che l'essenza dei diritti fondamentali delle persone interessate venga rispettata anche nell'ambito dell'acquisizione di informazioni all'estero.

Capoverso 4:
Il *PS* auspica che le attività di acquisizione a favore degli organi di vigilanza e di controllo siano scrupolosamente documentate.

AInt accoglie favorevolmente l'inserimento nella LSI delle attività svolte dal SIC all'estero. Tuttavia, i motivi addotti nel rapporto esplicativo non giustificano la rinuncia all'obbligo di autorizzazione, alla comunicazione a posteriori e alla protezione giuridica. Manca infatti una disposizione che definisca in quali casi il SIC è autorizzato ad agire all'estero.
Un esame della proporzionalità effettuato sotto la direzione del SIC cadrà sempre a favore degli interessi della Svizzera in materia di sicurezza e quindi non consente di tener conto dei diritti fondamentali delle persone interessate.
AInt si dice preoccupata per il fatto che con il presente avamprogetto la Svizzera dimostra una palese noncuranza per il rispetto del diritto nelle attività all'estero e pretende una soluzione rispettosa dei diritti fondamentali per quanto riguarda le attività del SIC all'estero. L'avamprogetto viola gli obblighi assunti in virtù del diritto internazionale.

Articolo 33

SSU e *ASUI* chiedono una sezione a se stante per l'esplorazione radio (poiché questa merita di essere parificata all'esplorazione dei segnali via cavo).

Per il *CCCZH* l'intero articolo è sprovvisto di legittimità, poiché mette a repentaglio le relazioni con l'estero e il SIC non ha alcun motivo di operare all'estero.

Capoverso 1:
Il *Partito Pirata* si chiede come pensi di fare il SIC per *distinguere* tra segnali all'estero e segnali in Svizzera.

Capoverso 3:
Il *Partito Pirata* auspica che la legge stabilisca i termini.

Capoverso 6:
A giudizio del *CCCZH* l'espressione «il più presto possibile» è troppo accondiscendente.

Sezione 7: Esplorazione dei segnali via cavo (art. 34 – 38)

La *SSU* e l'*ASUI* si rallegrano che l'esplorazione dei segnali via cavo venga disciplinata e assoggettata alla procedura prevista per le misure di acquisizione soggette ad autorizzazione, poiché in tal modo si evita sin dall'inizio che l'acquisizione di informazioni dilaghi, come succede talvolta all'estero.

L'*UDC* nota che l'esplorazione dei segnali via cavo assume un'importanza crescente a livello internazionale e fa presente che la LSI deve ispirarsi sotto il profilo terminologico, tecnico e amministrativo alla LSCPT riveduta.

Il *Partito Pirata* deplora che si trascuri la questione dei diritti fondamentali e teme che si accumuli una marea di dati la cui analisi richiederà anni di lavoro e provocherà ingenti costi ma non avrà la benché minima utilità.

Il *PVL* si oppone perlomeno a una sorveglianza totale dei flussi di dati sulle linee di telecomunicazione internazionali.

dirittifondamentali.ch, i *Verdi*, i *GDS* e la *SPF* si oppongono all'esplorazione dei segnali via cavo, in particolare perché viola il segreto delle telecomunicazioni che in Svizzera protegge illimitatamente l'agire individuale nel traffico delle telecomunicazioni.

Non riuscendo a scorgere quale possa essere l'utilità dell'esplorazione dei segnali via cavo, considerato che i diritti fondamentali degli individui all'estero non beneficiano di alcuna protezione e visto il possibile danno di reputazione che la Svizzera rischia di subire, *DigGes* si oppone di principio all'esplorazione dei segnali via cavo. Altrimenti auspica un disciplinamento dell'informazione della popolazione circa l'entità delle misure adottate e la creazione di un'autorità di controllo indipendente, analoga a quella istituita per l'esplorazione radio.

A giudizio del *CCCZH*, gli articoli che disciplinano l'esplorazione dei segnali via cavo sono una fregatura (un «PRISM alla svizzera») e vanno soppressi.

L'*asut* si dichiara contraria alle nuove disposizioni sull'esplorazione dei segnali via cavo, poiché non sono ancora sufficientemente mature.
È inoltre sconcertata dal fatto che in questa legge si voglia già introdurre una base legale per una misura di sorveglianza totale quando ancora non si dispone di conoscenze sufficienti su realizzazione tecnica e organizzativa, onere, proporzionalità, entità, utilità e efficacia di una simile misura. Oltretutto, non si capisce in che modo i dettami della legge debbano essere attuati nella prassi (in particolare, sarebbe praticamente impossibile evitare che con l'esplorazione dei segnali via cavo vengano rilevati e memorizzati anche segnali e dati personali puramente interni alla Svizzera).
Per questi motivi tanto l'*asut* quanto *Swisscom* considerano assolutamente indispensabile che si proceda preliminarmente a un'analisi costi-benefici e a uno studio di fattibilità approfondito, sulla cui base le formulazioni vaghe delle disposizioni applicabili all'esplorazione dei segnali via cavo dovranno in seguito essere precisate.

I *Verdi*, il *PVL*, l'*UDC*, *dirittifondamentali.ch*, i *GDS* e la *SPF* sono anch'essi del parere che prima di creare una base legale vi siano ancora molte questioni da chiarire. Il Consiglio federale è pertanto pregato di indicare chiaramente nel messaggio ad esempio gli obiettivi, l'utilità, i metodi, la probabile entità, le risorse di personale necessarie, la fattibilità tecnica e i costi dell'esplorazione dei segnali via cavo. Non si capisce ancora neppure in che cosa possa consistere il valore aggiunto per lo stesso servizio informazioni.

Articolo 34

Capoverso 4:
Lettera c:
Il *Partito Pirata* chiede che nella legge siano stabiliti termini fissi.

Articolo 35

Il *PVL* esprime la propria approvazione per il previsto obbligo di autorizzazione.

Articolo 36

Il *TAF* auspica che le disposizioni concernenti la procedura di autorizzazione vengano precisate indicando se i termini sono intesi in giorni lavorativi o in giorni civili.

Articolo 37

Capoverso 3:
DigGes auspica che sia previsto un obbligo di informazione delle persone interessate nel caso in cui l'esplorazione riguardasse dati su persone in Svizzera che fossero poi analizzati con i riferimenti personali.

Articolo 38

Capoverso 4:
L'*asut* osserva che per esperienza i costi per gli offerenti di prestazioni di telecomunicazione sono molto elevati, poiché per le attività di sorveglianza delle reti di cavi l'onere si moltiplica rispetto alle attività di esplorazione radio più volte menzionate nel rapporto e oggi praticate. Gli offerenti di prestazioni di telecomunicazione dovrebbero essere indennizzati integralmente per tutti i costi che ne derivano, e non solo per i costi incorsi per la fornitura dei segnali al servizio incaricato dell'esecuzione.

La *Swico* dubita che le indennità coprano anche solo approssimativamente i costi.

Il *Partito Pirata* chiede che i costi siano integralmente assunti dal SIC e che venga pubblicato un rapporto annuale sul budget destinato a questo compito. Anche *dirittifondamentali.ch*, i *Verdi*, i *GDS* e la *SPF* sono preoccupati dell'enormità dei costi cagionati agli offerenti di prestazioni di telecomunicazione e del loro insufficiente indennizzo.

Capitolo 4: Elaborazione dei dati e archiviazione (art. 39 − 59)

L'*UDC* ritiene che il sistema sia stato ponderato ed esprime pertanto un parere favorevole al riguardo.

La *swico* chiede che venga creato un articolo autonomo sulla memorizzazione dei dati, compreso un disciplinamento vincolante della durata di tale memorizzazione, poiché a suo avviso le altre disposizioni dell'avamprogetto (ad es. art. 40 cpv. 4, art. 52 o art. 59) non contribuiscono a chiarire per quanto tempo i dati acquisiti possano essere effettivamente memorizzati.

Il *CCCZH* ritiene che, in diversi punti, le autorizzazioni di accesso siano definite in maniera contrastante (ad es. art. 42 cpv. 2 lett. b). La durata di conservazione dovrebbe essere sancita nella legge.

Articolo 39

Capoverso 1:
AR e *VD* considerano la formulazione troppo vaga e ritengono che sia opportuno precisare le categorie di dati e lo scopo dell'elaborazione almeno a livello di ordinanza.

Per soddisfare il criterio della densità normativa (particolarmente elevata nei processi di elaborazione dei dati con un potenziale di rischio così alto come nel caso dei sistemi d'informazione del SIC), questa disposizione dovrebbe essere assolutamente concretizzata. Il *PS* propone di stabilire tale esigenza nell'articolo 42 capoverso 2:
Art. 42 cpv. 2 a^{bis} (nuovo)
a^{bis} ..le categorie di dati personali degni di particolare protezione e dei profili della personalità.

In tale ambito, il *PS* si aspetta che, nelle disposizioni esecutive, il Consiglio federale:
- limiti ai collaboratori del SIC appositamente incaricati l'autorizzazione di elaborare i dati contenuti nei diversi sistemi d'informazione;
- limiti la ricerca di dati in più sistemi ai collaboratori del SIC che dispongono delle autorizzazioni di accesso necessarie per i sistemi d'informazione in questione (partendo dal presupposto che si tratti di un ristretto numero di collaboratori, cosa che altrimenti andrebbe precisata);
- limiti la procedura di richiamo al solo indice per quanto riguarda i contenuti e, a livello istituzionale, ad autorità di polizia, giudiziarie e di protezione dello Stato chiaramente definite.

Secondo il *PS* questi criteri dovrebbero essere annunciati in modo inequivocabile nel messaggio del Consiglio federale.

Capoverso 2:
BS, il *PS* e la *Privatim* considerano questa disposizione problematica in quanto un principio fondamentale del diritto in materia di protezione dei dati stabilisce che possono essere elaborati esclusivamente dati esatti. Soltanto nel rapporto esplicativo, infatti, si evincerebbe che la disposizione in questione si riferisce ad attività di disinformazione o a false informazioni.

AR, BL, BS e *VD*, come pure *PS* e *Privatim*, raccomandano il seguente adeguamento:
[2] Al SIC è consentito elaborare ulteriormente informazioni rivelatesi come attività di disinformazione o false informazioni se ciò è necessario per la valutazione della situazione o di una fonte. Esso contrassegna i dati in questione come dati inesatti.

Per il *Partito Pirata* il problema è rappresentato soprattutto dal fatto che i dati inesatti verrebbero condivisi anche con partner esteri e potrebbero inoltre confluire in altre banche dati.

Il *CCCZH* chiede la cancellazione di tutti i dati inesatti.

Per *dirittifondamentali.ch*, i *Verdi*, i *GDS*, la *SPF* e l'*USAM* è ovvio che i dati inesatti debbano essere immediatamente cancellati. Se necessario, i riscontri su attività di disinformazione e false informazioni potrebbero essere registrati senza problemi in una nuova comunicazione priva di errori.

Capoverso 3:
dirittifondamentali.ch, i *Verdi*, i *GDS*, la *SPF* e l'*USAM* ritengono che il principio sancito in questa disposizione, secondo cui il SIC può trasferire i medesimi dati in più sistemi d'informazione e, nell'ambito di tale trasferimento, si applicano le direttive del nuovo sistema d'informazione in questione, non sia seria e determini un cosiddetto «data management by

chaos», ovvero una gestione caotica dei dati. Copiando le informazioni in altri sistemi, infatti, si modificherebbero anche i relativi attributi, come i termini per le verifiche periodiche o la durata massima di conservazione. Inoltre, se ripetuta in diversi sistemi, l'informazione subirebbe varie modifiche dovute ai trasferimenti, il che, prima o poi, darebbe inevitabilmente luogo a una banca dati inconsistente.

Articolo 40

AG e *VD* accolgono favorevolmente le misure previste per migliorare il controllo della qualità nell'ambito della sorveglianza dei dati.

L'*OVPD TG* deplora il fatto che, in seguito al raggruppamento dei dati concernenti la sicurezza interna con quelli relativi alla sicurezza esterna nel nuovo sistema IASA SIC, venga meno il principio, applicato finora, secondo cui i dati relativi alla sicurezza interna dovrebbero essere rilevanti ed esatti. La nuova disposizione stabilisce soltanto che il SIC valuta autonomamente la rilevanza e l'esattezza dei dati. Anche riguardo all'articolo 39 capoverso 2, particolarmente delicato dal punto di vista politico-giuridico e del diritto in materia di protezione dei dati, l'*OVPD TG* raccomanda pertanto che, nelle nuove banche dati riunite, continui a essere consentita l'elaborazione di dati personali di carattere interno esclusivamente se tali dati sono rilevanti ed esatti e che, in caso contrario, sia previsto l'obbligo di cancellare i dati in questione.

Il *CCCZH* considera problematico il fatto che il controllo della qualità non figuri tra le competenze fondamentali del SIC.

dirittifondamentali.ch, i *Verdi*, i *GDS* e la SPF ritengono che una discussione sul controllo della qualità sia superflua finché si dispone di una banca dati così inconsistente.

Capoverso 3:
Poiché, nella maggior parte dei casi, i dati rinviati al mittente saranno costituiti da dati risultanti da accertamenti preliminari dei Cantoni, che dovranno essere ulteriormente compressi, nel capoverso 3 sarebbe opportuno conferire alle autorità d'esecuzione cantonali la facoltà di elaborare ulteriormente i dati rinviati al mittente e di archiviarli nella banca dati preliminare del SIC (*CCPCS, AR, BE, SZ, TG, ZG*).

Capoverso 4:
Secondo la *PP2*, in questo caso occorrerebbe fissare un termine entro cui verificare se i dati sono ancora necessari. Occorrerebbe inoltre prevedere la cancellazione automatica qualora, alla scadenza del termine, non fosse stata ancora confermata l'ulteriore necessità dei dati.

Capoverso 5:
BS e *TI* accolgono favorevolmente l'approccio secondo cui il controllo interno della qualità deve essere sancito nella legge.

Il *PS* approva espressamente il fatto che nell'avamprogetto della LSI venga stabilito il controllo della qualità, già introdotto con successo in vari ambiti, ma chiede disposizioni più dettagliate. È inoltre dell'avviso che il controllo interno della qualità debba occuparsi anche di altri aspetti oltre che della semplice verifica «della rilevanza e dell'esattezza dei dati personali»:

Capoverso 5
a. … l'esattezza dei dati personali nel sistema IASA-GEX SIC. Verifica il contenuto dei rilevamenti, segnatamente l'indicazione della fonte, la valutazione dell'informazione nonché la data della prossima valutazione complessiva e conferma il rilevamento definitivo dei dati. Soltanto in presenza di tale conferma possono essere rilevate nuove informazioni sulla stessa persona.

Per quanto riguarda i doppi rilevamenti, l'avamprogetto della LSI dovrebbe essere integrato in modo esplicito:

Capoverso 5
b^{bis} (nuovo) verifica periodicamente l'adeguatezza di tutti i rilevamenti multipli.

Articolo 41

CCPCS, AR, BE, GL, GR, SO, SZ, TG, UR, ZG e *ZH* accolgono favorevolmente il fatto che, nell'ambito dell'applicazione della LSI, le autorità d'esecuzione cantonali non possano più gestire proprie collezioni di dati.
Tale disposizione precisa, da un lato, che i dati elaborati dalle autorità d'esecuzione su mandato della Confederazione sono dati federali (il che garantisce la tanto auspicata chiarezza in merito all'organo competente per il controllo della protezione dei dati presso le autorità d'esecuzione cantonali, ovvero l'IFPDT) e, dall'altro, favorisce indiscutibilmente una maggiore sicurezza dei dati nell'ambito del servizio informazioni.

I Cantoni chiedono anche che continui a essere garantita alle autorità d'esecuzione cantonali la possibilità di una registrazione e di un'analisi di bassa soglia dei cosiddetti dati risultanti da accertamenti preliminari, poiché altrimenti andrebbero perse preziose informazioni relative alla valutazione della situazione e ciò potrebbe limitare l'attività operativa delle autorità d'esecuzione cantonali in tale campo (proprio nei settori che riguardano la sovranità della Confederazione e dei Cantoni).
Occorrerebbe inoltre consentire alle autorità d'esecuzione cantonali la consultazione reciproca dei rispettivi dati risultanti da accertamenti preliminari.

GE deplora il fatto che, secondo il presente avamprogetto, i Cantoni non possano gestire proprie collezioni di dati.

VD ritiene che la disposizione concernente i dati della Confederazione non sia chiara e auspica una precisazione.

La *Privatim*, *BS* e *GR* spiegano che le autorità cantonali non diventano organi federali ai sensi dell'articolo 2 capoverso 1 lettera b in combinato disposto con l'articolo 3 lettera h LPD se elaborano «dati della Confederazione» in virtù della LSI e che per tali autorità si applica il diritto formale in materia di protezione dei dati vigente nel relativo Cantone. Le disposizioni materiali concernenti la protezione dei dati sono invece contemplate nella LSI, che le autorità d'esecuzione cantonali sono tenute ad applicare. L'articolo 41 LSI dovrebbe pertanto essere completato come segue:

«L'elaborazione di informazioni secondo la presente legge sottostà al diritto federale e cantonale in materia di protezione dei dati.»

BE riterrebbe appropriato che la Confederazione si assumesse anche la responsabilità delle attività svolte dagli organi cantonali su mandato del SIC. A tale proposito ravvisa inoltre, per motivi di chiarezza, l'esigenza di un'adeguata base legale, da definire in questa sede o, più avanti, nell'articolo 69.

NE si chiede come debba essere disciplinata la memorizzazione dei dati intermedi che non sono ancora pronti per essere integrati nella collezione di dati della Confederazione.

Articolo 42

CCPCS, AR, BE, GR, JU, NE, SO, SZ, TG, ZG e *ZH* chiedono una verifica di fondo del disciplinamento delle autorizzazioni di accesso ai sistemi da parte delle autorità d'esecuzione cantonali.

GE ritiene che la menzione dei singoli sistemi d'informazione nella legge sia indispensabile al fine di ottemperare all'obbligo di trasparenza per quanto riguarda la protezione dei dati e tutelare la sfera privata. Tuttavia, per poter restare al passo con i rapidi sviluppi tecnici a cui tali sistemi sono per natura soggetti, sarebbe necessario introdurre una disposizione che consenta al Consiglio federale di adeguare l'elenco mediante ordinanza fino alla regolare revisione della legge.

La *DigGes* avverte che, visti i molteplici sistemi che compongono l'architettura informatica proposta, la proliferazione incontrollata di dati non sempre consistenti, nonché troppo spesso conservati oltre il termine di cancellazione previsto dalla legge, è a dir poco scontata. L'unica soluzione a questi problemi sarebbe pertanto quella di limitare notevolmente sin dall'inizio, rispetto a oggi, la quantità dei dati acquisiti e di creare successivamente un organo centrale per la loro gestione. Le collezioni di dati specifiche per il rispettivo campo di applicazione non dovrebbero contenere copie dei dati, bensì riferimenti alle registrazioni di questi ultimi nel sistema d'informazione centrale. L'organo centrale per la gestione dei dati dovrebbe inoltre essere responsabile della cancellazione dei dati conformemente alla legge nonché dei contatti con la popolazione per quanto riguarda l'esercizio dei diritti in materia di protezione dei dati. L'organo centrale per la gestione dei dati non sostituirebbe il previsto organo incaricato del controllo della qualità.

RefLMSI respinge il raggruppamento dei dati concernenti l'interno e l'estero in un'unica banca dati.

Secondo la *SSU* e l'*ASUI*, i sistemi d'informazione dovrebbero essere definiti in forma astratta nella LSI. In tale ambito sarebbe necessario articolare i sistemi su diversi livelli e definirli adeguatamente nella legge a seconda del loro scopo, delle informazioni che vi vengono elaborate e memorizzate, del livello di protezione richiesto e delle relative misure di protezione, nonché della cerchia di persone autorizzate ad accedervi. L'assegnazione degli attuali sistemi d'informazione ai vari livelli formulati in modo generale e astratto dovrebbe invece avvenire mediante ordinanza.

Capoverso 1:
Secondo il *PBD*, anche i nomi dei sistemi informatici dovrebbero eventualmente essere inseriti in un allegato, in quanto andrebbero di volta in volta adeguati ai progressi della tecnica e modificati di conseguenza.

Capoverso 2:
Per il *PS* è decisivo il fatto che il requisito dell'elevata densità normativa venga applicato anche alle disposizioni dell'ordinanza che concretizzano la legge. Ritiene pertanto che sia necessario disciplinare con la dovuta accuratezza il contenuto dei vari sistemi, la cerchia di utenti e la durata di conservazione dei dati, in modo tale da rispettare il principio di legalità anche nell'ambito della delega. Il *PS* propone dunque la seguente precisazione:

[2] Per ogni sistema d'informazione del SIC il Consiglio federale disciplina a livello di ordinanza:

Articolo 43

Il *CCCZH* considera indecente il fatto che, con l'Archivio dei dati residui, il SIC voglia coprire gli altri dati sensibili che intende memorizzare.

Articolo 46

UR accoglie favorevolmente la soluzione proposta, la quale prevede che l'INDEX SIC venga utilizzato per il coordinamento tra Confederazione e Cantoni e funga da piattaforma per l'elaborazione dei dati da parte delle autorità cantonali.

BE, *GR* e *SZ* ritengono che, per poter adempiere i loro compiti in maniera completa e ottimale, le autorità d'esecuzione cantonali dovrebbero avere la possibilità di consultare reciprocamente i rispettivi dati risultanti da accertamenti preliminari e gli archivi. Il rapporto esplicativo relativo all'avamprogetto andrebbe pertanto adeguato di conseguenza.

Articolo 48

Il *CCCZH* ritiene che sia assurdo concedere a organi privati o ad autorità estere l'accesso a una collezione di dati del servizio informazioni, poiché tali dati si sottrarrebbero a qualsiasi base legale e non sarebbero più controllabili.

Articolo 49

CCPCS, AR, BE, GR, JU, NE, SO, SZ, TG, ZG e *ZH* sono dell'avviso che occorra concedere alle autorità d'esecuzione cantonali l'accesso al Portale OSINT. Poiché in questo caso si tratta di dati accessibili a chiunque, un'autorizzazione d'accesso non appare problematica. Inoltre, in caso contrario si correrebbe il rischio di doppi rilevamenti.

Il *CCCZH* ritiene che questa sia l'unica banca dati legittima poiché le informazioni sono state rese pubbliche direttamente dalle persone interessate. La presente disposizione andrebbe pertanto integrata sancendo l'accesso pubblico alla banca dati. In tal modo, in un'ottica di intelligenza collettiva, anche terzi indipendenti potrebbero accertarsi delle minacce per la Svizzera.

Articolo 50

CCPCS, AR, BE, GE, JU, NE, TG e *ZH* ritengono che non abbia senso negare l'accesso alle autorità d'esecuzione cantonali, soprattutto se si considerano i numerosi accertamenti che *GE* e *ZH* devono effettuare su mandato del SIC riguardo alle persone che transitano negli aeroporti. Per i collaboratori cantonali non sarebbe molto logico, in caso di ricerche nel proprio aeroporto, chiedere prima informazioni al SIC a Berna, ovvero allo stesso organo da cui hanno ricevuto il mandato.

Il *PS* ritiene che sia necessario un chiarimento in quanto dalle formulazioni dei capoversi 1 e 2 non emergono restrizioni. Secondo tali capoversi i rilevamenti dovrebbero e potrebbero quindi riguardare anche cittadine e cittadini incensurati come pure formalità doganali che non comportano assolutamente alcuna minaccia.
Il rapporto precisa invece che si tratta esclusivamente dei «dati relativi all'entrata di determinate persone provenienti da certi Paesi ai fini dell'individuazione tempestiva di attività di spionaggio e proliferazione». Anche se, successivamente, il capoverso 4 specifica in effetti che il Consiglio federale stabilisce l'estensione di questo sistema d'informazione, al fine di evitare malintesi il *PS* propone di evidenziare tale aspetto già al capoverso 1:
[1] … serve all'identificazione di determinate persone che …

Articolo 52

dirittifondamentali.ch, i *Verdi*, i *GDS* e la *SPF* affermano che i dati provenienti dall'esplorazione dei segnali via cavo non devono essere inseriti nell'Archivio dei dati residui, ma vanno anch'essi memorizzati in archivi di dati protetti.

Articolo 53

Capoverso 1:
Per *ZH* non è chiaro dove vengano memorizzati i dati provenienti da misure di acquisizione soggette ad autorizzazione all'estero e, pertanto, acquisiti senza autorizzazione.

Articolo 54

La *DigGes* si chiede come debba effettivamente essere eseguita la verifica in questione, tanto più che essa non figura nell'elenco dei compiti dell'organo incaricato del controllo della qualità di cui all'articolo 40, ed esprime il dubbio che si tratti in ogni caso soltanto di un progetto irrealizzabile o di una mistificazione.

Il *Partito Pirata* chiede che, prima della comunicazione, un organo indipendente ne verifichi la motivazione e la proporzionalità.

Articolo 55

AG considera positivo il fatto che, dal canto suo, il Servizio delle attività informative della Confederazione venga di principio obbligato anche a fornire appoggio alle autorità di perseguimento penale mettendo a loro disposizione i propri riscontri.

Il cosiddetto «data mining» non è accettabile per il *PLR*. Pertanto, dovrebbero essere comunicati esclusivamente dati acquisiti nell'ambito di una sorveglianza e che sono stati richiesti al SIC (analogamente a quanto disposto dall'art. 278 CPP).

La *DigGes* ribadisce che la comunicazione è ammissibile soltanto se serve a sventare una minaccia diretta nei confronti della sicurezza interna o esterna conformemente all'articolo 4 capoverso 1 lettera a. In qualsiasi altro contesto, sussisterebbe una violazione dei diritti dell'uomo. Per la *DigGes* deve inoltre essere garantito che le autorità non comunichino in nessun caso a ditte private le informazioni ricevute.

dirittifondamentali.ch, i *Verdi*, i *GDS*, la *SPF* e l'USAM ritengono che questa disposizione contraddica il principio della separazione tra il servizio informazioni e le autorità di polizia. I dati provenienti da misure di acquisizione soggette ad autorizzazione dovrebbero sottostare al divieto di utilizzazione secondo l'articolo 277 CPP in quanto sono stati acquisiti mediante sorveglianze non autorizzate nell'ambito della procedura penale e rilevati senza alcun sospetto iniziale («fishing expedition»).

La *PP1* è dell'avviso che il SIC non dovrebbe essere né autorizzato né obbligato a inoltrare di propria iniziativa alle autorità di perseguimento penale informazioni su reati ottenute nell'ambito della sua attività di acquisizione, i cosiddetti «reperti casuali» ai sensi dell'articolo 278 CPP (nessun obbligo legale di denuncia secondo l'art. 302 CPP).
Di principio, i dati dovrebbero essere comunicati soltanto su richiesta dell'autorità di perseguimento penale (fatta eccezione per la comunicazione di informazioni alla polizia o ai servizi di sicurezza al fine di sventare una minaccia concreta ai sensi dell'art. 17 cpv. 1). In quest'ottica, la *PP1* propone una verifica, un adeguamento e un disciplinamento differenziato delle disposizioni dell'articolo 4 capoverso 2 e dell'articolo 55 capoversi 2 a 4.

Capoverso 1:
Il *PS* propone di elencare nella LSI stessa le autorità che devono essere designate dal Consiglio federale o, almeno, di prevedere che il Consiglio federale definisca un elenco di tali autorità in un'ordinanza:
[1] … autorità interessate in un'ordinanza.

Capoverso 2:
Per *ZH* e la *CAIS* non è chiaro come i riscontri ottenuti possano continuare a essere utilizzati qualora venisse invocata la protezione delle fonti nell'ambito di procedimenti investigativi e giudiziari.

In passato il SIC si è più volte rifiutato di comunicare i riscontri ai fini del perseguimento penale e della prevenzione di reati. Anche il disastroso fallimento delle autorità di intelligence in

Germania riguardo alla cellula terroristica «nationalsozialistischer Untergrund» (Clandestinità nazionalsocialista) dimostra tuttavia la necessità di evitare che i riscontri ottenuti nell'ambito di attività informative giungano troppo tardi o non giungano affatto alle competenti autorità di perseguimento penale e alle autorità preposte alla prevenzione dei reati e al mantenimento dell'ordine pubblico. Il *PS* propone pertanto di chiarire come segue il capoverso 2:
[2] … il SIC li mette a loro disposizione senza indugio e di propria iniziativa garantendo la protezione delle fonti.

Capoverso 3:
ZH e la *CAIS* ritengono che i riscontri ottenuti mediante la sorveglianza dei computer (a meno che non riguardino comunicazioni) non possano essere utilizzati dalle autorità di perseguimento penale poiché in tale ambito il CPP non contempla alcuna misura di questo genere.

Tali informazioni possono essere comunicate esclusivamente nel rispetto della proporzionalità, che secondo il *Partito Pirata* sussiste soltanto se il reato rientra tra gli scopi di cui all'articolo 4. Nel dubbio, i dati non dovrebbero essere comunicati.

Articolo 56

Il *Partito Pirata* rimanda alle sue osservazioni sull'articolo 10.

Il *PS* accoglie favorevolmente le disposizioni di cui ai capoversi 1 e 3 e propone di integrare il capoverso 2 lettera a rafforzando, analogamente a quanto disposto dalla LMSI, le possibilità di perseguimento penale transfrontaliero come segue:
a. … di un crimine o un delitto punibile anche in Svizzera;

Il *CCCZH* chiede che il SIC non venga autorizzato a comunicare dati all'estero, poiché in tal modo questi dati si sottrarrebbero a qualsiasi base legale.

La *DigGes* vuole introdurre in questo articolo un rinvio a un nuovo articolo ancora da redigere. Il nuovo articolo dovrebbe: garantire che i dati messi a disposizione delle autorità estere da parte del SIC vengano utilizzati anche da tali autorità soltanto in conformità alle disposizioni legali svizzere; garantire che il buon esito dell'applicazione di questo principio possa essere controllato da un organo indipendente; offrire agli interessati la possibilità di esercitare a livello internazionale i propri diritti in materia di protezione dei dati; informare gli interessati in merito alla comunicazione all'estero di dati riferiti alla propria persona; specificare i tipi di dati che possono essere inseriti in sistemi d'informazione internazionali e le condizioni necessarie a tal fine.

dirittifondamentali.ch, i *Verdi*, i GDS, la *SPF* e l'*USAM* chiedono che, nell'ambito della comunicazione dei dati, per i riscontri provenienti da misure di acquisizione soggette ad autorizzazione si garantisca in ogni caso un assoluto divieto di utilizzazione ai sensi dell'articolo 277 CPP.

Capoverso 2:
La *DigGes* chiede di assicurare che i riscontri provenienti da misure di acquisizione soggette ad autorizzazione vengano utilizzati esclusivamente al fine di sventare minacce esistenti nei confronti della sicurezza interna ed esterna conformemente all'articolo 4 capoverso 1 lettera a e che, pertanto, non vengano comunicati a Paesi che non offrono tale garanzia.
La *DigGes* presenta le seguenti richieste:

Lettera a:
La Svizzera non può contribuire a scardinare lo Stato di diritto in altri Paesi. Questa disposizione andrebbe pertanto stralciata.

Lettera b:
Questa disposizione dovrebbe essere integrata con l'obbligo di subordinare all'autorizzazione dell'autorità giudiziaria la trasmissione di informazioni qualora essa non fosse inequivocabilmente nell'interesse della persona in questione.

Lettera e:
Questa disposizione dovrebbe essere integrata specificando che in tale contesto può trattarsi esclusivamente di sventare minacce nei confronti della sicurezza interna ed esterna conformemente all'articolo 4 capoverso 1 lettera a.

Capoverso 3:
La *PP2* chiede che non vengano trasmessi dati provenienti da una sorveglianza illegale.

Articolo 57

Per *CCCZH* l'articolo è troppo generico e ammette dunque la comunicazione a qualsiasi organo.

Il *Partito Pirata* chiede un'autorizzazione da parte di un organo indipendente e la previa informazione della persona in questione.

Capoverso 2:
Lettera b:
La *DigGes* vorrebbe integrare il testo come segue:
«qualsiasi trasmissione di informazioni che esuli dalla comunicazione del nome, dell'indirizzo e degli elementi d'indirizzo nel settore delle telecomunicazioni come il numero di telefono, l'indirizzo e-mail e l'indirizzo IP, deve essere previamente autorizzata da un giudice se non è inequivocabilmente nell'interesse della persona in questione.»
Al giudice dovrebbe inoltre sempre essere presentata, oltre alla richiesta del SIC, una replica redatta da un funzionario indipendente.

Articolo 58

Il *Partito Pirata* chiede lo stralcio del capoverso 7, poiché dopo un termine così lungo non dovrebbe essere consentita soltanto una risposta standard senza possibilità di impugnazione. Il principio di trasparenza esige inoltre che al richiedente venga fornita una risposta nel più breve tempo possibile. L'onere di lavoro eccessivo di cui al capoverso 8 non dovrebbe avere alcuna rilevanza per il richiedente.

Il *CCCZH* ritiene che il diritto d'accesso in questione rappresenti un «null statement» e che debba essere modificato poiché inaccettabile in questa forma.

AInt osserva che il diritto d'accesso si riferisce anche alle persone non registrate, ma in tale ambito è prevista una limitazione al capoverso 2. Ritiene inoltre che il capoverso 9 sia formulato in modo molto restrittivo, in quanto anche in altri casi il diritto d'accesso potrebbe essere più importante dell'interesse al mantenimento del segreto. *AInt* è anche dell'avviso che l'inversione dell'onere della prova a carico della persona che richiede le informazioni rafforzi ulteriormente l'ingerenza nei diritti fondamentali e raccomanda pertanto di riprendere la formulazione del vigente articolo 18 capoverso 9 LMSI o di trovare un'altra formulazione che tenga debitamente conto del diritto d'accesso.

La *DigGes* ritiene che la procedura d'informazione debba essere assolutamente semplificata e impostata in modo più facilmente accessibile per i cittadini. A ogni richiesta andrebbe sempre fornita una risposta immediata e completa, nella misura in cui ciò non pregiudichi la sicurezza interna o esterna. In caso contrario, dovrebbe essere possibile appellarsi all'IFPDT come autorità indipendente.

dirittifondamentali.ch, i *Verdi*, i *GDS* e la *SPF* ritengono che il diritto d'accesso indiretto si sia rivelato inadeguato e rappresenti una pura angheria, tanto che oggi quasi nessuno sceglierebbe questa opzione, e giungono alla conclusione che, di fatto, attualmente il diritto d'accesso non esiste.
Il diritto d'accesso dovrebbe in sostanza essere definito conformemente alla LPD, altrimenti andrebbe stralciata almeno la restrizione, contemplata dal capoverso 8, secondo cui l'informazione viene fornita esclusivamente se ciò non comporta un onere di lavoro eccessivo.

Articolo 59

Per il *PS* è fondamentale che i dati non più necessari o destinati alla distruzione non siano distrutti, ma vengano innanzitutto offerti all'Archivio federale a fini di archiviazione. La consapevolezza che l'operato del servizio informazioni, pur essendo attualmente segreto, dopo alcuni decenni possa essere reso pubblico da un organo indipendente e, di conseguenza, discusso, favorirebbe infatti una procedura accurata e responsabile da parte del servizio informazioni stesso.
Il *PS* propone di introdurre una disposizione analoga a quella contenuta nell'articolo 61 capoverso 1 del disegno di legge federale sul servizio informazioni civile (LSIC), ovvero:
[1] Il SIC offre all'Archivio federale, a fini di archiviazione, i dati e i documenti non più necessari o destinati alla distruzione. Al fine di evitare la distruzione di dati e atti degni di essere archiviati, l'Archivio federale può consultare periodicamente l'indice per la relativa verifica.

Naturalmente è essenziale che, dopo l'archiviazione, il SIC non possa più accedere ai dati. Dovrebbe pertanto essere aggiunto un nuovo capoverso volto a garantire che il SIC non ottenga il via libera per l'accesso a dati inizialmente destinati alla distruzione ma successivamente archiviati:
[1bis] L'accettazione da parte dell'Archivio federale di dati e documenti destinati alla distruzione garantisce che, durante il termine di protezione, essi non possano essere consultati né dal SIC né da qualsiasi altra autorità o persona ad esso collegata.
Qualora, nel singolo caso, fosse inevitabile attingere a tali dati e documenti per tutelare un interesse pubblico preponderante, sarebbe necessario prevedere una chiara responsabilità politica a tal fine. La competenza per una simile decisione dovrebbe pertanto spettare esclusivamente al Consiglio federale (o, eventualmente, almeno al capo del DDPS):
[1ter] Per tutelare un interesse pubblico preponderante o proteggere l'integrità fisica e la vita di terzi, il Consiglio federale può autorizzare il SIC a consultare, nel singolo caso, i dati personali trasmessi da quest'ultimo all'Archivio federale a fini di archiviazione.

Il *PS* considera inoltre inaccettabile l'obbligo ai sensi del capoverso 1 di distruggere tutti i dati e i documenti del SIC provenienti da relazioni dirette con servizi di sicurezza esteri e propone pertanto di introdurre una disposizione analoga a quelle contenute nell'articolo 61 capoversi 3 e 4 del disegno di legge federale sul servizio informazioni civile (LSIC), ovvero:
[1quater] I dati e i documenti provenienti da relazioni dirette con servizi di sicurezza esteri e dall'attività informativa operativa sono archiviati dall'Archivio federale in locali del SIC particolarmente protetti. Sottostanno a un termine di protezione di 50 anni.
[1quinquies] Il SIC distrugge i dati e i documenti designati dall'Archivio federale come non degni di essere archiviati.

Il *CCCZH* trova assurda la conservazione dei dati sensibili per 50 anni, poiché ciò comporta praticamente una sorveglianza a vita delle persone interessate.

<u>Capoverso 3:</u>
Il *Partito Pirata* chiede lo stralcio di questa disposizione alludendo al caso Tinner.

Articolo 60

Il *PS* considera ovvia la necessità di una base legale per la fornitura di prestazioni da parte del SIC a favore di terzi. Ritiene inoltre chiari e condivisibili gli esempi di casi riportati nel rapporto esplicativo in merito al capoverso 1.
Osserva tuttavia come nel rapporto non si faccia riferimento al capoverso 2. A quali individui privati e a quali enti si applica questa disposizione? In quali casi e in quali scenari?
A tale riguardo, il PS formula la seguente richiesta: l'articolo 60 capoverso 2 deve essere completamente stralciato o almeno integrato con chiari criteri restrittivi e spiegato nel messaggio.

Il *CCCZH* è favorevole all'incremento della sicurezza dei sistemi informatici locali, ma ritiene che i relativi posti debbano essere aumentati in seno a MELANI o SCOCI e non presso il SIC.

Riguardo al capoverso 2, *economiesuisse* cita come esempio la crisi libica. In simili casi le prestazioni del SIC dovrebbero essere a disposizione anche quando non sussiste un interesse informativo diretto, ma è presente un interesse pubblico (anche di natura macroeconomica). La restrizione contemplata dal capoverso 2 andrebbe dunque stralciata oppure sarebbe necessario estendere il campo d'applicazione.

L'*USAM* chiede un elenco completo delle prestazioni.

Articolo 61

Il *PLR* ritiene che la lista d'osservazione sia uno strumento adeguato che serve a garantire trasparenza.

dirittifondamentali.ch, i *Verdi*, i *GDS* e la *SPF* chiedono che le priorità tematiche e regionali specificate nel mandato fondamentale vengano obbligatoriamente sottoposte all'organo di controllo parlamentare. Lo stesso vale per la lista di determinati gruppi da porre sotto osservazione e per la lista d'osservazione. Tali liste dovrebbero inoltre essere sottoposte a riserva di giurisdizione.

<u>Capoverso 2:</u>
Il *Partito Pirata* ritiene che il mandato politico fondamentale del Consiglio federale e la lista d'osservazione debbano essere pubblici e che il capoverso 2 vada stralciato. Anche la *DigGes* è dell'avviso che la lista d'osservazione debba essere pubblica.

Per il *CCCZH* questa disposizione rappresenta un pericolo per il controllo pubblico del SIC. Quest'ultimo dovrebbe assumersi la responsabilità dell'elaborazione delle domande di accesso e di mediazione, come pure dei processi.

<u>Capoverso 3:</u>
L'*UDC* e la *DigGes* rifiutano la competenza del Consiglio federale di concludere autonomamente accordi.

Articolo 62

Nell'ottica della libertà d'azione e della flessibilità, la *CAIS* accoglie favorevolmente il fatto che il Consiglio federale possa incaricare il SIC di acquisire riscontri in ambiti che esulano dal mandato ordinario, soprattutto limitando le deroghe secondo il capoverso 2.

L'*USAM* ritiene che la formulazione di questa disposizione sia troppo aperta. Almeno i casi di esclusione (ad es. questioni di diritto fiscale, contrattuale o societario) dovrebbero essere disciplinati in modo esplicito. L'*USAM* osserva inoltre che nel rapporto esplicativo viene trala-

sciata la dimostrazione degli scopi per i quali il SIC può essere impiegato o meno, creando così «zone grigie».

Articolo 63

GE è dell'avviso che, visto il particolare status della Svizzera, al Consiglio federale debba essere conferita la competenza di stabilire autonomamente una lista di criteri. Anche *BE* considera la formulazione troppo restrittiva e teme che, in questo modo, i gruppi nazionali che minacciano esclusivamente la sicurezza interna non vengano addirittura mai inseriti nella lista d'osservazione.

Capoverso 1:
Secondo il *PS* è sbagliato prevedere un automatismo nella seconda frase del capoverso 1. Ritiene infatti che l'elaborazione di queste liste di sanzioni non soddisfi sempre i requisiti dello Stato di diritto e ricorda come anche il Consiglio d'Europa sia giunto alla medesima conclusione. Il *PS* è dunque dell'avviso che l'automatismo in questione debba essere eliminato:
[1] *… che minaccino la sicurezza interna o esterna. (Stralciare il resto)*

Articolo 64

ZH e la CAIS chiedono che, nei casi in cui il divieto di determinate attività è correlato a un procedimento penale, il modo di procedere venga concordato con il pubblico ministero competente.

dirittfondamentali.ch, i *Verdi*, i *GDS* e la *SPF* temono che, a seconda della composizione politica del Consiglio federale, possa verificarsi un abuso della disposizione in questione e chiedono pertanto lo stralcio senza sostituzione di questa inutile e sproporzionata ingerenza preventiva nelle libertà democratiche.

Capoverso 1:
Il *PBD* propone di sostituire «e» con «o», poiché ogni singolo fattore costituisce già in sé un presupposto per il divieto di determinate attività.

Capoverso 2:
Il *PBD* ritiene che il divieto debba essere applicato ed eventualmente revocato su richiesta (e non mediante una limitazione temporale).

La *PP1* parte dal presupposto che un divieto di determinate attività ordinato dal Consiglio federale sia soggetto alla verifica da parte del Tribunale amministrativo federale conformemente all'articolo 71 capoverso 1 e si chiede inoltre come debbano essere gestiti in tribunale i mezzi di prova da mantenere segreti. In simili casi si applicano gli articoli 27 capoverso 1 lettera a e 28 PA?

Sezione 2: Controllo e vigilanza in materia di servizio informazioni (art. 65 − 70)

Secondo *BS*, la fitta rete di autorità di controllo e di vigilanza contemplata dall'avamprogetto è, in questa forma, eccezionale per uno Stato. Ritiene tuttavia che non sia soltanto tale rete, di per sé, a migliorare la vigilanza sulle attività informative. Per il controllo del servizio informazioni vengono infatti menzionati a più riprese i tre parametri di verifica «legalità, adeguatezza ed efficacia».
BS ritiene che effettuare controlli e vigilare in maniera efficace sulle attività informative sia indispensabile per evitare sovrapposizioni di competenze, violazioni dei doveri d'ufficio, eccessi di zelo ed esagerazioni. Una vigilanza efficace conferisce infatti al servizio informazioni, sul piano dello Stato di diritto, la legittimità di cui ha assolutamente bisogno per svolgere

la sua importante attività preventiva nel campo di tensioni tra libertà personale e sicurezza collettiva.

Per la *CAIS*, i controlli e la vigilanza conformemente agli articoli 65 segg. sono adeguati alla vasta gamma di competenze del SIC.

L'*UDC* ritiene che i meccanismi proposti garantiscano la legalità e la proporzionalità delle attività del SIC.

La *PP1* si chiede se, visti i molteplici altri compiti da adempiere, il Dipartimento, il Consiglio federale e la DelCG possano davvero svolgere un'attività di controllo efficiente. Ritiene pertanto opportuno verificare se, per il controllo dell'attività del SIC, estremamente importante dal punto di vista politico-giuridico, il Consiglio federale, nel quadro dell'articolo 68, non debba piuttosto impiegare, al posto del Dipartimento (art. 16 cpv. 3), un'autorità di vigilanza indipendente, dotata della necessaria competenza tecnica nonché connessa esclusivamente al SIC e non vincolata alle istruzioni di altre autorità.

La *Privatim* critica la mancata considerazione del fatto che l'elaborazione di dati personali sottostà all'autorità cantonale indipendente di vigilanza sulla protezione dei dati. L'articolo 68 capoverso 3 lettera b non può includere la vigilanza dei Cantoni sulla protezione dei dati, in quanto un'ordinanza del Consiglio federale non ha di un rango normativo sufficiente per modificare la Costituzione o una legge. Disciplinando in maniera chiara la vigilanza in materia di protezione dei dati da parte degli incaricati cantonali della protezione dei dati si eviterebbero incertezze e si impedirebbe l'insorgere di conflitti di competenza:
Articolo 70:
[2] Per la vigilanza in materia di protezione dei dati sulle autorità d'esecuzione cantonali è competente esclusivamente l'autorità cantonale di vigilanza sulla protezione dei dati.

Articolo 65

BS è dell'avviso che, sotto il titolo «Controllo autonomo da parte del SIC», debbano essere disciplinati esplicitamente i seguenti aspetti: l'obbligo di collaborazione con gli organi di controllo cantonali, il coordinamento delle attività di controllo e i resoconti.
Oltre alla legalità, il controllo autonomo dovrebbe includere anche l'adeguatezza, l'efficacia e l'economicità.

L'*OVPD TG* ritiene, da un lato, che un simile controllo autonomo non solo sia inadeguato a causa della non indipendenza del SIC, ma che rappresenti anche un'ingerenza nei diritti dei Cantoni. Il suo obiettivo sarebbe infatti quello di negare ai Cantoni la facoltà di controllare in maniera completa e soprattutto indipendente le proprie autorità di sicurezza nell'ambito della legge prevista.

Il *Partito Pirata* chiede un'autorità di controllo indipendente e non sottoposta al capo del DDPS.

Per il *CCCZH* questa disposizione rappresenta un «null statement» e serve esclusivamente a rassicurare.

Articoli 66 segg.

Per il *PS* è determinante il fatto che l'alta vigilanza politica e il controllo vengano garantiti in maniera capillare dal DDPS, dal Consiglio federale e dalla DelCG.

Articolo 66

Capoverso 1:
BS chiede, per quanto riguarda l'oggetto di un controllo autonomo interno all'Amministrazione, che l'attività del SIC non venga verificata soltanto sotto il profilo della legalità, dell'adeguatezza e dell'efficacia, bensì anche in relazione alla sua economicità.

Capoverso 4:
Il *CCCZH* non vuole che l'accesso a documenti ufficiali venga limitato mediante la LTras.

Articolo 67

Capoverso 1:
BS chiede che l'esplorazione radio non venga verificata esclusivamente sotto il profilo della legalità, bensì anche in relazione alla sua adeguatezza.

Capoverso 2:
BS vorrebbe integrare questo capoverso con una frase:
«*Essa è autonoma e indipendente nell'adempimento dei propri compiti."*

Capoverso 6:
Il *CCCZH* non vuole che l'accesso a documenti ufficiali venga limitato mediante la LTras.

Articolo 68

Capoverso 1:
BS chiede che l'attività del SIC non venga controllata soltanto sotto il profilo della legalità, dell'adeguatezza e dell'efficacia, bensì anche in relazione alla sua economicità.

Capoverso 2:
BS vorrebbe aggiungere in questo capoverso che il Consiglio federale, dopo essere stato informato dal DDPS, deve informare regolarmente a sua volta l'Assemblea federale, i Cantoni e l'opinione pubblica. I contenuti di questa informazione devono inoltre essere stabiliti nella legge.

Capoverso 3:
Il *CCCZH* vuole stralciare tutte le disposizioni secondo cui la vigilanza finanziaria sul SIC richiede una particolare tutela del segreto, in quanto il SIC viene finanziato con il denaro dei contribuenti e l'opinione pubblica dovrebbe pertanto essere a conoscenza delle sue spese. Il *CCCZH* ritiene inoltre che il popolo svizzero abbia il diritto di sapere in che modo la Confederazione sperpera il denaro per ledere la sfera privata delle persone.

Articoli 69 − 70

AR, BE, BL e la *CLI* si chiedono se la DelCG sia effettivamente in grado di garantire nel debito modo la vigilanza sui 26 servizi d'esecuzione cantonali.

BL rifiuta chiaramente il modello di vigilanza proposto e ritiene che gli articoli 69 e 70 debbano essere riformulati. I Cantoni dovrebbero infatti disporre di pieni diritti di vigilanza riguardo ai propri collaboratori, incluso il pieno diritto di ispezione delle attività dei collaboratori del Cantone da parte dell'autorità cantonale di vigilanza e della Commissione della gestione del Parlamento cantonale.

La *CLI* formula le seguenti richieste (come anche *AR, BE, BS, JU* e *TI*):
- la limitazione alla DelCG dell'alta vigilanza parlamentare secondo gli articoli 69 e 70 capoverso 2 deve essere stralciata;

- la vigilanza cantonale sulla funzione di servizio e l'alta vigilanza cantonale dovrebbero continuare ad essere possibili non soltanto *de jure*, ma anche *de facto*;
- sarebbe necessario introdurre un disciplinamento che non ammetta zone d'ombra nella vigilanza e nell'alta vigilanza e che non contraddica il principio secondo cui l'alta vigilanza cantonale va di pari passo con la vigilanza cantonale sulla funzione di servizio (principio di accessorietà).

Articolo 69:

Secondo l'*ASNI*, la Delegazione delle Commissioni della gestione delle Camere federali dovrebbe poter esercitare funzioni di vigilanza illimitate, ovvero senza scadenze temporali e con la possibilità di accedere a tutte le misure dell'attività informativa e alla relativa applicazione.

Articolo 70

Con la disposizione contemplata dall'articolo 70, il Consiglio federale si attiene alla concezione attuale, che prevede la ripartizione tra Confederazione e Cantoni della vigilanza sulle autorità d'esecuzione cantonali. *CCPCS, AR, BE, GR, SO* e *UR* accolgono favorevolmente tale soluzione, sottolineando come la disposizione di cui all'articolo 35 O-SIC si sia dimostrata ampiamente efficace. Una soluzione integralmente federale, con conseguente assorbimento dei collaboratori delle autorità d'esecuzione cantonali nell'Amministrazione federale, comporterebbe invece notevoli svantaggi.

BS condivide, di principio, la decisione di attenersi all'attuale organizzazione decentrata con le autorità d'esecuzione cantonali e il ricorso a organi di vigilanza per assistere l'autorità cantonale di vigilanza (art. 2, 7 e 70), ma ritiene che la relativa motivazione nel rapporto esplicativo debba essere formulata in modo più dettagliato.

AG si chiede se la verifica da parte degli incaricati cantonali della protezione dei dati consideri anche gli aspetti della legalità e della proporzionalità del rilevamento dei dati e se per la consultazione di dati della Confederazione elaborati dal Cantone (come per l'autorità cantonale di vigilanza secondo l'articolo 35a O-SIC) sia necessaria un'autorizzazione del SIC. Secondo *AG* tali questioni non vengono né disciplinate nell'avamprogetto di legge né trattate nel rapporto esplicativo. Sarebbe necessario cogliere l'occasione per un chiarimento.

Secondo il capoverso 1, i collaboratori delle autorità d'esecuzione cantonali incaricate dai Cantoni di compiti secondo la presente legge sottostanno al diritto cantonale che regge la funzione di servizio e all'autorità cantonale di vigilanza dei rispettivi superiori. La vigilanza in materia di protezione dei dati sulle autorità d'esecuzione cantonali non rientrerebbe tuttavia esclusivamente nella sfera di competenza dei superiori delle autorità d'esecuzione cantonali, come indicato a pagina 73 del rapporto esplicativo, ma figurerebbe in particolare tra i compiti della relativa autorità cantonale responsabile della protezione dei dati, che controlla l'elaborazione dei dati degli organi pubblici nel proprio Cantone. Il controllo dell'elaborazione dei dati degli organi pubblici della Confederazione (SIC) spetterebbe invece all'IFPDT. In tale contesto e al fine di chiarire la disposizione in questione, *BL*, *BS*, *GR*, *TI* e l'*OVPD TG* ritengono opportuno integrare l'articolo 70 con un ulteriore capoverso del seguente tenore: «*Per la vigilanza in materia di protezione dei dati sulle autorità d'esecuzione cantonali è competente l'autorità cantonale di vigilanza sulla protezione dei dati.*»

BE deplora il fatto che la nuova LSI non si esprima in merito alla vigilanza sulla protezione dei dati e ritiene che, al fine di evitare questioni di competenza tra la Confederazione e il Cantone, la vigilanza sulla protezione dei dati debba essere integralmente affidata all'Incaricato federale della protezione dei dati e della trasparenza, dal momento che il SIC gestisce i sistemi d'informazione previsti (cfr. art. 42 in combinato disposto con l'art. 41 cpv. 1). Secondo *BE*, inoltre, l'articolo 69 deve essere integrato con una disposizione relativa alla

vigilanza sulla protezione dei dati (in alternativa, sarebbe indispensabile un'adeguata integrazione in tal senso nella sezione 4 «Disposizioni particolari sulla protezione dei dati»).

Per *OW* non è chiaro se, nel quadro delle attività svolte dalle autorità d'esecuzione cantonali rigorosamente su mandato del Servizio delle attività informative della Confederazione, tali autorità vadano considerate organi federali e, di conseguenza, siano soggette alla vigilanza della Confederazione in materia di protezione dei dati. Ciò corrisponde alla prassi attuale che si intende mantenere. *OW* chiede pertanto di disciplinare concretamente nell'articolo 70 la competenza della Confederazione per la vigilanza sugli organi d'esecuzione cantonali in materia di protezione dei dati. Sottolinea inoltre come non siano soggette alla vigilanza della Confederazione in materia di protezione dei dati le elaborazioni, da parte dei Cantoni, di dati di intelligence o di polizia giudiziaria ai sensi dell'articolo 41 capoverso 2.

SZ è dell'avviso che le autorità competenti a livello cantonale secondo l'articolo 7, nella misura in cui operano entro il campo di applicazione del SIC, debbano considerarsi organi federali e, di conseguenza, siano soggette alla vigilanza della Confederazione in materia di protezione dei dati. Ciò corrisponde alla prassi attuale, tuttavia *SZ* raccomanda di sancire nell'articolo 70 (Vigilanza cantonale), o almeno nel messaggio sulla LSI, la competenza della Confederazione per la vigilanza in materia di protezione dei dati anche sugli organi cantonali competenti.

TI ritiene che sia necessario precisare (ev. nell'art. 41 e nel messaggio), che i dati secondo la presente legge sottostanno alla legislazione federale e cantonale in materia di protezione dei dati.

ZH ha invitato a prendere posizione anche l'Incaricato cantonale della protezione dei dati, il quale solleva la questione relativa alla protezione dei dati a livello cantonale. In tale ambito, riferendosi tra l'altro all'articolo 41 e ai relativi commenti nel rapporto esplicativo (pag. 59), l'Incaricato cantonale della protezione dei dati afferma che, fino al momento dell'immissione dei dati nei sistemi federali da parte degli organi d'esecuzione cantonali, viene applicato il diritto cantonale in materia di protezione dei dati. Chiede inoltre un disciplinamento della vigilanza cantonale sulla protezione dei dati agli articoli 65 segg. (capitolo 6, sezione 2), nonché un chiarimento complessivo delle relative questioni e la loro spiegazione nell'ambito del messaggio del Consiglio federale.

La *CAIS* ritiene che le attuali disposizioni, mantenute negli articoli 2, 7 e 70 dell'avamprogetto, non si siano rivelate efficaci dal punto di vista dello Stato di diritto, come verrebbe tra l'altro dimostrato dal fatto che per anni non è stata in realtà esercitata alcuna vigilanza sugli organi d'esecuzione cantonali. Afferma inoltre che tale assenza di vigilanza non può essere ammessa in un ambito così sensibile.
La *CAIS* sottolinea anche come la complessa delimitazione tra l'autorità cantonale di vigilanza e la vigilanza della Confederazione funzioni in pratica soltanto nel caso in cui il SIC faccia tutto il possibile per andare incontro alle esigenze dei Cantoni.
Nel quadro del SIC sarebbe necessario cogliere l'occasione per eliminare la situazione ibrida degli organi d'esecuzione cantonali, che risulta problematica dal punto di vista dello Stato di diritto. Sia la delimitazione delle competenze tra il SIC e i Cantoni che la collaborazione tra il servizio informazioni e la polizia/il pubblico ministero dovrebbero essere disciplinate in maniera semplice e chiara in un'apposita disposizione.

<u>Capoverso 3:</u>
La disposizione prevista all'articolo 70 capoverso 3 lettera a continua a garantire la possibilità di istituire o di mantenere un organo di controllo. Secondo *BS* sarebbe inoltre coerente attenersi alla summenzionata organizzazione decentrata con autorità d'esecuzione cantonali. Qualora nei Cantoni venisse mantenuto l'attuale modello, che prevede la possibilità di istituire organi di controllo per assistere l'autorità cantonale di vigilanza, anche a livello cantonale dovrebbe essere garantita una vigilanza efficiente e completa. A tale riguardo, *BS* ritiene

che, per assicurare una vigilanza efficace nel Cantone, sia necessario prevedere un diritto di consultazione pieno e incondizionato.

BS è dell'avviso che la tematica della vigilanza cantonale debba essere disciplinata dettagliatamente a livello di legge. Ciò comprende anche, in particolare, un disciplinamento secondo cui all'autorità cantonale di vigilanza e agli organi di controllo che la assistono spetta un diritto di consultazione illimitato, almeno per quanto concerne i dati e le informazioni a cui hanno accesso le autorità nel Cantone (INDEX SIC, PES). Inoltre, i contenuti delle competenze dell'autorità cantonale di vigilanza illustrati nel rapporto esplicativo (pag. 73) dovrebbero essere disciplinati in maniera altrettanto esplicita a livello di legge.

Articolo 71

Il *PLR* è favorevole alla procedura di ricorso proposta e la considera una garanzia per lo Stato di diritto.

Il *TAF* ritiene problematico che, in determinati casi, vengano presentati alla corte competente del Tribunale ricorsi riguardanti decisioni adottate proprio dal presidente della corte in questione. La possibilità di istituire un'altra corte all'interno del Tribunale amministrativo federale non risolverebbe tale problema.
Il *TAF* sarebbe favorevole a una rigorosa separazione tra l'autorità giudiziaria, responsabile di autorizzare misure di acquisizione, e l'autorità di ricorso, anche per evitare un accumulo di funzioni nella stessa autorità giudiziaria. Propone pertanto di attribuire la competenza per l'esame del ricorso a un'altra autorità giudiziaria federale, ovvero, in questo caso, al Tribunale penale federale. Questa soluzione avrebbe anche il vantaggio di mantenere la possibilità di ricorso al Tribunale federale contemplata dal capoverso 1.

Secondo il *TF* la protezione giuridica proposta contraddice il ricorso generale al Tribunale federale. Il *TF* è dell'avviso che, anche nel settore del servizio informazioni, eventuali gravi ingerenze nei diritti fondamentali possano essere corrette dalla Corte suprema nel quadro delle disposizioni generali di protezione giuridica della LTF.
L'ultima frase del capoverso 1 dovrebbe pertanto essere stralciata e sostituita con un capoverso o un articolo a parte:
«*Contro le decisioni su ricorso del Tribunale amministrativo federale è ammesso il ricorso al Tribunale federale. La procedura è retta dalla LTF.*»

Articolo 73

GE accoglie favorevolmente il fatto che nella LSI venga sancita la disponibilità a collaborare con i Cantoni e, in particolare, a mettere a disposizione mezzi tecnici.

Secondo *NE* dall'articolo si evincono i compiti delle autorità d'esecuzione cantonali, ma non i mezzi che esse potrebbero impiegare a tal fine. Presumibilmente potrebbe trattarsi delle misure di acquisizione non soggette ad autorizzazione, ma ciò non risulta dal testo.

Il *CCCZH* vede in questa disposizione una conferma del fatto che il SIC assumerebbe, in un certo qual modo, una funzione di coordinamento tra Confederazione e Cantoni con diritto di sovranità in campo informativo e ritiene che un simile controllo delle informazioni non sia tollerabile in uno Stato democratico.

Modifica di altri atti legislativi

Numero 2 LAr:

BE e la *Privatim* ritengono che, in virtù del principio di proporzionalità, i dati non più necessari debbano essere di principio distrutti. Una deroga a tale principio sarebbe possibile sotto forma di archiviazione per scopi storici. Dal punto di vista delle persone interessate, una si-

mile archiviazione avrebbe pressoché lo stesso impatto di una distruzione, poiché verrebbe comunque esclusa l'utilizzazione dei dati da parte del servizio mittente ai fini dell'adempimento del compito originario, garantendo in tal modo la protezione della personalità degli interessati. Questa è la procedura scelta dal legislatore nella legge sull'archiviazione, tuttavia la modifica prevista contempla una soluzione opposta. Poiché, con la deroga prevista, i dati resterebbero a disposizione dei servizi mittenti senza alcuna limitazione temporale, e visto che ciò non riguarderebbe soltanto il SIC ma tutti i servizi mittenti, l'archiviazione diventerebbe uno strumento finalizzato alla conservazione permanente dei dati per i servizi mittenti stessi.
La *Privatim* propone pertanto di rinunciare totalmente a questa modifica, mentre secondo *BE* occorrerebbe formulare in modo restrittivo nel testo nella legge le condizioni necessarie per la consultazione dei dati. La condizione generica secondo cui la consultazione è ammessa qualora i servizi mittenti ne abbiano bisogno per la valutazione di minacce nei confronti della sicurezza interna ed esterna potrebbe infatti, con molta probabilità, dare adito a gravi ingerenze nei diritti della personalità.
BE vorrebbe inoltre che nel rapporto venisse spiegato il motivo per cui si debba derogare al principio legale proprio in un ambito delicato dal punto di vista della protezione dei dati come quello della protezione dello Stato.

Per il *CCCZH* questa modifica non è accettabile.

Numero 3 LTras:

Il *PPD* condivide l'opinione secondo cui le informazioni di intelligence debbano essere particolarmente protette, ma accoglie con favore anche la decisione di rinunciare alla totale esclusione del SIC dal campo di applicazione della LTras.

Per il *CCCZH* la LTras non dovrebbe essere modificata in nessun caso. Piuttosto, bisognerebbe prestare particolare attenzione proprio al SIC, che dovrebbe imparare a gestire le domande di accesso e a motivarne i rifiuti.

L'*Università di Ginevra* dubita che, per i documenti riguardanti l'acquisizione di informazioni, sia giustificabile un'esclusione dal campo di applicazione della LTras, tanto più che finora in questo settore sono state registrate pochissime domande di accesso e il già previsto meccanismo di deroga per la protezione di dati sensibili dovrebbe essere sufficiente. Inoltre, qualora venisse escluso dal campo di applicazione della LTras, il SIC si sottrarrebbe al controllo giudiziario finale.

Numero 5 CC:

Il *CCCZH* non vorrebbe concedere al SIC un «accesso illimitato» per rovistare nei registri.

Numero 6 CP:

Secondo il *CCCZH* l'introduzione di simili disposizioni nel CP è scandalosa poiché mina lo Stato di diritto (cfr. anche la critica agli art. 15 e 16).

La *PP1* propone di valutare l'eventuale necessità di adeguare la nota marginale dell'articolo 267 CP nel caso in cui la rivelazione di informazioni interne del SIC a terzi debba rientrare nel campo di applicazione degli articoli 267 e 320 CP.

Numero 8 LM:

La *SSU* e l'*ASUI* accolgono favorevolmente la concessione al Servizio informazioni dell'esercito dell'autorizzazione legale formale per l'osservazione aerea e satellitare.

Numero 9 LSIM:

Il *CCCZH* ritiene che l'accesso da parte del SIC ai dati del personale dell'esercito non sia necessario.

Numero 11 LCStr:

Per il *CCCZH* la verifica dell'autorizzazione a condurre spetta alla polizia.

Numero 12 LSCPT:

SG ritiene che le disposizioni proposte debbano fare riferimento al progetto di revisione totale della LSCPT.

Numero 13 LTC:

Il *CCCZH* non vorrebbe che, nella legge, lo Stato venisse definito come un disturbatore.

Numero 14 LAVS:

Il *CCCZH* è critico e ritiene che lo Stato non svolga la sua funzione di esempio se appare come un evasore.

Numero 15 LAI:

Il *CCCZH* vorrebbe porre fine alla maniacale raccolta di dati da parte del SIC.

Numero 16 LPP:

Il *CCCZH* vorrebbe porre fine alla maniacale raccolta di dati da parte del SIC.

Numero 17 LAMal:

Il *CCCZH* vorrebbe porre fine alla maniacale raccolta di dati da parte del SIC.

Numero 18 LAINF:

Il *CCCZH* vorrebbe porre fine alla maniacale raccolta di dati da parte del SIC.

Numero 20 LADI:

Il *CCCZH* vorrebbe porre fine alla maniacale raccolta di dati da parte del SIC.

6. Ulteriori osservazioni

BS afferma che la menzionata esigenza della densità normativa si applica anche alle disposizioni che devono ancora essere concretizzate in un'ordinanza e che nell'avamprogetto vengono delegate al Consiglio federale.

Nel rapporto esplicativo si afferma che l'alta vigilanza parlamentare sull'esecuzione della presente legge spetta esclusivamente alla DelCG delle Camere federali. È fuor di dubbio che la DelCG, in virtù del suo incarico contemplato dall'articolo 53 della legge sul Parlamento, si faccia carico degli oneri principali in materia di alta vigilanza parlamentare sul settore della protezione dello Stato e dei servizi informazioni. Il compito dell'alta vigilanza finanziaria viene tuttavia attribuito, nell'articolo 51, alla *DelFin*. Nei casi di sovrapposizione delle rispettive sfe-

re di competenza, le due delegazioni operano in stretta collaborazione sulla base di una convenzione. Il rapporto esplicativo concernente l'avamprogetto sarebbe dunque incompleto. La *DelFin* chiede pertanto che nel messaggio sulla LSI si presti attenzione a questo aspetto al fine di evitare eventuali incertezze al momento dell'interpretazione della legge.

Il *PBD* e l'*Università di Ginevra* ritengono che l'avamprogetto debba essere coordinato con altri progetti legislativi attualmente in corso, in particolare con la revisione totale della LSCPT. In tale contesto, la *swico* chiede di rinviare l'avamprogetto concernente la LSI fino alla conclusione della revisione della LSCPT, in modo da poter valutare ancora una volta la LSI in base alle nuove disposizioni della LSCPT dopo che queste ultime saranno entrate in vigore.

Il *PBD* chiede in un intervento parlamentare la creazione di un Centro di competenza per la sicurezza in ambito TIC e si aspetta anche dal SIC l'istituzione di un simile centro.

BS e *ZH* segnalano la mancanza, nell'avamprogetto, di disposizioni relative alla delimitazione tra le attività della polizia, del servizio informazioni e delle autorità di perseguimento penale, sottolineando come tale delimitazione sia assolutamente necessaria. Tale aspetto dovrebbe essere almeno spiegato nel messaggio.

La *SSU* ritiene che andrebbe stralciata la menzione della Delegazione Sicurezza del Consiglio federale, a suo avviso senza precedenti in una legge federale, in quanto non si tratta di un organo del nostro Stato federale.

La *PP1* raccomanda di sottoporre a una consultazione o a un'indagine conoscitiva presso le più importanti associazioni professionali ed economiche, nonché presso le organizzazioni IT, l'indubbiamente voluminosa futura ordinanza concernente la LSI adottata dal Parlamento.

La *PP2* vorrebbe che la legge sancisse l'obbligo di pubblicare statistiche dettagliate sul numero delle misure autorizzate e di quelle rifiutate nonché sul tipo di misure e sul numero delle comunicazioni differite o non effettuate.

Mancanza di una base costituzionale esplicita

Secondo *BS,* per quanto riguarda la portata e l'ampiezza della competenza (implicita) della Confederazione, restano ancora molte incertezze. Una base costituzionale esplicita e sufficientemente precisa sarebbe quindi necessaria anche soltanto per garantire trasparenza e chiarezza in questo importante settore specifico. Inoltre, il significativo ampliamento delle competenze del SIC previsto nell'avamprogetto per quanto riguarda l'acquisizione di informazioni comporterebbe inevitabilmente ingerenze gravi nei diritti fondamentali, cosa che già di per sé renderebbe necessaria una legittimazione costituzionale del servizio informazioni.
BS è dell'avviso che, in una prima fase, debba essere sottoposto al popolo e ai Cantoni un articolo costituzionale che, di principio, conferisca al SIC la necessaria legittimazione. In tale contesto, il popolo e i Cantoni dovrebbero poter decidere se vogliono o meno un servizio informazioni con scopi nettamente più ampi rispetto a quelli attuali.
Secondo *BS*, l'attività del SIC dovrebbe essere codificata in modo unitario nell'ambito di una legge formale soltanto dopo la conclusione di tale procedura.

SO ritiene che, nel rapporto esplicativo, la tematica dell'assenza di una base costituzionale esplicita venga trattata in maniera insufficiente e considera non trasparente il mancato riferimento nell'avamprogetto all'implicita rinuncia a creare una base costituzionale.
Vista la notevole rilevanza dal punto di vista dei diritti fondamentali, constatata nel rapporto esplicativo, *SO* ritiene che la decisione di estendere i compiti della protezione dello Stato senza una relativa base costituzionale esplicita non solo non sia opportuna dal punto di vista della politica istituzionale, ma rappresenti anche un punto debole dell'avamprogetto, che

potrebbe compromettere a livello politico l'approvazione delle nuove misure di acquisizione (di per sé accolte favorevolmente da *SO*).

Secondo *AInt* l'avamprogetto si fonda sul presupposto che la competenza della Confederazione ad agire per emanare la LSI derivi dagli articoli 54 (Affari esteri) e 57 (Sicurezza) Cost. *AInt* ritiene che tale derivazione sia controversa, pur affermando che, comunque la competenza a legiferare viene riconosciuta con il riferimento a una «competenza implicita». Riscontra inoltre una forte dicotomia tra il presente avamprogetto e la tutela costituzionale dei diritti fondamentali e dei diritti dell'uomo, tanto che per un simile progetto legislativo potrebbero essere richieste particolari giustificazioni costituzionali. Le ingerenze del servizio informazioni andrebbero infine ben oltre la protezione dello Stato, motivo per cui *AInt* ritiene che la base costituzionale non sia sufficiente per l'emanazione di una legge sul servizio informazioni.

Il *Centre Patronal* e la *CVAM* ritengono che, in relazione alla base costituzionale, nel rapporto esplicativo venga palesemente indicata la necessità di ulteriori chiarimenti su tale questione. Per un tema così delicato, l'unica soluzione adeguata sarebbe una base costituzionale esplicita (ad es. un'integrazione dell'art. 57 Cost.).

La *SSU* e l'*ASUI* ritengono fermamente che la base costituzionale indiretta per il servizio informazioni esista e sia pienamente sufficiente. Oltre che dagli articoli 54 e 57 Cost. menzionati nel rapporto esplicativo, ciò risulterebbe anche già dall'articolo 2 Cost, in particolare dal capoverso 1 e dalla seconda parte del capoverso 4, in combinato disposto con tutti gli articoli riguardanti compiti concreti della Confederazione nel cui ambito vengono tutelati interessi nazionali essenziali. La costituzionalità indiretta si evincerebbe tuttavia anche dalla recente storia della Costituzione: negli anni '90 del secolo scorso, quando la Costituzione federale è stata aggiornata codificando esplicitamente tutto il diritto costituzionale fino ad allora non scritto, i servizi informazioni esistevano già, ma non è stato ritenuto necessario creare una base costituzionale esplicita per disciplinarli.

Collaborazione con i Cantoni

La *CCPCS, AR, BE, FR, SG, SO, SZ, TG, TI, UR, VD* e *ZG* ritengono che il disciplinamento delle attività e delle competenze delle autorità d'esecuzione cantonali non sia stato definito in maniera soddisfacente. Secondo le disposizioni esplicite dell'avamprogetto, tali autorità continuano, come finora, a ricevere i relativi mandati dalle autorità federali (art. 7 cpv. 2) e a essere indennizzate da queste ultime (art. 73 cpv. 5), ma, in futuro, nell'ambito dell'attività per la quale hanno ricevuto il mandato, lavoreranno esclusivamente su banche dati federali (art. 41 cpv. 1) e verranno controllate da diversi servizi federali, tra cui anche la Delegazione delle Commissioni della gestione delle Camere federali (art. 65 segg.). Anche il perfezionamento in materia di intelligence avviene tramite il SIC (art. 73 cpv. 3).
Il disciplinamento statuito corrisponde essenzialmente alla situazione attuale, in cui i mezzi delle autorità cantonali preposte all'acquisizione di informazioni vengono impiegati prevalentemente per l'adempimento di compiti secondo la LMSI (ad es. l'assegnazione dei mandati, la gestione tecnica, il controllo, la responsabilità e la direzione dei servizi spettano essenzialmente al SIC). Le autorità cantonali si occupano inoltre dell'intelligence nell'ambito della polizia di sicurezza in vista di impieghi per il servizio d'ordine di polizia, che sottostà alla rispettiva polizia cantonale. Tuttavia, sebbene le autorità d'esecuzione cantonali siano quindi strumenti importanti per il SIC, esse non vengono praticamente menzionate nella nuova legge, dove, nella maggior parte dei casi, si parla esclusivamente del SIC. Tale contraddizione non viene risolta in modo soddisfacente né dall'articolo 2 (Autorità e persone soggette alla presente legge) né dall'articolo 73 (Esecuzione da parte dei Cantoni). La presente legge prevede però notevoli ingerenze nei diritti fondamentali, motivo per cui è necessario fissare esigenze elevate per quanto concerne il principio di determinatezza. La terminologia scelta crea inoltre confusione poiché non precisa se il termine «SIC» comprenda o meno anche le collaboratrici e i collaboratori delle autorità d'esecuzione cantonali. È dunque assolutamente necessario ovviare a questa mancanza di chiarezza. I Cantoni hanno bisogno di una base lega-

le chiara. Una volta che la competenza della Confederazione a legiferare in merito alle attività informative dei Cantoni nell'ambito della sicurezza interna della Svizzera sarà stata definita in maniera incontestabile, tale questione di competenza potrà essere chiarita senza problemi. In questo senso, l'avamprogetto andrebbe integrato/precisato come segue:
nuovo capoverso 3 all'articolo 7: «*Nel quadro della loro attività ai fini della presente legge, le autorità d'esecuzione cantonali dispongono di competenze analoghe a quelle del SIC per quanto concerne l'acquisizione di informazioni secondo gli articoli 11 a 21.*»
oppure
completamento degli *articoli* 11 – 21 con: «*Il SIC e le autorità d'esecuzioni cantonali....*»

Per *AG* è positivo che anche in futuro si preveda di attribuire una grande importanza alle autorità cantonali.

GR accoglie favorevolmente la concezione del presente avamprogetto di legge secondo cui il SIC adempie i compiti concernenti le attività informative congiuntamente alle autorità d'esecuzione cantonali, le quali rappresenterebbero dunque un importante strumento del SIC. Il mantenimento, nell'avamprogetto di legge, dell'attuale organizzazione decentrata e della stretta collaborazione con i Cantoni, che hanno dato buone prove, è da considerarsi estremamente positivo, come pure il fatto che le autorità d'esecuzione cantonali non gestiscano più alcuna collezione di dati propria nel campo di applicazione della presente legge.

JU e *NW* accolgono favorevolmente le disposizioni relative all'indennità per i Cantoni e alla collaborazione in materia di formazione, che rappresentano la prosecuzione di una prassi ormai collaudata.

Il *PPD* ritiene che non venga disciplinato in modo chiaro fino a che punto le autorità d'esecuzione cantonali stesse siano autorizzate ad acquisire informazioni e ad applicare misure nell'ambito della loro attività ai fini della presente legge.

Il *PVL* trova adeguata la decisione di mantenere nella forma attuale la collaborazione con i Cantoni, ma si chiede se l'attribuzione dell'alta vigilanza sulle attività dei Cantoni nell'ambito della nuova legge alla Delegazione delle Commissioni della gestione sia appropriata e praticabile. Questo punto dovrebbe pertanto essere ulteriormente analizzato insieme ai Cantoni ed eventualmente adeguato in vista dell'elaborazione del messaggio.

Ripercussioni finanziarie sui Cantoni

La *CCPCS*, *AR, BE, GR, SO, TG, VD, ZG* e *ZH* chiedono che i Cantoni ricevano indennità finanziarie per l'aumento dell'onere derivante dalle procedure e dagli strumenti stabiliti nella nuova LSI (cfr. art. 73 cpv. 5) e, soprattutto, che si tenga conto del fatto che l'applicazione dei nuovi strumenti per l'acquisizione di informazioni comporteranno un considerevole aumento dell'onere anche per le autorità d'esecuzione cantonali. Per quanto riguarda il SIC, invece, nel rapporto esplicativo il fabbisogno di personale supplementare per le nuove misure di acquisizione previste è stimato a 16 posti di lavoro.

NE e *SZ* partono dal presupposto che non si registreranno cambiamenti a livello finanziario e che, pertanto, dal punto di vista dei Cantoni non sussiste alcuna necessità d'intervento in tale ambito.

BS ritiene che, in seguito al previsto obbligo per i Cantoni di collaborare all'esecuzione della LSI, a livello finanziario la Confederazione debba farsi carico di tutte le spese tecniche e relative al personale. La maggior parte dei Cantoni, infatti, difficilmente sarebbe in grado di eseguire tutti i mandati del SIC, o anche solo alcuni di essi, con i propri mezzi tecnici e le proprie risorse umane.

Osservazione sul rapporto esplicativo

Per l'*USAM* le affermazioni riportate al numero 1.5 del rapporto esplicativo sono chiare, complete e comprensibili e corrispondono all'intenzione dell'avamprogetto di legge. Ciò non significa tuttavia che esse siano corrette. L'*USAM* fa notare, ad esempio, che nel rapporto manca una distinzione tra terrorismo ed estremismo violento. Inoltre, non viene precisata, o almeno collocata in modo strategico, la nozione di «interessi nazionali essenziali», né vengono spiegate le misure preventive contro un eccessivo attivismo delle autorità.

7. Sintesi delle risposte al questionario

Partecipanti:
AG, AI, PBD, BE, BS, FR, GL, PVL, CAIS, Conferenza delle direttrici e dei direttori della sicurezza delle città svizzere KSSD, LU, OW, SG, SO, SSU, PS, UDC, SZ, TG, TI, VS, ASUI, ZG (23)

1. Domande generali

a) Ad eccezione del *PVL*, tutti i partecipanti ritengono che i punti principali dell'avamprogetto esposti al numero 1.5 del rapporto siano completi e comprensibili e che non manchi nessun elemento essenziale.
Il *PBD* osserva che il complesso avamprogetto assume un carattere restrittivo a causa delle descrizioni troppo dettagliate, in particolare riguardo a minacce nuove e attualmente ancora sconosciute oppure a futuri sistemi informatici.
SO ritiene che sarebbe necessario un riferimento alla base costituzionale mancante.
Il *PVL* constata l'assenza di riferimenti all'esplorazione dei segnali via cavo (come pure la *SSU* e l'*ASUI*) e ai cambiamenti concernenti l'alta vigilanza sulle attività dei Cantoni.
SZ vorrebbe che venisse spiegata la procedura che la Confederazione intende seguire per quanto riguarda l'acquisizione di informazioni nell'ambito dell'estremismo violento, visto che, con la rinuncia alla sua inclusione tra le misure soggette ad autorizzazione, vengono tralasciati rischi significativi.

b) Quasi tutti i partecipanti ritengono che l'avamprogetto sia formulato e strutturato in maniera comprensibile (ad eccezione di *PBD*, *SG*, *TG*).
La *CAIS* propone di rinunciare alla formulazione di aspetti ovvi.
Secondo *SG* la presenza di numerosi e ampi articoli con molti capoversi rende più difficile la comprensione e la sistematica è poco chiara, il che, soprattutto in un atto legislativo con gravi ingerenze nei diritti fondamentali, rappresenta un problema.
La *SSU* e l'*ASUI* ritengono che alcune disposizioni correlate tra loro siano troppo sparpagliate all'interno della legge (ad es. le disposizioni relative alla tutela delle persone come la protezione delle fonti, l'armamento, le coperture ecc.).

2. Oggetto e scopo (art. 1)

a) Soltanto *CAIS*, *LU*, la *SSU*, *SZ*, *TI* e l'*ASUI* ritengono che le condizioni necessarie per un impiego del SIC al fine di tutelare altri interessi nazionali essenziali secondo il capoverso 3 e l'articolo 62 non siano formulate con sufficiente precisione.
Il *PBD* propone di rendere possibile tale impiego anche con un'autorizzazione a posteriori.
La *CAIS* vede nelle disposizioni un circolo vizioso.
Per *LU* le disposizioni sono formulate in maniera troppo ampia e mancano gli esempi.
SZ auspica una descrizione più precisa del termine per evitare che possano essere ammessi tutti gli impieghi possibili.
La *SSU* e l'*ASUI* ritengono necessario precisare che gli altri interessi nazionali essenziali devono rientrare nella competenza costituzionale della Confederazione Svizzera e che, in caso contrario, è indispensabile una domanda da parte di diversi Cantoni.

b) Ad eccezione di *PVL*, *PS*, *TG* e TI, i partecipanti ritengono che le considerazioni del rapporto descrivano questa futura possibilità di assegnare mandati al SIC in maniera sufficientemente chiara e comprensibile.
AI vorrebbe che venissero menzionati i punti relativi alle infrastrutture critiche e alle reti d'informazione.
BS ritiene che sarebbe troppo complicato, nonché inutile, qualificare o quantificare ulteriormente la tutela dell'ordinamento costituzionale fondamentale ecc.
PVL, *SSU*, *VS* e *ASUI* vorrebbero che venissero riportati esempi di altri interessi nazionali essenziali. VS ritiene che il termine venga utilizzato in maniera completamente diversa in altri atti legislativi.
Secondo la *CAIS* è necessario rinunciare a spiegazioni più dettagliate per tutelare il necessario margine di manovra.

3. Misure di acquisizione soggette ad autorizzazione (art. 22 segg)

a) Tutti i partecipanti ad eccezione di *BE* e *SG* ritengono che le condizioni per l'impiego delle nuove misure di acquisizione soggette ad autorizzazione proposte siano formulate in maniera sufficientemente chiara e restrittiva.
SG critica il fatto che, sebbene le misure di acquisizione menzionate siano previste anche nella procedura penale, i termini vengono utilizzati in modo diverso. In questo caso sarebbe pertanto necessario riprendere in parte la terminologia della revisione della LSCPT (nel cui ambito vengono già correttamente adeguate le formulazioni del CPP che generano confusione).
LU ritiene che i termini «non soggette ad autorizzazione» e «soggette ad autorizzazione» non siano appropriati. Inoltre, per quanto riguarda la scelta nel catalogo di misure, il criterio della proporzionalità di ogni misura di acquisizione concreta dovrebbe essere descritto in maniera più chiara, nonché sancito nella legge.
Per *BE* non è chiaro il ruolo dei Cantoni nell'esecuzione delle misure.
Il *PBD* è dell'avviso che la formulazione dovrebbe consentire anche, in un secondo momento, metodi investigativi oggi ancora sconosciuti e ritiene che, per determinati impieghi (scenari d'emergenza), la complessa procedura di autorizzazione sia troppo lenta e anacronistica.

b) Tutti i partecipanti ad eccezione di *SO* e *ZG* affermano che le misure proposte sono complete e non superflue.
La *CAIS* ritiene che sia garantita la necessaria apertura nei confronti di eventuali sviluppi futuri.
SZ si chiede se l'elenco dettagliato di cui all'articolo 22 capoverso 1 lettere b − d sia necessario o se non debba essere invece incluso nella lettera a.
TI ritiene che l'armonizzazione tra il SIC e la polizia sia problematica, in quanto anche a livello cantonale sussistono esigenze preventive e attualmente gli scambi reciproci non sono regolari.

c) La descrizione della procedura di autorizzazione a più livelli nell'avamprogetto di legge è considerata sufficientemente trasparente da tutti i partecipanti. Soltanto *TI* e *VS* ritengono che la procedura non sia abbastanza equilibrata per quanto riguarda la tutela dei diritti fondamentali.
Per *AI* la procedura è più che equilibrata, mentre *SZ* considera superfluo il controllo politico e ritiene che sia sufficiente il controllo da parte del Tribunale amministrativo federale.
La *SSU* e l'*ASUI* ritengono che il Consiglio federale debba chiarire esplicitamente ancora una volta, nel messaggio e in seno alle Camere federali, che, in situazioni normali, il numero delle ingerenze non sarà superiore a quello indicato. Inoltre, previa consultazione della Delegazione Sicurezza, il giudizio dovrà spettare innanzitutto al Dipartimento e solo successivamente al Tribunale amministrativo federale.

4. Acquisizione di informazioni all'estero (art. 32 segg.)

a) Tutti i partecipanti considerano appropriato e sufficiente il disciplinamento dell'acquisizione di informazioni all'estero. Soltanto *FR* ritiene che le misure di acquisizione previste dovrebbero essere menzionate nella legge.
Per *SO* il previsto obbligo di documentazione compensa adeguatamente la disparità di trattamento tra le misure di acquisizione in Svizzera e quelle all'estero.
Dal punto di vista della sistematica della legge, la *SSU* e l'*ASUI* si chiedono se i capoversi 5 e 6 siano collocati al posto giusto.

b) Soltanto il *PVL* ritiene che la motivazione della rinuncia a una procedura di autorizzazione per le misure di acquisizione all'estero non sia comprensibile e sottolinea come, su tale argomento, il rapporto non sia chiaro e dia luogo a equivoci. Per quanto riguarda l'esplorazione di segnali via cavo, in particolare, non sarebbe del tutto corretta l'affermazione secondo cui all'estero non è necessaria alcuna procedura di autorizzazione. Inoltre, il rapporto non spiegherebbe in maniera chiara il motivo per cui l'esplorazione radio non necessita di una procedura di autorizzazione.

5. Elaborazione dei dati (art. 39 segg.)

a) La delega al Consiglio federale (art. 42 cpv. 2 lett. d) del disciplinamento della durata di conservazione dei dati nei singoli sistemi d'informazione del SIC è considerata appropriata da tutti i partecipanti.
SZ accoglie favorevolmente la maggiore flessibilità che tale delega comporta in caso di nuovi sviluppi.
La *SSU* e l'*ASUI* vorrebbero che l'assegnazione concreta dei singoli sistemi alle rispettive categorie di dati, definite dalla legge in maniera generale e astratta, fosse disciplinata a livello di ordinanza.

b) *SO*, *SSU*, *PS*, *TG*, *TI* e *ASUI* ritengono che i criteri per la sua definizione non siano né appropriati né sufficienti.
SO è dell'avviso che l'«utilità» come unico criterio non basti e che almeno l'ordinanza dovrebbe definire criteri sufficientemente concreti per i relativi sistemi d'informazione. Sarebbe necessario parlare di durata «massima» di conservazione.
La *SSU* e l'*ASUI* ricordano che sarebbe necessario tenere conto anche del «diritto all'oblio» della persona interessata.

6. Prestazioni (art. 60)

a) Tra i partecipanti, soltanto *SO* ritiene che la disposizione relativa alla fornitura da parte del SIC di prestazioni a favore di terzi non sia né appropriata né necessaria. La *SSU* e l'*ASUI* si esprimono incertezza al riguardo.

b) *FR*, *PVL*, *LU* e *PS* ritengono che le possibili prestazioni del SIC non siano sufficientemente definite. Nessun partecipante segnala la mancanza di prestazioni essenziali necessarie a terzi.
FR vorrebbe una precisazione delle prestazioni nella legge.
Il *PVL* ritiene che sarebbero necessarie anche disposizioni riguardanti l'indennizzo e la fatturazione di tali prestazioni.
SZ accoglie favorevolmente il fatto che, grazie alla formulazione aperta, le prestazioni non vengano fissate in maniera definitiva e possano pertanto essere adeguate in base alle necessità.