13.025

Messaggio concernente la legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)

del 27 febbraio 2013

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di revisione totale della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

Nel contempo vi proponiamo di togliere dal ruolo i seguenti interventi parlamentari:

2007	M	06.3170	Lotta alla cibercriminalità. Protezione dei fanciulli (N 22.6.2007; S 11.12.2007, Schweiger Rolf)
2010	M	07.3627	Obbligo di registrazione delle carte prepagate Wi-Fi (N 3.6.2009, Glanzmann-Hunkeler Ida; S 18.3.2010)
2010	P	10.3097	Individuare i cibercriminali (S 10.6.2010, Commissione degli affari giuridici CSt)
2011	M	10.4133	Aumentare la durata di conservazione dei registri di assegnazione degli indirizzi Internet Protocol (N 18.3.2011, Barthassat Luc; S 20.9.2011)
2012	M	10.3831	Revisione della LSCPT (N 16.3.2012, Schmid-Federer Barbara; S 24.9.2012)
2012	M	10.3876	Revisione della LSCPT (N 16.3.2012, Eichenberger-Walther Corina; S 24.9.2012)
2012	M	10.3877	Revisione della LSCPT (N 16.3.2012, [von Rotz Christoph] Schwander Pirmin; S 24.9.2012)
2012	P	11.4042	Sorveglianza tramite cavalli di Troia (1) (N 28.2.2012, Commissione degli affari giuridici CN)
2012	P	11.4043	Sorveglianza tramite cavalli di Troia (2) (N 28.2.2012, Commissione degli affari giuridici CN)
2012	P	11.4210	Costo della sorveglianza penale delle telecomunicazioni (S 5.3.2012, Recordon Luc)

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

27 febbraio 2013

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ueli Maurer
La cancelliera della Confederazione, Corina Casanova

Compendio

La presente revisione totale della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) vuole evitare che, attualmente o negli anni a venire, le necessarie sorveglianze della corrispondenza postale e del traffico delle telecomunicazioni eseguite nell'ambito di procedimenti penali siano ostacolate dall'impiego delle nuove tecnologie (p. es. la telefonia criptata via Internet). L'obiettivo non è sorvegliare di più ma sorvegliare meglio. A tal fine si prevede di adeguare la LSCPT e il Codice di procedura penale (CPP) all'evoluzione tecnologica degli ultimi anni e, nella misura del possibile, ai prevedibili sviluppi futuri del settore.

Situazione iniziale

Gli importanti progressi tecnologici realizzati negli ultimi anni nel settore delle telecomunicazioni offrono agli utenti una moltitudine di possibilità di interazioni. Nella grande maggioranza dei casi queste possibilità sono utilizzate per scopi leciti. Tuttavia, possono essere impiegate anche a scopi criminali. Si constata tuttavia che le nuove tecnologie, per esempio la telefonia criptata via Internet, agevolano la commissione dei reati. È pertanto necessario dotarsi di mezzi che consentano di chiarire i reati commessi per mezzo di queste tecnologie.

L'applicazione del diritto svizzero continua però a essere limitata dal principio della territorialità delle leggi; il perseguimento penale negli affari con carattere internazionale viene così complicato (p. es. se vengono impiegati conti e-mail aperti presso determinati fornitori all'estero). La globalizzazione virtuale rappresenta un problema fondamentale per l'applicazione del diritto nel settore di Internet a cui la presente revisione non riesce peraltro a porre rimedio.

L'obiettivo principale della presente revisione totale della LSCPT è di permettere la sorveglianza delle persone fortemente sospettate di aver commesso reati gravi. Come già attualmente, non si vogliono consentire sorveglianze generalizzate in assenza di sospetti di reato, né si vogliono autorizzare sorveglianze preventive; la libertà personale è così tutelata. Un altro obiettivo della revisione è di permettere l'esecuzione di sorveglianze, a prescindere da qualsivoglia procedimento penale, per ritrovare persone scomparse e per ritrovare i condannati latitanti.

Le disposizioni procedurali penali della LSCPT sono state trasferite nel Codice di procedura penale (CPP), entrato in vigore il 1° gennaio 2011. Gli obiettivi della presente revisione della LSCPT non richiedono soltanto la revisione totale della legge ma anche la modifica di alcune disposizioni procedurali del CPP. Nuove possibilità di sorveglianza vanno integrate nel CPP e nella Procedura penale militare (PPM).

Contenuto del progetto

La presente revisione totale modifica la struttura della LSCPT, dotandola di una sistematica coerente con una nuova numerazione delle disposizioni. Alcuni articoli

sono precisati e completati. Alcune questioni importanti finora disciplinate soltanto nell'ordinanza sono ora trattate nella legge.

Il progetto prevede le seguenti modifiche e innovazioni materiali:

- *i compiti del Servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni sono precisati ed estesi;*
- *vi è una notevole estensione del campo d'applicazione personale della legge. Diverse categorie di persone saranno tenute a collaborare;*
- *la portata dell'obbligo di collaborare è disciplinata in modo graduato per ciascuna categoria in funzione dell'attività specifica da essa svolta;*
- *i dati raccolti durante la sorveglianza sono conservati in modo centralizzato e l'accesso a questi dati, la loro consultazione e la durata della conservazione sono disciplinati;*
- *la durata di conservazione dei dati secondari passa da sei a 12 mesi;*
- *il ricorso a speciali dispositivi di sorveglianza (come gli IMSI-catcher) e a speciali programmi informatici (GovWare) è consentito da chiare basi legali;*
- *la normativa sulla protezione del segreto professionale è adeguata;*
- *come già attualmente, sarà possibile ricorrere alla sorveglianza al di fuori di un procedimento penale per ritrovare una persona scomparsa. D'ora innanzi sarà anche possibile ricercare un condannato a una pena o a una misura detentiva;*
- *sono proposte specifiche disposizioni penali nonché una disposizione relativa alla sorveglianza amministrativa;*
- *è pure proposta una nuova regolamentazione dei mezzi di ricorso contro le decisioni del Servizio e delle censure ricevibili.*

È invece mantenuto il regime attuale in materia di emolumenti e indennità.

Indice

Messaggio

1 Punti essenziali del progetto

1.1 Situazione iniziale

Negli ultimi anni nel settore delle telecomunicazioni e in particolare in quello di Internet sono stati fatti importanti progressi tecnologici che danno agli utenti una grande libertà e molte possibilità di interazione. Le nuove tecnologie, in particolare nel settore di Internet, possono essere utilizzate a fini illegali come i mezzi di comunicazione classici, segnatamente nei settori della pornografia infantile, della criminalità organizzata e degli stupefacenti. La varietà, la grande disponibilità e il semplice uso di queste nuove tecnologie di comunicazione agevolano inoltre la commissione di reati.

L'evoluzione tecnologica non ha soltanto complicato la sorveglianza del traffico delle telecomunicazioni sotto il profilo tecnico; la tecnologia ha infatti sorpassato la legislazione. Così, una sorveglianza di fatto possibile può essere problematica o inammissibile dal punto di vista giuridico, perché non più chiaramente coperta da una base legale. L'assenza di un mezzo giuridico per obbligare i puri fornitori di servizi e-mail a conservare i dati secondari o la frequente impossibilità della sorveglianza della comunicazione criptata via e-mail o della telefonia via Internet a meno di disporre di speciali programmi informatici (GovWare), il cui impiego nell'ambito del diritto vigente è molto contestato, sono esempi che illustrano questa incertezza del diritto. Di conseguenza, occorre provvedere affinché l'impiego delle nuove tecnologie non impedisca le sorveglianze necessarie per elucidare i reati. L'estensione della cerchia dei fornitori obbligati a collaborare permetterà di raggiungere questo obiettivo.

Il principio della territorialità delle leggi limita l'applicazione del diritto svizzero (p. es. in caso di apertura di conti e-mail ubicati all'estero da parte di persone residenti in Svizzera). Nei casi transnazionali (p. es. in caso di utilizzazione di conti e-mail di un fornitore all'estero) la rapidità e l'efficacia del perseguimento penale sono pregiudicati dalla necessità di ricorrere all'assistenza giudiziaria. In queste circostanze, i dati ricercati sovente non possono essere ottenuti in tempo utile (o non possono esserlo per niente). Il disegno non modifica questa situazione.

1.2 La nuova normativa proposta

Lo scopo della revisione totale della legge federale del 6 ottobre 2000[1] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) è innanzitutto di migliorare la sorveglianza senza estenderla. Si tratta prima di tutto di consentire la sorveglianza di persone pesantemente sospettate di aver commesso reati gravi. Invece, non c'è alcun motivo di consentire la sorveglianza dei cittadini in assenza di sospetti o di compiere sorveglianze preventive. Al di fuori dei procedimenti penali, la sorveglianza è autorizzata soltanto per la ricerca di persone scomparse o di condannati.

1 RS **780.1**

Il disegno (D-LSCPT) precisa e completa i compiti del Servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio). Il campo d'applicazione personale viene notevolmente esteso; la portata degli obblighi di collaborare è tuttavia disciplinata, rispettando il principio della proporzionalità, in maniera graduata e in funzione dell'attività specifica di ciascuna categoria di persone. Si prevede di aumentare il periodo durante il quale i dati raccolti nel corso della sorveglianza saranno conservati nel sistema di trattamento del Servizio.

L'obbligo di conservare i dati secondari passa da sei a 12 mesi come il periodo durante il quale questi dati sono disponibili per le autorità di perseguimento penale.

La nuova LSCPT introduce anche un'altra novità, nella misura in cui disciplina le conseguenze penali e amministrative del mancato rispetto dei loro obblighi da parte dei fornitori tenuti a collaborare. Contiene inoltre una disposizione relativa ai rimedi giuridici contro le decisioni del Servizio e alle censure ricevibili.

Le disposizioni della LSCPT relative alla procedura sono state trasferite nel nuovo Codice di procedura penale (CPP)[2], entrato in vigore il 1° gennaio 2011. Gli obiettivi perseguiti non richiedono soltanto la revisione totale della LSCPT ma anche la revisione di alcune disposizioni procedurali del CPP. Due nuove possibilità di sorveglianza sono state integrate nel CPP: in futuro sarà possibile ricorrere a speciali dispositivi di sorveglianza (p. es. gli «IMSI-catcher») e a particolari programmi informatici (i cosiddetti GovWare) fondandosi su una chiara base legale. La normativa relativa alla protezione del segreto professionale è pure stata adeguata. Tutte queste modifiche sono state apportate anche nella Procedura penale militare del 23 marzo 1979[3] (PPM).

Questi aspetti sono esaminati in dettaglio in seguito (v. n. 1.4 e 2).

1.3 Genesi

1.3.1 Mandato del Consiglio federale

Nel marzo 2006, il Consiglio federale ha incaricato il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC) e il Dipartimento federale di giustizia e polizia (DFGP) di esaminare le questioni rimaste aperte in materia di sorveglianza delle telecomunicazioni ai fini del perseguimento penale e di indennità ai fornitori di servizi di telecomunicazione per le attività svolte nell'ambito della sorveglianza. Il mandato ha dato origine a un rapporto della Segreteria generale del DFGP (SG DFGP), che illustra i settori in cui è auspicabile una revisione della LSCPT. Nel maggio 2007, la SG DFGP ha conferito all'Ufficio federale di giustizia (UFG) l'incarico di elaborare un avamprogetto (AP-LSCPT) corredato di un rapporto esplicativo.

2 RS **312.0**
3 RS **322.1**

1.3.2 Gruppo d'esperti

Nel settembre 2008 l'UFG ha istituito, a fini di consulenza, un gruppo di esperti costituito di rappresentanti del Ministero pubblico della Confederazione (MPC), della Polizia giudiziaria federale (PGF), dell'Ufficio federale delle comunicazioni (UFCOM), dell'Associazione svizzera delle telecomunicazioni (asut), delle autorità cantonali di perseguimento penale e del Centro servizi informatici – Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni presso il DFGP (Servizio) e dell'UFG. Quest'ultimo, elaborando l'AP-LSCPT, ha tenuto conto dei pareri espressi in seno al gruppo di esperti.

1.3.3 Avamprogetto e procedura di consultazione

Il 19 maggio 2010, il nostro Collegio ha posto in consultazione l'AP-LSCPT[4] e il relativo rapporto esplicativo[5]. La consultazione è terminata il 18 agosto 2010. Vi hanno partecipato tutti i Cantoni, i partiti politici, le organizzazioni attive nell'ambito del perseguimento penale, quelle attive nel settore delle telecomunicazioni e diverse altre organizzazioni interessate[6].

Al DFGP sono pervenuti 106 pareri per un totale di circa 700 pagine. Tutti i Cantoni si sono pronunciati come pure 6 partiti politici e 74 organizzazioni. I pareri sono stati riassunti in un rapporto del maggio 2011[7].

Sostanzialmente, ci preme innanzitutto rilevare che tutti i partecipanti hanno riconosciuto, o si sono astenuti dal metterla in discussione, la necessità di adeguare la LSCPT alle evoluzioni tecniche di questi ultimi anni. Sono comunque state formulate numerose riserve, in parte di natura strutturale e generale, per quanto concerne le diverse disposizioni proposte. È stato necessario rielaborare completamente certune disposizioni. A suscitare reazioni sono stati soprattutto i temi esposti qui di seguito.

- Campo d'applicazione personale: numerosi partecipanti ne hanno sostenuto l'estensione. Molti si sono invece opposti o hanno chiesto di riformulare l'articolo 2 capoverso 1 lettera b AP–LSCPT per motivi di chiarezza o perché la disposizione si spingeva troppo oltre, in particolare per quanto concerne la sua portata o le sue implicazioni economiche per gli interessati. È pure stata contestata l'integrazione degli hosting provider nel campo d'applicazione personale della legge, nella misura in cui sono fornitori di servizi Internet.
- Conservazione centralizzata a lungo termine nel sistema informatico del Servizio dei dati raccolti durante la sorveglianza: questa forma di conservazione dei dati è stata approvata da molti partecipanti che hanno però auspicato alcuni adeguamenti, a volte importanti, segnatamente il mantenimento dell'invio per posta, su supporti di dati, dei dati non ottenuti tramite la sorveglianza di Internet. Un numero importante di partecipanti ha sottolineato

4 www.admin.ch/ch/i/gg/pc/documents/1719/Vorlage.pdf
5 www.admin.ch/ch/i/gg/pc/documents/1719/Bericht.pdf
6 www.admin.ch/ch/i/gg/pc/documents/1719/Adressatenliste.pdf
7 www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ve-ber-i.pdf

l'estrema complessità della normativa prevista e la sua eventuale incompatibilità con il CPP. Altri interpellati si sono opposti alla conservazione centralizzata e, per motivi di sicurezza, all'accesso mediante procedura di richiamo presso il Servizio che si prevedeva di concedere anche all'imputato e al suo difensore.

– Assenza di un obbligo del Servizio di verificare la legalità delle sorveglianze ordinate: un consistente numero di partecipanti ha chiesto che il Servizio sia sottoposto all'obbligo di verificare la legalità degli ordini di sorveglianza trasmessigli.

– Persone obbligate a collaborare: un gruppo importante di partecipanti alla consultazione ritiene che gli obblighi concreti delle persone assoggettate alla legge non siano disciplinati con sufficiente chiarezza.

– Obbligo generale dei fornitori di servizi di telecomunicazione di identificare gli utenti che accedono a Internet: un numero relativamente importante di interpellati si è rallegrato che la norma in questione sia riveduta in questo senso, in particolare per quanto concerne l'utilizzazione dei sistemi messi a disposizione dei clienti negli hotel, negli Internet café e simili. Numerosi partecipanti hanno invece chiesto di rinunciare a questa modifica della norma pertinente, perché tale obbligo sarebbe sproporzionato, se non irrealizzabile e inefficace.

– Prolungamento della durata di conservazione dei dati secondari da 6 a 12 mesi: in linea di massima, numerosi partecipanti hanno accolto favorevolmente il prolungamento. In molti si sono tuttavia opposti alla relativa disposizione o ne hanno chiesto la modifica facendo valere che la norma permetterebbe di conservare, per un periodo ancora più lungo, in modo sistematico e a titolo preventivo, dati concernenti persone al di sopra di ogni sospetto e hanno invocato le forti spese cagionate dal prolungamento.

– Soppressione dell'indennità dei fornitori di servizi postali e di telecomunicazione: numerosi partecipanti sono favorevoli a tale soppressione, poiché ritengono che l'indennità non si integri in modo armonioso nel sistema della legge. Molti altri hanno comunque rifiutato la soppressione dell'indennità perché il perseguimento penale è un compito dello Stato e deve quindi essere a carico della collettività, altri hanno stigmatizzato la necessità di acquisire infrastrutture costose per soddisfare i nuovi requisiti di legge o chiesto l'adozione di una normativa più graduata.

– Rimedi giuridici contro le decisioni di sorveglianza del Servizio: un numero importante di interpellati ha chiesto di prevedere espressamente la possibilità per i fornitori obbligati a collaborare di far esaminare da un giudice la legalità della decisione di sorveglianza notificata loro dal Servizio.

– Intercettazione dei dati mediante l'introduzione di GovWare nei sistemi informatici di terzi: un gran numero di partecipanti ha accolto con favore la possibilità di fare ricorso a GovWare, in particolare in considerazione del fatto che il problema del criptaggio dei dati sta assumendo sempre maggiore importanza. Un consistente gruppo di partecipanti si oppone tuttavia a questa utilizzazione di GovWare o ha formulato ampie riserve a tale riguardo in particolare tenuto conto della grave violazione della vita privata degli interessati che sussisterebbe nel caso in cui fosse possibile accedere a tutti i dati

contenuti in un sistema informatico (perquisizione online). Hanno inoltre rilevato i rischi eccessivi per la sicurezza informatica, i pericoli per l'affidabilità e l'integrità delle prove e, infine, hanno evocato la necessità di questa modalità di sorveglianza soltanto per i reati più gravi previsti nell'articolo 269 capoverso 2 CPP.

1.3.4 Adeguamenti successivi alla consultazione

Il messaggio poggia sull'AP-LSCPT sottoposto a consultazione e tiene conto delle principali obiezioni, osservazioni e proposte fondate contenute nei pareri dei partecipanti. Giova rilevare che il disegno è frutto di profonde modifiche, talora fondamentali, dell'AP-LSCPT.

Le modifiche concretizzate a seguito della consultazione sono presentate in appresso:

- il campo di applicazione personale della legge è stato precisato ed esteso a diverse categorie di persone e fornitori («persone obbligate a collaborare»); queste categorie sono caratterizzate dalle loro attività specifiche;
- i rispettivi obblighi delle diverse categorie di persone obbligate a collaborare sono stati precisati e completati. La portata degli obblighi di collaborazione è quindi stata definita attraverso l'attività specifica di ciascuna delle categorie di persone considerate;
- il DFGP avrà facoltà di istituire un organo consultivo per agevolare l'attuazione delle sorveglianze e dare continuità allo sviluppo del settore; l'organo è composto di rappresentanti delle cerchie interessate;
- il disegno prevede di rendere più pertinenti, semplificandole e adeguandole alle necessità delle autorità (in particolare delle autorità preposte al perseguimento penale), le disposizioni concernenti la conservazione centralizzata a lungo termine dei dati raccolti durante la sorveglianza nel sistema informatico del Servizio. Ciò riduce l'onere amministrativo del Servizio;
- il disegno prevede anche espressamente di rendere più efficace il sistema istituendo una base legale per un'interfaccia di trasferimento elettronico delle copie dei dati raccolti nel sistema del Servizio durante la sorveglianza in una banca dati prevista dalla legge del 13 giugno 2008[8] sui sistemi d'informazione di polizia della Confederazione (LSIP);
- il Servizio potrà compiere un esame materiale più ampio, sotto il profilo del diritto amministrativo, degli ordini di sorveglianza che gli vengono trasmessi. Se tale esame dovesse rivelare un problema, il Servizio sarà tenuto a informarne l'autorità che ha ordinato la sorveglianza e quella abilitata ad approvarla. Questa disposizione non mira a consentire un esame materiale di questioni relative alla procedura penale;
- si rinuncia a imporre ai fornitori di servizi di telecomunicazione un obbligo generale di identificare gli utenti che accedono a Internet;

8 RS **361**

– sono previste disposizioni relative al rispetto («compliance») da parte dei fornitori dei servizi di telecomunicazione degli obblighi relativi all'esecuzione delle sorveglianze del traffico delle telecomunicazioni. Sono pure previste disposizioni sulle conseguenze della violazione di questi obblighi;
– si rinuncia a sopprimere l'indennità dovuta ai fornitori di servizi postali e di telecomunicazione;
– il Servizio sarà competente per perseguire e giudicare i reati secondo la LSCPT. La legge federale del 22 marzo 1974[9] sul diritto penale amministrativo (PA) è applicabile;
– le persone obbligate a collaborare potranno far controllare da un giudice la legalità delle decisioni di sorveglianza notificate loro dal Servizio;
– l'intercettazione dei dati del traffico delle telecomunicazioni con l'introduzione di GovWare nei sistemi informatici di terzi deve essere ammissibile per i reati per i quali è permessa un'inchiesta mascherata (cfr. elenco dell'art. 286 cpv. 2 CPP). L'elenco più esteso dei reati per i quali è possibile la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (art. 269 cpv. 2 CPP) non è applicabile in caso di ricorso a GovWare.

1.4 Principali modifiche

1.4.1 Campo d'applicazione personale

Il campo d'applicazione personale è notevolmente esteso. Esso determina chi è assoggettato alla legge, vale a dire le persone che hanno degli obblighi in virtù della legge stessa. Nel campo d'applicazione personale della LSCPT vigente rientrano soltanto i fornitori di servizi postali o di servizi di telecomunicazione, tra i quali vi sono i fornitori di accesso a Internet, i gestori di reti di telecomunicazione interne e di centralini privati. Vi sono tuttavia anche altre persone o imprese in possesso di dati relativi alla corrispondenza postale o al traffico delle telecomunicazioni che possono essere necessari alle autorità di perseguimento penale. Tenuto conto di tali problemi, il campo d'applicazione personale è stato precisato nel disegno. Vi rientrano ora sei categorie di persone diverse («persone obbligate a collaborare»), a seconda delle loro attività specifiche. Si tratta delle seguenti categorie di persone:

– i fornitori di servizi postali (la Posta svizzera, i servizi di corriere ecc.);
– i fornitori di servizi di telecomunicazione (p. es. gli operatori telefonici classici);
– i fornitori di servizi che si fondano su servizi di telecomunicazione («fornitori di servizi di comunicazione derivati»; p. es. coloro che forniscono esclusivamente servizi e-mail);
– i gestori di reti di telecomunicazione interne (p. es. le reti interne delle imprese, «Intranet»);
– le persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazione (p. es. alberghi o cybercafé);

9 RS **313.0**

– i rivenditori professionali di carte o mezzi analoghi (carte prepagate ecc.) che permettono di accedere a una rete pubblica di telecomunicazione.

L'estensione degli obblighi di collaborazione è disciplinata separatamente per ciascuna categoria di persone nel rispetto del principio della proporzionalità (cfr. n. 1.4.6).

Per i dettagli rinviamo al commento all'articolo 2.

1.4.2 Organo consultivo

Il DFGP avrà la facoltà di istituire un organo consultivo composto di rappresentanti dei diversi attori del settore della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (DFGP, Servizio, Cantoni, autorità di perseguimento penale, fornitori di servizi postali e di telecomunicazione) per consentire un'esecuzione senza difficoltà delle sorveglianze e assicurare la continuità nello sviluppo del settore. In considerazione degli interessi contrari, talora contraddittori, di questi diversi attori, l'esperienza insegna che la loro collaborazione nel contesto di un organo consultivo è essenziale. Questa collaborazione già avviene su base informale senza essere prevista in un testo di legge.

Per i dettagli rinviamo al commento all'articolo 5.

1.4.3 Conservazione centralizzata a lungo termine dei dati raccolti durante la sorveglianza

Secondo il diritto vigente, il Servizio trasmette per posta alle autorità (di perseguimento penale) supporti di dati che contengono tutti i dati raccolti durante la sorveglianza del traffico delle telecomunicazioni. Il Servizio elimina i dati non appena l'autorità conferma al Servizio di averli ricevuti. I dati sono conservati nel fascicolo giudiziario, come qualsiasi altro mezzo di prova.

Secondo il disegno, questi dati vanno ora centralizzati nel sistema informatico del Servizio, dove sono conservati a lungo termine. Si tratta di tutti i dati della sorveglianza del traffico delle telecomunicazioni, compresi i dati delle sorveglianze telefoniche tradizionali e quelli della sorveglianza di Internet. Il principale argomento a favore di questo cambiamento è l'aumento dei dati risultanti dalla sorveglianza di Internet, circostanza che ne complica sempre più la trasmissione per via postale su supporti di dati, e il fatto che è sempre più difficile conservare e gestire questi supporti.

Nel nuovo sistema proposto dal disegno, le autorità (di perseguimento penale) accedono online ai dati riguardanti i fascicoli di loro competenza conservati nel sistema informatico del Servizio. Anche le parti, compreso l'imputato e il suo avvocato, potranno accedervi online. A determinate condizioni, i dati potranno come attualmente essere trasmessi su supporti mobili.

Per i dettagli rinviamo al commento agli articoli 6–14.

1.4.4 Interfaccia tra il sistema informatico del Servizio e la rete dei sistemi d'informazione di polizia dell'Ufficio federale di polizia

La rete dei sistemi d'informazione dell'Ufficio federale di polizia (fedpol) è in primo luogo utilizzata da fedpol e dalle polizie cantonali per valorizzare le informazioni ottenute nell'ambito delle inchieste penali. Il trasferimento elettronico online nei sistemi d'informazione di cui agli articoli 10 e 13 LSIP di una copia dei dati contenuti nel sistema informatico gestito dal Servizio presenta diversi vantaggi rispetto al trasferimento «manuale». Consente in particolare di guadagnare tempo e denaro e consolida la sicurezza dei dati (riduzione del rischio di perdita di dati e del rischio di errori che pregiudicano la qualità dei dati). Il passaggio al trasferimento elettronico dei dati non deve assolutamente avere per conseguenza l'elusione delle regole di accesso al sistema del Servizio e al relativo sistema d'informazione ai sensi della LSIP.

Per i dettagli rinviamo al commento all'articolo 14.

1.4.5 Esame materiale degli ordini di sorveglianza da parte del Servizio

Oltre all'esame formale già previsto nel diritto vigente, il Servizio potrà d'ora innanzi eseguire un esame materiale sotto il profilo del diritto amministrativo degli ordini di sorveglianza trasmessigli e dovrà avvertire l'autorità che ha ordinato la sorveglianza (di norma il pubblico ministero) e l'autorità d'approvazione (di norma il giudice dei provvedimenti coercitivi) se ritiene che l'esame ha rivelato un problema. Il Servizio potrà anche esaminare se l'ordine di sorveglianza trasmessogli è previsto nella legislazione e se tecnicamente è adeguato. Il Servizio non potrà invece esaminare gli aspetti materiali di questioni relative alla procedura penale; questo esame è infatti di competenza dell'autorità abilitata ad approvare le sorveglianze.

L'autorità che ha ordinato la sorveglianza e l'autorità d'approvazione potranno tenere conto del parere del Servizio, ma non saranno obbligate a farlo, e revocare o non autorizzare la sorveglianza ordinata. Questo meccanismo evita che il Servizio debba prendere una decisione «alla cieca» in seguito a un ordine di sorveglianza problematico e che i problemi possano essere esaminati da un'autorità giudiziaria soltanto su ricorso del fornitore interessato. Numerose incertezze possono così essere risolte in una fase precedente e con semplicità. Un rimedio giuridico particolare per regolare in giudizio eventuali divergenze tra il Servizio e l'autorità ordinante non è necessario. Siffatto rimedio giuridico è superfluo anche in considerazione della portata della tutela giurisdizionale di cui godono le persone obbligate a collaborare.

Per i dettagli rinviamo al commento all'articolo 16 lettera b.

1.4.6 Obblighi di collaborazione

Nella LSCPT vigente gli obblighi di collaborare non sono sufficientemente chiari. In considerazione del progresso tecnico del traffico delle telecomunicazioni negli ultimi anni le persone obbligate a collaborare devono inoltre fornire prestazioni supplementari.

Negli articoli 26–30 gli obblighi delle diverse categorie di persone obbligate a collaborare sono quindi stati sistematizzati, precisati, completati e definiti in funzione dell'attività specifica di ciascuna categoria.

In considerazione del carattere tecnico della materia, non occorre che la legge disciplini questi obblighi nei dettagli, cosa che sarà fatta in un'ordinanza del Consiglio federale; le disposizioni saranno inserite nell'ordinanza del 31 ottobre 2001[10] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT), come già è il caso secondo il diritto vigente. A determinate condizioni, il Consiglio federale potrà anche dispensare i fornitori di servizi di telecomunicazione da alcuni obblighi. Esso può tuttavia sottoporre alcune persone obbligate a collaborare (p. es. i fornitori di servizi e-mail) a tutti gli obblighi più estesi previsti per i fornitori di servizi di telecomunicazione o a parte di essi.

Le disposizioni esecutive tecniche e amministrative, che hanno per obiettivo la buona esecuzione con costi minimi dei tipi di sorveglianza abituali, non saranno più contenute come oggi nelle direttive del Servizio ma in ordinanze del DFGP.

Va menzionato che per motivi di fattibilità si rinuncia a prevedere un obbligo generale dei fornitori di servizi di telecomunicazione di identificare gli utenti di Internet, anche se in questo modo si tollera una lacuna nella sorveglianza.

Per i dettagli si veda il commento agli articoli 19–30.

1.4.7 Prolungamento della conservazione dei dati secondari e del periodo durante il quale possono essere ottenuti

A differenza dei cosiddetti dati di contenuto, i dati secondari non forniscono informazioni sul contenuto dell'invio o della telecomunicazione, ma informano soltanto sull'identità di coloro tra i quali si è svolta la corrispondenza o la comunicazione, sul momento e sul luogo in cui è avvenuta. Per perseguire i reati in modo più efficace si prevede di prolungare da sei a 12 mesi il periodo di conservazione dei dati secondari. Questi dati sono conservati «in riserva» per agevolare eventuali inchieste penali future e sono indispensabili per lottare contro la criminalità. I dati secondari non possono essere ottenuti a titolo preventivo ma per principio soltanto nell'ambito di un procedimento penale con l'autorizzazione dell'autorità competente per approvare le sorveglianze.

Questo prolungamento va posto in relazione con le richieste della mozione Schweiger 06.3170 (Lotta alla cibercriminalità. Protezione dei fanciulli) e della mozione Barthassat 10.4133 (Aumentare la durata di conservazione dei registri di assegnazione degli indirizzi Internet Protocol). La problematica affrontata da queste mozioni riguarda non soltanto i dati secondari di telecomunicazione bensì anche i dati secon-

10 RS **780.11**

dari postali. Le esperienze acquisite dalle autorità di perseguimento penale svizzere nell'ambito del diritto vigente mostrano infatti che l'attuale durata prescritta per la conservazione di questi dati (sei mesi) è troppo breve, poiché sovente questo termine è completamente o in gran parte trascorso quando l'autorità è in grado di ordinare una sorveglianza.

Per i dettagli si veda il commento agli articoli 19 capoverso 4 e 26 capoverso 5 nonché all'articolo 273 capoverso 3 CPP e 70*d* capoverso 3 PPM.

1.4.8 Informazioni sulla natura e le caratteristiche dei servizi

Per garantire la corretta esecuzione delle sorveglianze, il Servizio deve anche poter anticipare le difficoltà che potrebbero insorgere nel quadro delle sorveglianze future. Esso non deve reagire soltanto ai problemi occorsi nell'esecuzione di una nuova sorveglianza. I fornitori di servizi di telecomunicazione dovranno quindi spiegare al Servizio, su sua richiesta, quali servizi hanno messo sul mercato e quali intendono mettere sul mercato nei sei mesi successivi indicando cosa permettono di fare, fermo restando che i collaboratori del Servizio sono soggetti al segreto d'ufficio (art. 320 CP).

Per i dettagli si veda il commento all'articolo 25.

1.4.9 Rispetto degli obblighi e conseguenze della loro violazione («compliance»)

Per garantire la buona esecuzione delle sorveglianze, la legge contiene ora regole sul rispetto («compliance») degli obblighi da parte dei fornitori di servizi di telecomunicazione e disciplina le conseguenze della violazione di questi obblighi. Le relative disposizioni riguardano segnatamente la facoltà di fornire le informazioni e di attuare le sorveglianze. I fornitori, a loro spese, possono affidare in tutto o in parte a terzi l'esecuzione di questi compiti; rimangono tuttavia vincolati ai pertinenti obblighi.

Queste disposizioni riguardano anche la prova della disponibilità a informare e a sorvegliare. Disciplinano inoltre le conseguenze finanziarie in caso di insufficiente disponibilità.

Per i dettagli si veda il commento agli articoli 32–34.

1.4.10 Sorveglianze al di fuori di procedimenti penali

La sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni nei casi d'emergenza in cui occorre ritrovare una persona scomparsa non è più limitata ai dati secondari, contrariamente a quanto prevede l'articolo 3 della LSCPT vigente. Infatti la legge permetterà di ottenere anche il contenuto degli invii nell'ambito della corrispondenza postale e del traffico delle telecomunicazioni, poiché tali informazioni possono consentire di scoprire il luogo dove si trova la persona scomparsa. Questa sorveglianza è sussidiaria rispetto alle altre misure che

possono essere adottate per trovare la persona ricercata. È anche permesso il ricorso ai dispositivi tecnici di sorveglianza di cui all'articolo 269bis CPP, come gli IMSI-catcher, che vanno tuttavia impiegati in modo sussidiario rispetto ai summenzionati mezzi di ricerca. Questo tipo di sorveglianza può permettere di ritrovare una persona scomparsa anche nel caso in cui le misure di sorveglianza del traffico delle telecomunicazioni di tipo classico si sono rivelate inefficaci. In caso di necessità resta possibile sorvegliare la corrispondenza postale e il traffico delle telecomunicazioni di un terzo non implicato invece di quelli della persona scomparsa, come prevede l'articolo 3 capoverso 1 LSCPT vigente.

La sorveglianza evocata sopra deve poter essere ordinata anche per ritrovare un condannato a una pena detentiva o una persona nei cui confronti è stata disposta una misura privativa della libertà. La sorveglianza, possibile nell'ambito di un procedimento penale in corso, deve essere ammissibile anche nei casi menzionati. La sorveglianza possibile nell'ambito di un procedimento penale pendente deve esserlo anche quando non vi è soltanto un grave sospetto (art. 269 cpv. 1 lett. a CPP) ma anche qualora sia stata pronunciata una sentenza definitiva ed esecutiva.

La procedura relativa alle sorveglianze compiute al di fuori dei procedimenti penali è in linea di massima retta per analogia dagli articoli 274–279 CPP.

Per i dettagli si vedano il commento agli articoli 35–37 e il n. 1.4.14.

1.4.11 Disposizioni penali

La presente revisione contiene disposizioni penali che puniscono la violazione di obblighi che potrebbero pregiudicare la sorveglianza. Tali sanzioni devono tuttavia essere pronunciate soltanto sussidiariamente rispetto a disposizioni penali più severe le cui condizioni sono pure adempite. Si tratta per esempio delle disposizioni penali sulla protezione del segreto d'ufficio (art. 320 CP) o del segreto postale e del segreto delle telecomunicazioni (art. 321ter CP) o del favoreggiamento (art. 305 CP). L'esperienza mostra che i fornitori importanti di servizi di telecomunicazione sono in linea di massima consapevoli dei loro obblighi e li adempiono.

In caso di inosservanza delle ingiunzioni del Servizio, occorre applicare una norma penale che riprende il meccanismo dell'articolo 292 CP. In considerazione delle economie che una persona obbligata a collaborare può realizzare non eseguendo un'ingiunzione di sorveglianza del Servizio, il massimo della multa (10 000 franchi secondo l'art. 292 CP) non avrebbe effetto dissuasivo. Appare quindi giustificata una disposizione specifica che preveda una pena più severa.

Tenuto conto della mozione Schweiger 06.3170 (Lotta alla cibercriminalità. Protezione dei fanciulli), il disegno prevede un'altra disposizione penale che punisce la violazione dell'obbligo di conservare i dati secondari. Sono altresì puniti la violazione degli obblighi di documentazione (in particolare la registrazione di dati personali o di clienti), in occasione della consegna di carte o di mezzi analoghi che permettono di accedere a una rete pubblica di telecomunicazione senza sottoscrivere un abbonamento (p. es. mediante carte SIM prepagate). L'esperienza mostra infatti che

una tale sanzione è necessaria per far rispettare questi obblighi di documentazione[11]. Come attualmente, è punito anche il fatto di non serbare il segreto sulla sorveglianza nei confronti di terzi.

Il perseguimento e il giudizio dei succitati reati è di competenza del Servizio. A favore di questa soluzione vi sono numerosi argomenti: il Servizio è l'organo che meglio può venire a conoscenza di fatti costituenti siffatti reati. Inoltre, l'articolo 39 punisce l'inosservanza degli ordini del Servizio. Peraltro, occorre rilevare che la LSCPT conferisce al Servizio compiti di sorveglianza amministrativa. Infine, il perseguimento e il giudizio di questi reati richiedono conoscenze tecniche molto approfondite di cui probabilmente le autorità di perseguimento penale dei Cantoni dispongono in misura minore rispetto al Servizio.

Viste le competenze del Servizio questi reati sono perseguiti e giudicati conformemente al DPA.

Per i dettagli si veda il commento agli articoli 39 seg.

1.4.12 Sorveglianza amministrativa

Occorre garantire che soltanto le persone e le imprese che rispettano le prescrizioni in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni possano operare sul mercato svizzero. Rendere parzialmente applicabile per analogia l'articolo 58 della legge del 30 aprile 1997[12] sulle telecomunicazioni (LTC) contribuisce a realizzare questo obiettivo. Il Servizio può così pronunciare intimazioni in caso di violazione delle prescrizioni in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Si instaura così un sistema di sanzioni amministrative distinto e complementare al sistema delle sanzioni penali (cfr. n. 1.4.11). Il Servizio esercita le sue competenze di sorveglianza in modo vincolante per le persone obbligate a collaborare. Tale non è però il caso nei confronti delle autorità che ordinano le sorveglianze e delle autorità abilitate ad approvarle, visto che non è dotato di una competenza decisionale che si imponga a queste autorità (cfr. n. 1.4.5).

Per i dettagli si veda il commento all'articolo 41.

1.4.13 Rimedi giuridici contro le decisioni del Servizio sulla sorveglianza

La LSCPT vigente non contiene disposizioni sui rimedi giuridici contro le decisioni del Servizio; è applicabile unicamente l'articolo 32 dell'attuale OSCPT.

Per motivi di chiarezza e di certezza del diritto, nella legge viene introdotta una disposizione sulla tutela giurisdizionale contro le decisioni del Servizio. La disposizione riprende i principi del diritto in vigore. Le persone obbligate a collaborare possono così far esaminare da un giudice la legalità della decisione di sorveglianza

11 Thomas Hansjakob, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2ª ed., San Gallo 2006, n. 2 ad art. 19*a* OSCPT.

12 RS **784.10**

notificata loro dal Servizio, senza tuttavia poter invocare questioni che riguardano il procedimento penale (p. es. la sussistenza di gravi sospetti secondo l'art. 269 cpv. 1 lett. a CPP o l'adempimento delle condizioni per la sorveglianza di un terzo secondo l'art. 270 lett. b CPP).

In considerazione del carattere urgente che spesso ha una sorveglianza, il ricorso contro una decisione di sorveglianza del Servizio non ha effetto sospensivo. È tuttavia previsto che l'autorità di ricorso possa attribuire l'effetto sospensivo al ricorso.

Per i dettagli si veda il commento all'articolo 42.

1.4.14 Ricorso a dispositivi tecnici di sorveglianza

Il complemento al CPP (e alla PPM) deve consentire al pubblico ministero (e al giudice istruttore militare) di fare più ampia utilizzazione di dispositivi come gli IMSI-catcher per identificare apparecchi di comunicazione mobili (non soltanto apparecchi di telefonia mobile) e di conseguenza i loro utenti. Questo impiego dell'IMSI-catcher si aggiunge all'ascolto e alla registrazione delle comunicazioni e alla localizzazione degli apparecchi o utenti sunnominati. Oltre a costituire una misura necessaria al perseguimento dei reati, questo complemento si giustifica anche poiché l'identificazione è una misura che lede in modo meno tangibile la sfera privata degli utenti rispetto alla localizzazione, all'ascolto e alla registrazione delle conversazioni[13].

Il ricorso a un IMSI-catcher ordinato dal pubblico ministero sottostà all'approvazione del giudice dei provvedimenti coercitivi in quanto misura di sorveglianza del traffico delle telecomunicazioni oggetto dell'articolo 269 CPP.

Per i dettagli si veda il commento all'articolo 269bis CPP e all'articolo 70bis PPM.

1.4.15 Ricorso a Government Software

Il progetto completa il CPP (e la PPM) con una base legale ad hoc che permette al pubblico ministero (e al giudice istruttore militare) di ordinare nell'ambito di un procedimento penale (ma non a titolo preventivo) e nel rispetto di condizioni restrittive l'utilizzazione di programmi informatici comunemente noti come GovWare. L'impiego di GovWare deve rimanere sussidiario rispetto alle misure di sorveglianza classiche, fermo restando il principio della proporzionalità.

I GovWare sono introdotti in un sistema informatico al fine di intercettare il contenuto delle comunicazioni e dei dati secondari. Il ricorso ai GovWare è tuttavia ammissibile soltanto per i reati per i quali può essere ordinata un'inchiesta mascherata (cfr. l'elenco dell'art. 286 cpv. 2 CPP). L'elenco più esteso dei reati per i quali è possibile una sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (cfr. art. 269 cpv. 2 CPP) non è applicabile al ricorso ai GovWare. Ovviamente, questi programmi sono introdotti in un sistema informatico all'insaputa del suo detentore. Questo tipo di sorveglianza non richiede la collaborazione di un

13 Sophie de Saussure, Le IMSI-Catcher: fonctions, applications pratiques et légalité, Jusletter 30.11.2009, n. marg. 45–56 e 70

fornitore di servizi di telecomunicazione. Il Servizio non svolge alcun compito particolare nell'impiego del GovWare.

Possono così essere ottenuti non soltanto i dati relativi alla telefonia via Internet e alla corrispondenza tramite e-mail ma anche tutti i dati relativi al traffico delle telecomunicazioni, di cui fa parte anche la corrispondenza via Internet. Per «sistema di trattamento dei dati» si intende ogni apparecchio che permette il traffico delle telecomunicazioni, mediante la rete telefonica o un altro mezzo, come i computer (portatili) o i telefoni portatili.

La perquisizione online di un sistema di trattamento dei dati mediante un GovWare, perquisizione che consente di accedere a tutti i dati personali (p. es. documenti, foto) è vietata. È pure escluso il ricorso a un GovWare per utilizzare la webcam o il microfono di un computer per scopi diversi dalla sorveglianza del traffico delle telecomunicazioni, per esempio per sorvegliare un locale.

Le autorità di perseguimento penale (della Confederazione e dei Cantoni) si sono servite in alcuni casi di GovWare sulla base delle disposizioni di procedura penale in vigore prima dell'entrata in vigore del CPP. Vi è disaccordo sull'ammissibilità nel diritto vigente dell'utilizzazione dei GovWare; questa possibilità è per lo più rifiutata[14]. Occorre dunque adottare una base legale ad hoc per poter ricorrere ai GovWare ai fini e nelle condizioni summenzionati.

Per maggiori dettagli si veda il commento all'articolo 269ter CPP e all'articolo 70ter PPM.

1.4.16 Blocco dell'accesso ai servizi di telecomunicazione

A determinate condizioni si prevede di assoggettare i fornitori di servizi di telecomunicazione a un obbligo di bloccare l'accesso di taluni clienti alla telefonia e a Internet per contribuire a identificare le persone che accedono a questi servizi senza aver sottoscritto un abbonamento (p. es. mediante carte SIM prepagate).

Per i dettagli si veda il commento all'articolo 6*a* LTC.

1.4.17 Confronto con il diritto estero, segnatamente europeo

Nei Paesi limitrofi della Svizzera vigono regimi di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni simili all'ordinamento previsto nel presente progetto. Vi è tuttavia qualche differenza rispetto alla presente normativa.

Per quanto concerne i dati secondari, occorre innanzitutto menzionare la direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006[15]. Essa autorizza la conservazione di questi dati per sei mesi al minimo e, in linea di massima, per due anni al massimo dalla data della comunicazione.

14 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 16; di diverso parere Sylvain Métille, op. cit., n. 37

15 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L 105 del 13.4.2006, pag. 54.

In Germania il ricorso a dispositivi come gli IMSI-catcher è autorizzato. Se la sorveglianza dei dati del traffico delle telecomunicazioni mediante GovWare sia legalmente ammissibile nell'ambito di un procedimento penale è aspramente contestato. Tuttavia, nel rispetto di condizioni severe, è ammissibile fare ricorso ai GovWare a titolo preventivo per compiere una perquisizione online, che comprende la sorveglianza dei dati relativi al traffico delle telecomunicazioni. La conservazione dei dati secondari, prevista per una durata di sei mesi dalla data della comunicazione, rimane controversa. La Corte costituzionale tedesca ha infatti dichiarato contrarie al diritto le prescrizioni relative alla registrazione di questi dati, precisando però che il principio della conservazione di tali dati non lo è se sono utilizzati soltanto in relazione con i reati più gravi.

In Austria, la durata della conservazione dei dati secondari è di sei mesi dalla data della comunicazione. Il ricorso agli IMSI-catcher è pure permesso. Il governo austriaco intende creare una base legale al fine di poter utilizzare i GovWare per compiere in determinati casi perquisizioni online, operazioni che comprendono la sorveglianza dei dati relativi al traffico delle telecomunicazioni. Negli ultimi mesi il relativo progetto è stato esaminato dal Parlamento austriaco.

In Francia, la durata di conservazione dei dati secondari è di 12 mesi dalla data della comunicazione. Il ricorso agli IMSI-catcher è permesso. La perquisizione online nel senso esposto sopra è consentita a determinate condizioni.

In Italia, la durata di conservazione dei dati secondari varia da 12 a 24 mesi dalla data della comunicazione, in funzione del tipo di dati di cui si tratta. Il ricorso agli IMSI-catcher e ai GovWare non sembra essere esplicitamente disciplinato.

1.5 Interventi parlamentari

Degli interventi parlamentari relativi alla revisione della LSCPT ancora pendenti[16] ci occupiamo nel commento alle singole disposizioni del disegno. Proponiamo di toglierli dal ruolo.

16 Cfr. n. 2.4, 2.6 e 2.10 (ad art. 19, 26 e 39) ad 06.3170 Mo. Schweiger Rolf: Lotta alla cibercriminalità. Protezione dei fanciulli, del 24.3.2006; n. 2.1 e 2.6 (ad art. 2, 21, 26, 28 e 29) ad 07.3627 Mo. Glanzmann-Hunkeler Ida: Obbligo di registrazione delle carte prepagate Wi-Fi, del 3.10.2007; n. 2.6 (ad art. 26) ad 10.4133 Mo. Barthassat Luc: Aumentare la durata di conservazione dei registri di assegnazione degli indirizzi Internet Protocol, del 17.12.2010; n. 2.2, 2.3, 2.6, 2.9 e 2.12 (ad art. 6–18, 23 e 35, art. 269bis–269ter CPP e art. 70bis–70ter PPM) ad 10.3831 Mo. Schmid-Federer Barbara: Revisione della LSCPT, del 1.10.2010; n. 2.2, 2.3, 2.4, 2.7 e 2.10 (ad art. 6–18, 26 e 38, art. 269bis–269ter CPP e art. 70bis –70ter PPM) ad 10.3876 Mo. Eichenberger-Walther Corina : Revisione della LSCPT, del 1.10.2010; n. 2.2, 2.3, 2.6, 2.9 e 2.12 (ad art. 6 à 18, 26 et 38, art. 269bis e 269ter CPP e art. 70bis e 70ter PPM) ad 10.3877 Mo. (von Rotz Christoph) Schwander Pirmin: Revisione della LSCPT, del 1.10.2010; n. 2.12 (ad art. 269bis –269ter CPP e art. 70bis–70ter PPM) ad 11.4042 Po. Commissione degli affari giuridici CN: Sorveglianza tramite cavalli di Troia (1), del 11.11.2011; n. 2.12 (ad art. 269bis–269ter CPP e art. 70bis–70ter PPM) ad 11.4043 Po. Commissione degli affari giuridici CN: Sorveglianza tramite cavalli di Troia (2), del 11.11.2011 ; n. 2.9 (ad art. 38) ad 10.4210 Po. Recordon Luc: Costo della sorveglianza penale delle telecomunicazioni, del 23.12.2011.

2 Commento ai singoli articoli

2.1 Sezione 1: Disposizioni generali

Art. 1 Campo d'applicazione materiale

L'articolo 1 definisce il campo d'applicazione materiale della LSCPT.

Il *capoverso 1* non è oggetto di modifiche fondamentali rispetto alla versione vigente. Il campo d'applicazione materiale comprende la sorveglianza della corrispondenza postale. Comprende anche la sorveglianza del traffico delle telecomunicazioni secondo l'articolo 269 capoverso 1 CP e conformemente alla definizione di telecomunicazione secondo gli articoli 2 e 3 lettera c LTC. La corrispondenza via Internet comprende segnatamente la corrispondenza via e-mail[17] ed è un genere particolare di traffico delle telecomunicazioni. La sua sorveglianza rientra dunque nel campo d'applicazione materiale della LSCPT. È evidente che la telefonia via Internet, che è una forma di corrispondenza via Internet, è pure una forma di traffico delle telecomunicazioni, cosicché anche la sua sorveglianza rientra nel campo d'applicazione. L'ammissibilità di una sorveglianza non dipende dalla via della trasmissione dei dati né dalle tecnologie utilizzate. Come la telefonia convenzionale, la telefonia via Internet è soggetta al segreto delle telecomunicazioni secondo l'articolo 43 LTC. L'articolo 269 CPP sancisce la base legale per la dispensa da questo segreto al fine di ottenere le prove necessarie nell'ambito di una procedimento penale[18].

Con la modifica del *capoverso 1 lettera a* sono soppresse le menzioni del carattere federale o cantonale del procedimento. Infatti queste menzioni non sono più necessarie, dopo l'entrata in vigore del CPP, che si applica sia ai procedimenti della Confederazione sia a quelli dei Cantoni e prevede l'esecuzione di sorveglianze della corrispondenza postale e del traffico delle telecomunicazioni nell'ambito di questi procedimenti.

Il *capoverso 1 lettera b* sostanzialmente non subisce modifiche rispetto alla sua formulazione nel diritto vigente.

La menzione del salvataggio contenuta nel *capoverso 1 lettera c* della LSCPT vigente può essere soppressa perché questo obiettivo risulta logicamente dalla volontà di ricerca della persona scomparsa (art. 35). Il *capoverso 1 lettera c* riguarda anche la ricerca di persone in caso di catastrofe (cfr. commento dell'art. 35).

Il *capoverso 1 lettera d* prevede d'ora innanzi l'applicazione della LSCPT alla ricerca, in base a una sentenza definitiva ed esecutiva, di una persona condannata a una pena detentiva o nei confronti della quale è stata disposta una misura di privazione della libertà, indipendentemente dal reato commesso (cfr. commento dell'art. 36).

Il *capoverso 2* riguarda, come il capoverso 3 della LSCPT vigente, le informazioni sui servizi di pagamento assoggettati alla legge del 17 dicembre 2010[19] sulle poste (LPO). Sono eliminati i riferimenti al carattere federale o cantonale delle disposizioni in questione per tenere conto dell'entrata in vigore del CPP che si applica ai procedimenti federali e cantonali e che disciplina l'obbligo di testimoniare e

17 Bernard Corboz, *Les infractions en droit suisse*, vol. II, Berna 2010, n. 6 ad art. 321ter CP.
18 Thomas Hansjakob, *Einsatz von GovWare – zulässig oder nicht?*, Jusletter 5.12.2011, n. 14.
19 RS **783.0**

l'obbligo di informare le autorità (art. 284 e 285). Nell'ambito della sua attività connessa con il traffico dei pagamenti, la posta va considerata un «istituto analogo» a una banca ai sensi dell'articolo 284 CPP. Il rinvio del *capoverso 2* concerne per esempio anche le corrispondenti disposizioni della PPM.

Art. 2 Campo d'applicazione personale

L'*articolo 2* definisce, come fa l'articolo 1 capoverso 2 della LSCPT vigente, il campo d'applicazione personale della LSCPT, vale a dire le persone assoggettate a tale legge e a cui la stessa impone obblighi. Tutte queste persone sono indicate nel disegno e nel presente messaggio con l'espressione generica «persone obbligate a collaborare». I diversi obblighi di sorveglianza di ciascuna categoria di persone sono disciplinati in particolare negli articoli 19–30 del disegno.

Durante la consultazione, sono stati formulati pareri discordanti sull'estensione del campo d'applicazione personale proposta nell'AP-LSCPT. Un certo numero di Cantoni e organizzazioni che operano nell'ambito del perseguimento penale si sono espressi a favore dell'estensione. Ma molti partecipanti, segnatamente le organizzazione di protezione dei consumatori e dei fornitori di servizi di telecomunicazione, si sono invece opposti all'estensione proposta o hanno chiesto di riformulare l'articolo 2 capoverso 1 lettera b AP-LSCPT. Si trattava di stabilire se l'articolo 2 capoverso 1 lettera b AP-LSCPT fosse comprensibile e se la sua portata e le sue implicazioni economiche per gli interessati non fossero eccessive. Occorreva anche stabilire se fosse opportuno far rientrare gli hosting provider nel campo d'applicazione personale della legge. Per il rimanente, vedi il rapporto sui risultati della consultazione[20].

Effettivamente il campo d'applicazione personale della legge non è definito in modo sufficientemente chiaro dal diritto vigente, in particolare il testo dell'articolo 2 capoverso 1 lettera b AP-LSCPT. La disposizione poteva essere interpretata facendo rientrare nel campo d'applicazione qualsiasi persona che, in un modo o nell'altro, si occupava di dati di comunicazione (p. es. un'impresa che si limita a offrire soluzioni per la sicurezza delle reti). Ciò era eccessivo, anche in considerazione dei costi occasionati a queste persone. Questa mancanza di chiarezza è stata di conseguenza corretta nel disegno.

Nel disegno proponiamo obblighi differenti per le diverse categorie di persone (cfr. commento delle lett. a–f), caratterizzate dalle loro attività, ciascuna di queste attività dovendo essere considerata indipendentemente dalle altre. Una stessa impresa può certamente ricadere in diverse categorie a seconda delle sue attività e dunque avere obblighi di sorveglianza distinti in funzione delle sue attività (cfr. art. 19–30). La LSCPT si applica a qualsiasi persona che adempie le condizioni delle diverse categorie citate, indipendentemente dal fatto che si tratti di una persona fisica o di un organismo, poco importa se quest'ultimo sia una persona giuridica o no o che abbia carattere statale o no.

Il campo d'applicazione personale è così precisato e modificato rispetto al diritto in vigore che menziona soltanto i fornitori di servizi postali e di telecomunicazione, di cui fanno parte i fornitori di accesso a Internet e gli esercenti di reti di telecomunicazione interne e di centrali domestiche. In effetti, oltre alle persone menzionate, ve ne

20 www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ve-ber-i.pdf

sono altre che possono possedere in un determinato momento dati relativi alla corrispondenza postale o al traffico delle telecomunicazioni suscettibili di interessare le autorità di perseguimento penale nell'ambito della lotta contro la criminalità. È pertanto legittimo che preveda di assoggettarle a determinati obblighi nell'ambito della sorveglianza di tale corrispondenza e di tale traffico. Citiamo, per esempio, il caso degli hosting provider che sono fornitori di servizi Internet (cfr. commento della lett. c).

Il campo d'applicazione personale è così modificato rispetto alla legge vigente poiché, a differenza di quest'ultima, la nuova LSCPT non prevede che i fornitori di servizi postali o di telecomunicazione entrino nel campo d'applicazione soltanto se assoggettati a concessione o all'obbligo di notifica (cfr. commento delle lett. a e b)[21].

La *lettera a* non concerne soltanto la Posta Svizzera in quanto fornitrice di servizi postali ma anche tutti gli altri operatori che forniscono questi servizi sul mercato postale. Contrariamente a quanto prevede la LSCPT vigente, l'assoggettamento di un fornitore di servizi postali alla nuova LSCPT non dipende dal fatto che sia assoggettato alla concessione o all'obbligo di notifica. Ne risulta in particolare che entrano nel campo d'applicazione della legge anche i fornitori di servizi postali che non sono assoggettati all'obbligo di notifica ordinaria secondo l'articolo 3 dell'ordinanza del 29 agosto 2012 sulla posta[22]. Citiamo a titolo di esempio i servizi di corriere e i servizi rapidi di posta. Invece, i servizi bancari offerti da alcuni fornitori di servizi postali non sono presi in considerazione in quanto attività (cfr. anche commento all'art. 1 cpv. 2).

La *lettera b* riguarda gli operatori principali del settore della sorveglianza del traffico delle telecomunicazioni, vale a dire i fornitori di servizi di telecomunicazione. La definizione del fornitore di servizi di telecomunicazione ai sensi della LSCPT si trova nella legislazione in materia di telecomunicazioni all'articolo 3 lettere a–c, in particolare lettera b LTC, e all'articolo 2 dell'ordinanza del 9 marzo 2007[23] sui servizi di telecomunicazione (OST). Cosa sia o non sia un fornitore di servizi di telecomunicazione ai fini della succitata normativa vale anche per la LSCPT. In sintesi, il fornitore di servizi di telecomunicazione si impegna a trasportare o a trasmettere informazioni per conto di un terzo (ai sensi dell'art. 3 lett. a e c LTC). Le persone di cui alla lettera c, come gli hosting provider, non sono fornitori di servizi di telecomunicazione, *a fortiori*, poiché non trasmettono né trasportano dati essi stessi (cfr. commento alla lett. c). Le medesime considerazioni valgono per le persone di cui alla lettera e, come per esempio gli Internet o cyber café e gli alberghi, poiché non trasmettono dati essi stessi (cfr. commento alla lett. e). La situazione è la medesima per le persone di cui alla lettera d poiché non trasmettono dati per conto di un terzo, per il pubblico (cfr. commento alla lett. d). Sono invece considerati fornitori di servizi di telecomunicazione i grandi operatori presenti sul mercato svizzero, come Swisscom, Orange, Sunrise e Cablecom che danno agli utenti la possibilità di telefonare mediante telefono fisso o cellulare, o di accedere a Internet. I fornitori di accesso a Internet costituiscono in effetti dei fornitori di servizi di telecomunicazione ai sensi della legislazione in materia di telecomunicazioni e, di conseguenza, ai sensi della LSCPT e ciò indipendentemente dall'esercizio di un'altra attività come

21 Thomas Hansjakob, op. cit. (nota 11), n. 24 ad art. 1 LSCPT.
22 RS **783.01**
23 RS **784.101.1**

quella di operatore telefonico. Ben diversa è invece la situazione degli altri fornitori di servizi Internet, segnatamente gli hosting provider. Se del caso questi ultimi ricadono sotto la lettera c (cfr. per il rimanente il commento della lett. c).

Diversamente dalla LSCPT vigente, la *lettera b* non prevede che soltanto i fornitori di servizi di telecomunicazione assoggettati a concessione o all'obbligo di notifica (art. 4 cpv. 1 LTC) entrano nel campo d'applicazione. È quindi teoricamente possibile che un fornitore di servizi di telecomunicazione sia dispensato dagli obblighi derivanti dalla legislazione in materia di telecomunicazioni in virtù degli articoli 4 capoverso 2 LTC e 3 OST ma non dagli obblighi previsti dalla regolamentazione in materia di sorveglianza delle telecomunicazioni, fermo restando che anche questa normativa può prevedere siffatte dispense (cfr. commento dell'art. 26 cpv. 6).

La *lettera c* riguarda persone che non fornendo accesso a Internet non sono considerate fornitori di servizi di telecomunicazione ai sensi della legge per l'attività che esercitano (cfr. commento della lett. b) ma svolgono comunque un ruolo nel processo del traffico delle telecomunicazioni in particolare via Internet, fornendo servizi che possono essere offerti soltanto in relazione con l'attività di un fornitore di servizi di telecomunicazione, più precisamente di un fornitore di accesso a Internet. Queste persone non sono fornitori di servizi di telecomunicazione, *a fortiori*, poiché non trasmettono né trasportano dati esse stesse. Senza un fornitore di servizi di telecomunicazione che trasmetta dati, tali persone, seppur fornendo servizi Internet, non possono fornire i loro servizi. In seguito queste persone saranno quindi chiamate «fornitori di servizi di comunicazione derivati».

Le *lettera c* riguarda i fornitori di servizi Internet che permettono una comunicazione unilaterale che rende possibile il caricamento di documenti (p. es. Google docs o Microsoft office.live.com), e quelli che consentono una comunicazione multilaterale rendendo possibile la comunicazione tra utenti (p. es. Facebook); in proposito poco importa che si tratti di una comunicazione sincrona o asincrona. Vanno per esempio considerati tali i fornitori di spazio di archiviazione di e-mail, i diversi generi di hosting provider che ospitano applicazioni o servizi di e-mail (p. es. .gmx), che offrono la collocazione di server o «server housing» e l'accesso (p. es. Green.ch e Colt), che offrono servizi di «Facility Management» senza servizi di comunicazione (collocazione pura) o servizi «cloud», piattaforme di chat, piattaforme di scambio di documenti e fornitori di servizi di telefonia via Internet del tipo peer-to-peer (p. es. Skype peer-to-peer). Occorre rilevare che un'impresa che propone un prodotto di criptaggio non «permette» la comunicazione ai sensi della lettera c ma tutt'al più la agevola, ragion per cui la presente disposizione non si applica e non rientra di conseguenza nel campo d'applicazione personale. Occorre pure rilevare che una determinata impresa, per esempio Swisscom, può esercitare attività che ne fanno sia un fornitore di servizi di telecomunicazione sia una delle persone di cui alla lettera c (attività di e-mail provider o di hosting provider). Se del caso, potrà avere obblighi di sorveglianza distinti, in funzione delle sue diverse attività (cfr. art. 26 e 27).

Va tuttavia precisato che – come dimostrano le imprese menzionate a titolo di esempio – l'integrazione delle persone secondo la *lettera c* nel campo d'applicazione personale non dovrebbe suscitare speranze smisurate per quanto concerne la sorveglianza del traffico delle telecomunicazioni. In effetti, molti importanti fornitori di servizi Internet hanno sede all'estero dove si trova anche la loro infrastruttura. L'apertura di determinati conti e-mail ubicati all'estero da parte di persone che vivono in Svizzera, di per sé servizi tecnicamente controllabili, è un esempio che illustra questa situazione. Prevedere in generale che le autorità svizzere potrebbero

accedere senza problemi ai dati in questione sarebbe quindi poco realista e problematico poiché contravverrebbe al principio della territorialità delle leggi. Una tale normativa non è prevista nella legge vigente. Per quanto concerne l'obbligo di deposito dei dati secondari dei fornitori di servizi di comunicazione derivati, rinviamo al commento dell'articolo 27 capoverso 2.

Le persone di cui alla *lettera d* non sono considerate fornitori di servizi di telecomunicazione (cfr. commento alla lett. b), poiché non forniscono servizi ai terzi, al pubblico ma unicamente a una cerchia limitata di persone che possiedono una particolare caratteristica; queste reti non sono pertanto accessibili a tutti. Citiamo come esempio un'impresa che mette a disposizione dei suoi collaboratori una rete affinché possano comunicare tra loro (cfr. art. 2 OST). Si tratta delle persone di cui al vigente articolo 1 capoverso 4 LSCPT. È tuttavia stato soppresso il riferimento agli esercenti di reti di telecomunicazioni interne, poiché anche le centrali domestiche rientrano nella definizione di rete di telecomunicazioni interna poiché richiedono l'esistenza di una rete. Si veda il commento dell'articolo 28.

La *lettera e* riguarda le persone che mettono il loro accesso a disposizione di terzi. Si può trattare di alberghi, ristoranti, caffè, Internet caffè o cyber caffè, ospedali, scuole ecc. che mettono il loro accesso a Internet (Wifi, fisso o di altro tipo) a disposizione di terzi, in particolare dei loro clienti o pazienti, alunni ecc. Può anche trattarsi di semplici individui che fanno altrettanto, volontariamente o no, per dei terzi. L'integrazione di queste persone nel campo d'applicazione personale è in particolare una conseguenza di quanto richiesto dalla mozione 07.3627 Glanzmann-Hunkeler. In effetti, queste persone non sono attualmente menzionate. Esse non sono considerate fornitori di servizi di telecomunicazione, poiché non trasmettono esse stesse informazioni per conto di terzi ma delegano questa funzione ai fornitori di servizi di telecomunicazione come Swisscom, Orange, Sunrise e Cablecom (cfr. commento della lett. b). Per quanto concerne il rapporto tra gli obblighi delle persone di cui alla lettera e e la mozione 07.3627 Glanzmann-Hunkeler, rinviamo al commento dell'articolo 29.

La *lettera f* è formulata in modo relativamente ampio per tenere conto dell'evoluzione tecnologica. La disposizione riguarda in particolare non soltanto il settore della telefonia mobile ma anche quello della telefonia fissa e di Internet e riguarda quindi innanzitutto i rivenditori di mezzi come le schede SIM prepagate e le carte di accesso senza fili a Internet prepagate. Essa non riguarda invece i venditori di semplici schede telefoniche che permettono di telefonare senza denaro dalle cabine telefoniche (p. es. «taxcard» dotate di un credito e vendute nei chioschi). I rivenditori di cui alla *lettera f* (p. es. Interdiscount, Media Markt e Mobilzone) non sono fornitori di servizi di telecomunicazione (cfr. commento della lett. b) ma vendono i mezzi di tali fornitori (p. es. Swisscom, Orange e Sunrise). L'integrazione dei rivenditori di carte d'accesso prepagate wifi a Internet nel campo d'applicazione personale è segnatamente una conseguenza di quanto richiesto dalla mozione 07.3627 Glanzmann-Hunkeler. Le persone di cui alla *lettera f* attualmente non entrano nel campo d'applicazione della legge. Questa disposizione vuole inoltre contribuire a colmare una lacuna per quanto concerne l'obbligo dei fornitori di servizi di telecomunicazione di registrare i dati dei clienti ai quali consegnano schede SIM prepagate (cfr. commento dell'art. 30). Per quanto concerne gli obblighi dei rivenditori di schede prepagate d'accesso wifi a Internet, si veda il commento dell'articolo 30.

Art. 3 Servizio di sorveglianza

L'*articolo 3* riprende e completa l'articolo 2 della vigente LSCPT.

Dal *capoverso 1* risulta che il Servizio funge da interfaccia tra le autorità di perseguimento penale che ordinano la sorveglianza e le persone che entrano nel campo d'applicazione della legge (in particolare i fornitori di servizi di telecomunicazione) che eseguono le sorveglianze ordinate. Giova rilevare in proposito che esso svolge tale ruolo soltanto per le misure di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni secondo l'articolo 269 CPP, per quanto concerne cioè le sorveglianze di tipo classico. Non svolge invece alcun ruolo particolare nell'utilizzazione di dispositivi tecnici di sorveglianza come gli IMSI-catcher o i GovWare, la qual cosa implica che non occorre che riceva i relativi ordini (cfr. per i dettagli il commento degli art. 269bis e 269ter CPP).

Il *capoverso 2* riprende l'articolo 2 capoverso 2 della LSCPT vigente. L'indipendenza del Servizio riguarda la relazione con il DFGP e il Consiglio federale e non la relazione con le autorità di perseguimento penale. Rispetto a queste ultime, il Servizio è comunque indipendente dal punto di vista gerarchico; ciò significa che non vi è diritto di impartire direttive al Servizio né di agire in sua vece nel suo ambito di competenza. Il Servizio è tuttavia vincolato dagli ordini di sorveglianza che possono essere eseguiti e sono stati emessi dalle autorità di perseguimento penale. La sua indipendenza dal DFGP e dal Consiglio federale è primordiale e gli permette di assumere questa funzione di esecuzione: se fosse vincolato all'ordine approvato da un'autorità giudiziaria e alle eventuali direttive del DFGP dovrebbe servire due padroni. Essendo un'autorità politica, il DFGP sarebbe inoltre in una posizione scomoda in quanto autorità di vigilanza se dovesse assumere la responsabilità di atti del Servizio predefiniti da ordini approvati da un'autorità giudiziaria. Per quanto concerne il diritto del personale, la legge del 24 marzo 2000[24] sul personale della Confederazione e l'ordinanza del 3 luglio 2001[25] sul personale della Confederazione si applicano ai rapporti di lavoro degli impiegati del Servizio.

La collaborazione secondo il *capoverso 3* deve essere reciproca. Spetta in particolare alle autorità menzionate in questo capoverso, segnatamente l'UFCOM e le autorità di perseguimento penale, sostenere nei limiti della legge il Servizio nell'esecuzione dei suoi compiti. Il *capoverso 3* non intende conferire un compito di controllo del rispetto della legislazione sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni ai partner del Servizio. La sorveglianza amministrativa è in effetti oggetto dell'articolo 41.

Art. 4 Trattamento di dati personali

L'*articolo 4* trae ispirazione dall'attuale articolo 7 capoverso 1 OSPCT. Esso riguarda in particolare la polizia e non soltanto nel caso in cui agisce di moto proprio ma anche quando esegue gli ordini del pubblico ministero. I dettagli relativi alle modalità del trattamento dei dati secondo la presente disposizione sono ancora regolati nella succitata ordinanza.

24 RS **172.220.1**
25 RS **172.220.111.3**

Art. 5 Organo consultivo

Tenuto conto delle possibili collisioni tra gli interessi dei diversi attori nel settore della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, l'esperienza mostra che la loro collaborazione in seno all'organo consultivo è essenziale per la buona esecuzione delle sorveglianze e un efficace sviluppo del settore. È quanto mostra l'esperienza. Una tale collaborazione già sussiste su base informale senza essere prevista in alcun testo di legge. La nuova disposizione sottolinea tuttavia l'importanza della collaborazione e incoraggia gli attori a impegnarsi a fondo in seno a un organo formalmente istituito. Per raggiungere questo obiettivo, non è necessario che l'organo sia dotato di competenze decisionali. Basta conferirgli un ruolo consultivo che può tuttavia esercitare in modo attivo, formulando raccomandazioni di moto proprio. L'*articolo 5* permette al Consiglio federale di formalizzare questa collaborazione.

Il *capoverso 1* costituisce la base legale di una collaborazione formale tra questi diversi attori nel settore della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Esso dà al DFGP la possibilità di istituire un organo consultivo a tal fine composto da rappresentanti dei diversi attori del settore.

Il *capoverso 2* stabilisce un quadro sommario delle attività dell'organo consultivo e ne menziona gli obiettivi.

Il *capoverso 3* affida al DFGP il compito di adottare le disposizioni di dettaglio relative alla composizione e al funzionamento dell'organo consultivo che il capoverso 1 gli dà la possibilità di istituire.

Il DFGP inoltre stabilisce concretamente quali organizzazioni partecipano all'organo consultivo e chi determina quali persone fisiche possono rappresentare tali organizzazioni. In considerazione del fatto che si vuole ottenere innanzitutto uno scambio di esperienze tra le autorità e le imprese interessate, la composizione dell'organo dovrebbe anche poter essere determinata ad hoc, in funzione delle speciali conoscenze (di natura tecnica o amministrativa) richieste. In questo senso è pure possibile prevedere un ordinamento nel quale ogni organizzazione può semplicemente delegare una persona in funzione dei temi trattati e delle sue competenze. Occorre inoltre stabilire se vi sono altre persone che possono essere invitate a partecipare all'organo consultivo e, se del caso, con quali competenze. Il DFGP dovrà per esempio anche decidere chi occuperà le cariche di presidente e di segretario dell'organo consultivo e con quali competenze; potrà inoltre stabilire le modalità della presa di decisioni e dell'eventuale pubblicazione dei suoi pareri e delle sue raccomandazioni, nonché definire le informazioni che devono eventualmente essere tutelate dal segreto di funzione. I membri non saranno indennizzati dalla Confederazione ma dall'organizzazione che rappresentano.

2.2 Sezione 2: Sistema informatico per il trattamento dei dati nel quadro della sorveglianza del traffico delle telecomunicazioni

Gli articoli 6–14 disciplinano il funzionamento, sotto il profilo del trattamento dei dati, del nuovo sistema informatico per il trattamento dei dati nel quadro della sorveglianza del traffico delle telecomunicazioni gestito dal Servizio, vale a dire

l'«Interception System Schweiz» (ISS). Questo sistema conterrà in particolare i dati raccolti durante le sorveglianze del traffico delle telecomunicazioni conformemente all'articolo 269 CPP, vale a dire in relazione con le sorveglianze di tipo classico. Non conterrà invece i dati raccolti con sorveglianze compiute mediante dispositivi tecnici di sorveglianza come gli IMSI-catcher o i GovWare. È infatti previsto che l'ISS serva soltanto per i dati connessi con le attività del Servizio. I dati raccolti con gli IMSI-catcher o i GovWare non ne fanno parte e l'ISS non è un sistema di polizia (cfr. per i dettagli il commento degli art. 269bis e 269ter CPP).

Dopo aver risposto al numero 3 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander 10.3877 (Revisione della LSCPT), abbiamo analizzato la questione dell'opportunità di sottoporre questo sistema alla legge federale del 13 giugno 2008[26] sui sistemi d'informazione di polizia della Confederazione (LSIP). Siamo giunti alla conclusione che non è il caso perché la LSIP si applica soltanto a sistemi d'informazione gestiti da fedpol (art. 1 e 2 LSIP), mentre il nuovo sistema informatico per il trattamento dei dati nel quadro della sorveglianza del traffico delle telecomunicazioni sarà unicamente di competenza del Servizio. A favore di quanto precede milita anche il fatto che il Servizio non è un'autorità penale, in particolare non è un'autorità di perseguimento penale.

La conservazione centralizzata dei dati a lungo termine e gli articoli 6–13 AP-LSCPT, segnatamente gli articoli 9–11 AP-LSCPT, hanno suscitato reazioni diverse nell'ambito della procedura di consultazione. Molti Cantoni e organizzazioni del settore del perseguimento penale, nonché la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) si sono espressi a favore del principio della conservazione centralizzata, chiedendo delle modifiche secondo il modello del sistema attuale. Altri partecipanti alla consultazione, in particolare i Cantoni, hanno chiesto che la conservazione centralizzata sia limitata ai dati della sorveglianza di Internet, in considerazione della loro mole e che gli altri dati continuino a essere inviati per posta su supporti di dati. Un numero consistente di Cantoni e di organizzazioni del settore del perseguimento penale si è espresso in modo più critico. Alcuni hanno sottolineato la grande complessità della normativa prevista da questi articoli e la loro eventuale incompatibilità con il CPP. Altri si sono opposti alla conservazione centralizzata di questi dati presso il Servizio e all'accesso online a tali dati concesso anche all'imputato e al suo difensore, preferendo ottenerli su supporti di dati. Altri ancora hanno rivolto all'avamprogetto le due critiche illustrate qui appresso.

Dopo aver esaminato la questione, il nostro Consiglio propone, con il sostegno del Servizio e di alcuni rappresentanti delle autorità di perseguimento penale, che i dati raccolti durante la sorveglianza del traffico delle telecomunicazioni siano conservati a lungo termine nel sistema informatico gestito dal Servizio. Ciò per tutti i dati raccolti durante le sorveglianze del traffico delle telecomunicazioni, vale a dire sia i dati delle tradizionali sorveglianze telefoniche sia quelli risultanti dalle sorveglianze di Internet. Il presente messaggio prevede tuttavia disposizioni più pertinenti, più semplici e più praticabili riguardo alla conservazione dei dati di quelle previste nell'AP-LSCPT (cfr. il commento degli art. 9–11).

26 RS **361**

La procedura proposta dal disegno sostituisce il regime attuale in cui il Servizio trasmette per posta alle autorità (di perseguimento penale) tutti i dati raccolti su supporti di dati. In virtù della normativa vigente non appena le autorità confermano al Servizio di aver ricevuto i dati, quest'ultimo li elimina dal sistema. I dati, eventualmente trascritti dalla polizia o da altri servizi, sono conservati nel fascicolo giudiziario, come qualsivoglia atto del fascicolo.

Secondo la procedura proposta dal disegno, le autorità (di perseguimento penale) possono accedere ai dati della sorveglianza del traffico delle telecomunicazioni riguardante fascicoli di loro competenza mediante un accesso online al sistema informatico del Servizio. Le parti (compresi l'imputato e il suo avvocato) potranno accedervi online da un terminale d'accesso messo a disposizione presso l'autorità che tiene il fascicolo. Come attualmente, i dati risultanti dalla sorveglianza del traffico delle telecomunicazioni continueranno a poter essere trasmessi, su richiesta e nel rispetto di determinate condizioni, ma a patto di essere criptati su supporti di dati mobili. Non è così auspicabile che, nelle procedure di assistenza giudiziaria internazionale, le autorità straniere possano ottenere questi dati accedendo al sistema del Servizio.

Nella procedura di consultazione il passaggio al sistema di conservazione (a lungo termine) centralizzato dei dati nel sistema informatico del Servizio è stato criticato. A favore di questa soluzione depone tuttavia soprattutto il seguente fatto: il volume di dati raccolti durante le sorveglianze, in particolare le sorveglianze di Internet, aumenta a dismisura; ciò che pone difficoltà sempre maggiori nella trasmissione alle autorità per via postale su supporti di dati. Inoltre, soprattutto per i Cantoni più grandi, lo stoccaggio dei supporti di dati è sempre più complicato, segnatamente per motivi di spazio. Gli sviluppi tecnici previsti per i prossimi anni dovrebbero confermare questa tendenza. La modifica proposta permette di porre rimedio a questo problema. Permette anche di migliorare la sicurezza dei dati evitando determinati rischi connessi con il sistema attuale che prevede l'invio dei dati per posta (p. es. la perdita, il furto o la copia dei supporti di dati). Inoltre, la modifica migliora la collaborazione tra le diverse autorità di perseguimento penale che tengono il fascicolo da cui dipendono i dati di comunicazione. Nel sistema proposto il Servizio deve tenere conto dell'evoluzione della tecnica per assicurare a lungo termine la leggibilità dei dati centralizzati nel sistema che gestisce; ciò evita inoltre che ogni Cantone debba adempiere questo compito da sé. La modifica agevola inoltre l'impiego dei programmi di gestione dei dati ed evita i rischi di incompatibilità tra il sistema del Servizio e quelli che sarebbero gestiti in modo decentralizzato dai Cantoni.

La conservazione centralizzata a lungo termine dei dati raccolti durante la sorveglianza del traffico delle telecomunicazioni comporta un aumento delle spese della Confederazione. Può tuttavia avere per conseguenza la diminuzione delle spese dei Cantoni per l'infrastruttura. Le maggiori spese che la Confederazione dovrà sostenere in seguito all'aumento dei termini di conservazione dei dati presso il Servizio potrebbero ripercuotersi sugli emolumenti pagati dalle autorità di perseguimento penale, segnatamente quelle dei Cantoni (art. 38 cpv. 3). Queste spese supplementari sono tuttavia accettabili, tenuto conto dei miglioramenti connessi con questo cambiamento e dell'esiguità dei costi delle sorveglianze rispetto ai costi totali del perseguimento penale. Questi costi sono distinti da quelli legati all'acquisizione dell'ISS. Rinviamo al n. 3.1.

Art. 6 Principio

L'*articolo 6* si ispira all'articolo 8 capoverso 1 della vigente OSCPT. Esso abilita il Servizio a gestire un siffatto sistema. Il sistema può essere composto da numerosi sottosistemi e funzionare su server diversi. I dati contenuti nel sistema sono indicati nell'articolo 8. Il sistema non contiene i dati raccolti durante la sorveglianza delle comunicazioni postali che sono direttamente trasmessi all'autorità che ha ordinato la sorveglianza conformemente all'articolo 19. La sicurezza del sistema sarà adeguatamente garantita (cfr. in particolare il commento all'articolo 12).

Art. 7 Scopo del sistema di trattamento

La *lettera a* indica lo scopo principale dell'ISS. Esso rimane immutato rispetto a quello dell'attuale sistema per il trattamento dei dati nel quadro della sorveglianza del traffico delle telecomunicazioni, fatta salva la consultazione online. La disposizione fa riferimento ai dati di contenuto delle comunicazioni e ai dati secondari delle telecomunicazioni. Per il rimanente si veda il commento dell'articolo 8 lettera a e b. L'articolo 9 definisce chi ha accesso ai dati e in quali casi non è concesso l'accesso online. Per il rimanente si vedano le spiegazioni introduttive al numero 2.2.

L'obiettivo indicato nella *lettera b* è perseguito con la conservazione centralizzata a lungo termine dei dati. Per il rimanente si vedano le spiegazioni introduttive al numero 2.2.

La *lettera c* riguarda le informazioni oggetto degli articoli 15, 21 e 22. È l'articolo 23 a disciplinare le modalità applicabili a queste informazioni, segnatamente per quanto concerne l'accesso. Per il rimanente vedi il commento degli articoli 15 e 21–23.

Come prevede la *lettera d* il sistema informatico permetterà di trattare i dati indicati nell'articolo 8. Le funzione di trattamento evocatevi non sono destinate all'imputato (né al suo rappresentante). Quest'ultimo avrà accesso ai dati che lo riguardano (cfr. commento dell'art. 9 cpv. 1) nel rispetto delle disposizioni della procedura penale. L'impiego da parte delle autorità di perseguimento penale dei dati raccolti mediante la sorveglianza avrà luogo nei pertinenti sistemi di informazione della rete dei sistemi di informazione di polizia dell'Ufficio federale di polizia (cfr. commento dell'art. 14).

La *lettera e* concerne l'esecuzione degli ordini di sorveglianza del traffico delle telecomunicazioni e il controllo dell'esecuzione (p. es. controlling, registrazione dei mandati, attribuzione dei mandati e amministrazione).

Art. 8 Contenuto del sistema di trattamento

Nell'*articolo 8 lettere a e b* è fatta menzione dei dati che è possibile ottenere da una sorveglianza del traffico delle telecomunicazioni. Per i dettagli, si veda il commento dell'articolo 26 capoverso 1. Per quanto concerne le *lettere c e d* si veda il commento dell'articolo 7 lettere c ed e.

Art. 9 Accesso al sistema di trattamento

Nella procedura di consultazione l'articolo 9 AP-LSCPT ha riscosso critiche. È stato rilevato che il disciplinamento proposto è troppo complicato, non tiene conto dei rischi di disfunzioni che può provocare e non considera le attuali possibilità di

rimettere un fascicolo, di riunire o disgiungere i procedimenti ed è di sopraggiunta inutile. Il nostro Collegio ritiene che queste critiche sono in buona parte giustificate. Di conseguenza, il disegno propone una normativa più pertinente, più semplice e più praticabile per le autorità, in particolare per le autorità di perseguimento penale; infatti, rispetto all'articolo 9 AP-LSCPT, dalla nuova regola risulta una riduzione dell'onere amministrativo del Servizio.

Il *capoverso 1* corrisponde sostanzialmente alla situazione giuridica attuale. Il Servizio è competente per porre in essere i diritti di accesso online al sistema di trattamento. È l'autorità che ha ordinato la sorveglianza o quella che dirige in seguito il procedimento da cui dipendono i dati raccolti, quindi l'autorità che tiene il fascicolo, ad avere accesso al sistema di trattamento. La formulazione proposta nel *capoverso 1* consente quindi evidentemente all'autorità, a cui è stato rimesso il fascicolo da cui dipendono i dati raccolti mediante la sorveglianza, di accedere a tali dati, anche se non ha essa stessa ordinato la sorveglianza. Si tratta in particolare dei casi di riunione dei procedimenti e di quelli in cui un'autorità è investita di una causa in seguito a ricorso. L'autorità di cui al *capoverso 1* è il detentore della collezione di dati (cfr. art. 13). Conformemente al principio della proporzionalità, l'autorità secondo il *capoverso 1* può accedere mediante procedura di richiamo soltanto ai dati contenuti nel sistema di trattamento raccolti durante una determinata sorveglianza ma non a tutti i dati raccolti durante una sorveglianza e contenuti nel sistema. Secondo la normativa proposta, i poliziotti che lavorano a un fascicolo possono, se autorizzati dal pubblico ministero che tiene il fascicolo, accedere mediante procedura di richiamo ai dati raccolti durante una sorveglianza. Soltanto le autorità svizzere possono accedere al sistema gestito dal Servizio. Non è infatti auspicabile che autorità straniere possano avervi accesso, in particolare nei casi di procedure di assistenza giudiziaria internazionale (cfr. cpv. 4). Giova pure rilevare che le parti, compreso l'imputato e il suo avvocato, potranno anche accedere mediante procedura di richiamo, nell'esercizio del diritto di essere sentito (art. 29 cpv. 2 della Costituzione federale [Cost.][27]), ai relativi dati di telecomunicazione facendo uso di un terminal d'accesso messo a loro disposizione presso l'autorità che tiene il fascicolo.

La normativa del *capoverso 2* permette di evitare che l'autorità di cui al capoverso 1 e le persone da essa designate accedano ai dati quando non tengono più il fascicolo, vale a dire a dati di cui non hanno più bisogno. Un'autorità può continuare a tenere un fascicolo per molti anni. Ma non è per forza necessario che l'accesso ai dati resti attivo durante tutto questo periodo. Appare di conseguenza ragionevole prevedere un meccanismo per disattivare l'accesso dopo un certo periodo e per riattivarlo. Il nostro Consiglio può emanare le relative disposizioni in virtù dell'articolo 12 capoverso 2.

Il dovere di informare di cui al *capoverso 3* da un canto consente di garantire il rispetto del capoverso 2, dall'altro permette al Servizio di sapere se deve concedere, come prevede il capoverso 1, l'accesso online ai dati raccolti durante una sorveglianza nel caso in cui sia contattato da un'autorità diversa da quella che ha ordinato la sorveglianza (cfr. anche commento del cpv. 1). Il nostro Collegio potrà fissare le modalità dell'informazione oggetto del *capoverso 3*.

Il *capoverso 4* prevede due casi in cui i dati della sorveglianza del traffico delle telecomunicazioni possono, come attualmente, essere trasmessi su supporti mobili di

27 RS **101**

dati se possibile in forma criptata: se l'autorità svizzera che tiene il fascicolo deve trasmettere i dati a un'autorità straniera (*lett. a*), fermo restando che non è auspicabile che le autorità straniere possano ottenere questi dati accedendo online al sistema, e se i dati non possono essere consultati online per motivi tecnici (*lett. b*). Per quanto concerne il criptaggio, si veda anche il commento dell'articolo 12 capoverso 2.

Art. 10 Diritto di consultare gli atti e diritto d'accesso ai dati

Anche l'articolo 10 AP-LSCPT è stato contestato da numerosi partecipanti alla consultazione. È stato in particolare fatto valere che la disposizione è in parte inutile, perché il CPP contiene disposizioni adeguate per proteggere i dati personali e farvi rinvio è superfluo o non pertinente. Secondo il nostro Collegio le critiche sono in parte giustificate. Il disegno propone dunque una normativa modificata per tenere conto di queste critiche.

Il *capoverso 1* disciplina i diritti di consultazione e di accesso ai dati raccolti nel quadro di un procedimento penale (art. 1 cpv. 1 lett. a) o di una domanda d' assistenza giudiziaria (art. 1 cpv. 1 lett. b), sia che si tratti di una domanda d' estradizione o di una domanda di un altro genere di assistenza giudiziaria. La disposizione distingue i diritti nell'ambito di un procedimento pendente (*lett. a)* da quelli che sussistono dopo la chiusura del procedimento (*lett. b)*. Il *capoverso 1 lettera a* stabilisce che, nel quadro di una procedura penale pendente, al diritto di consultare gli atti e al diritto d'accesso ai dati si applica il diritto di procedura applicabile. Questi diritti sono retti dal CPP e da altre leggi procedurali come la PPM. Nei fatti, il *capoverso 1* rinvia in particolare agli articoli 97, 101 e 279 CPP. Il *capoverso 1 lettera b* riguarda il diritto d'accesso ai dati dopo la chiusura del procedimento. Ne risulta che questo diritto è retto in particolare dagli articoli 8 e 9 della legge federale del 19 giugno 1992[28] sulla protezione dei dati (LPD), se l'autorità incaricata della domanda di assistenza giudiziaria è un'autorità federale. Se l'autorità incaricata della domanda è un'autorità cantonale e se il diritto cantonale non garantisce un livello di protezione adeguato, l'articolo 37 capoverso 1 LDP si applica a titolo sussidiario al diritto d'accesso ai dati.

Giova rilevare qualche particolarità relativa alla procedura di assistenza giudiziaria. Per quanto concerne i dati raccolti in esecuzione di una domanda di estradizione, questi diritti sono retti dagli articoli 18*a* capoverso 4 della legge federale del 20 marzo 1981[29] sull'assistenza giudiziaria internazionale in materia penale (AIMP), dagli articoli 26 e 27 della legge federale del 20 dicembre 1968[30] sulla procedura amministrativa (PA) applicabile in virtù dell'articolo 12 capoverso 1 primo periodo AIMP e degli articoli 8 e 9 LPD. Negli altri casi di assistenza giudiziaria, i diritti dell'interessato sono retti dagli articoli 18*a* capoverso 4 e 80*b* AIMP, dall'articolo 9 della legge federale del 3 ottobre 1975[31] relativa al trattato conchiuso con gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale e dell'articolo 46 della legge federale del 22 giugno 2001[32] sulla cooperazione con la Corte penale internazionale (LCPI) nonché dagli articoli 8 e 9 LPD se l'autorità che si occupa della domanda di assistenza giudiziaria è un'autorità della Confederazione, o dal diritto

28 RS **235.1**
29 RS **351.1**
30 RS **172.021**
31 RS **351.93**
32 RS **351.6**

cantonale se questa autorità è un'autorità cantonale. Occorre rilevare che la legge federale del 21 dicembre 1995[33] concernente la cooperazione con i tribunali internazionali incaricati del perseguimento penale delle violazioni gravi del diritto internazionale umanitario (art. 2) e le Convenzioni internazionali concluse dalla Svizzera in materia di assistenza giudiziaria internazionale con gli Stati esteri (p. es. con il Canada e il Brasile) prevedono l'applicazione dell'AIMP, segnatamente degli articoli 18*a* capoverso 4 e 80*b*. Se l'autorità che si occupa della domanda è il pubblico ministero di un Cantone, l'articolo 37 capoverso 1 LPD è applicabile a titolo sussidiario (cfr. *supra*). L'autorità, nei cui confronti sono esercitati questi diritti, deve essere in grado, se questi diritti sono limitati e per quanto necessario, di rispondere alla domanda senza rivelare informazioni coperte dal segreto di funzione.

Il *capoverso 2* riguarda il diritto d'accesso ai dati raccolti durante la ricerca di persone scomparse (art. 1 cpv. 1 lett. c) o condannate (art. 1 cpv. 1 lett. d). Si applicano gli articoli 8 e 9 LPD se l'autorità che tiene il fascicolo è un'autorità della Confederazione. L'articolo 37 capoverso 1 LPD si applica invece a titolo sussidiario al diritto d'accesso ai dati raccolti mediante la sorveglianza, nel caso in cui l'autorità che tiene il fascicolo è un'autorità cantonale e se il diritto cantonale non garantisce un livello di protezione adeguato. L'articolo 279 CPP si applica inoltre per analogia nella misura in cui chi è stato sorvegliato deve esserne informato dall'autorità che ha ordinato la sorveglianza (cfr. anche il commento dell'art. 37 cpv. 2).

La normativa prevista nel *capoverso 3* indica chiaramente, anche se ciò può non sembrare evidente, che il Servizio possiede soltanto i dati ma che il detentore della collezione di dati è l'autorità che ha accesso al sistema di trattamento, in virtù dell'articolo 9. È evidente che se l'ultima autorità che ha tenuto il fascicolo ha cessato formalmente di esistere (p. es. in caso di fusione con un'altra autorità o di integrazione in quest'ultima), l'autorità che le succede è competente ai sensi del *capoverso 3*. Se una domanda di accesso ai dati è formulata al Servizio, quest'ultimo deve trasmetterla senza indugio all'autorità competente.

Il *capoverso 4* dà al Consiglio federale il mandato di disciplinare l'esercizio di questi diritti tenendo conto delle particolarità tecniche del sistema di trattamento. Si tratta in particolare del caso in cui la consegna delle copie con i risultati delle sorveglianze – consegna ordinata dalla procedura applicabile, in particolare dall'articolo 102 capoverso 3 CPP – presenta problemi tecnici, per esempio perché il volume di dati è molto importante (cfr. anche le spiegazioni introduttive al n. 2.2). Le cerchie interessate saranno consultate sulle relative disposizioni del Consiglio federale.

Art. 11 Termine di conservazione dei dati

Anche l'articolo 11 AP-LSCPT è risultato controverso nella procedura di consultazione. Secondo molti la normativa proposta, segnatamente il previsto sistema di annuncio, è eccessivamente complessa, provoca costi e comporta anche un inutile onere amministrativo. È pure stato rilevato che il termine di conservazione dovrebbe essere stabilito dalle vigenti regole del CPP per evitare di avere diverse normative in collisione. Il nostro Consiglio considera in parte giustificate queste critiche. Il disegno propone di conseguenza una normativa più semplice che genera oneri amministrativi minori per le autorità, segnatamente per le autorità di perseguimento penale, rispetto all'articolo 11 AP-LSCPT.

33 RS **351.20**

Il contenuto del *capoverso 1*, che riguarda i dati raccolti nel quadro di un procedimento penale (art. 1 cpv. 1 lett. a), si impone in modo evidente. Il CPP o gli altri diritti di procedura applicabili come la PPM contengono infatti disposizioni adeguate sulla conservazione dei fascicoli. In questi casi sarebbe inoltre contraddittorio applicare più normative – una secondo il diritto di procedura penale applicabile accanto a un'altra normativa specifica prevista nella LSCPT. Di fatto, il *capoverso 1* rinvia in particolare al regime degli articoli 99 capoverso 2, 100 e 103 capoverso 1 CPP. I dati devono essere conservati nel fascicolo (art. 100 CPP) e possono esservi integrati mediante un link verso il luogo dove sono conservati; il fascicolo deve essere conservato fintanto che il termine di prescrizione dell'azione penale e della pena non è stato compiuto (art. 103 cpv. 1 CPP). Di conseguenza, i dati personali devono essere conservati nel fascicolo fintanto che tale termine di prescrizione non è scaduto (art. 99 cpv. 2 CPP).

La durata di conservazione massima dei dati nel sistema di trattamento è indicata nel *capoverso 2* (art. 1 cpv. 1 lett. b) e si giustifica in particolare per il fatto che le procedura di assistenza giudiziaria dura sovente a lungo. Questa durata corrisponde ai termini massimi di prescrizione dell'azione penale e della pena del diritto svizzero, a prescindere dai casi di imprescrittibilità e di prolungamento della pena. Occorre inoltre rilevare che i termini applicabili in un caso concreto possono essere più lunghi nel diritto dello Stato che ha chiesto assistenza giudiziaria.

La durata massima di conservazione dei dati nel sistema di trattamento, prevista nel *capoverso 3* (art. 1 cpv. 1 lett. c), si giustifica in particolare tenuto conto del fatto che è in gioco il bene giuridico più prezioso, la vita umana, e che una persona può essere considerata scomparsa per un periodo molto lungo.

Il contenuto del *capoverso 4 primo periodo* (art. 1 cpv. 1 lett. d) si impone sostanzialmente per le medesime ragioni evocate nel commento del capoverso 1. Il *capoverso 4 primo periodo* rinvia in particolare al regime risultante dagli articoli 99 capoverso 2, 100 e 103 capoverso 1 CPP (cfr. per il rimanente il commento del cpv. 1). La durata di conservazione massima dei dati nel sistema di trattamento indicata nel *capoverso 4 secondo periodo* (art. 1 cpv. 1 lett. d) si giustifica segnatamente tenuto conto del fatto che è in gioco il bene giuridico più prezioso, la vita umana, e che una persona può non essere localizzata per un periodo molto lungo. Occorre rilevare che le misure privative della libertà non si prescrivono, a differenza di quanto accade in linea di massima per le pene detentive. Se i dati sono stati raccolti nel quadro della ricerca di una persona condannata a una pena detentiva o nei confronti della quale è stata disposta una misura privativa della libertà, la durata massima della conservazione dei dati è la durata più lunga.

Secondo il *capoverso 5*, è l'autorità che tiene il fascicolo o, se non ve n'è più una, l'ultima ad averlo tenuto che deve svolgere le pratiche affinché i dati conservati nel sistema di trattamento siano soppressi dal Servizio alla scadenza dei termini secondo i capoversi 1–4. A tal fine, questa autorità deve assicurare sul lungo periodo il controllo di tali termini. Ciò può ben inteso comportare un aumento dei compiti amministrativi di queste autorità; l'aumento resta tuttavia entro margini accettabili perché può essere gestito con un'adeguata organizzazione del controllo dei termini. Questa soluzione è preferibile a quella proposta dall'articolo 11 capoverso 5 AP-LSCPT che prevedeva di affidare al Servizio la responsabilità di controllare il rispetto dei termini di cui ai capoversi 1–4 ricorrendo a un'autorità centrale per informare l'autorità che tiene il fascicolo o l'ultima ad averlo fatto della prossima scadenza di un dato termine. Questa soluzione richiederebbe in effetti un onere amministrativo spropor-

zionato per il Servizio e per le citate autorità. Queste ultime dovrebbero prima di tutto comunicare al Servizio, per ciascuna sorveglianza, il termine applicabile secondo i capoversi 1–4. La comunicazione sarebbe indispensabile poiché il termine varia a seconda del contenuto del fascicolo (p. es. la pena prevista per il reato determina il termine di prescrizione dell'azione penale e la pena pronunciata influisce sul termine di prescrizione della pena) e il Servizio non ha accesso al fascicolo. In proposito non bisogna trascurare il fatto che il reato come pure la pena pronunciata e di conseguenza il termine di conservazione dei dati possono cambiare con le diverse istanze, complicando ulteriormente il lavoro di controllo dei termini. È inoltre logico che sia l'autorità che tiene il fascicolo o l'ultima ad averlo fatto, e non il Servizio, a compiere queste pratiche poiché essa è il detentore della collezione di dati (cfr. art. 13). Questa autorità deve anche informare il Servizio di un eventuale trasferimento necessario per rispettare il diritto vigente, prima che questi dati non siano soppressi dal sistema del Servizio. L'autorità che tiene il fascicolo o l'ultima che lo ha tenuto deve inoltre informare il Servizio di un eventuale trasferimento dei dati necessario secondo il diritto applicabile, prima che il Servizio elimini questi dati dal sistema. Si tratta in particolare di rispettare le eventuali disposizioni federali e cantonali in materia di archiviazione. La normativa in materia di archiviazione prevede l'applicazione delle disposizioni della collettività (Confederazione o Cantoni) da cui dipende l'autorità che tiene il fascicolo o l'ultima ad essersene occupata poiché essa è considerata il detentore dei dati (cfr. art. 13). Riguardo alla nozione di autorità che tiene il fascicolo si veda il commento dell'articolo 10 capoverso 3.

Il compito del Servizio di prendere contatto con l'autorità competente trent'anni dopo la fine della sorveglianza per informarsi su cosa fare dei dati ancora contenuti nel sistema di trattamento è semplicemente una misura precauzionale. In effetti la disposizione intende garantire la soppressione dei dati che avrebbero dovuto essere eliminati dal sistema conformemente ai capoversi 1–4 ma non lo sono stati (p. es. perché l'autorità ha dimenticato di informare il Servizio).

Nell'esercizio della competenza conferitagli dal *capoverso 6*, il Consiglio federale dovrà segnatamente tenere conto delle particolarità tecniche del sistema di trattamento. Potrà per esempio prevedere che l'autorità di perseguimento penale registri il termine di conservazione di tutti i dati o di una parte di essi nel sistema di trattamento e che contatti il Servizio per dargli istruzioni entro una data determinata prima della scadenza del termine di conservazione, in modo tale da lasciargli abbastanza tempo per eseguire queste istruzioni. Il Consiglio federale potrà per esempio anche prevedere che tutti i dati o parte di essi siano automaticamente eliminati se l'autorità non contatta il Servizio in tempo utile.

Art. 12 Sicurezza

La regola prevista nel *capoverso 1* si giustifica poiché il Servizio, anche se non è il detentore della collezione di dati (cfr. anche commento dell'art. 13), gestisce il sistema di trattamento in cui i dati sono registrati: i dati sono di fatto in suo possesso.

In base al *capoverso 2*, il Consiglio federale potrà segnatamente emanare disposizioni sul controllo dell'accesso ai dati e sulle circostanze in cui dovranno essere criptati (cfr. anche art. 9 e relativo commento). Le cerchie interessate saranno consultate sulle disposizioni proposte dal Consiglio federale in virtù del *capoverso 2*.

Il *capoverso 3* si ispira all'articolo 9 capoverso 2 OSCPT vigente. Per sicurezza dei dati ai sensi della presente disposizione si intende in particolare la confidenzialità e l'integrità dei dati.

Art. 13 Responsabilità

Secondo l'*articolo 13* sono le autorità che hanno accesso al sistema di trattamento ad essere considerate i detentori della collezione di dati e non il Servizio, che gestisce il sistema di trattamento e si limita a mettere in opera i diritti d'accesso a quest'ultimo (cfr. anche commento degli art. 9 e 12).

Art. 14 Interfaccia con la rete dei sistemi d'informazione di polizia dell'Ufficio federale di polizia

Il *capoverso 1* pone una base legale esplicita per la copiatura e il trasferimento elettronico nei sistemi d'informazione di cui agli articoli 10, 12 e 13 LSIP dei dati contenuti nel sistema informatico del Servizio per il trattamento dei dati nel quadro sorveglianza del traffico delle telecomunicazioni, in particolare dei dati raccolti durante la sorveglianza. Si vuole così consentire il loro trattamento in seno a questi sistemi. Per effettuare la copiatura e il trasferimento la legislazione applicabile a questi sistemi deve evidentemente autorizzare il trattamento dei dati anche in questi ultimi (*lett. a)*.

Soltanto le persone che dirigono il procedimento devono poter accedere ai dati nel relativo sistema d'informazione secondo la LSIP (*lett. b)*. Finalmente quest'ultima condizione dovrebbe figurare nella LSIP. Questa integrazione non può tuttavia essere concretizzata in modo soddisfacente per motivi di sistematica legislativa. Una revisione della LSIP è comunque prevista; essa permetterà di disciplinare la questione dell'accesso ai dati contenuti nei sistemi d'informazione secondo la LSIP dandole un'adeguata collocazione sistematica nella LSIP medesima.

Questi sistemi d'informazione sono gestiti da fedpol e sono in particolare utilizzati dalla polizia federale e dalle polizie cantonali per gestire le informazioni ottenute nell'ambito delle inchieste penali che comprendono i dati raccolti durante la sorveglianza del traffico delle telecomunicazioni. Rispetto alla copiatura e al trasferimento «manuali» la copiatura e il trasferimento elettronico hanno taluni vantaggi come i risparmi di tempo e di spese nonché una maggiore sicurezza dei dati (riduzione del rischio di perdita dei dati e del rischio di errore che compromette la qualità dei dati). I dati contenuti nel sistema del Servizio rimangono nel sistema dopo essere stati trasferiti nel sistema d'informazione secondo la LSIP, ragione per cui si parla di «copia».

Secondo il *capoverso 2*, la copia e il trasferimento dei dati secondo il capoverso 1 sono eseguiti automaticamente con ordini impartiti da una persona abilitata ad accedere sia al sistema di trattamento del Servizio (art. 9) sia al sistema d'informazione secondo la LSIP. In effetti, il passaggio a questa modalità di trasferimento elettronico dei dati non deve portare a eludere le regole d'accesso a questi sistemi. Le autorità di perseguimento penale, e non il Servizio, sono responsabili della legalità della copia e del trasferimento dei dati dal sistema di trattamento del Servizio al relativo sistema d'informazione secondo la LSIP.

2.3 Sezione 3: Compiti del Servizio

I compiti del Servizio sono legati all'esecuzione degli ordini di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Il disegno non concede invece competenze normative e regolamentari al Servizio nell'ambito dell'esecuzione delle sorveglianze; queste competenze spettano al DFGP (art. 31 cpv. 3). Quanto precede soddisfa le richieste presentate nel numero 1 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander (Revisione della LSCPT) secondo cui i compiti normativi e regolamentari del Servizio devono sostanzialmente essere distinti dai compiti di esecuzione delle sorveglianze.

Art. 15 Informazioni sui servizi di telecomunicazione

Sostanzialmente l'*articolo 15* riprende l'articolo 14 capoversi 2 e 2bis della LSCPT vigente con l'eccezione del rinvio (cfr. commento dell'art. 21). Tuttavia, sebbene la nozione di «collegamento (di telecomunicazione)» sia intesa in senso esteso, riteniamo opportuno sostituire nel disegno questa nozione con quella di «servizi di telecomunicazione», poiché con l'evoluzione tecnica la nozione di «collegamento (di telecomunicazione)» si è rivelata troppo restrittiva. Infatti i fornitori mettono soltanto a disposizione servizi o applicazioni senza che i loro utenti possano esigere un determinato collegamento. Questi servizi di telecomunicazione comprendono anche i servizi relativi a Internet (cfr. anche il commento dell'art. 1 cpv. 1).

Il *capoverso 1 lettera a* è oggetto di alcune integrazioni rispetto all'articolo 14 capoverso 2 lettera a LSCPT. Contrariamente a quanto lascia intendere il testo di quest'ultima disposizione, probabilmente a causa di una distrazione del legislatore, le informazioni non devono poter essere chieste soltanto per determinare i servizi e le persone da sorvegliare, ossia per sottoporli a sorveglianza, ma anche per determinare chi comunica con il Servizio sorvegliato, anche nel caso in cui non si volesse ordinare la sorveglianza dei Servizi di ciascuno di questi interlocutori[34]. Per meglio soddisfare i requisiti del principio della legalità, la disposizione precisa che i dati possono essere forniti all'autorità (di perseguimento penale) designata dall'autorità che può ordinare la sorveglianza o da quella che la approva, e non soltanto da queste due ultime. La polizia, segnatamente, potrà ottenere questi dati, perché in linea di massima sarà incaricata di utilizzarli.

Il *capoverso 1 lettera b* riprende l'articolo 14 capoverso 2 lettera b della vigente LSCPT. Questa disposizione non riguarda soltanto i compiti di polizia in relazione con i procedimenti penali ma anche i compiti che la polizia svolge indipendentemente dai procedimenti penali[35]. Va precisato che detta disposizione non richiede un ordine del pubblico ministero affinché le forze di polizia ottengano le informazioni non assoggettate al segreto delle telecomunicazioni e il cui ottenimento non costituisce un provvedimento coercitivo (cfr. il commento dell'art. 21). La polizia può infatti prendere l'iniziativa di chiedere le informazioni al Servizio e le ottiene in particolare nell'ambito degli articoli 306 e seguenti CPP.

Il *capoverso 1 lettera c* corrisponde all'articolo 14 capoverso 2 lettera c della LSCPT in vigore.

34 Thomas Hansjakob, op. cit. (nota 11), n. 16 ad art. 14 LSCPT.
35 Thomas Hansjakob, op. cit. (note 11), n. 18 ad art. 14 LSCPT; cfr. il messaggio del 1° luglio 1998 relativo alla LSCPT vigente, FF **1998** 3355.

Il *capoverso 2 lettera a* riprende sostanzialmente l'articolo 14 capoverso 2bis della LSCPT vigente adeguando, in conseguenza del cambiamento di struttura del disegno, il riferimento contenutovi.

L'articolo 23 della legge federale del 19 dicembre 1986[36] sulla concorrenza sleale (LCSl) in combinato disposto con l'articolo 10 capoverso 3 LCSl dà alla Confederazione il diritto di sporgere querela per un atto di concorrenza sleale che pregiudica interessi collettivi. Nella situazione attuale, l'attuazione di questo diritto è molto difficile per quanto concerne le chiamate pubblicitarie indesiderate, che sono atti di concorrenza sleale ai sensi dell'articolo 3 capoverso 1 lettera u LCSl. In effetti, in considerazione dei frequenti cambiamenti di numero telefonico delle imprese pubblicitarie che effettuano le chiamate e dei call center, la Confederazione è sovente confrontata a un solo reclamo che riguarda un unico numero. Di conseguenza, in assenza di un interesse collettivo, la Confederazione non ha la legittimazione per sporgere querela anche se in molti casi è possibile che si tratti di un'unica impresa che utilizza diversi numeri telefonici. I dati che la Confederazione potrà d'ora innanzi ottenere in virtù del *capoverso 2 lettera b* sono necessari per eliminare l'incertezza concernente il suo diritto di sporgere querela nei casi concreti di chiamate pubblicitarie indesiderate e le consentirà di lottare in modo efficace contro questo fenomeno. L'autorità della Confederazione competente in linea di massima per sporgere querela è la Segreteria di Stato dell'economia[37].

Art. 16 Compiti generali nell'ambito della sorveglianza

L'*articolo 16* indica i compiti del Servizio nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Questi compiti sono ripresi dagli attuali articoli 11 e 13 LSCPT. Contrariamente alla LSCPT vigente, il disegno non contiene più articoli relativi ai compiti specifici del Servizio nell'ambito della sorveglianza della corrispondenza postale, a differenza di quanto invece è previsto per la sorveglianza del traffico delle telecomunicazioni (cfr. commento dell'art. 17).

La *lettera a* si ispira agli articoli 11 capoverso 1 lettera a e 13 capoverso 1 lettera a della LSCPT vigente e riguarda l'esame formale dell'ordine di sorveglianza da parte del Servizio. La disposizione conferisce un compito di coordinamento al Servizio. Questo controllo verte anche sulla completezza e sulla chiarezza dell'ordine di sorveglianza[38]. Come già attualmente il Servizio dovrà verificare se il reato figura nel catalogo dei reati che possono essere oggetto di una sorveglianza. Per fare in modo che l'ordine di sorveglianza possa se del caso essere rettificato quanto prima, il Servizio deve potersi rivolgere direttamente all'autorità che ha ordinato la sorveglianza (oltre all'autorità che ha approvato la sorveglianza e che deve essere informata di questo contatto ai fini della sua futura decisione sulla decisione ordinata). Ciò è particolarmente opportuno se il Servizio ritiene che quanto richiesto nell'ordine di sorveglianza non sia chiaro. Se necessario, il nostro Consiglio potrà stabilire in un'ordinanza il termine entro il quale il Servizio dovrà contattare la summenzionata autorità. Nonostante questo obbligo del Servizio, occorre precisare che l'autorità che ha ordinato la sorveglianza è responsabile della validità della sua

36 RS **241**
37 Cfr. art. 1 cpv. 1 dell'ordinanza del 12 ottobre 2011 concernente il diritto di azione della Confederazione nel quadro della legge contro la concorrenza sleale (RS **241.3**).
38 Thomas Hansjakob, op. cit. (nota 11), n. 2–10 ad art. 11 LSCPT.

decisione, tanto più che essa non è tenuta a seguire le raccomandazioni del Servizio. Per il rimanente, si veda per analogia il commento della lettera b.

La *lettera b* prevede che il Servizio esegua un esame materiale dell'ordine di sorveglianza sotto il profilo del diritto amministrativo. Anche questa disposizione conferisce un compito di coordinamento al Servizio. Accogliendo in questo modo la richiesta di molti partecipanti alla consultazione, il disegno consolida il potere di esame del Servizio rispetto a quanto previsto nell'AP-LSCPT riguardo alla sorveglianza del traffico delle telecomunicazioni. Questa disposizione non riguarda l'esame materiale dell'ordine di sorveglianza rispetto alle disposizioni di procedura penale applicabili e menzionate agli articoli 269 e seguenti CPP e 70 e seguenti PPM, ossia non concerne esclusivamente le questioni relative alla procedura penale. Di conseguenza, non spetta per esempio al Servizio determinare se la sorveglianza ordinata può dare o no risultati interessanti che possono essere utilizzati in una data inchiesta penale. Questo esame è in effetti esclusivamente consegnato all'autorità che approva la sorveglianza (cfr. anche il commento dell'art. 42 cpv. 2).

La *lettera b* affida questo compito al Servizio per evitare che esso debba trasmettere a una persona che entra nel campo d'applicazione della legge un ordine di sorveglianza che ritiene adempiere le condizioni menzionate dalla disposizione, senza averne dapprima informato l'autorità che ha ordinato la sorveglianza o l'autorità d'approvazione. Questo meccanismo serve in particolare a semplificare le modalità per rendere più attente l'autorità che ha ordinato la sorveglianza e l'autorità d'approvazione ad eventuali problemi connessi con un ordine di sorveglianza. L'autorità che ha ordinato la sorveglianza e l'autorità d'approvazione possono tenere conto del parere del Servizio e, se del caso, revocare la sorveglianza o non approvarla, ma non sono obbligate a tenerne conto. I fautori dell'introduzione di un rimedio giuridico (procedura d'opposizione o di ricorso) per regolare eventuali divergenze di opinione tra il Servizio e l'autorità che ha ordinato la sorveglianza ritengono insufficiente questo meccanismo di controllo (obbligo di avvertire del Servizio). Essi sostengono in particolare che, come mostra l'esperienza, non tutte queste divergenze possono essere risolte con il dialogo. Ritengono anche che non sarebbe logico attribuire al Servizio un potere di cognizione limitato sulla decisione di sorveglianza, in considerazione del fatto che l'autorità di ricorso eventualmente incaricata, per esempio da un fornitore di servizi di telecomunicazione scontento della decisione, non sarebbe sottoposta a tale limitazione. Nonostante quanto precede, riteniamo che il proposto meccanismo di controllo (obbligo di avvertire del Servizio) sia necessario e sufficiente, segnatamente per evitare le complicazioni inutili connesse con un ricorso, per esempio il ricorso presentato da un fornitore di servizi di telecomunicazione, contro la decisione del Servizio di fare eseguire una sorveglianza che presenta una delle caratteristiche elencate alla *lettera b*. Non appare invece necessario istituire un rimedio giuridico, seppur sprovvisto di effetto sospensivo, per regolare eventuali divergenze di opinione tra il Servizio e l'autorità che ha ordinato la sorveglianza. A questo proposito giova tenere presente che il Servizio è in fin dei conti un'autorità esecutiva, un'interfaccia tra le autorità di perseguimento penale e i fornitori di servizi di telecomunicazione, cosicché questo genere di rimedio giuridico sarebbe in sé contrario al sistema. Occorre rilevare che il Servizio è pienamente competente per esaminare, sotto il profilo del diritto amministrativo, l'ordine di sorveglianza sul quale si fonda la sua decisione di sorveglianza destinata a un fornitore di servizi di telecomunicazione e se del caso per completarlo. Il «potere di cognizione» del Servizio non è pertanto limitato rispetto a quello di cui dispone il

Tribunale amministrativo federale. Inoltre, occorre precisare che il dialogo tra il Servizio e le autorità di perseguimento penale che risulta necessariamente dalla *lettera b* permette in un certo modo la riconsiderazione legale degli ordini di sorveglianza. In questo contesto occorre anche situare i progressi che risulteranno dal nuovo strumento dell'organo consultivo, previsto nell'articolo 5. In questo ambito le autorità di perseguimento penale possono in particolare essere informate in merito a quanto tecnicamente possibile e il Servizio potrà comprendere con maggiore precisione quale sia l'utilità delle sorveglianze ordinate. L'ordine di sorveglianza trasmesso al Servizio è inoltre oggetto del controllo di un'autorità giudiziaria, vale a dire il giudice dei provvedimenti coercitivi (art. 274 CPP) a cui il Servizio deve peraltro trasmettere il suo parere secondo la *lettera b*. Questa autorità indipendente può certamente decidere di non approvare la sorveglianza per motivi inerenti alla procedura penale; in questo caso, le informazioni raccolte saranno in principio distrutte e non potranno essere utilizzate (art. 277 CPP). Introdurre un rimedio giuridico per disciplinare le eventuali divergenze di opinione tra il Servizio e l'autorità che ha ordinato la sorveglianza appare tanto meno giustificato per il fatto che l'articolo 42 capoverso 2 consente ormai ai fornitori di servizi di telecomunicazione di difendersi dinanzi al Tribunale amministrativo federale contro le decisioni di sorveglianza trasmesse dal Servizio. Oltre al Servizio, l'autorità che ha ordinato la sorveglianza potrà essere invitata dal Tribunale amministrativo federale a spiegare il proprio ordine di sorveglianza. Un tale ricorso può impedire l'esecuzione da parte di un fornitore di servizi di telecomunicazione di un ordine di sorveglianza pronunciato da un'autorità di perseguimento penale (cfr. per i dettagli il commento dell'art. 42). Rammentiamo infine che, nonostante l'obbligo di avviso del Servizio, è l'autorità che ha ordinato la sorveglianza ad essere responsabile dell'ineccepibilità della decisione di sorveglianza; tanto più che tale autorità non è tenuta a seguire l'avviso del Servizio.

Sono considerati inadeguati ai sensi della *lettera b* gli ordini di sorveglianza che, tenuto conto delle caratteristiche tecniche della fattispecie, non sono in grado di fornire risultati utilizzabili. La LSCPT, l'OSCPT e il CPP permettono di stabilire se una determinata sorveglianza è prevista dalla legge. È opportuno precisare che il criterio di cui deve tenere conto il Servizio per stabilire se l'esecuzione della sorveglianza è tecnicamente possibile non consiste nelle possibilità tecniche di eseguire la decisione ma nello stato della tecnica nel momento in cui la sorveglianza va eseguita. Se colui che è tenuto a farlo non è in grado di eseguire la sorveglianza, il Servizio può eseguire esso stesso la sorveglianza o affidarla a un terzo (cfr. art. 34 cpv. 1 e relativo commento).

Il termine di cui alla *lettera b* entro il quale il Servizio è tenuto a informare l'autorità che ha ordinato la sorveglianza e l'autorità d'approvazione deve evidentemente essere particolarmente breve, segnatamente per consentire all'autorità che ha ordinato la sorveglianza, se del caso, di ordinare rapidamente un'altra sorveglianza. Il Consiglio federale può se necessario stabilire questo termine.

Il compito affidato al Servizio dalla *lettera c* va considerato in relazione con gli articoli 20 e 24. Contrariamente all'articolo 26 capoverso 2, la presente disposizione riguarda le informazioni che l'autorità che ha ordinato la sorveglianza deve ottenere prima di ordinare la sorveglianza.

La *lettera d* riprende sostanzialmente gli articoli 11 capoverso 1 lettera b e 13 capoverso 1 lettera b della LSCPT attuale. Questa disposizione è in parte analoga all'articolo 33 capoverso 5 che non riguarda però la procedura di esecuzione di una

sorveglianza ma la procedura di prova della disponibilità a informare e sorvegliare, anche in seguito a una sorveglianza che non si è svolta in modo ottimale. Con la menzione del compito di controllo dell'esecuzione della sorveglianza da parte del Servizio si intende sottolineare il ruolo d'intermediario che quest'ultimo svolge tra le autorità di perseguimento penale e i fornitori di servizi di telecomunicazione.

La *lettera e* riprende sostanzialmente l'articolo 13 capoverso 1 lettera f della LSCPT vigente che si applica alla sorveglianza del traffico delle telecomunicazioni. Questo compito è stato esteso alla sorveglianza della corrispondenza postale, la qual cosa ha pure pienamente senso in questo settore. Questa disposizione va posta in relazione con gli articoli 271 e 274 capoverso 4 lettera a CPP nonché con gli articoli 70*b* e 70*e* cpv. 4 lett. a PPM. Questi articoli indicano il regime applicabile alla sorveglianza nel caso in cui sia necessario tutelare un segreto professionale di cui l'autorità di perseguimento penale non deve prendere atto (cfr. commento degli art. 271 CPP e 70*b* PPM). Il Servizio prende i provvedimenti necessari per porre in essere le misure decise nel quadro dei succitati articoli; ma non esegue da sé la cernita menzionatavi (art. 271 cpv. 1 CPP e art. 70*b* cpv. 1 PPM).

La *lettera f* si ispira agli articoli 11 capoverso 1 lettera d e 13 capoverso 1 lettera g dell'attuale LSCPT. Il Servizio deve ormai disporre di una copia scritta della domanda di proroga.

La *lettera g* riprende gli articoli 11 capoverso 1 lettera c e 13 capoverso 1 lettera h dell'attuale LSCPT.

La *lettera h* riprende gli articoli 11 capoverso 1 lettera g e 13 capoverso 1 lettera k dell'attuale LSCPT.

La *lettera i* è necessaria tenuto conto della complessità del sistema.

La *lettera j* riprende sostanzialmente gli articoli 11 capoverso 2 prima frase e 13 capoverso 2 lettera e della LSCPT vigente e li completa con consigli operativi.

I compiti di cui all'articolo 13 capoverso 2 lettere a–d della LSCPT vigente non sono ripresi nell'*articolo 16*. Non corrispondono infatti più a compiti che il Servizio deve eseguire su richiesta o a compiti che esso debba svolgere, per mancanza di mezzi o perché non sono più necessari.

Art. 17 Compiti nell'ambito della sorveglianza del traffico delle telecomunicazioni

L'articolo 17 enuncia gli specifici compiti del Servizio in materia di sorveglianze del traffico delle telecomunicazioni, esclusa la corrispondenza postale. Questo articolo è anche applicabile alle sorveglianze eseguite dai fornitori di servizi di comunicazione derivati, se il Consiglio federale fa uso della competenza attribuitagli dall'articolo 27 capoverso 3 (cfr. art. 27 cpv. 3 e relativo commento).

La *lettera a* si ispira all'articolo 15 capoverso 2 prima frase della LSCPT attuale. Il termine «numero» non è adatto al traffico via Internet e potrebbe essere sostituito dal termine «collegamento». Vista l'evoluzione tecnica, non è tuttavia opportuno sostituire questa nozione con quella di «servizi» (cfr. commento dell'art. 15 *in initio*). Il principio consacrato è tuttavia conservato nella misura in cui la sorveglianza viene in linea di massima affidata al fornitore di servizi di telecomunicazione che gestisce il servizio in questione. Evidentemente, la *lettera a* presuppone che il Servizio sia in grado di determinare per quale fornitore di servizi di telecomunicazione l'esecuzione

tecnica della sorveglianza comporta l'onere minore, la qual cosa non è sempre possibile. A tal fine il Servizio affida l'esecuzione della sorveglianza fondandosi sull'ordine dell'autorità che l'ha ordinata. L'istruzione dell'autorità su questo punto non vincola il Servizio. In linea di massima, l'autorità che ordina la sorveglianza non deve pronunciarsi in modo vincolante su questi aspetti. In virtù della sua funzione e dei suoi compiti, il Servizio è competente – eventualmente dopo aver contattato l'autorità che ha ordinato la sorveglianza (cfr. art. 16 lett. b o lett. a n. 3) – per determinare il fornitore adeguato. In una fase precedente il Servizio dovrà fornire a questa autorità le informazioni che potrà ottenere affinché la sorveglianza possa essere ordinata (art. 16 lett. c).

La *lettera b* si ispira all'articolo 13 capoverso 1 lettera c della LSCPT attuale, adeguandolo al funzionamento del nuovo sistema informatico per il trattamento dei dati nel quadro della sorveglianza del traffico delle telecomunicazioni, che in linea di massima non prevede più che questi dati siano messi a disposizione delle autorità interessate mediante l'invio di supporti di dati e di documenti per via postale ma mediante un diritto d'accesso al sistema informatico (cfr. art. 6 segg.). Per soddisfare i requisiti del principio della legalità, la disposizione si ispira al contenuto degli articoli 15 capoverso 1 lettera b e 23 lettera b della vigente OSCPT per precisare che il Servizio permette la consultazione delle comunicazioni anche all'autorità di perseguimento penale designata dall'autorità che ha ordinato la sorveglianza, e non più soltanto a quest'ultima. In particolare la polizia può consultare i dati perché in linea di massima sarà incaricata di utilizzarli.

La *lettera c* modifica e completa il testo dell'articolo 13 capoverso 1 lettera d della LSCPT vigente, quest'ultima disposizione disciplina il collegamento diretto, una modalità particolare ed eccezionale di esecuzione di una sorveglianza. I dati ottenuti nel quadro di una sorveglianza transitano in linea di massima attraverso il Servizio, che funge da interfaccia tra i fornitori di servizi di telecomunicazione incaricati di eseguire le sorveglianze e l'autorità che ha ordinato la sorveglianza; i dati sono registrati nel sistema del Servizio. Tale è pure il caso se viene ordinata una sorveglianza in tempo reale, vale a dire una sorveglianza non retroattiva. Se la sorveglianza è eseguita sotto forma di collegamento diretto, il fornitore di servizi di telecomunicazione fornisce i dati direttamente all'autorità interessata, senza passare dal Servizio, la qual cosa esclude la registrazione dei dati nel sistema del Servizio. L'autorità registra dunque da sé questi dati. La *lettera c* definisce le condizioni in cui è possibile servirsi del collegamento diretto nell'ambito di una sorveglianza. I casi in cui può essere fatto ricorso al collegamento diretto sono quelli in cui il Servizio non è in grado, per motivi tecnici, di svolgere il ruolo d'interfaccia tra fornitori di servizi di telecomunicazione e autorità. Sono fatti salvi l'articolo 271 capoverso 2 CPP e l'articolo 70*b* capoverso 2 PPM nella versione derivante dal CPP. Le limitazioni del ricorso al collegamento diretto non diminuiranno l'efficacia del lavoro delle autorità di perseguimento penale, nella misura in cui non provocheranno ritardi nel loro lavoro. I dati ottenuti nel quadro di una sorveglianza in tempo reale non eseguita mediante collegamento diretto sono immediatamente messi a disposizione delle autorità interessate, con qualche secondo di ritardo soltanto, mediante il sistema del Servizio. Per meglio soddisfare i requisiti del principio della legalità, la disposizione precisa, ispirandosi per analogia al contenuto degli articoli 15 capoverso 1 lettera b e 23 lettera b dell'OSCPT attuale che le comunicazioni possono anche essere direttamente trasmesse all'autorità (di perseguimento penale) designata dall'autorità che ha ordinato la sorveglianza e non soltanto a quest'ultima. Queste comunicazioni

potranno così in particolare essere direttamente trasmesse alla polizia, che in linea di massima è competente per utilizzare le comunicazioni ottenute mediante la sorveglianza.

La *lettera d* trae ispirazione dall'articolo 13 capoverso 1 lettera e della LSCPT vigente. La nozione di dati secondari vi è adeguata rispetto a quella contenuta in quest'ultima disposizione. Sui motivi e la portata di questi cambiamenti, si veda il commento dell'articolo 26 capoverso 1 lettera b. La *lettera d* adegua il testo dell'articolo 13 capoverso 1 lettera e della LSCPT vigente al funzionamento del nuovo sistema informatico per il trattamento dei dati nel quadro della sorveglianza del traffico delle telecomunicazioni, funzionamento che in linea di massima non prevede più la messa a disposizione di questi dati alle autorità interessate mediante invii postali di supporti di dati e di documenti ma mediante un diritto d'accesso a questo sistema (cfr. art. 6 segg.). Per meglio soddisfare i requisiti del principio della legalità, precisiamo inoltre nella disposizione, traendo ispirazione per analogia dal contenuto degli articoli 15 capoverso 1 lettera b e 23 lettera b della OSCPT vigente, che il Servizio consente la consultazione dei dati anche all'autorità (di perseguimento penale) designata dall'autorità che ha ordinato la sorveglianza e non più a quest'ultima soltanto. La polizia segnatamente può consultare i dati perché in linea di massima sarà incaricata di utilizzarli.

Il compito secondo la *lettera e* è il corollario delle misure che deve prendere il Servizio secondo gli articoli citati in questa disposizione.

La *lettera f* rinvia agli articoli 32–34.

La cernita secondo la *lettera g* si distingue da quella di cui all'articolo 271 CPP e 70b PPM sul segreto professionale e può essere eseguita soltanto su richiesta dell'autorità che ha ordinato la sorveglianza. Il Servizio può eseguire soltanto una cernita automatizzata, gli altri tipi di cernita sono complicati o impossibili. A differenza di quanto prevedeva l'avamprogetto, è il Servizio stesso che deve eseguire la cernita necessaria per isolare alcuni tipi di dati nel flusso di dati in questione. È più delicato affidare questo compito a terzi in particolare ai fornitori di servizi di telecomunicazione, anche soltanto per questioni di responsabilità dell'integrità dei dati. In tale flusso di dati occorre per esempio separare i dati relativi alla televisione da quelli riguardanti il traffico e-mail. L'autorità che ha ordinato la sorveglianza farà una tale domanda soltanto se non desidera consultare un maggior volume di dati o nella misura in cui ciò sia tecnicamente necessario per utilizzare correttamente i dati desiderati che fanno parte di un dato flusso; occorre infatti considerare che la quantità di dati che compongono un flusso di dati può essere tale da rendere difficile o impossibile la loro utilizzazione. Per garantire la trasparenza necessaria a un apprezzamento obiettivo delle prove, il fascicolo penale dovrà se del caso menzionare che è stata messa agli atti soltanto una parte del flusso di dati in questione.

Art. 18 Controllo di qualità

L'*articolo 18* riguarda come gli articoli 32–34 la garanzia della buona esecuzione delle sorveglianze.

Il *capoverso 1* si prefigge di permettere al Servizio di prendere le misure di controllo per rimediare a un problema di qualità constatato dall'autorità di perseguimento penale o dal Servizio medesimo, in relazione con i dati forniti dai fornitori di servizi di telecomunicazione. Un tale problema si pone per esempio se l'autorità di perse-

guimento penale constata che i dati secondari ottenuti durante una sorveglianza retroattiva rivelano comunicazioni che non figurano nelle registrazioni delle conversazioni ottenute nell'ambito di una sorveglianza in tempo reale. L'obiettivo di questa disposizione è di permettere al Servizio di anticipare le situazioni problematiche mediante controlli preventivi per verificare che non vi siano problemi che possono pregiudicare il buon andamento delle sorveglianze. È evidente che, in base all'articolo 3 capoverso 3 e anche in base all'articolo 5, il Servizio deve informare l'autorità di perseguimento penale interessata in merito a eventuali problemi relativi alla qualità dei dati; questi problemi possono in effetti essere determinanti ai fini di un procedimento.

Il *capoverso 2* prevede che se, per eseguire i succitati controlli, il Servizio deve prendere atto del contenuto dei dati consegnati dai fornitori di servizi di telecomunicazione, e tale è il caso se esegue un controllo dei dati di una sorveglianza reale, vale a dire una sorveglianza che riguarda un «bersaglio» e dati reali, esso deve dapprima ottenere l'autorizzazione dell'autorità che ha ordinato la sorveglianza o dell'autorità che tiene in seguito il fascicolo. Il Servizio non può in effetti prendere atto del contenuto dei dati, anche se sono in suo possesso poiché registrati nel suo sistema. Una tale autorizzazione non è invece necessaria se il Servizio esegue un controllo che non richiede la presa d'atto dei dati, come nel caso di una sorveglianza fittizia nell'ambito di un controllo preventivo, vale a dire di un controllo riguardante un «bersaglio» test (fittizio) e dati fittizi.

2.4 Sezione 4: Obblighi nell'ambito della sorveglianza della corrispondenza postale

Art. 19 Obblighi dei fornitori di servizi postali

L'*articolo 19* sostituisce l'articolo 12 della LSCPT vigente.

Il *capoverso 1* riprende sostanzialmente l'articolo 12 capoverso 1 dell'attuale LSCPT. Gli invii postali e i dati secondari postali devono essere consegnati direttamente all'autorità che ha ordinato la sorveglianza (o all'autorità da essa designata) e non al Servizio, contrariamente a quanto vale in linea di massima per i dati forniti nell'ambito di una sorveglianza del traffico delle telecomunicazioni (cfr. art. 26 cpv. 1). Il *capoverso 1* cita due tipi principali di sorveglianza per quanto concerne i dati già contemplati nel sistema della LSCPT vigente, vale a dire la sorveglianza riguardante il contenuto della corrispondenza postale (dati di contenuto; lett. a) e quella concernente i dati secondari della corrispondenza (lett. b) che non permettono di prendere atto del contenuto della corrispondenza. La definizione dei dati secondari postali è modificata rispetto a quella prevista nel diritto vigente, che contiene un'inutile enumerazione di determinate categorie di dati, ma non vi sono cambiamenti nel contenuto materiale della nozione. Il cambiamento della definizione ha per corollario il cambiamento operato nell'articolo 273 capoverso 1 CPP e 70*d* PPM. Per soddisfare i requisiti del principio della legalità, il capoverso 1 precisa, traendo ispirazione per analogia dal contenuto dell'articolo 11 lettera b dell'attuale OSCPT, che le corrispondenze e i dati possono essere forniti anche all'autorità di perseguimento penale designata dall'autorità che ha ordinato la sorveglianza, e non più soltanto a quest'ultima. La polizia potrà segnatamente consultare i dati e le corri-

spondenze poiché in linea di massima sarà incaricata di utilizzarli. L'obbligo dei fornitori di servizi postali di fornire informazioni supplementari previsto nell'articolo 12 capoverso 1 della vigente LSCPT è eliminato. In effetti, queste informazioni non dipendono dalle conoscenze dei fornitori di servizi postali ma di persone determinate, come ad esempio il postino, e devono essere ottenute attraverso canali normali, vale a dire con l'audizione dell'interessato in qualità di testimone[39]. Occorre evidentemente precisare che, per soddisfare il loro obbligo di fornire i dati considerati, gli interessati sono tenuti a fornire tali dati, la qual cosa presuppone che essi conservino i dati secondari. Non è prevista la registrazione nel sistema del Servizio dei dati raccolti durante la sorveglianza della corrispondenza postale.

Il *capoverso 2* indica semplicemente due altri tipi di sorveglianza eseguiti in momenti diversi; questi generi di sorveglianza sono già contemplati nel sistema attuale: la sorveglianza in tempo reale e la sorveglianza retroattiva, definite ai numeri 3 e 4 dell'allegato dell'attuale OSCPT.

Il *capoverso 3* è una norma che delega al Consiglio federale la competenza di precisare dei punti attualmente già disciplinati nell'OSCPT. Attualmente il Consiglio federale impone soltanto l'obbligo di conservare o di fornire i dati secondari disponibili; tali dati esistono per esempio per gli invii postali con giustificativo di distribuzione, ma non ve ne sono per il semplice invio di una lettera. È opportuno precisare che, contrariamente ai fornitori di servizi di telecomunicazione (cfr. art. 26 cpv. 6), il disegno non prevede la possibilità di dispensare determinate categorie di fornitori di servizi postali da alcuni loro obblighi legali. Ciò è in particolare dovuto al fatto che gli obblighi menzionati nel capoverso 1 non sono complessi da eseguire sotto il profilo tecnico (certamente meno di quelli dei fornitori di servizi di telecomunicazione), al fatto che i fornitori di servizi postali devono consegnare soltanto i tipi di dati secondari menzionati sopra e al fatto che questi dati secondari non riguardano tutti gli invii postali. L'obbligo di conservazione non riguarda quindi tutti i fornitori di servizi postali. Per determinare il regime applicabile alla sorveglianza della corrispondenza, occorre determinare per ogni nuovo servizio, come i servizi di posta elettronica, se si tratta di un servizio postale o di un servizio di telecomunicazione. Un adeguamento delle disposizioni esecutive può rivelarsi necessario per i servizi di nuovo genere che presentano caratteristiche sia di servizio postale sia di servizio di telecomunicazione.

Il *capoverso 4* si ispira all'articolo 12 capoverso 2 dell'attuale LSCPT e riguarda la durata di conservazione dei dati secondari nel settore della corrispondenza postale. Questo obbligo significa che i fornitori di servizi postali devono, come è il caso secondo la vigente LSCPT, conservare «in riserva» per eventuali future istruzioni penali i dati secondari di tutte le corrispondenze. Spetta al Consiglio federale designare questi dati secondari in applicazione della competenza attribuitagli dal capoverso 3. Questa normativa è necessaria per consentire ai citati fornitori di soddisfare l'obbligo loro imposto dal capoverso 1 lettera b in caso di sorveglianza retroattiva, fermo restando che i dati indicati in questa disposizione sono assolutamente indispensabili per lottare contro la criminalità. Il prolungamento da sei a dodici mesi, dalla data della corrispondenza, della durata della conservazione dei dati secondari nel settore della corrispondenza postale va segnatamente posto in relazione con la mozione Schweiger 06.3170 (Lotta alla cibercriminalità. Protezione dei fanciulli), che, tra le altre cose, chiedeva un tale prolungamento della durata di conservazione

39 Thomas Hansjakob, op. cit. (nota 11), n. 4 ad art. 12 LSCPT.

dei dati secondari nel settore del traffico delle telecomunicazioni, compreso Internet (cfr. commento dell'art. 26 cpv. 5). La problematica affrontata dalla mozione, vale a dire la perdita di dati importanti per le inchieste penali, è rilevante non soltanto per i dati secondari nel settore del traffico delle telecomunicazioni ma anche in quello della corrispondenza postale. È quindi logico che l'aumento della durata di conservazione si applichi anche ai dati secondari postali. Per il rimanente, si veda per analogia il commento dell'articolo 26 capoverso 5. Il nostro Collegio ritiene accettabile la maggior mole di lavoro amministrativo che dovranno sbrigare i fornitori di servizi postali in seguito all'aumento della durata di conservazione dei dati secondari, tanto più che questi dati devono già oggi essere conservati, che la conservazione non è complessa sotto il profilo tecnico e che i fornitori devono conservare soltanto alcuni tipi di dati di questa categoria (cfr. commento del cpv. 3). Non sussistono quindi motivi validi per stabilire una diversa durata di conservazione (più breve) per i dati secondari postali.

Il fatto che le corrispondenze postali siano oggetto di una sorveglianza non implica necessariamente che la persona sorvegliata non possa ottenerle. Il *capoverso 5* si iscrive in questo ordine di idee. Tuttavia, il fornitore di servizi postali non può recuperare le corrispondenze e consegnarle alla persona sorvegliata prima di aver ottenuto l'accordo dell'autorità che ha ordinato la sorveglianza o dell'autorità a cui ha rimesso il fascicolo. È evidente che l'autorità potrà rifiutare il suo accordo, per esempio se le corrispondenze devono essere confiscate o servire da mezzi di prova. È pure evidente che, a meno di violare l'articolo 39 capoverso 1 lettera d, il fornitore di servizi postali non può rendere noto alla persona sorvegliata il fatto che le corrispondenze postali, che gli vengono consegnate, sono state oggetto di una sorveglianza. Si procederà a una tale comunicazione se del caso nell'ambito e alle condizioni dell'articolo 279 CPP.

Art. 20 Informazioni precedenti un ordine di sorveglianza

L'*articolo 20* riguarda le informazioni che vanno ottenute prima di ordinare una sorveglianza. Tali informazioni possono in particolare essere utili nei casi in cui si prende in considerazione una sorveglianza speciale, che presenta cioè caratteristiche particolari rispetto alle sorveglianze abituali.

2.5 Sezione 5: Informazioni relative alla sorveglianza del traffico delle telecomunicazioni

Un folto gruppo di partecipanti alla consultazione, di quasi tutte le cerchie interpellate, ha chiesto che fossero precisati gli obblighi di collaborare non sufficientemente esplicitati né nella legge vigente né nell'AP-LSCPT. Per i dettagli si veda la sintesi dei risultati della consultazione[40].

Anche il nostro Collegio ritiene che i diversi obblighi di collaborare e tollerare devono essere chiariti. Il chiarimento è effettuato negli articoli 21–25 (Sezione 5: Informazioni relative alla sorveglianza della corrispondenza delle telecomunica-

40 www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ve-ber-i.pdf

zioni), negli articoli 26–30 (Sezione 6: Obblighi nell'ambito della sorveglianza del traffico delle telecomunicazioni) e negli articoli 31–34 (Sezione 7: Garanzia della disponibilità a informare e sorvegliare dei fornitori di servizi di telecomunicazione). La portata dell'obbligo di collaborare vi è definita in modo graduato in funzione delle diverse attività specifiche.

Non occorre invece disciplinare i dettagli di questi obblighi nella legge; i dettagli devono infatti essere regolati dal Consiglio federale nell'ordinanza (OSCPT). Questa flessibilità è molto importante poiché la differenza tra fornitori di servizi di telecomunicazione classici (Swisscom) e il fenomeno relativamente nuovo dei fornitori di servizi di comunicazione derivati (p. es. Google) sta scemando sempre più. Di conseguenza, il Consiglio federale deve ottenere la competenza di assoggettare i fornitori di servizi di comunicazione derivati che offrono servizi di grande importanza economica o che servono un gran numero di utenti a tutti gli obblighi o a parte degli obblighi previsti per i fornitori di servizi di telecomunicazione (cfr. per i dettagli il commento dell'art. 27 cpv. 3). Occorre dunque che il Consiglio federale ottenga la competenza di dispensare i fornitori di servizi di telecomunicazione da alcuni obblighi legali, in particolare quelli che offrono servizi di telecomunicazione di debole importanza economica o nel settore dell'educazione (cfr. per i dettagli il commento dell'art. 26 cpv. 6).

Art. 21 Informazioni sui servizi di telecomunicazione

L'*articolo 21* riprende sostanzialmente l'articolo 14 capoversi 2–4 della vigente LSCPT e lo completa. Il concetto di «servizi (di telecomunicazione)» sostituisce quello di «collegamenti (di telecomunicazione)» che, in seguito all'evoluzione tecnica, si è rivelato troppo restrittivo (cfr. commento dell'art. 15). Anche i fornitori di servizi di accesso a Internet sono assoggettati a questa disposizione (cfr. commento dell'art. 2 lett. b) e i servizi di telecomunicazione comprendono Internet (cfr. commento dell'art. 1 cpv. 1). Attualmente, nel settore della telefonia mobile, i fornitori di servizi di telecomunicazione sono obbligati a registrare le carte SIM prepagate, mentre nel nuovo diritto questo obbligo sarà esteso al settore di Internet (carte wireless prepagate e altri mezzi analoghi). Questa estensione è richiesta nella mozione Glanzmann-Hunkeler 07.3627 (Obbligo di registrazione delle carte prepagate Wi-Fi) che sostanzialmente chiede che siano registrati come le carte SIM prepagate anche gli utenti di questi mezzi, in particolare per impedire lo scaricamento anonimo da Internet di immagini o video a carattere pedofilo. Questo obbligo riguarderà anche i mezzi che consentono di accedere a una rete di telefonia fissa.

Le informazioni menzionate all'*articolo 21* non sono coperte dal segreto delle telecomunicazioni a differenza del contenuto delle comunicazioni e dei dati secondari; queste informazioni possono quindi essere comunicate nell'ambito di una procedura semplificata[41], come è il caso sotto l'egida della vigente LSCPT, e possono essere ottenute senza che a tal fine occorrano provvedimenti coercitivi. La loro comunicazione non soggiace quindi alle condizioni restrittive dell'articolo 269 CPP, in particolare non soggiace all'elenco dei reati del capoverso 2 di tale disposizione[42] e non deve essere autorizzata dall'autorità d'approvazione (art. 274 CPP). Queste informazioni sono molto importanti affinché le inchieste possano progredire[43] e a date

41 Cfr. il messaggio del 1° luglio 1998 relativo alla LSCPT vigente, FF **1998** 3354.
42 Thomas Hansjakob, op. cit. (nota 11), n. 1–4 e 23 ad art. 14 LSCPT.
43 Cfr. il messaggio del 1° luglio 1998 relativo alla LSCPT vigente, FF **1998** 3354.

condizioni possono permettere di ordinare una sorveglianza alle condizioni severe di cui all'articolo 269 CPP. Evidentemente per poter adempiere il loro obbligo di fornire le informazioni e le indicazioni di cui all'*articolo 21* queste persone devono disporne, la qual cosa presuppone che le conservino. Le persone che devono ricevere le informazioni sono indicate nell'articolo 15. Occorre precisare che, in virtù dell'articolo 15 capoverso 1 lettere a e b, le informazioni possono essere fornite direttamente alla polizia, senza che il pubblico ministero debba ordinarlo nel caso dell'articolo 15 capoverso 1 lettera b (cfr. per i dettagli cfr. il commento di queste disposizioni).

Le informazioni di cui al *capoverso 1* lettere a–d devono essere consegnate anche ai fornitori di servizi di telecomunicazione se i loro clienti non hanno sottoscritto un abbonamento (cfr. cpv. 2); se i loro clienti non hanno sottoscritto un abbonamento, devono inoltre essere registrati i dati di cui al capoverso 1 lettera e. Le modalità della registrazione dei dati secondo l'articolo 21 capoverso 1 lettera a sono disciplinate dal Consiglio federale (cfr. per i dettagli il commento dell'art. 23). In tal modo i fornitori di servizi di telecomunicazione sono in grado di rendere accessibili le informazioni di cui al *capoverso 1* mediante il sistema di commutazione delle domande di informazioni sui servizi di telecomunicazione (attualmente chiamato CCIS) gestito dal Servizio in collaborazione con i succitati fornitori. Per i pertinenti obblighi dei rivenditori di mezzi come le carte prepagate rinviamo all'articolo 30.

Il *capoverso 1 lettera a* riprende l'articolo 14 capoverso 1 lettera a della vigente LSCPT e vi aggiunge il nome e la data di nascita. Si tratta dei classici elementi d'identificazione, anche per le autorità e ai fini menzionati nell'articolo 15.

Il *capoverso 1 lettera b* riprende sostanzialmente l'articolo 14 capoverso 1 lettera b della LSCPT vigente. Visto che l'articolo 3 lettera f LTC contiene l'espressione «parametri di comunicazione» poi definita all'articolo 3 lettera g della legge, il rinvio della lettera b viene completato di conseguenza per motivi di chiarezza.

Il *capoverso 1 lettera c* si ispira all'articolo 14 capoverso 1 lettera c dell'attuale LSCPT e utilizza la forma plurale. Nei casi in cui si vuole sorvegliare una persona è infatti utile conoscere tutti i tipi di servizi (p. es. telefonia fissa, mobile e Internet) di cui essa dispone. Ciò permette di determinare con conoscenza di causa quale tipo di servizi occorra sorvegliare e di evitare di dover interrogare i fornitori di servizi di telecomunicazione per ciascuno dei diversi tipi di servizi di cui dispone.

La norma di delegazione di cui al *capoverso 1 lettera d* dà al Consiglio federale la competenza di obbligare i fornitori di servizi di telecomunicazione a consegnare al Servizio altri tipi di informazioni utili sui servizi di telecomunicazione, come la data di attivazione del servizio, lo statuto del servizio (p. es. attivo, bloccato o disdetto), il numero PUK, i numeri SIM, IMEI e IMSI, le fatture, le modalità di pagamento di queste ultime e i contratti. Questa norma consente anche all'Esecutivo di obbligarli a fornire dati utili di genere diverso da quelli di cui alla lettera a che consentono anche di identificare le persone, come per esempio le fotocopie dei documenti di identità. Il Consiglio federale potrà per esempio prescrivere che la registrazione avvenga soltanto su presentazione di un passaporto o di una carta d'identità valida o di un altro documento di viaggio riconosciuto che permette di entrare o risiedere in Svizzera, che siano registrati il genere e il numero del documento d'identità e che occorra farne inoltre una fotocopia. Alcuni di questi tipi di informazioni supplementari sono già attualmente menzionati nelle direttive del Servizio e possono di conseguenza già essere ottenuti dalle autorità di perseguimento penale. È quindi molto probabile che

il nostro Collegio riprenda almeno queste informazioni in un'ordinanza. Le disposizioni da noi proposte in virtù del *capoverso 1 lettera d* saranno poste in consultazione presso le cerchie interessate. In virtù dell'articolo 15 capoverso 1 lettere a e b, se il Consiglio federale lo prevede (cfr. cpv. 5), le informazioni potranno essere fornite direttamente alla polizia, senza che il pubblico ministero debba ordinarlo nel caso dell'articolo 15 capoverso 1 lettera b mediante un sistema di commutazione delle domande di informazioni sui servizi di telecomunicazione (CCIS). Non occorre che il trattamento di questi dati sia previsto in una legge in senso formale (art. 17 LPD), come la LSCPT, poiché non si tratta di dati personali degni di particolare protezione ai sensi dell'articolo 3 lettera c LPD. Il presente disegno di legge non contiene una disposizione che elenca questi tipi di informazioni, poiché avrebbe una densità eccessiva per figurare in una legge. Queste informazioni devono invece figurare in un'ordinanza.

Il *capoverso 1 lettera e* prevede l'obbligo dei fornitori di servizi di telecomunicazione di indicare il nome e cognome della persona che ha consegnato, a titolo oneroso o no, il mezzo che permette di accedere ai servizi (carte SIM prepagate o altri mezzi simili, carte «wireless» prepagate o altri mezzi simili e i mezzi che permettono di accedere a una rete di telefonia fissa); va inoltre indicato il punto di vendita in cui è avvenuta la consegna. Questo obbligo è in particolare necessario per stabilire chi è venuto meno alle prescrizioni sulla registrazione dei dati oggetto del capoverso 1 lettere a–d. Per quanto concerne i corrispondenti obblighi dei rivenditori di tali mezzi, vedi l'articolo 27.

Il c*apoverso 2* disciplina l'obbligo di registrare i dati di cui al capoverso 1 e di mantenerli disponibili; la sottoscrizione di un abbonamento da parte dei clienti dei fornitori di servizi di telecomunicazione non ha alcun ruolo. Il capoverso 2 riprende in parte e adegua l'articolo 15 capoverso 5bis della LSCPT vigente, estendendo peraltro l'obbligo dei fornitori di servizi di telecomunicazione di fornire le informazioni richieste. Occorre rilevare che questo obbligo concerne attualmente le carte SIM prepagate e altri mezzi analoghi nel settore della telefonia mobile e che d'ora innanzi riguarderà anche le carte «wireless» (di accesso senza fili) prepagate e altri mezzi simili nel settore di Internet. Questa estensione riprende quanto richiesto dalla mozione 07.3627 Glanzmann-Hunkeler. Logicamente, d'ora in avanti soggiacciono alla disposizione anche i mezzi per accedere a una rete di telefonia fissa, indipendentemente dalla sottoscrizione di un abbonamento. È in effetti necessario disporre delle citate informazioni sulla relazione commerciale con un cliente che non ha concluso un abbonamento. Nell'ambito della lotta contro il terrorismo questa necessità si è fatta sentire per quanto concerne le carte SIM prepagate. La vigente LSCPT contempla un termine di due anni a decorrere dall'avvio di una relazione commerciale durante il quale devono essere fornite queste informazioni. Il termine di due anni era stato scelto in considerazione del fatto che, nel momento dell'entrata in vigore dell'articolo 15 capoverso 5bis LSCPT vigente, vale a dire il 1° agosto 2004, era stato deciso di soprassedere alla registrazione retroattiva delle carte SIM prepagate acquistate prima del 1° agosto 2002 che sarebbe stata eccesiva[44]. Il termine può essere soppresso perché ormai non è più questione di registrazione retroattiva. Questa soppressione rende necessaria l'adozione di una disposizione transitoria per le carte SIM prepagate e altri mezzi analoghi (art. 45 cpv. 4). Precisiamo inoltre che il succitato obbligo di informare vale soltanto per le informazioni fornite per la

44 Thomas Hansjakob, op. cit. (nota 11), n. 22 ad art. 15 LSCPT.

registrazione da effettuare prima della consegna di una carta SIM prepagata da parte di un fornitore di servizi di telecomunicazione (o di altri mezzi analoghi), di carte «wireless» prepagate (o di altri mezzi analoghi) o di mezzi per accedere a una rete di telefonia fissa nel momento dell'apertura della relazione commerciale, e non sui dati riguardanti le persone che potrebbero acquisire tali mezzi in seguito. In altri termini, un fornitore di servizi di telecomunicazione deve essere in grado di fornire soltanto le informazioni da lui richieste in occasione della consegna di un dato mezzo e non i dati su eventuali futuri acquirenti del mezzo medesimo. Qualsiasi altro regime comporterebbe formalità e oneri amministrativi eccessivi (cfr. anche il commento dell'art. 6*a* LTC).

Occorre rilevare che il *capoverso 2* non limita la portata dell'articolo 22.

La violazione degli obblighi di registrazione è sanzionata dall'articolo 39 capoverso 1 lettera c.

Art. 22 Informazioni per identificare gli autori di reati commessi via Internet

L'*articolo 22* riprende sostanzialmente l'articolo 14 capoverso 4 LSCPT vigente e prevede un dovere di collaborazione dei fornitori di servizi di telecomunicazione che, per quanto loro possibile, devono adoperarsi per consentire questa identificazione. Questa disposizione non obbliga tuttavia i fornitori di servizi di telecomunicazione a fornire il nome della persona che utilizza effettivamente un computer, poiché su questo non hanno alcun controllo; sono invece per esempio tenuti, nella misura in cui il Consiglio federale impone loro l'obbligo, a fornire il nome della persona alla quale è stato attribuito il numero IP in questione. Come nella LSCPT vigente, la comunicazione delle informazioni secondo l'*articolo 22* può avere luogo in modo semplificato (cfr. il commento dell'art. 21).

L'articolo 22 riguarda l'identificazione degli autori di reati commessi su Internet; il *capoverso 1* fa riferimento a tutti i dati che consentono tale identificazione[45]. A fini di identificazione, è previsto l'ottenimento agevolato dei dati secondari come l'attribuzione di un IP dinamico (non attribuito in anticipo)[46]. Per coerenza con il ruolo di interfaccia del Servizio, le indicazioni devono essere fornite al Servizio e non all'autorità competente come nel diritto attuale[47].

A differenza dell'articolo 14 capoverso 4 LSCPT vigente, formulato in modo ampio, il *capoverso 2* contiene una norma di delegazione che dà espresso mandato al Consiglio federale di menzionare sul modello dell'articolo 27 OSCPT vigente i dati che i fornitori di servizi di telecomunicazione sono tenuti a fornire. Le cerchie interessate saranno consultate sulle proposte del Consiglio federale conformemente al *capoverso 2*.

Anche le persone di cui all'articolo 2 lettere c e d detengono informazioni che possono essere utili nel contesto dell'*articolo 22*. Il *capoverso 3* richiede tuttavia, come corollario degli articoli 27 capoverso 2 e 28 capoverso 2, che forniscano soltanto le indicazioni a loro disposizione (almeno quelle disponibili nel momento in cui ne viene fatta domanda).

45 Thomas Hansjakob, op. cit. (note 11), n. 25 ad art. 14 LSCPT.
46 Thomas Hansjakob, op. cit. (note 11), n. 26 ad art. 14 LSCPT.
47 Thomas Hansjakob, op. cit. (note 11), n. 24 ad art. 14 LSCPT.

Il nostro Collegio ritiene comunque che la normativa non sia sufficiente per identificare efficacemente gli autori di reati commessi via Internet. Per questo motivo la delega del *capoverso 4*, a corollario dell'articolo 27 capoverso 3, consente all'Esecutivo di obbligare, rispettando condizioni restrittive (cfr. per analogia il commento dell'art. 27 cpv. 3), le persone di cui all'articolo 2 lettera c a fornire indicazioni supplementari, analoghe a quelle che devono fornire i fornitori di servizi di telecomunicazione.

Art. 23 Modalità di rilevamento dei dati e della fornitura di informazioni

Il *capoverso 1* prevede che il Consiglio federale stabilisca le modalità di rilevamento dei dati di cui agli articoli 21 capoverso 1 lettera a e 22 capoverso 2 primo periodo. Esso può per esempio prevedere che la registrazione sia effettuata soltanto su presentazione di una passaporto o di una carta d'identità valida o di un altro documento di viaggio riconosciuto per entrare o risiedere in Svizzera, che siano rilevati il tipo e il numero del documento d'identità e che di quest'ultimo sia effettuata una copia.

Il *capoverso 2* riprende l'articolo 14 capoverso 3 primo periodo della LSCPT vigente.

Sotto l'egida della vigente LSCPT, il nostro Collegio aveva deciso di rendere accessibili online i dati menzionati all'articolo 21 capoverso 1 alle autorità indicate nell'articolo 15 e ciò mediante un sistema di commutazione delle domande di informazioni sui collegamenti di telecomunicazione (noto come CCIS) elaborato e gestito dal Servizio in collaborazione con i fornitori di servizi di telecomunicazione (art. 19 segg. OSCPT vigente). Le informazioni che non possono essere ottenute in questo modo lo sono su richiesta (in linea di massima via fax) rivolta al Servizio che poi la inoltra ai fornitori di servizi di telecomunicazione. Il nostro Collegio non aveva dunque voluto consentire alle autorità secondo l'articolo 15 di accedere direttamente alle cartelle esistenti e non accessibili al pubblico. Il *capoverso 3* permette al nostro Collegio di modificare il sistema attuale. Se lo ritiene opportuno, può per esempio prevedere che tutti i dati di cui agli articoli 21 e 22 siano resi disponibili online tramite il sistema di commutazione delle domande di informazione sui servizi di telecomunicazione. Le autorità di polizia di cui all'articolo 15 capoverso 1 lettera b potranno di moto proprio chiedere e ottenere dal Servizio i dati di cui agli articoli 21 e 22 senza che a tal fine sia necessario un ordine del pubblico ministero (cfr. per i dettagli il commento dell'art. 15 cpv. 1 lett. b).

Art. 24 Informazioni precedenti un ordine di sorveglianza

Diversamente dall'articolo 26 capoverso 2, l'articolo 24 concerne le informazioni che occorre ottenere prima di ordinare una sorveglianza. Tali informazioni (p. es. la posizione di un'antenna di telefonia mobile) possono essere utili in particolare se si prevede di ordinare una sorveglianza speciale, vale a dire con caratteristiche particolari rispetto alle sorveglianze abituali.

Art. 25 Informazione sui servizi

L'*articolo* 25, come gli articoli 32–34, si prefigge di garantire la corretta esecuzione delle sorveglianze in modo tale da evitare le lacune nella sorveglianza. Si vuole in particolare consentire al Servizio di anticipare le difficoltà che potrebbero insorgere nel quadro delle future sorveglianze e di non contentarsi di reagire ai problemi che si

presentano durante l'esecuzione delle sorveglianze. Va precisato che l'*articolo 25* prevede unicamente l'informazione del Servizio sulla natura e sulle caratteristiche dei servizi in questione e non sulle caratteristiche della tecnologia sulla quale i servizi in questione si fondano. In effetti non è necessario conoscere le caratteristiche di questa tecnologia, l'importante è poter eseguire le sorveglianze conformemente agli articoli 18 e 32–34. Nei fatti, i fornitori di servizi di telecomunicazione dovranno, su richiesta del Servizio, spiegare a quest'ultimo quali sono i servizi che offrono e in cosa consistono, cioè cosa permettono di fare. Ciò indipendentemente dal fatto che il Servizio sia stato sviluppato dal fornitore di servizi di telecomunicazione o no o dal fatto che impiega una tecnologia sviluppata da un terzo. L'organo consultivo di cui all'articolo 5 è per il Servizio il canale ideale per l'ottenimento di queste informazioni. Sembra così possibile rinunciare a obbligare i fornitori di servizi di telecomunicazione a informare spontaneamente il Servizio, senza essere prima stati interpellati da quest'ultimo.

È possibile che i collaboratori del Servizio prendano atto in questo modo di segreti d'affari dei fornitori di servizi di telecomunicazione. Orbene, a questo proposito occorre rilevare che questi collaboratori sono sottoposti al segreto di funzione e che un collaboratore del Servizio che rivela tali segreti può essere colpevole di violazione del segreto di funzione (art. 320 CP).

Il termine di sei mesi di cui all'*articolo 25* è stato introdotto per evitare che i fornitori di servizi di telecomunicazione debbano fornire le informazioni in una fase in cui ancora non hanno la certezza di mettere sul mercato un determinato servizio. Va comunque fatto notare che, in linea di massima, i fornitori di servizi di telecomunicazione pianificano il loro bilancio con 12 mesi di anticipo e vogliono poter disporre di un termine transitorio di 12 mesi per introdurre il nuovo sistema di sorveglianza. Il termine di sei mesi si prefigge quindi di evitare lavoro superfluo non soltanto ai fornitori di servizi di telecomunicazione ma anche al Servizio. A seconda dei casi, il Servizio avrà bisogno di tempi più lunghi per compiere le procedure necessarie per eseguire correttamente le sorveglianze. Nonostante quanto precede, abbiamo rinunciato a un termine superiore a sei mesi perché sarebbe eccessivo per i fornitori di servizi di telecomunicazione. Intanto, si dovrà assumere il rischio che in alcuni casi potrebbe non essere possibile eseguire una sorveglianza. Giova rilevare che la normativa proposta non impedisce di certo ai fornitori di servizi di telecomunicazione di cambiare e adeguare la loro pianificazione dei servizi che intendono mettere sul mercato in futuro; un altro regime limiterebbe eccessivamente le possibilità di queste imprese di affermarsi su un mercato delle telecomunicazioni in costante mutamento.

2.6 Sezione 6: Obblighi nell'ambito della sorveglianza del traffico delle telecomunicazioni

Per le osservazioni generali sugli obblighi di informazione e di sorveglianza e sui risultati della procedura di consultazione rinviamo alle spiegazioni introduttive della sezione 5.

Art. 26 Obblighi dei fornitori di servizi di telecomunicazione

L'*articolo 26* sostituisce il vigente articolo 15 LSCPT sugli obblighi dei fornitori di servizi di telecomunicazione. Soddisfa in particolare la legittima richiesta espressa durante la consultazione di precisare gli obblighi di collaborare, segnatamente quelli dei fornitori di servizi di telecomunicazione, che non sono espressi con sufficiente chiarezza né nella legge vigente né nell'AP-LSCPT. Per i dettagli si veda la sintesi dei risultati della consultazione[48]. Il presente disegno elimina inoltre i compiti specifici che l'AP-LSCPT aveva affidato ai fornitori di servizi di telecomunicazione in relazione con l'impiego di Government Software (GovWare); un'analisi più approfondita ha infatti rivelato che non occorre un aiuto o concorso particolare dei fornitori di servizi di telecomunicazione affinché le autorità di perseguimento penale possano impiegare i GovWare (cfr. anche il commento dell'art. 280 lett. d CPP).

Il *capoverso 1* menziona due tipologie di sorveglianza, già contemplate nella LSCPT vigente, e le distingue in funzione dei tipi di dati. Si tratta della sorveglianza del contenuto del traffico delle telecomunicazioni inviate o ricevute (dati di contenuto; *lett. a*) e della sorveglianza che riguarda unicamente i dati secondari di tale traffico (*lett. b*) che non consentono di conoscere il contenuto delle singole comunicazioni. Come indica l'articolo 8 lettera b la definizione dei dati secondari di telecomunicazione è semplificata rispetto alla definizione del diritto vigente, senza però mutare il significato materiale della nozione. È così soppressa la menzione dei «dati relativi al traffico e alla fatturazione», poiché tale categoria di dati rientra nella nuova definizione dei dati secondari. Le espressioni «sorvegliato» e «dati indicanti con chi» riguardano più il servizio utilizzato (p. es. il collegamento) che le persone che lo utilizzano. In effetti, l'oggetto della sorveglianza è per esempio il collegamento della persona sorvegliata (che può anche essere sconosciuta) in comunicazione con un altro collegamento attribuito a una data persona che non è per forza quella che ha utilizzato o utilizza questo secondo collegamento nel momento in questione. Il cambiamento della definizione dei dati secondari implica la modifica dell'articolo 273 capoverso 1 CPP e 70*d* capoverso 1 PPM. Il *capoverso 1* copre ben inteso i dati riguardanti gli accessi a Internet, poiché l'accesso a Internet è una modalità del traffico delle telecomunicazioni (cfr. il commento dell'art. 1 cpv. 1). La formulazione del capoverso 1 permette in particolare di rilevare il contenuto di un SMS (*lett. a*), i dati secondari di un SMS (*lett. b*) e i semplici tentativi di stabilire una comunicazione (p. es. nel caso in cui la persona che il sorvegliato cerca di raggiungere non risponde al telefono; *lett. b*). È evidente che per soddisfare il loro obbligo di fornire i dati considerati, gli interessati devono averli a loro disposizione, la qual cosa presuppone che conservino i dati secondari. Per spiegazioni più dettagliate della nozione di dati secondari si veda il commento del capoverso 5. Il riferimento all'articolo 17 lettera c vuole soltanto rammentare che, se la sorveglianza è eseguita mediante collegamento diretto, i dati raccolti sono eccezionalmente trasmessi direttamente all'autorità che ha ordinato la sorveglianza o all'autorità (in linea di massima un'autorità di perseguimento penale) da essa designata e non dapprima al Servizio che di principio svolge il ruolo dell'intermediario. Spetterà al Consiglio federale determinare entro quale termine si possono esigere tali dati dai fornitori di servizi di telecomunicazione. I fornitori di servizi di telecomunicazione devono fornire i dati chiesti dall'autorità che ha ordinato la sorveglianza. Se quest'ultima lo vuole,

48 www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ve-ber-i.pdf

devono quindi, nella misura in cui ciò sia ragionevolmente esigibile nel caso concreto, compiere una cernita per isolare determinati tipi di dati dal flusso di dati in questione in modo da fornire soltanto i dati richiesti (p. es. dati Internet, senza i dati della televisione via Internet). Per il rimanente si veda il commento dell'articolo 17 lettera f.

Il *capoverso 2* riprende gli obblighi necessari per l'esecuzione della sorveglianza previsti nella LSCPT attuale (art. 15 cpv. 1 primo periodo e cpv. 4 secondo periodo). A differenza dell'articolo 24, in questo ambito sono prese in considerazione le informazioni necessarie quando viene ordinata una sorveglianza. Tra le informazioni a cui fa riferimento la presente disposizione vi sono in particolare quelle relative alla tecnica di comunicazione utilizzata e agli apparecchi adoperati dai singoli[49]. Imponendo agli interessati l'obbligo minimo di tollerare la sorveglianza nonché obblighi accessori necessari per permetterne l'esecuzione, il *capoverso 2* vuole colmare in una certa misura la lacuna nella sorveglianza creata dal capoverso 6. Ispirandosi in parte alla normativa contenuta nella vigente LSCPT per quanto concerne la sorveglianza di una rete di telecomunicazione interna o di una centralina domestica, il disegno prevede che la sorveglianza sia eseguita dal Servizio o da una persona da esso incaricata, in particolare la polizia. Ciò non significa che il Servizio possa trasferire compiti amministrativi a privati ai sensi dell'articolo 178 capoverso 3 della Costituzione federale (Cost)[50]. Il Servizio rimane in effetti responsabile dell'esecuzione del compito delegato. Per quanto concerne l'obbligo di depositare i dati secondari dei fornitori dispensati secondo il capoverso 6, si veda il commento a questa disposizione.

Il *capoverso 3* va posto in relazione con l'articolo 17 lettera a e riprende un obbligo esistente nella LSCPT vigente (art. 15 cpv. 2 secondo periodo) e necessario per l'esecuzione della sorveglianza. Su richiesta dell'autorità che ha ordinato la sorveglianza inoltrata dal Servizio, vi è anche la possibilità di fornire i dati direttamente al Servizio in particolare per motivi di confidenzialità.

Oltre a quelle indicate nel capoverso 1, il *capoverso 4* menziona altre due importanti tipologie di sorveglianza – già previste nella LSCPT vigente – in base al momento dell'esecuzione: la sorveglianza in tempo reale e la sorveglianza retroattiva, definite ai numeri 3 e 4 dell'allegato della OSCPT vigente. I dati che possono essere ottenuti nel quadro di una sorveglianza retroattiva sono dati secondari che nel linguaggio tecnico sono chiamati «dati conservati» («retained data»).

L'obbligo di cui al *capoverso 5* impone ai fornitori di servizi di telecomunicazione di conservare in riserva per eventuali future inchieste penali i dati secondari di tutte le comunicazioni, come è il caso nella LSCPT vigente (art. 15 cpv. 3). Spetta al Consiglio federale definire questi dati secondari facendo uso della competenza accordatagli dall'articolo 31. Evidentemente ciò implica la conservazione dei dati riguardanti le comunicazioni di tutte le persone nei confronti delle quali non è stata aperta un'istruzione né lo sarà per tutta la durata di conservazione dei dati, fermo restando che queste persone rappresentano l'enorme maggioranza della popolazione. Questa normativa è tuttavia necessaria affinché i fornitori di servizi di telecomunicazione possano adempiere il loro obbligo di cui al capoverso 1 lettera b nel quadro di una sorveglianza retroattiva, sempre che i dati che sono oggetto di questa disposizione siano assolutamente indispensabili per la lotta contro la criminalità. Questi

49 Thomas Hansjakob, op. cit. (nota 11), n. 5 ad art. 15 LSCPT.
50 RS **101**

dati, a differenza di quelli a cui fa riferimento il capoverso 1 lettera a (cosiddetti dati di contenuto), non forniscono informazioni sul contenuto della comunicazione. Occorre inoltre precisare che questi dati non possono essere ottenuti che nel rispetto degli articoli 269 e seguenti CPP, vale a dire in particolare con l'approvazione dell'autorità competente per approvare le sorveglianze ordinate (tribunale dei provvedimenti coercitivi) nel quadro di un procedimento penale e non a titolo preventivo. Ciò dà agli interessati una forte garanzia legale che li protegge da eventuali abusi. L'interessato potrà inoltre presentare ricorso contro la sorveglianza (art. 279 CPP). Facciamo notare che i fornitori di servizi di telecomunicazione conservano peraltro già oggi tutti questi dati o una parte di essi per almeno un anno, in particolare per ragioni commerciali e per motivi connessi con la fatturazione.

Il *capoverso 5* indica la durata di conservazione dei dati secondari di telecomunicazione che passa da sei a dodici mesi dalla data della comunicazione. Questo prolungamento è richiesto dal numero 2 della mozione Schweiger 06.3170 (Lotta alla cibercriminalità. Protezione dei fanciulli) e dalla mozione Barthassat 10.4133 (Aumentare la durata di conservazione dei registri di assegnazione degli indirizzi Internet Protocol). I motivi dell'aumento da sei a dodici mesi della durata di conservazione di tali dati – di cui fanno segnatamente parte i dati sull'attribuzione dei numeri IP, oggetto della mozione Barthassat 10.4133 – sono legati all'efficacia del perseguimento penale, segnatamente nel settore della lotta contro la pedopornografia, il crimine organizzato e il terrorismo. In effetti, le esperienze delle autorità di perseguimento penale mostrano che la durata di conservazione dei dati di sei mesi è troppo breve, poiché tale termine è spesso già completamente scaduto o lo è in gran parte quando lo stato del procedimento consente all'autorità di ordinare una sorveglianza. In conseguenza di ciò a volte può essere impossibile dare seguito a una domanda di assistenza giudiziaria, o identificare un imputato o peggio ancora una vittima, per esempio un minore vittima di atti pedofili. In considerazione degli interessi pubblici in gioco, l'aumento da sei a dodici mesi della durata di conservazione dei dati è compatibile con i diritti fondamentali delle persone i cui dati vengono così conservati. Il nostro Collegio ha già sostenuto questa posizione nel suo rapporto del 9 giugno 2006 sul postulato del 21 febbraio 2005 della Commissione della politica di sicurezza del Consiglio degli Stati 05.3006 (Lotta più efficace contro il terrorismo e il crimine organizzato)[51]. Questa durata va in particolare posta in relazione con la direttiva dell'Unione europea 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006. Questa direttiva autorizza la conservazione dei dati che corrispondono ai dati considerati secondari in Svizzera per un minimo di sei mesi fino a un massimo, in linea di principio, di due anni dalla data della comunicazione[52]. Nella procedura di consultazione l'aumento della durata di conservazione ha riscosso un ampio consenso. Critiche sono però state espresse dagli ambienti dei fornitori di servizi di telecomunicazione, che hanno rilevato i costi supplementari a loro carico. Secondo il nostro Consiglio, il proposto aumento della durata di conservazione non genererà costi supplementari sproporzionati per le persone che dovranno adempiere a questo obbligo di conservazione. Inoltre, ricordiamo che i fornitori di servizi di telecomunicazione conservano già oggi tutti i dati o una parte di essi per almeno un anno. L'allungamento da sei a dodici mesi del periodo durante il quale i dati secondari possono essere chiesti con effetto retroattivo

51 www.admin.ch/ch/i/ff/2006/5223.pdf
52 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:IT:PDF

(art. 273 cpv. 3 CPP e art. 70*d* cpv. 3 PPM) fa da corollario all'allungamento della durata di conservazione di questi dati; è giustificato dalle medesime considerazioni ed è nell'interesse di una maggiore efficacia.

Il *capoverso 6* dà al Consiglio federale la possibilità di dispensare alcuni fornitori di servizi di telecomunicazione da obblighi che richiedono determinati preparativi da parte loro (per opposizione al semplice obbligo di tollerare una sorveglianza o di fornire i dati disponibili), in funzione di specifiche caratteristiche. Queste caratteristiche permettono per esempio di ritenere che tali persone non possono *a priori* possedere dati interessanti per una sorveglianza del traffico delle telecomunicazioni. Tale può essere il caso delle persone che offrono servizi di telecomunicazione nel settore dell'educazione o li offrono a un numero molto esiguo di clienti. Nei fatti questa possibilità di accordare dispense si avvicina a quanto previsto nell'ordinamento vigente secondo il quale entrano nel campo d'applicazione personale della legge e sono pertanto gravati da obblighi in virtù della medesima soltanto i fornitori di servizi di telecomunicazione assoggettati alla concessione o all'obbligo di notificazione (art. 1 cpv. 2 LSCPT vigente in combinato disposto con art. 4 cpv. 2 LTC e con art. 3 OST). Il *capoverso 6* impone a queste persone l'obbligo di fornire i dati secondari di cui dispongono senza tuttavia costringerle a conservare questi dati, diversamente da quanto prevede in linea di massima la regola (cfr. cpv. 5). Queste persone soggiacciono tuttavia all'obbligo minimo di tollerare una sorveglianza nonché a obblighi accessori necessari per permetterne l'esecuzione (cfr. cpv. 2). È tuttavia opportuno tenere presente che questi obblighi non permettono di colmare interamente la lacuna creata dal *capoverso 6*. Il regime proposto può in effetti portare alla perdita di dati secondari che normalmente potrebbero essere ottenuti nel quadro di una sorveglianza retroattiva e alla perdita di dati normalmente ottenuti nel quadro di una sorveglianza in tempo reale, dato che i tempi necessari per avviare una sorveglianza aumentano, poiché il Servizio o la persona da esso incaricata necessita di tempo a tal fine.

Occorre menzionare a questo proposito che il presente disegno propone – malgrado le richieste della mozione Glanzmann-Hunkeler 07.3627 (Obbligo di registrazione delle carte prepagate Wi-Fi) e il fatto che si tollera così una lacuna nella sorveglianza – di rinunciare a imporre al fornitore di servizi di telecomunicazione, che fornisce una rete lasciata a disposizione dei terzi dal suo utente, un obbligo di identificare tali utenti (e non soltanto i loro computer). Per il rimanente si veda il commento dell'articolo 29.

Art. 27 Obblighi dei fornitori di servizi di comunicazione derivati

Occorre innanzitutto precisare che l'*articolo 27* non deve suscitare aspettative eccessive, visto che molti fornitori importanti dei servizi Internet a cui la disposizione fa riferimento hanno sede all'estero dove pure si trova la loro infrastruttura. Per il rimanente si veda il commento dell'articolo 2 lettera c.

Il *capoverso 1* impone ai fornitori l'obbligo minimo di tollerare una sorveglianza nonché obblighi accessori necessari per permetterne l'esecuzione. La sorveglianza concerne dati che il sorvegliato invia mediante un siffatto fornitore (p. es. nel caso di servizi e-mail) o registra presso il fornitore medesimo (p. es. nel caso di servizi di cloud storage). Il disegno prevede che sia il Servizio o una persona che agisce su suo mandato, in particolare la polizia, a eseguire la sorveglianza. Ciò non significa che il Servizio possa trasferire compiti amministrativi a privati conformemente all'arti-

colo 178 capoverso 3 Cost. Il Servizio rimane in effetti responsabile dell'esecuzione del compito.

Il *capoverso 2* impone a queste persone l'obbligo di consegnare i dati secondari di cui dispongono (almeno quelli disponibili nel momento in cui viene presa la decisione di sorveglianza) senza tuttavia costringerle a conservarli, a differenza di quanto vale in linea di massima per i fornitori di servizi di telecomunicazione (art. 26 cpv. 5). Rispetto alla normativa ordinaria applicabile ai fornitori di servizi di telecomunicazione, con questo regime si possono perdere dati ottenibili nel quadro di una sorveglianza retroattiva e dati ottenibili nel quadro di una sorveglianza in tempo reale, visto che i tempi di cui il Servizio o la persona che agisce su mandato di quest'ultimo hanno bisogno per avviare la sorveglianza sono più lunghi.

Il deposito di dati secondari corrisponde in linea di massima a una sorveglianza retroattiva e costituisce un caso particolare di sequestro (art. 263 segg. CPP); in effetti, a differenza di una sorveglianza in tempo reale, in questo caso vengono sequestrati presso il fornitore dati di comunicazione già esistenti che riguardano un sorvegliato. Tale deposito costituisce un caso speciale, poiché questi dati fanno parte del contenuto della comunicazione. Per attribuire correttamente, sotto il profilo materiale e giuridico, l'informazione intercettata (in tempo reale), è necessario disporre di più ampie informazioni come i dati secondari (quante volte la persona ha consultato un dato sito Internet, in quali momenti ecc.). Quanto ha detto una persona è importante ma altrettanto lo è sapere quando lo ha detto e a chi. Per loro natura queste informazioni si trovano in possesso dei fornitori di servizi di telecomunicazione. Per questa ragione i fornitori – a seconda del tipo (cfr. art. 2) – possono essere obbligati a conservare i dati secondari o a fornirli nella misura in cui ne dispongono. Ulteriori informazioni vanno fornite, all'occorrenza, se necessarie per il perseguimento penale.

L'obbligo di deposito non è una novità bensì figura già tra le regole della procedura penale classica (art. 263 segg. CP). In considerazione della stretta connessione tra questi dati e il contenuto di una comunicazione, e visto che i dati sono acquisiti dai fornitori di cui all'articolo 2 e che questi ultimi sono in parte perfino tenuti a conservare i dati secondari, è materialmente corretto disciplinare nella LSCPT questo particolare tipo di sequestro dotandolo di una base nell'ambito della legislazione speciale (p. es. art. 21, 22, 27 cpv. 2, 28 cpv. 2).

Le spiegazioni precedenti valgono in generale per il deposito dei dati secondari (cfr. art. 8 lett. b, art. 19 cpv. 1 lett. b e art. 26 cpv. 1 lett. b); valgono, per esempio, anche per le informazioni necessarie a identificare gli autori di reati su Internet, che potrebbero essere ottenute presso un fornitore di servizi «cloud» (cfr. art. 22). Dal punto di vista giuridico, il fatto di disciplinare questi obblighi di deposito speciali nella LSCPT presenta inoltre il vantaggio di aumentare le esigenze da soddisfare per ottenere le informazioni desiderate. Un ordine di sequestro (vale a dire un ordine di sorveglianza) deve imperativamente essere approvato dal giudice dei provvedimenti coercitivi (art. 269 in combinato disposto con art. 272 CPP), la qual cosa consolida la protezione giuridica dell'imputato. Nel caso del sequestro classico ai sensi dell'articolo 263 CPP, ciò non è necessario e il giudice (dei provvedimenti coercitivi) interviene soltanto nell'ambito dell'apposizione dei sigilli (o nell'ambito di una domanda di dissigillamento; cfr. art. 248 CPP)[53].

[53] Cfr. anche Marc Jean-Richard-dit-Bressel in: Niggli/Heer/Wiprächtiger (ed.), Basler Kommentar, Schweizerische Strafprozessordnung, Basilea 2011, n. 20 ad art. 269 CPP.

Il Consiglio federale può arrivare alla conclusione che la normativa secondo i capoversi 1 e 2 non è sufficiente per consentire una sorveglianza adeguata. Per questo motivo il *capoverso 3* gli permette di conferire a queste persone obblighi supplementari rispetto a quelli previsti nella disposizione citata, sul modello di quelle che devono in linea di massima rispettare i fornitori di servizi di telecomunicazione. Il Consiglio federale potrà così prescrivere a queste persone obblighi che richiedono da parte loro preparativi attivi, in opposizione ai semplici obblighi di cui ai capoversi 1 e 2. In questo contesto molto tecnico e in costante evoluzione, non è possibile formulare una regola più precisa. Questa norma contiene inoltre criteri restrittivi che possono essere concretizzati. È dunque ammissibile. Essa si giustifica in particolare visto che riguarda un settore tecnico in rapida evoluzione, segnatamente per quanto concerne gli attori coinvolti e i servizi proposti. Ciò rende necessario adeguare rapidamente la legislazione in funzione dei nuovi bisogni in materia di sorveglianza. La nozione di necessità contenuta in questa norma fa riferimento a situazioni ripetutesi o che si presenteranno ripetutamente nel futuro e nelle quali gli obblighi di cui ai capoversi 1 e 2 non consentono di ottenere i dati voluti (cfr. le spiegazioni contenute nel commento dei capoversi 1 e 2) e per le quali è quindi ragionevole sottomettere i fornitori a obblighi di sorveglianza più estesi del semplice obbligo di tollerare la sorveglianza o di fornire i dati disponibili. La necessità del carattere ragionevole degli obblighi supplementari a cui vanno sottoposti questi fornitori si esprime anche attraverso altri criteri menzionati nel *capoverso 3,* vale a dire la grande importanza economica dei servizi forniti e il numero importante di utenti di questi servizi. Concretizzare questi criteri e determinare se sono soddisfatti nel caso concreto, spetta al Consiglio federale. Fondandosi su questa norma di delega, il Consiglio federale provvedere a mantenere le possibilità di sorveglianza che già sussistono. Provvederà in particolare a rendere gli obblighi supplementari previsti da tale norma applicabili ai servizi e-mail forniti dalle grandi imprese, fermo restando che l'attuale OSCPT già lo prevede per i fornitori di servizi di telecomunicazione che forniscono tali servizi. Senza questi obblighi supplementari, le possibilità di sorveglianza ipotizzabili sotto l'egida della nuova LSCPT saranno più limitate di quelle previste dalla LSCPT attuale, la qual cosa non è conforme allo scopo principale della revisione totale della legge.

Nella misura in cui il Consiglio federale fa uso della competenza attribuitagli dal *capoverso 3,* le disposizioni del presente disegno concernenti le sorveglianze che devono eseguire i fornitori di servizi di telecomunicazione sono applicabili per analogia, poiché il Consiglio federale sottopone così le persone di cui all'articolo 2 lettera c a tutti gli obblighi dei fornitori di servizi di telecomunicazione o a parte di tali obblighi. In questo caso ai fornitori di servizi di comunicazione derivati sono applicabili le disposizioni che si riferiscono espressamente soltanto ai fornitori di servizi di telecomunicazione (p. es. art. 4, 17 lett. a–d, 24 seg. e 32).

Art. 28 Obblighi degli esercenti di reti di telecomunicazione interne

L'*articolo 28 capoverso 1* impone alle persone in oggetto l'obbligo minimo ma sufficiente di tollerare una sorveglianza e gli obblighi accessori necessari per permetterne l'esecuzione. Questo obbligo minimo corrisponde agli obblighi previsti nella LSCPT attuale per gli esercenti di reti di telecomunicazione interne e di centrali domestiche. Ispirandosi in parte alla normativa della vigente LSCPT sulla sorveglianza di una rete di telecomunicazione interna o di una centrale domestica, il disegno prevede che la sorveglianza sia eseguita dal Servizio o da una persona

che agisce su suo mandato, in particolare la polizia. Ciò non significa che il Servizio può trasferire compiti amministrativi a privati conformemente all'articolo 178 capoverso 3 Cost. Il Servizio rimane in effetti responsabile dell'esecuzione del compito in questione.

Il *capoverso 2* impone inoltre alle persone in oggetto l'obbligo di consegnare i dati secondari di cui dispongono (almeno quelli disponibili nel momento in cui è presa la decisione di sorveglianza) senza tuttavia obbligarli a conservare questi dati. Rispetto alla normativa ordinaria applicabile ai fornitori di servizi di telecomunicazione, con questo regime si possono perdere dati secondari ottenibili nel quadro di una sorveglianza retroattiva e dati ottenibili nel quadro di una sorveglianza in tempo reale, visto che i tempi di cui il Servizio o la persona che agisce su mandato di quest'ultimo hanno bisogno per avviare la sorveglianza sono più lunghi. È tuttavia opportuno rinunciare a imporre obblighi supplementari che richiedono preparativi attivi da parte degli interessati che dovrebbero fornire sforzi sproporzionati, anche se è plausibile che la mozione Glanzmann-Hunkeler 07.3627 (Obbligo di registrazione delle carte prepagate Wi-Fi), poco chiara su questo punto, persegua questo obiettivo.

Art. 29 Obblighi delle persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazione

L'*articolo 29 capoverso 1* impone alle persone in oggetto l'obbligo minimo ma sufficiente di tollerare una sorveglianza e obblighi accessori necessari per permetterne l'esecuzione. Sulla falsariga della normativa vigente, il disegno prevede che la sorveglianza sia eseguita dal Servizio o da una persona che agisce su suo mandato, in particolare la polizia. Ciò non significa che il Servizio può trasferire compiti amministrativi a privati conformemente all'articolo 178 capoverso 3 Cost. Il Servizio rimane in effetti responsabile dell'esecuzione del compito in questione.

Il *capoverso 2* impone inoltre alle persone in oggetto l'obbligo di consegnare i dati secondari di cui dispongono (almeno quelli disponibili nel momento in cui è presa la decisione di sorveglianza) senza tuttavia costringerli a conservare questi dati. Rispetto alla normativa ordinaria applicabile ai fornitori di servizi di telecomunicazione, con questo regime si possono perdere dati ottenibili nel quadro di una sorveglianza retroattiva e dati ottenibili nel quadro di una sorveglianza in tempo reale, visto che i tempi di cui il Servizio o la persona che agisce su mandato di quest'ultimo hanno bisogno per avviare la sorveglianza sono più lunghi.

È tuttavia opportuno rinunciare a imporre obblighi supplementari che richiedono preparativi attivi da parte degli interessati che dovrebbero fornire sforzi sproporzionati. Ciò vale anche per l'obbligo di identificazione che pare chiedere la mozione Glanzmann-Hunkeler 07.3627 (Obbligo di registrazione delle carte prepagate Wi-Fi). Un tale obbligo di identificazione delle persone a cui fa riferimento questo articolo porrebbe inoltre problemi pratici. In effetti le persone, che si tratti di individui o di alberghi, ristoranti, caffè, ospedali, scuole, attività commerciali, Comuni eccetera, che concedono di accedere liberamente alla loro rete dovrebbero chiedere un documento d'identità e annotare in un registro chi ha avuto accesso alla rete e in quale momento. Una tale registrazione richiede parecchio lavoro, non è sempre affidabile e non è necessariamente compatibile con l'attività del terzo (p. es. rapido consumo di un caffè in un locale pubblico che permette l'accesso alla propria rete Wi-Fi).

La mozione menzionata in precedenza sembra chiedere che sia sancito un obbligo di identificazione degli utenti (e non soltanto dei loro computer) delle reti lasciate a disposizione dei terzi.

Se siffatto obbligo fosse effettivamente previsto dalla legislazione, dovrebbe essere a carico del fornitore di servizi di telecomunicazione che fornisce la rete alla persona che la lascia a disposizione dei terzi e non a carico di quest'ultima. Sembra che i fornitori di servizi di telecomunicazione sotto il profilo tecnico siano in grado di identificare gli utenti di queste reti e i loro computer, come previsto nell'articolo 22 AP-LSCPT che aveva suscitato reazioni di segno diverso durante la consultazione. Secondo i fautori di questa modalità di identificazione, per un albergo o un negozio dovrebbe essere facile mettere l'accesso a Internet a disposizione di un cliente tramite un codice, un SMS o il suo indirizzo e-mail personale. La maggioranza dei grandi fornitori di servizi di telecomunicazione offrono già questa possibilità in Svizzera. Concretamente, ciò può per esempio essere fatto previa identificazione dell'utente (p. es. mediante il telefono cellulare o la sua carta di credito), prima di poter ottenere accesso a Internet dal fornitore di servizi di telecomunicazione che mette a disposizione la rete della persona che la lascia a disposizione dei terzi. I fautori di questa identificazione fanno inoltre valere che l'accesso anonimo a Internet non è possibile in alcuni Paesi vicini della Svizzera e in Svezia. Siffatta normativa si giustifica di certo nell'ottica della lotta contro la criminalità. Nonostante quanto precede, va tenuto presente che questa regolamentazione, oltre a causare lavoro supplementare ai fornitori di servizi di telecomunicazione, avrebbe un impatto molto forte: decreterebbe di fatto la fine della libertà nell'uso che offrono attualmente le reti Wi-Fi, anche se queste potranno continuare ad essere utilizzate. L'obbligo di identificazione non costituirebbe inoltre una panacea perché vi sono possibilità tecniche di eluderlo. Il presente disegno propone quindi di rinunciarvi malgrado il contenuto della mozione Glanzmann-Hunkeler 07.3627 (Obbligo di registrazione delle carte prepagate Wi-Fi) e il fatto che in questo modo si tollera una lacuna nella sorveglianza.

Art. 30 Obblighi dei rivenditori professionali di carte e di mezzi analoghi

L'*articolo 30* si prefigge di colmare una lacuna della legislazione in vigore. La lacuna riguarda la registrazione, da parte delle persone oggetto della presente disposizione, dei dati relativi all'identità dei clienti a cui forniscono i mezzi per accedere a una rete pubblica di telecomunicazione senza concludere un abbonamento. In effetti, la legislazione vigente obbliga soltanto i fornitori di servizi di telecomunicazione a registrare i dati. Di conseguenza, i rivenditori oggetto della presente disposizione (p. es. Interdiscount, Media Markt e Mobilezone) che ottengono questi mezzi dai fornitori di servizi di telecomunicazione (p. es. Swisscom, Orange e Sunrise) – in particolare le carte SIM prepagate e le carte prepagate Wi-Fi per l'accesso a Internet – non ancora intestati, non sono tenuti a registrare i dati del cliente, che resta quindi anonimo. È questa una lacuna ingiustificata nella sorveglianza. Le persone in oggetto sono ora tenute a comunicare i dati al fornitore di servizi di telecomunicazione alla cui rete il mezzo venduto dà accesso (p. es. Swisscom, Orange e Sunrise), affinché questi possa a sua volta registrarli e metterli così a disposizione del sistema di commutazione delle domande d'informazione sui servizi di telecomunicazione (detto CCIS) gestito dal Servizio in collaborazione con i fornitori di servizi di telecomunicazione. Vedi anche il commento dell'articolo 21 capoverso 2. La violazione degli obblighi previsti all'*articolo 30* è sanzionata dall'articolo 39 capoverso 1 lettera c.

Giova precisare che le semplici carte telefoniche (p. es. «taxcard» dotate di un credito e vendute nei chioschi) non sottostanno all'obbligo di cui all'*articolo 30.*

2.7 Sezione 7: Garanzia della disponibilità a informare e sorvegliare dei fornitori di servizi di telecomunicazione

Come l'articolo 18, gli articoli 31–34 intendono innanzitutto garantire una corretta esecuzione delle sorveglianze del traffico delle telecomunicazioni. Si tratta segnatamente della possibilità di esaminare la capacità dei fornitori di servizi di telecomunicazione di fornire le informazioni e di sorvegliare i servizi di telecomunicazione designati, e questo conformemente al diritto applicabile. Si tratta dunque di una questione di rispetto («*compliance*») dei relativi obblighi. In questo contesto non si può sostenere che si tratta di un'attività di «certificazione», come era il caso degli articoli 18 e 24 AP-LSCPT, visto che la procedura prevista non si prefigge di verificare il rispetto di determinati standard per prodotti o servizi.

Art. 31 Disposizioni esecutive sui tipi di informazioni e di sorveglianza

L'*articolo 31* è una norma di delega al Consiglio federale (cpv. 1 e 2) e al DFGP (cpv. 3). Queste due autorità devono poter stabilire i dettagli della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. A questo riguardo occorre stabilire quali dettagli debbano essere disciplinati.

La separazione tra gli aspetti relativi al diritto amministrativo (LSCPT) e alla procedura penale (CPP) soddisfa l'esigenza espressa nel numero 2 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander 10.3877 (Revisione della LSCPT). Questo esame separato è ragionevole perché la LSCPT e il CPP hanno destinatari diversi e si prefiggono di disciplinare oggetti diversi. In parole povere, se il CPP pone l'imputato al centro dell'attenzione, la LSCPT concerne il fornitore nei settori della corrispondenza postale e del traffico delle telecomunicazioni che è tenuto a collaborare alla sorveglianza dell'imputato secondo la procedura penale. La LSCPT in qualche modo segue il CPP.

Un esame superficiale dell'*articolo 31* può dare l'impressione che possano essere ordinati tipi di sorveglianza non autorizzati, che mancano di una base legale sufficientemente precisa (cfr. art. 8 par. 2 della Convenzione del 4 novembre 1950[54] per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali [CEDU] e art. 13 cpv. 1 e 36 cpv. 1 Cost.). Tale non è tuttavia il caso, poiché gli articoli 269–279 CPP (in particolare gli art. 269–269ter nella loro versione modificata) regolano adeguatamente l'ammissibilità dei diversi tipi di sorveglianza sotto il profilo della procedura penale. La LSCPT non deve fornire indicazioni su questi aspetti di procedura penale ma deve garantire, per quanto possibile, l'attuazione tecnica delle sorveglianze ammissibili sotto il profilo della procedura penale (fatta salva la ricerca in caso d'emergenza e la ricerca di condannati). I tipi di sorveglianza devono essere dis-

54 RS **0.101**

ciplinati proprio in senso tecnico nella LSCPT o nella OSCPT soltanto in relazione con questo aspetto tecnico e di diritto amministrativo.

Ogni sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni può, secondo le circostanze della fattispecie, essere ammissibile per i sorvegliati. In questo contesto la garanzia giuridica dei diritti fondamentali non è data dalle disposizioni dettagliate di un'ordinanza ma dalla procedura penale. I risultati di una sorveglianza (in tempo reale o retroattiva; contenuti di comunicazioni o dati secondari) non possono in effetti essere utilizzati senza approvazione giudiziaria; in casi del genere la sorveglianza deve essere interrotta e i dati raccolti devono essere distrutti (art. 277 CPP).

Di conseguenza, la base legale che permette di utilizzare GovWare o IMSI-catcher e tipi di sorveglianza relativi agli elementi d'indirizzo e alla ricerca per zona di copertura d'antenna deve figurare nel CPP, quella per la collaborazione dei fornitori di servizi di telecomunicazione nella LSCPT[55]:

– nell'ottica della LSCPT è irrilevante che si impieghi GovWare oppure IMSI-catcher, dato che essi non richiedono la collaborazione dei fornitori di servizi di telecomunicazione. Sotto il profilo della procedura penale, occorre tuttavia creare una nuova base legale, poiché la loro utilizzazione esula dal quadro dei tipi di sorveglianza finora disciplinati (cfr. il commento degli art. 269bis e 269ter CPP);

– nell'ottica della procedura penale, la ricerca per zona di copertura d'antenna[56] secondo la dottrina e la giurisprudenza[57] è ammissibile a determinate condizioni (ottenimento di dati secondari ai sensi dell'art. 273 CPP, purché siano adempiute le condizioni poste dall'art. 269 cpv. 1 lett. b e c CPP). Non occorre una base legale particolare. Secondo il Tribunale federale, la ricerca per zona di copertura d'antenna non lede in modo grave i diritti fondamentali a condizione che questo mezzo di identificazione degli utenti sia impiegato come ultima ratio, che vi siano sospetti gravi, che vada chiarito un crimine, che l'autore possa essere sufficientemente individuabile e che non si ottengano i contenuti delle comunicazioni[58]. Va tenuto presente che la ricerca per zona di copertura d'antenna deve essere autorizzata dal giudice dei provvedimenti coercitivi (art. 273 cpv. 2 CPP) e che il pubblico ministero deve presentare al giudice l'ordine di sorveglianza necessario a tal fine con la pertinente motivazione (compresi gli atti determinanti del fascicolo) (art. 274 cpv. 1 CPP). Sotto il profilo della LSCPT, la ricerca per zona di copertura d'antenna non ha alcuna particolarità che richieda l'esecuzione di modifiche di tale legge, poiché questo tipo di sorveglianza è soltanto una modalità

55 Cfr. anche DTF **130** II 249, 253 segg. e DTAF 2009/46, consid. 3.1.3, 3.2, 3.3.

56 La ricerca per zona di copertura d'antenna permette in un primo momento di ottenere retroattivamente i dati secondari senza riferimento a persone relativi all'insieme delle comunicazioni via telefonia mobile avvenute durante un certo periodo di tempo attraverso una determinata cellula dell'antenna. In un secondo tempo, grazie a diversi parametri predefiniti si intersecano le connessioni di due o più antenne; si veda al riguardo l'esempio di Thomas Hansjakob, op. cit. (nota 11), n. 18 ad art. 16 OSCPT e i fatti presentanti nella DTF **137** IV 340, 341 seg. Questa misura di sorveglianza serve a individuare e identificare l'autore in caso di gravi sospetti oggettivamente concretizzati che è stato commesso un crimine.

57 DTF **130** II 249 e **137** IV 340, 346 segg. (con rinvii alla dottrina).

58 DTF **137** IV 340, 349 segg.

dell'acquisizione dei dati secondari ed è già disciplinato nella vigente OSCPT (art. 16 lett. e OSCPT);

– le misure di sorveglianza relative a elementi di indirizzo stranieri non costituiscono novità per la procedura penale, poiché consistono nella sorveglianza di un numero straniero noto, per sapere se riceve chiamate da un utente in Svizzera. Esattamente come per la sorveglianza di un collegamento nazionale, questo genere di sorveglianza riguarda un determinato numero telefonico. Non si tratta di sorvegliare un collegamento terzo, la qual cosa è ammissibile soltanto alle condizioni prescritte dall'articolo 270 lett. b CPP[59]. La LSCPT disciplina unicamente la fattibilità tecnica e organizzativa e la questione di chi debba sopportare le spese della sorveglianza[60];

– per scrupolo di completezza occorre rilevare che le sorveglianze di Internet non necessitano di alcuna particolare base legale, poiché il loro disciplinamento negli articoli 269 CPP e 1 LSCPT è incontestato[61].

Riassumiamo facendo presente che la base legale che indica *se* una sorveglianza è ammissibile va ricercata negli articoli 269 e seguenti CPP (aspetto della procedura penale). Invece, la LSCPT indica *in quali modi* gli attori del settore della corrispondenza postale e del traffico delle telecomunicazioni possono essere obbligati a collaborare nel quadro di una tale sorveglianza (aspetto di diritto amministrativo). Al riguardo si veda anche il commento dell'articolo 42.

I *capoversi 1 e 2* sono norme di delega che attribuiscono al Consiglio federale la competenza di definire materie che già regola attualmente nell'OSCPT. Questa normativa consente per esempio di tenere conto del fatto che i dati secondari, che devono poter essere chiesti a un fornitore di servizi di telecomunicazione nell'ambito di una sorveglianza retroattiva del traffico delle comunicazioni telefoniche, comprese quelle avvenute via Internet, non devono per forza essere i medesimi richiesti nell'ambito di una sorveglianza retroattiva di Internet (riguardante dati diversi da quelli delle comunicazioni telefoniche). Una sorveglianza retroattiva di Internet non deve per esempio indicare necessariamente le pagine Internet consultate, poiché tale tipo di sorveglianza, benché concerna i dati secondari, equivarrebbe in una certa misura a una sorveglianza del contenuto delle comunicazioni. Le cerchie interessate saranno consultate sulle proposte che il nostro Consiglio formulerà in virtù *dei capoversi 1 e 2*. È opportuno indicare che è comunque possibile eseguire sorveglianze di tipo nuovo, che ancora non figurano nelle disposizioni esecutive ma sono coperte dal CPP. In un caso del genere, il fornitore di servizi di telecomunicazione non è obbligato a eseguire esso stesso la sorveglianza, come è in linea di massima il caso per i fornitori di servizi di comunicazione derivati (art. 27) o per i gerenti di reti di telecomunicazione interne (art. 28), ma dovrà soltanto permettere e

59 Per quanto concerne la formulazione confusa dell'art. 270 lett. b CPP («terzi» invece di «collegamenti di terzi», cfr. Thomas Hansjakob, op. cit. (nota 11), n. 10 ad osservazioni preliminari.

60 Cfr. DTAF 2009/46, consid. 3.2, 7.4 e 8.3. Il TAF non ha constatato violazioni dell'art. 13 cpv. 1 Cost. In una certa misura ciò è sorprendente poiché nel consid. 3.2 il TAF basa la propria decisione di non entrare nel merito sulla censura del fornitore di servizi di telecomunicazione secondo cui i diritti del sorvegliato sarebbero violati in assenza di una base legale.

61 Cfr. semplicemente Marc Jean-Richard-dit-Bressel in: Niggli/Heer/Wiprächtiger (ed.), Basler Kommentar, Schweizerische Strafprozessordnung, Basilea 2011, n. 15 seg. ad art. 269 CPP.

tollerare l'esecuzione di siffatta sorveglianza da parte del Servizio o di un terzo che agisce su suo mandato (cfr. art. 26 cpv. 2 e 32 cpv. 2).

Il *capoverso 3* prevede che i dettagli tecnici e amministrativi necessari per permettere la corretta esecuzione con costi minimi delle sorveglianze normalmente ammissibili cessano di essere disciplinati, come finora, nelle direttive del Servizio e saranno d'ora innanzi regolati da ordinanze del DFGP. Per quanto concerne le ordinanze molto tecniche e voluminose adottate a livello dipartimentale si prevede di pubblicare nella Raccolta ufficiale delle leggi federali soltanto un rinvio (art. 5 della legge federale del 18 giugno 2004[62] sulle raccolte del diritto federale e sul Foglio federale). In questo caso il testo completo sarà disponibile su una pagina Internet del DFGP.

Il disciplinamento dei dettagli tecnici e amministrativi in un'ordinanza implica che l'esecuzione delle sorveglianze in questione è standardizzata. Al riguardo vi sono standard internazionali di cui va tenuto conto. Giova rilevare che non tutti i tipi di sorveglianza ammissibili secondo il capoverso 1, coperti cioè dalla legislazione, sono necessariamente standardizzati. Per i casi speciali vi sono tipi speciali di sorveglianza che sono ammissibili ma non (ancora) standardizzati. Tale cambiamento di competenza è conforme con lo spirito del numero 1 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander 10.3877 (Revisione della LSCPT) secondo cui i compiti normativi e regolamentari del Servizio devono essere sostanzialmente distinti dai suoi compiti d'esecuzione delle sorveglianze. Il cambiamento renderà così più legittime le disposizioni in questione, che potranno essere elaborate nell'ambito dell'organo consultivo secondo l'articolo 5.

Art. 32 Disponibilità a informare e sorvegliare

L'*articolo 32* riguarda beninteso i tipi di sorveglianza dall'esecuzione, dai quali il fornitore di servizi di telecomunicazione non è dispensato in virtù dell'articolo 26 capoverso 6.

Il *capoverso 1* prevede che le informazioni siano fornite e le sorveglianze eseguite conformemente al diritto applicabile, in particolare nel rispetto delle modalità stabilite nella LSCPT, nella OSCPT e nelle ordinanze che regolano i dettagli tecnici e amministrativi. Per poter adempiere il loro obbligo di fornire le informazioni e i dati in questione, i fornitori di servizi di telecomunicazione devono essere in possesso dei citati dati e informazioni, ragione per cui sono tenuti a conservare le informazioni e i dati secondari.

L'obbligo di cui al *capoverso 2* dei fornitori di servizi di telecomunicazione implica un comportamento attivo da parte loro, conformemente alle direttive impartite dal Servizio (art. 16 lett. d). Devono di conseguenza fornire segnatamente le informazioni necessarie all'esecuzione della sorveglianza e se necessario garantire l'accesso ai loro impianti.

Il *capoverso 3* prevede che, a condizione di assumerne le spese, i fornitori di servizi di telecomunicazione possono affidare l'esecuzione di tutti i loro obblighi di informazione e sorveglianza a terzi, principalmente imprese specializzate nell'offerta di servizi di sorveglianza del traffico delle telecomunicazioni su ordine delle autorità

62 RS **170.512**

(*lawful interception*). Questa normativa consente una grande flessibilità. In particolare la presente regolamentazione non obbliga i fornitori di servizi di telecomunicazione a procurarsi le infrastrutture per adempiere questi obblighi. La normativa permette loro, per esempio, anche di associare i loro mezzi per adempiere insieme a questi obblighi, acquistando o noleggiando le infrastrutture necessarie. Per soddisfare i requisiti del capoverso 1 è quindi sufficiente, secondo il *capoverso 3*, che il fornitore di servizi di telecomunicazione sia in grado di fornire le informazioni e di eseguire le sorveglianze ricorrendo a un terzo o in collaborazione con quest'ultimo. Occorre tuttavia rilevare che, come finora, soltanto i fornitori di servizi di telecomunicazione sono assoggettati agli obblighi di informare e di sorvegliare e non le imprese terze a cui fanno capo. Per il rimanente si veda il commento dell'articolo 33 capoverso 1. Il *secondo periodo del capoverso 3* riguarda il rapporto di diritto privato tra i fornitori di servizi di telecomunicazione e il terzo che sceglie per eseguire i suoi obblighi. Il *terzo periodo del capoverso 3* concerne invece il rapporto di diritto amministrativo tra il Servizio e il terzo; questa regola si prefigge in particolare un buon svolgimento della sorveglianza, anche sotto il profilo della protezione e della qualità dei dati.

Art. 33 Prova della disponibilità a informare e sorvegliare

In questo caso, i fornitori di servizi di telecomunicazione devono dimostrare di essere in grado di fornire le informazioni e di eseguire le sorveglianze conformemente al diritto applicabile, in particolare nel rispetto delle modalità stabilite nella LSCPT, nella OSCPT e nelle ordinanze sui dettagli tecnici e amministrativi. I fornitori di servizi di telecomunicazione sopportano le spese della dimostrazione di cui al *capoverso 1*, e di conseguenza anche le spese risultanti dal ricorso a imprese terze per compiere tale dimostrazione. Un fornitore di servizi di telecomunicazione deve beninteso fornire tale prova soltanto per i tipi di sorveglianza dai quali non è dispensato in virtù dell'articolo 26 capoverso 6. Questo obbligo implica un comportamento attivo dei fornitori di servizi di telecomunicazione che devono in particolare fornire le informazioni necessarie alla dimostrazione nonché, se necessario, garantire l'accesso ai loro impianti. L'articolo 32 capoverso 3 permette al fornitore di servizi di telecomunicazione di adempiere i propri obblighi di informare e sorvegliare ricorrendo a un terzo o collaborando con quest'ultimo affidandogli l'esecuzione di tutti i suoi obblighi o di una parte di essi. In tal caso, il terzo potrà anche essere chiamato a dimostrare al Servizio di essere in grado di adempiere i succitati obblighi di informare e sorvegliare in vece del fornitore di servizi di telecomunicazione o in collaborazione con quest'ultimo; il terzo sosterrà così il fornitore di servizi di telecomunicazione nella dimostrazione che è obbligato a fare in virtù del *capoverso 1*. Se il terzo non è in grado di compiere la dimostrazione, il fallimento va ascritto al fornitore di servizi di telecomunicazione. Per il rimanente si veda il commento dell'articolo 32 capoverso 3.

Il *capoverso 2* permette al Servizio di ricorrere a terzi per verificare se il fornitore di servizi di telecomunicazione ha provato la sua disponibilità a informare e sorvegliare; ciò si giustifica in considerazione del fatto che questo controllo può necessitare un lungo lavoro, impossibile da svolgere con le risorse umane di cui dispone il Servizio. Questa possibilità del Servizio non equivale a trasferire compiti amministrativi a privati ai sensi dell'articolo 178 capoverso 3 Cost. Il Servizio rimane in effetti responsabile dell'esecuzione di tale compito. Se fa uso di questa possibilità, il Servizio secondo il capoverso 6 continua a dover rilasciare ai fornitori di servizi di

telecomunicazione un attestato in cui si certifica che hanno fornito la dimostrazione necessaria. Di conseguenza, esso è tenuto a controllare che il terzo da lui incaricato ha rispettato le modalità stabilite per compiere il controllo.

Fondandosi sul *capoverso 3*, il Servizio e il fornitore di servizi di telecomunicazione possono per esempio effettuare controlli della qualità, segnatamente su «bersagli» di controllo fittizi (cfr. art. 18 e relativo commento).

Secondo il *capoverso 4*, il fornitore di servizi di telecomunicazione controllato è tenuto a versare un emolumento al Servizio in contropartita della prestazione fornita da quest'ultimo. Spetta al Consiglio federale stabilire l'importo dell'emolumento: a tal fine terrà conto della natura della prestazione fornita dal Servizio.

Il *capoverso 5* si approssima all'articolo 16 lettera d, che tuttavia non riguarda una procedura di prova della disponibilità a informare e sorvegliare, anche in seguito a una sorveglianza che non si è svolta in modo ottimale, ma concerne la procedura di esecuzione di una sorveglianza. I fornitori di servizi di telecomunicazione sopportano le spese delle misure che devono adottare per colmare le lacune della loro disponibilità a informare e sorvegliare, poiché queste misure sono necessarie per consentire loro di adempiere i loro obblighi legali. Se non ottemperano alle ingiunzioni del Servizio di prendere le misure tecniche e organizzative per compensare le lacune nella loro disponibilità di informare e sorvegliare, potranno essere perseguiti in virtù dell'articolo 39 capoverso 1 lettera a.

Il contenuto dell'attestato e i dettagli quanto alla sua validità nel tempo saranno stabiliti in un'ordinanza del Consiglio federale conformemente al *capoverso 6.* L'attestato deve in particolare menzionare il suo campo d'applicazione materiale, vale a dire le informazioni e i tipi di sorveglianza che sono stati oggetto della dimostrazione, e il suo campo d'applicazione temporale, ossia fino a quando ha effetto, in particolare in vista di sviluppi tecnici. Questo attestato permette di ritenere che il fornitore di servizi di telecomunicazione è in grado di fornire i tipi di informazioni e di eseguire i tipi di sorveglianza di cui l'attestato fa stato. Esso consente quindi di ritenere che, per quanto concerne queste informazioni e sorveglianze, il fornitore di servizi di telecomunicazione soddisfa l'obbligo di cui al capoverso 1. Questo attestato ha anche conseguenze finanziarie per un fornitore di servizi di telecomunicazione che in un caso concreto non è in grado di eseguire una sorveglianza (cfr. art. 34, in particolare cpv. 2 lett. a).

Art. 34 Assunzione delle spese in caso di insufficiente collaborazione

L'*articolo 34* si applica a due tipi di carenza della disponibilità a sorvegliare. La disposizione riguarda innanzitutto il caso in cui un fornitore di servizi di telecomunicazione non è in grado di eseguire la sorveglianza anche se è disposto a farlo. Riguarda anche il caso in cui il fornitore rifiuta di ottemperare all'ingiunzione di sorveglianza del Servizio.

Il *capoverso 1* si applica se in un caso concreto il fornitore di servizi di telecomunicazione non è in grado, o non vuole, eseguire la sorveglianza secondo il diritto applicabile, vale a dire in particolare nel rispetto delle modalità stabilite nella LSCPT, nell'OSCPT e nelle ordinanze sui dettagli tecnici e amministrativi. Questa disposizione non riguarda beninteso i tipi di sorveglianza dalla cui esecuzione il fornitore di servizi di telecomunicazione non è dispensato in virtù dell'articolo 26 capoverso 6. Al fornitore di servizi di telecomunicazione è imputabile il mancato

adempimento degli obblighi di sorveglianza da parte di un'impresa terza incaricata in tutto o in parte di eseguire tali obblighi. Tale fornitore dovrà in questo caso sopportare anche le conseguenze secondo il *capoverso 1*. Per il rimanente si veda il commento degli articoli 31 e 32.

Il *capoverso 2* disciplina le eccezioni al principio stabilito nel capoverso 1 per l'assunzione delle spese e intende incitare i fornitori di servizi di telecomunicazione a ottenere la certificazione. Evidentemente un fornitore di servizi di telecomunicazione non è tenuto ad assumere le spese soltanto se non è in grado di eseguire la sorveglianza, malgrado abbia la volontà di farlo. Il tenore del *capoverso 2 lettera a* è ovvio. In effetti un fornitore di servizi di telecomunicazione che dispone di un attestato secondo l'articolo 33 capoverso 6 non è tenuto ad assumere le spese in questione, poiché l'attestato permette proprio di ritenere che il fornitore è in grado di eseguire i tipi di sorveglianza certificativi. È pure corretto che nell'ipotesi contemplata al *capoverso 2 lettera b,* il fornitore di servizi di telecomunicazione non deve assumere le conseguenze finanziarie del fallimento della sorveglianza. Si tratta segnatamente del caso in cui il Servizio non ha ancora avuto la possibilità di controllare il fornitore, in particolare per motivi legati a una mancanza di risorse.

2.8 Sezione 8: Ricerca d'emergenza e ricerca di condannati

Art. 35 Ricerca d'emergenza

L'*articolo 35* non trova posto nel CPP poiché la disposizione non si applica a un procedimento penale pendente. Questo articolo non si applica al rapimento o al sequestro di una persona in un luogo sconosciuto, perché in questi casi vi è un procedimento penale e il pubblico ministero potrà immediatamente ordinare le misure di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni necessarie per localizzare l'autore dell'atto. L'*articolo 35* si applica invece, per esempio, alla ricerca di persone in seguito a una catastrofe (inondazione, terremoto ecc.) nella misura in cui le condizioni previste sono adempite.

Secondo il *capoverso 1*, contrariamente da quanto previsto nell'articolo 3 della LSCPT vigente e nell'articolo 27 AP-LSCPT, la sorveglianza della corrispondenza postale o del traffico delle telecomunicazione attuata in caso d'emergenza non è più limitata all'identificazione degli utenti e ai dati relativi al traffico, vale a dire ai dati secondari. La sorveglianza permette ora di ottenere il contenuto degli invii per quanto concerne la corrispondenza postale e il contenuto delle comunicazioni per quanto concerne il traffico delle telecomunicazioni. Il contenuto degli invii e delle comunicazioni può fornire informazioni sul luogo in cui si trova la persona scomparsa e, nell'ambito del traffico delle telecomunicazioni, può consentire di verificare se è veramente la persona scomparsa a utilizzare il collegamento sorvegliato. Gli articoli 19–32 e le disposizioni esecutive dell'OSCPT precisano i tipi di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni ai sensi dell'articolo 269 CPP che possono essere ordinati e i soggetti dei diversi obblighi in materia di esecuzione della sorveglianza.

L'impossibilità di localizzare la persona scomparsa è attualmente una delle condizioni contenute nell'articolo 3 capoverso 2 LSCPT vigente e viene completata nel *capoverso 2* dalla condizione della eccessiva difficoltà. L'aggiunta è giustificata dal

fatto che la condizione dell'impossibilità, considerata in senso letterale, pone esigenze esorbitanti e sproporzionate rispetto al bene giuridico della persona scomparsa che occorre tutelare. Una sorveglianza di questo genere è così possibile, come negli articoli 269 capoverso 1 lettera c CPP e 36 capoverso 1, se le altre misure già adottate non hanno avuto successo oppure se le ricerche senza sorveglianza risulterebbero vane o eccessivamente complicate.

Il *capoverso 3* autorizza l'utilizzazione di speciali dispositivi tecnici di sorveglianza secondo l'articolo 269bis CPP per ritrovare una persona scomparsa. Concretamente ciò permette di utilizzare a tal fine dispositivi come gli IMSI-catcher. Questo efficace mezzo di sorveglianza può in particolare consentire di ritrovare una persona scomparsa anche se le classiche misure di sorveglianza del traffico delle telecomunicazioni non hanno dato esito positivo. L'utilizzazione di dispositivi speciali è tuttavia sussidiaria rispetto al ricorso alle misure classiche di sorveglianza (cfr. per analogia il commento dell'art. 269bis lett. b CPP). Attualmente il ricorso a dispositivi come l'IMSI-catcher non necessita l'intervento di un fornitore di servizi di telecomunicazione né che quest'ultimo abbia un comportamento tipicamente contrario all'articolo 321ter cpv. 1 CP e neppure che il Servizio intervenga a tal fine (e quindi non deve ricevere alcun ordine di sorveglianza). Per il rimanente si veda il commento dell'articolo 269bis CPP.

Se necessario, come prevede l'articolo 3 capoverso 1 LSCPT vigente, il *capoverso 4* permette, conformemente al principio costituzionale della proporzionalità, di sorvegliare la corrispondenza postale e il traffico delle telecomunicazioni non solo della persona scomparsa, ma anche quelli di un terzo non implicato. Ciò è in particolare opportuno se vi sono motivi di ritenere che la persona scomparsa utilizza il collegamento di questo terzo o lo chiama. Questa possibilità limita il diritto alla protezione della sfera privata del terzo, diritto tutelato dalla Costituzione federale e dal diritto internazionale (cfr. *infra* n. 5); di ciò va tenuto conto nell'apprezzamento di ogni fattispecie.

Art. 36 Ricerca di condannati

L'*articolo 36* introduce la possibilità di ricorrere a una sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni per ritrovare una persona condannata a una pena detentiva o nei cui confronti è stata disposta una misura privativa della libertà con una sentenza passata in giudicato. Questa sorveglianza, possibile nell'ambito di un procedimento penale in corso, deve essere ammissibile anche per perseguire il citato obiettivo; in effetti in questo caso secondo il *capoverso 1* vi è una sentenza passata in giudicato e non soltanto dei sospetti seppure gravi (art. 269 cpv. 1 lett. a CPP). Questa possibilità si impone anche perché è già prevista nell'ambito dell'assistenza giudiziaria internazionale[63] dall'articolo 18*a* capoverso 1 EIMP.

Nel *capoverso 1* si rinuncia a stabilire una durata minima della pena detentiva a partire dalla quale sia possibile ordinare una sorveglianza. La decisione dell'autorità competente di ordinare una sorveglianza sarà fondata sul principio della proporzionalità; l'autorità competente dovrà tenere conto in particolare dei seguenti elementi: la durata della pena detentiva da scontare pronunciata, il reato per il quale è stata pronunciata, l'eventuale pericolosità del condannato e il costo della sorveglianza.

63 Thomas Hansjakob, op. cit. (nota 11), n. 8 ad art. 1 LSCPT.

Come l'articolo 35, la presente normativa non va inserita nel CPP poiché non si applica nell'ambito di un procedimento penale pendente ma dopo che questo è terminato. Contrariamente a quanto è in linea di massima il caso per le sorveglianze ordinate nell'ambito delle procedure penali, la condizione dell'articolo 269 capoverso 2 CPP (catalogo di reati) non si applica alle sorveglianze che si prefiggono di ritrovare una persona condannata a una pena o a una misura detentiva (cfr. il rinvio dell'art. 37 cpv. 1). Ciò si giustifica in particolare perché in questo caso vi è una sentenza passata in giudicato e non più dei semplici sospetti, sia pure gravi (art. 269 cpv. 1 lett. a CPP). Come prevedono sostanzialmente gli articoli 269 capoverso 1 lettera c CPP e 35 capoverso 2 lettera a, questa misura di sorveglianza è sussidiaria rispetto alle altre misure che possono essere adottate per ritrovare il ricercato. La sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni secondo l'articolo 36 consente non soltanto di ottenere i dati che permettono di identificare gli utenti e i dati relativi al traffico, ossia i dati secondari, ma anche il contenuto degli invii nel settore della corrispondenza postale e in quello del traffico delle telecomunicazioni. Infatti, il contenuto degli invii e delle comunicazioni può fornire informazioni sul luogo in cui si trova il condannato scomparso e, nell'ambito del traffico delle telecomunicazioni, può permettere di verificare se veramente la persona utilizza il collegamento sorvegliato. Gli articoli 19–32 e le disposizioni esecutive dell'OSCPT precisano i tipi di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni ai sensi dell'articolo 269 CPP che possono essere ordinati e i soggetti dei diversi obblighi in materia di esecuzione della sorveglianza.

Il *capoverso 2* autorizza l'utilizzazione di speciali dispositivi tecnici di sorveglianza secondo l'articolo 269bis CPP per ritrovare un condannato scomparso. Concretamente ciò permette di utilizzare a tal fine dispositivi come gli IMSI-catcher. Questo efficace mezzo di sorveglianza può in particolare consentire di ritrovare una persona ricercata anche se le classiche misure di sorveglianza del traffico delle telecomunicazioni non hanno dato esito positivo. L'utilizzazione di dispositivi speciali è tuttavia sussidiaria rispetto al ricorso alle misure classiche di sorveglianza (cfr. per analogia il commento dell'art. 269bis lett. b CPP). Attualmente il ricorso a dispositivi come l'IMSI-catcher non necessita l'intervento di un fornitore di servizi di telecomunicazione né che quest'ultimo abbia un comportamento tipicamente contrario all'articolo 321ter cpv. 1 CP e non occorre che il Servizio intervenga a tal fine (e quindi non deve ricevere alcuna ordine di sorveglianza). Per il rimanente si veda il commento dell'articolo 269bis CPP.

Se le condizioni dell'articolo 270 CPP sono adempite per analogia, il *capoverso 3* permette di sorvegliare la corrispondenza postale e il traffico delle telecomunicazioni non solo della persona scomparsa, ma anche di un terzo non implicato. Ciò è per esempio il caso se vi sono motivi di ritenere che la persona scomparsa utilizza il collegamento di questo terzo o lo chiama. Per il rimanente si veda il commento dell'articolo 35 capoverso 4.

Art. 37 Procedura

L'*articolo 37* disciplina la procedura applicabile nei casi previsti agli articoli 35 e 36.

Il *capoverso 1* si applica sia all'articolo 36 sia all'articolo 35 e, a differenza della corrispondente disposizione dell'AP-LSCPT, riprende il contenuto dell'articolo 3

capoverso 3 LSCPT vigente, che riguarda però soltanto la ricerca di persone scomparse. Esso non fa riferimento alla lista di cui all'articolo 269 capoverso 2 CPP per quanto concerne la sorveglianza secondo l'articolo 36 (cfr. il commento dell'art. 36). Gli articoli citati vanno applicati soltanto per analogia, poiché il CPP concerne i procedimenti penali in corso, mentre le sorveglianze secondo gli articoli 35 e seguenti avvengono al di fuori di un procedimento penale.

Il *capoverso 2* prevede che le persone sorvegliate nell'ambito di una ricerca d'emergenza ne siano informate nei termini più brevi in deroga all'articolo 279 CPP. Nell'ambito della ricerca di condannati, può esservi un interesse a mantenere più a lungo segreta la sorveglianza o ad omettere completamente l'informazione, per esempio per permettere l'istruzione di un'inchiesta contro una persona che potrebbe aver favorito la fuga del ricercato (art. 279 cpv. 2 CPP per analogia). In una ricerca d'emergenza tale interesse non sussiste, la qual cosa giustifica la succitata deroga.

Il *capoverso 3* si rifà al contenuto dell'articolo 3 capoverso 4 dell'attuale LSCPT. La disposizione disciplina la competenza per ordinare e approvare la sorveglianza secondo gli articoli 35 e 36, fermo restando che tale competenza può spettare tanto alla Confederazione quanto ai Cantoni. Nell'ambito dell'assistenza giudiziaria internazionale in materia penale tali questioni sono disciplinate dall'articolo 18*a* AIMP. La competenza di ordinare la sorveglianza che consente di localizzare una persona perseguita spetta all'Ufficio federale di giustizia secondo l'articolo 18*a* capoverso 1 della succitata legge. Il fatto che la sorveglianza debba essere approvata da un'autorità giudiziaria non dovrebbe comportare perdite di tempo nell'attuazione della sorveglianza, contrariamente ai timori in questo senso espressi durante la consultazione. In effetti, come è il caso per una sorveglianza ordinata nell'ambito di una procedura penale e secondo l'interpretazione che va fatta dell'articolo 274 capoversi 1–3 CPP, la sorveglianza ordinata può iniziare anche prima che il giudice dei provvedimenti coercitivi l'abbia approvata.

2.9 Sezione 9: Spese ed emolumenti

Art. 38

Secondo il diritto vigente, le installazioni necessarie all'attuazione della sorveglianza sono a carico dei fornitori di servizi postali e di telecomunicazione. Questi ultimi ricevono tuttavia un'equa indennità per le spese cagionate da ciascuna sorveglianza eseguita. Oltre a questa indennità, le autorità che ordinano una sorveglianza devono versare un emolumento al Servizio per le sue prestazioni (art. 16 LSCPT vigente). L'articolo 2 dell'ordinanza del Consiglio federale del 7 aprile 2004[64] sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OEm-SCPT) fissa un emolumento complessivo per ciascun tipo di sorveglianza come pure l'indennità che ne fa parte; essa prevede inoltre che, contrariamente a quanto disposto nell'articolo 16 capoverso 1 della LSCPT vigente, questo emolumento globale deve essere versato al Servizio che poi trasmette l'indennità ai fornitori. L'avamprogetto posto in consultazione (art. 30 AP-LSCPT) prevedeva la soppressione dell'indennità dei fornitori in relazione con il programma di consolidamento 2011–2013.

64 RS **780.115.1**

All'estratto e all'analisi dei costi della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni è stato dedicato un rapporto esterno del 12 giugno 2012 commissionato dal Servizio[65]. Il rapporto doveva in particolare aiutare a definire la normativa da adottare nell'ambito del presente progetto riguardo al finanziamento dell'infrastruttura necessaria per attuare le sorveglianze, al versamento di un'eventuale indennità ai fornitori e al pagamento di un eventuale emolumento al Servizio.

Il contenuto del rapporto e le diverse varianti sono stati minuziosamente analizzati anche per quanto concerne la riduzione delle tariffe chiesta dal postulato Recordon 11.42.10 (Costo della sorveglianza penale delle telecomunicazioni). È stata presa in considerazione la variante che consiste nel versare un'equa indennità ai fornitori di servizi di telecomunicazione sia per il costo degli impianti sia per le spese cagionate da un provvedimento di sorveglianza. Questa variante è quella che meglio tiene conto della situazione in cui verrebbero a trovarsi i piccoli fornitori di servizi di telecomunicazione tenuti a investire per acquistare impianti di sorveglianza che a guardar bene non sarebbero mai chiamati a utilizzare. A tale riguardo occorre precisare che questi fornitori possono essere dispensati dagli obblighi legali che in linea di massima incombono ai fornitori di servizi di telecomunicazione (cfr. il commento dell'art. 26 cpv. 6), dispensa che permetterebbe di ridurre i succitati costi di investimento. In seguito alla citata analisi, abbiamo deciso, contrariamente alle proposte inviate in consultazione e che avevano suscitato reazioni diverse, di mantenere il sistema attuale: i fornitori continueranno a dover finanziare gli impianti necessari all'attuazione delle sorveglianze continuando a ricevere un'equa indennità per le spese cagionate dall'esecuzione di un provvedimento di sorveglianza; l'autorità, che ha ordinato una sorveglianza, continuerà a dover versare un emolumento al Servizio per le prestazioni effettuate in esecuzione della sorveglianza e il Consiglio federale fisserà le indennità e gli emolumenti relativi ai diversi tipi di sorveglianze. Non è opportuno confrontare l'obbligo di eseguire le sorveglianze con l'obbligo di consegna (art. 265 CPP) negando con un ragionamento per analogia il versamento di una congrua indennità ai fornitori per le spese da loro sostenute nell'ambito dell'esecuzione dell'ordine di sorveglianza. Infatti se il detentore di un mezzo di prova rifiuta di adempiere il suo obbligo di consegna, il mezzo di prova può essere sequestrato; tale non è il caso dei dati che devono essere raccolti mediante la sorveglianza del traffico delle telecomunicazioni.

Il *capoverso 1* riprende e completa l'articolo 16 capoverso 1 primo periodo della LSCPT vigente precisando che le *spese* per le installazioni sono a carico delle persone obbligate a collaborare. La disposizione implica segnatamente che le persone obbligate a collaborare devono assumere anche le spese connesse con la consegna dei dati al Servizio. La consegna dei dati è in effetti una componente della disponibilità di sorvegliare e di conseguenza deve, in quanto debito portabile, essere assunto dalle persone obbligate a collaborare. Questa disposizione significa in particolare che l'acquisizione e la manutenzione degli impianti per l'esecuzione della sorveglianza devono essere totalmente finanziate dai fornitori di servizi postali e di telecomunicazione, compresi i costi per il personale connessi con l'acquisizione e la manutenzione nonché le spese di ammortamento degli impianti. È il diritto applicabile, in particolare la LSCPT, l'OSCPT e le ordinanze tecniche e amministrative che

65 www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/ber-isc-ejpd-fda-pda-f.pdf

stabilisce gli obblighi che queste persone devono adempiere affinché la sorveglianza possa essere attuata e che i dati possano essere adeguatamente consegnati. Questi obblighi possono variare in funzione della persona obbligata a collaborare (cfr. in particolare art. 26 e 27).

Il *capoverso 2* riprende sostanzialmente l'articolo 16 capoverso 1 secondo periodo LSCPT vigente eliminando un errore redazionale nel testo tedesco. Questo capoverso riguarda le spese che le persone obbligate a collaborare sostengono in relazione con una data sorveglianza, escluse le spese sostenute per gli impianti, che sono oggetto del capoverso 1. I costi di ogni sorveglianza sono nella maggior parte dei casi in gran parte dovuti al personale; vi possono tuttavia essere anche costi di materiale. I fornitori ricevono una congrua indennità forfettaria per queste spese (p. es. 80 % delle spese effettive che possono essere indennizzate, cfr. art. 4*a* cpv. 4 OEm-SCPT). Questa indennità sarà stabilita in un'ordinanza del Consiglio federale (cfr. cpv. 4) e può non coprire la totalità delle spese variabili effettive di un fornitore. In proposito occorre pure tenere presente che l'impiego di servizi di telecomunicazione a scopo delittuoso è un rischio connesso con l'attività dei fornitori e che ciascun cittadino è tenuto a contribuire a chiarire i reati (secondo l'art. 167 CPP anche i testimoni ricevono una congrua indennità). Anche se è il Servizio che versa l'indennità ai fornitori, ne è debitrice l'autorità che ha ordinato la sorveglianza (cfr. per il rimanente il commento del cpv. 3). Il capoverso 2 si iscrive nel numero 4 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander 10.3877 (Revisione della LSCPT).

Il *capoverso 3* precisa espressamente, per motivi di chiarezza, quanto risulta dall'articolo 16 capoverso 2 LSCPT vigente, vale a dire che l'autorità che ha ordinato la sorveglianza è tenuta a versare un emolumento – stabilito nell'ordinanza del Consiglio federale (cfr. cpv. 4) – al Servizio per le prestazioni fornite da quest'ultimo in relazione con la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. In proposito si chiarisce che il Servizio riceve un emolumento complessivo dalle autorità che hanno ordinato la sorveglianza e che questo emolumento comprende non soltanto un emolumento dovuto per le prestazioni del Servizio (*lett. a*) bensì anche un'indennità per le prestazioni delle persone obbligate a collaborare (*lett. b*); il Servizio trasmette l'indennità alle persone obbligate a collaborare (cfr. cpv. 2).

Il *capoverso 4* riprende l'articolo 16 capoverso 2 LSCPT vigente, ossia la norma di delega che ha permesso al Consiglio federale di adottare l'attuale OEm-SCPT. Quando ripercuote i costi delle misure di sorveglianza, il Consiglio federale è vincolato ai principi della copertura delle spese e dell'equivalenza. Poiché attualmente il Servizio non copre i costi cagionati dalla copertura dei suoi compiti (tasso di copertura delle spese del 54 % nel 2012), occorre decidere se è giustificato mantenere l'attuale (basso) tasso di copertura delle spese, dal momento che il perseguimento penale è un compito dei Cantoni. Il nostro Consiglio esaminerà questa questione nei dettagli quando stabilirà gli emolumenti che devono versare le autorità ordinanti.

A questo riguardo occorre ancora menzionare che l'importo versato al Servizio dall'autorità ordinante a titolo di emolumento equivale a una spesa procedurale, più precisamente a un esborso, che l'autorità può ripercuotere integralmente o parzialmente su terzi, in particolare sull'imputato condannato, a condizione di rispettare le regole di procedura (art. 422, 425 e 426 CPP).

2.10 Sezione 10: Disposizioni penali

Art. 39 Contravvenzioni

L'*articolo 39* è stato modificato, rispetto alla versione inviata in consultazione, in particolare per tenere conto dei cambiamenti apportati all'articolo 40. Gli articoli 6 e 7 DPA sono in particolare applicabili per determinare a chi sono applicabili le disposizioni penali contenute nell'*articolo 39* (cfr. art. 40 e relativo commento).

Il *capoverso 1* risponde alla necessità di introdurre nella nuova LSCPT disposizioni penali che permettano di sanzionare efficacemente le persone assoggettate alla legge che non rispettano gli obblighi da essa imposti, poiché adottano comportamenti che possono ostacolare le sorveglianze. L'esperienza mostra che i fornitori importanti di servizi di telecomunicazione attivi sul mercato svizzero sono in linea di massima consapevoli dei loro obblighi. La multa massima prevista nel *capoverso 1* per la commissione intenzionale dei reati secondo le lettere a–d è superiore all'importo massimo di 10 000 franchi della multa prevista nell'articolo 292 CP (Disobbedienza a decisioni dell'autorità) (cfr. anche art. 106 cpv. 1 CP). Questo importo può essere troppo basso per dissuadere dai succitati reati, in particolare tenuto conto dei risparmi che possono essere realizzati con tali comportamenti. Beninteso, l'autorità chiamata a pronunciarsi su una multa secondo il *capoverso 1* terrà conto delle diverse circostanze della fattispecie, come l'atto commesso e la capacità economica dell'impresa interessata (cfr. art. 8 DPA e art. 106 cpv. 3 CP). Precisiamo che per altre contravvenzioni del diritto penale accessorio sono comminate multe massime per un importo inferiore o superiore ai 100 000 franchi previsti nel *capoverso 1*. La sanzione prevista nell'articolo 39 sarà sussidiaria rispetto a quella prevista in disposizioni penali più severe di altre leggi che pure potrebbero trovare applicazione. Pensiamo in particolare al favoreggiamento e alla violazione degli obblighi di serbare il segreto, pure disciplinati in modo dettagliato nel CP. Potrebbero anche verificarsi dei casi in cui un atto adempie sia la fattispecie dell'articolo 39 capoverso 1 lettera d sia quella più grave dell'articolo 320 o 321ter CP. In questi casi, l'autore del reato non va punito in base alla disposizione penale meno severa dell'*articolo 39* poiché non vi è alcuna ragione oggettiva di farlo.

Per l'inosservanza delle ingiunzioni del Servizio il *capoverso 1 lettera a* prevede una sanzione analoga a quella dell'articolo 292 CP. La sanzione dell'articolo 292 non ha tuttavia effetto dissuasivo. Questo è segnatamente dovuto alle economie che una persona assoggettata alla LSCPT può realizzare non eseguendo un'ingiunzione del Servizio, fondata su un ordine di sorveglianza dell'autorità competente, in linea di massima il pubblico ministero, o nel caso, analogo, in cui la persona assoggettata alla LSCPT non dà seguito alle ingiunzioni del Servizio di adottare le misure tecniche e organizzative per compensare i difetti della sua disponibilità di informare e sorvegliare (art. 33 cpv. 5). L'adozione di una disposizione specifica con una sanzione più severa di quella dell'articolo 292 CP è di conseguenza giustificata. Scopo accessorio di questo meccanismo è beninteso anche quello di incitare le persone assoggettate alla LSCPT a eseguire le ingiunzioni del Servizio nei tempi più brevi; esso non impedisce tuttavia a queste persone di contestare siffatte ingiunzioni conformemente alle regole della procedura federale (cfr. art. 42). Le regole sul controllo della validità dell'ingiunzione del Servizio da parte del giudice penale ordinario, incaricato del perseguimento di un reato secondo l'articolo 39 capoverso 1 lettera a,

sono le medesime regole che la dottrina[66] e la giurisprudenza hanno sviluppato per la violazione dell'articolo 292 CP.

Sempre al fine di permettere un'efficace esecuzione delle sorveglianze, la disposizione penale del *capoverso 1 lettera b* si fonda segnatamente sul numero 2 della mozione Schweiger 06.3170 (Lotta alla cibercriminalità. Protezione dei fanciulli) e sanziona la violazione dell'obbligo di conservare i dati secondari nel settore della corrispondenza mediante telecomunicazioni (art. 26 cpv. 5). Oltre al fatto che nemmeno in questo caso è sufficientemente severa per punire adeguatamente il comportamento in questione, la sanzione prevista dall'articolo 292 CP non consente di reprimere un tale comportamento. In effetti questo articolo si applica se, nonostante l'ordine di un'autorità, non vengono consegnati dati esistenti, ma non se i dati sono distrutti prima dell'ordine dell'autorità o se non sono stati raccolti o conservati. Questa disposizione va applicata con coerenza anche alla violazione dell'obbligo di conservare i dati secondari nel settore della corrispondenza postale (art. 19 cpv. 4).

Dopo la procedura di consultazione, i reati del capoverso 1 sono stati completati con il *capoverso 1 lettera c*. L'esperienza mostra in effetti che la sanzione prevista da questa fattispecie è necessaria per assicurare il rispetto dei relativi obblighi[67].

Il *capoverso 1 lettera d* riprende sostanzialmente gli articoli 12 capoverso 3 e 15 capoverso 7 LSCPT vigente. Questa disposizione riguarda tutti i fatti connessi con la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, vale a dire in particolare l'esistenza di una sorveglianza nonché tutte le informazioni concernenti tale sorveglianza – comprese le semplici domande fondate sull'articolo 15 – che sulla base della LSCPT sono scambiate tra le persone che rientrano nel campo d'applicazione della legge, il Servizio e le autorità[68]. In questa disposizione la nozione di «terzo» non comprende i subappaltatori di una persona obbligata a collaborare che vanno informati dei fatti per poter eseguire la sorveglianza. Contrariamente agli articoli 12 capoverso 3 e 15 capoverso 7 LSCPT vigente, la *lettera d* non sottopone tali fatti al segreto delle poste e delle telecomunicazioni ai sensi dell'articolo 321ter CP. La *lettera d* non riguarda la divulgazione a terzi dei dati di contenuto o dei dati secondari raccolti durante una sorveglianza della corrispondenza postale o del traffico delle telecomunicazioni; questo comportamento è oggetto dell'articolo 321ter CP. Per evitare errori può essere opportuno per il Servizio rendere attente le persone che entrano nel campo d'applicazione della legge alle conseguenze penali che, secondo la *lettera d*, potrebbe avere la divulgazione dei succitati fatti e dati.

Secondo l'articolo 105 capoverso 2 CP, applicabile in virtù dell'articolo 40 capoverso 1 e dell'articolo 2 DPA, il tentativo è punito soltanto nei casi espressamente previsti dalla legge. Il *capoverso 2* prevede una tale disposizione. Viste le conseguenze che tali comportamenti possono avere e per analogia con quanto vale per numerose contravvenzioni del diritto penale accessorio che sono perseguite e giudicate secondo il diritto penale amministrativo, il tentativo di commettere i reati menzionati alle lettere a–d merita di essere punito.

Il *capoverso 3* punisce la commissione per negligenza di questi comportamenti. Per quanto concerne i motivi della punizione della commissione per negligenza di questi

66 Bernard Corboz, op. cit., n. 11–16 ad art. 292 CP.
67 Thomas Hansjakob, op. cit. (nota 11), n. 2 ad art. 19*a* OSCPT.
68 Thomas Hansjakob, op. cit. (nota 11), n. 26 ad art. 15 LSCPT.

reati, vale per analogia quanto detto sopra riguardo al capoverso 2. La multa massima prevista nel *capoverso 3* per la commissione per negligenza dei reati è superiore all'importo massimo della multa prevista nell'articolo 106 capoverso 1 CP. Questo importo può in alcuni casi essere effettivamente troppo basso se si considerano le importanti conseguenze negative che i comportamenti puniti possono avere per un'inchiesta in corso. Per il rimanente si veda per analogia il commento del capoverso 1.

Art. 40 Giurisdizione

L'avamprogetto messo in consultazione (art. 32 AP-LSCPT) prevedeva che il perseguimento e il giudizio dei reati oggetto dell'articolo 39 spettasse ai Cantoni, conformemente al principio applicabile, e non a un'autorità amministrativa della Confederazione – nel caso specifico, il Servizio – ciò che escludeva l'applicazione della DPA. In sede di consultazione questo punto è stato criticato a giusto titolo. Il presente progetto prevede pertanto la soluzione inversa, abituale nel diritto penale accessorio.

Dal *capoverso 1* risulta che la complicità è punibile. E ciò senza che sia necessario indicarlo espressamente, visto il contenuto dell'articolo 5 DPA applicabile in virtù dell'articolo 40 e degli articoli 1 e 2 DPA. Gli articoli 6 e 7 DPA (Infrazioni commesse nell'azienda, da mandatari e simili) sono pure applicabili, anche senza che sia necessario indicarlo espressamente in virtù degli articoli 40 e degli articoli 1 e 2 DPA. La normativa degli articoli 6 e 7 DPA sostituisce il capoverso 4 dell'articolo 31 dell'AP-LSCPT. Questa regolamentazione è ragionevole, nella misura in cui si precisa che le «persone» oggetto della disposizione sono innanzitutto i fornitori di servizi postali e di telecomunicazione, i loro impiegati, i loro superiori e le imprese stesse. Inoltre, la prescrizione dell'azione penale e della pena per i reati di cui all'articolo 39 è retta dall'articolo 11 DPA integrato dall'articolo 333 capoverso 6 lettere b ed e CP, fintanto che i relativi termini non sono stati adeguati ai nuovi termini di prescrizione previsti nella parte generale del CP. Secondo questi articoli, l'azione penale per questi reati si prescrive in 4 anni e la pena in 7 anni e mezzo.

Come prevede il *capoverso 2,* è più ragionevole che la competenza di perseguire e giudicare le infrazioni ai sensi dell'articolo 39 sia attribuita al Servizio (che dovrà organizzarsi di conseguenza) piuttosto che ai Cantoni, come previsto nell'avamprogetto posto in consultazione (art. 32 AP-LSCPT). Vi sono diversi argomenti a favore di questa soluzione. Prima di tutto occorre rilevare che il Servizio si trova in generale in condizione di meglio prendere atto dei fatti che possono costituire siffatti reati. Inoltre, l'articolo 39 sanziona segnatamente il mancato rispetto delle ingiunzioni del Servizio. Occorre peraltro rilevare che la LSCPT conferisce al Servizio compiti di sorveglianza amministrativa. Infine, facciamo notare che il perseguimento e il giudizio dei reati richiedono in linea di massima conoscenze tecniche specifiche, che le autorità di perseguimento penale dei Cantoni probabilmente possiedono in misura minore del Servizio.

2.11 Sezione 11: Vigilanza e tutela giurisdizionale

Art. 41 Vigilanza

È importante che sul mercato svizzero possano operare soltanto le persone sottoposte alla LSCPT che rispettano la legislazione relativa alla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni . L'*articolo 41* sulla sorveglianza amministrativa delle persone assoggettate alla LSCPT si prefigge questo obiettivo e rende l'articolo 58 parzialmente applicabile per analogia. Esso instaura un sistema di sanzioni amministrative complementari rispetto al sistema delle sanzioni penali previste negli articoli 39 e seguente. Il Servizio esercita le sue competenze che risultano dall'*articolo 41* in modo vincolante nei confronti delle persone obbligate a collaborare (art. 2). Non può obbligare le autorità che ordinano le sorveglianze né le autorità d'approvazione, poiché non possiede competenza decisionale nei loro confronti (cfr. commento dell'art. 16 lett. a e b).

Il *capoverso 1* è una norma analoga all'articolo 58 capoverso 1 LTC. Il Servizio deve svolgere il ruolo di autorità di vigilanza nel settore della corrispondenza postale e del traffico delle telecomunicazioni, poiché è l'organo che meglio conosce la materia e le regole applicabili.

Il *capoverso 2* è invece una norma analoga all'articolo 58 capoverso 2 lettera a LTC. Indica le misure che il Servizio può adottare se constata una violazione del diritto in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Se del caso, questo articolo permette al Servizio di ingiungere agli interessati di porre rimedio alle carenze constatate o di prescrivere misure per prevenire le recidive. Il destinatario dell'ingiunzione deve informare il Servizio delle disposizioni prese. Il *secondo periodo del capoverso 2* è una norma analoga all'articolo 58 capoverso 5 LTC. Oltre a pronunciare le citate misure, il Servizio può agire sul piano penale fondandosi sull'articolo 40. Occorre precisare che possono essere pronunciate misure più incisive di quelle che il Servizio può adottare secondo il *capoverso 2*, come già è il caso oggi, in caso di violazione del diritto in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Queste misure sono di competenza del Dipartimento federale dell'ambiente, dei trasporti, dell'energia e della comunicazione, per quanto concerne la corrispondenza postale e dell'Ufficio federale della comunicazione e della Commissione federale della comunicazione per quanto concerne il traffico delle telecomunicazioni. Come è già il caso attualmente, l'Ufficio federale della comunicazione e la Commissione federale della comunicazione potranno agire in base agli articoli 58 e 60 LTC e il Servizio potrà informare queste autorità delle violazioni che ha constatato per consentire loro di adottare, se del caso, le succitate misure. Non è necessario adottare una disposizione, ispirandosi all'articolo 58 capoverso 2 lettera b LTC che permetta al Servizio di obbligare un fornitore di servizi di telecomunicazione a versare alla Confederazione un importo corrispondente a quello risparmiato non eseguendo la sorveglianza richiesta o non effettuando gli investimenti necessari per adempiere i suoi obblighi nel settore della vigilanza. In questo caso il fornitore evita in effetti una spesa ma non ottiene alcun vantaggio finanziario nei sensi della succitata disposizione. Il fornitore deve tuttavia versare al Servizio un importo definito alle condizioni dell'articolo 34. Inoltre, l'articolo 33 capoverso 5 permette al Servizio di ingiungere al fornitore di adottare determinate misure tecniche e organizzative per compensare queste carenze nel settore della sorveglianza. Finalmente, il fornitore potrà essere sanzionato penalmente per il mancato rispetto dell'ingiunzione di ese-

guire la sorveglianza o dell'ingiunzione secondo l'articolo 33 capoverso 5 (art. 39 cpv. 1 lett. a).

Art. 42 Tutela giurisdizionale

Occorre fin d'ora precisare che l'*articolo 42* non riguarda il rimedio giuridico dato alle persone che sono oggetto di una sorveglianza della corrispondenza postale o del traffico delle telecomunicazioni o alle persone toccate da tale sorveglianza; tale rimedio giuridico è retto dagli articoli 279 capoverso 3 CPP o 70*k* PPM. L'articolo 279 capoverso 1 CPP indica inoltre quali terzi sorvegliati devono essere ulteriormente informati; si tratta esclusivamente dei terzi ai sensi dell'articolo 270 lettera b CPP. Altri interessati, per esempio persone che hanno comunicato con il sorvegliato o persone che, nell'ambito di una ricerca per zona di copertura d'antenna o di ricorso a un IMSI-catcher, sono inevitabilmente registrate prima della cernita dei risultati della sorveglianza, non sono sottoposte all'obbligo di comunicazione secondo l'articolo 279 CPP e non hanno diritto di interporre reclamo ai sensi del capoverso 3 di tale disposizione. Ciò è giustificato poiché queste persone non sono sorvegliate ai sensi di legge. Gli articoli 269–279 CPP (in particolare gli art. 269–269ter CPP nella loro versione modificata) disciplinano in modo esaustivo l'ammissibilità di una sorveglianza dal profilo della procedura penale. Così i risultati di una sorveglianza (in tempo reale o retroattiva; i contenuti delle comunicazioni o i dati secondari) non possono per esempio essere utilizzati senza l'approvazione del giudice dei provvedimenti coercitivi (o del Tribunale militare di cassazione); a una sorveglianza non autorizzata è posto immediatamente fine e i dati raccolti sono distrutti (art. 277 CPP).

Le persone obbligate a collaborare in virtù della LSCPT (art. 2) sono interessate soltanto in modo indiretto da tali questioni di procedura penale, nella misura in cui devono eseguire o tollerare una sorveglianza. La LSCPT non deve quindi affrontare questioni di procedura penale; essa deve unicamente garantire l'attuazione tecnica delle sorveglianze ammissibili sotto il profilo della procedura penale (fatte salve la ricerca in caso d'emergenza e la ricerca di condannati). I rimedi giuridici delle persone assoggettate che entrano nel campo d'applicazione della LSCPT vanno disciplinati in questa sede soltanto in relazione con il citato aspetto tecnico e di diritto amministrativo. Questa concezione rispecchia l'opinione della dottrina e della giurisprudenza[69]. Le persone che entrano nel campo d'applicazione della LSCPT non possono fare valere censure concernenti la procedura penale nell'ambito di un ricorso di diritto amministrativo. L'ammissione del ricorso di diritto amministrativo di un fornitore di servizi di telecomunicazione non può quindi avere per conseguenza l'annullamento di una sorveglianza approvata dal giudice dei provvedimenti coercitivi ma può avere per sola conseguenza il fatto che il fornitore non sia tenuto di eseguire esso stesso la sorveglianza se non è in grado di farlo per motivi tecnici o organizzativi. Il fornitore è tuttavia obbligato a tollerare la sorveglianza eseguita dal Servizio o da un terzo (art. 26 cpv. 2) e a sostenere il Servizio nell'ambito dell'ese-

69 Thomas Hansjakob, op. cit. (nota 11), n. 3 ad art. 32 OSCPT; DTF **130** II 249, consid. 2.2.2 e 2.2.3. Vedi anche DTAF 2009/46, consid. 3.1.3, 3.2, 3.3 (non entrata in materia sulla censura del fornitore di servizi di telecomunicazione, secondo cui i diritti del sorvegliato sarebbero stati violati senza che vi fosse una base legale).

cuzione (art. 32 cpv. 2). Anche le spese possono essere oggetto di un ricorso di diritto amministrativo (cfr. il commento dell'art. 38).

È ragionevole operare una chiara distinzione tra la CPP e la LSCPT, poiché questi due testi di legge – come spiegato sopra – hanno destinatari diversi e cercano di disciplinare oggetti diversi (cfr. anche il commento dell'art. 31). Il fatto che i settori normativi siano distinti si ripercuote anche sui rimedi giuridici. La dualità dei rimedi giuridici è quindi una conseguenza della separazione tra il diritto amministrativo (LSCPT) e la procedura penale (CPP), la qual cosa corrisponde anche all'esigenza espressa nel numero 2 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander 10.3877 (Revisione della LSCPT).

Tenuto conto di quanto precede, il *capoverso 1* riguarda unicamente i rimedi giuridici contro le decisioni del Servizio che possono adire le persone obbligate a collaborare (art. 2) e le autorità che devono versare emolumenti al Servizio.

La LSCPT vigente non contiene disposizioni sui rimedi giuridici messi a disposizione delle persone obbligate a collaborare contro le decisioni del Servizio, in generale (p. es. in materia d'indennità), e in particolare contro le decisioni di quest'ultimo di far eseguire una sorveglianza fondata su un ordine di sorveglianza di un'autorità competente. Soltanto l'articolo 32 OSCPT vigente riconosce il diritto di queste persone di ricorrere contro una decisione del Servizio di far eseguire una sorveglianza. Nell'ambito di un tale ricorso, queste persone non possono però – come spiegato sopra – far valere questioni di natura tecnica o organizzativa legate all'esecuzione di una misura di sorveglianza loro richiesta. Per motivi di chiarezza e certezza del diritto, il progetto prevede ormai una disposizione che disciplina espressamente le vie di ricorso date alle persone assoggettate alla LSCPT contro le decisioni del Servizio.

Molti partecipanti alla procedura di consultazione hanno criticato la normativa proposta (art. 34 AP-LSCPT) secondo cui il ricorrente non poteva far controllare da un giudice la legalità della decisione di sorveglianza trasmessagli dal Servizio. Questa opinione non corrisponde però alla realtà. Da una parte, le decisioni del Servizio possono essere controllate conformemente alle disposizioni generali della procedura amministrativa per quanto concerne la messa in opera tecnica e organizzativa dell'ordine di sorveglianza. Dall'altra, la questione dell'ammissibilità dell'ordine di sorveglianza sotto il profilo della procedura penale è esaminata in tale ambito secondo le regole del diritto di procedura penale. La concezione secondo cui il Tribunale amministrativo federale dovrebbe poter controllare l'ammissibilità anche sotto il profilo della procedura penale metterebbe durevolmente in pericolo la certezza del diritto: siffatta competenza parallela farebbe sì che le decisioni del giudice dei provvedimenti coercitivi potrebbero essere revocate senza rispettare l'ordine delle istanze e con un cambiamento del rimedio giuridico non previsto dall'ordine giuridico. All'inverso, una decisione del Tribunale amministrativo federale sull'ammissibilità dell'ordine di sorveglianza sotto il profilo della procedura penale potrebbe rendere caduco un ricorso dell'imputato fondato sull'articolo 279 capoverso 3 CPP, ledendone così i diritti costituzionali.

In considerazione delle regole generali di procedura applicabili dinanzi al Tribunale amministrativo federale, il ricorrente può sottoporre al suo vaglio questioni giuridiche soltanto se ha un interesse giuridicamente protetto (art. 37 della legge del

17 giugno 2005[70] sul Tribunale amministrativo federale [LTAF] in combinato disposto con l'art. 48 cpv. 1 lett. c PA). Da ciò risulta che le persone obbligate a collaborare (art. 2), segnatamente i fornitori di servizi di telecomunicazione, non avranno comunque la qualità per agire per sollevare questioni riguardanti la procedura penale o la protezione dei dati delle persone tra cui si svolgono le comunicazioni. Una determinata situazione può certamente avere aspetti che sollevano questioni giuridiche connesse con la procedura penale e aspetti legati al diritto amministrativo (compreso il diritto della protezione dei dati). Di conseguenza, l'ammissibilità di un dato tipo di sorveglianza (p. es. la ricerca per zona di copertura d'antenna) riguarda sia il diritto di procedura penale sia il diritto della protezione dei dati (lo Stato può sorvegliare gli utenti di telefoni cellulari con la ricerca per zona di copertura d'antenna?) sia il rapporto di diritto amministrativo con i fornitori di servizi di telecomunicazione (i fornitori di servizi di telecomunicazione devono eseguire ricerche per zona di copertura d'antenna?). Tali questioni non devono tuttavia essere confuse, in considerazione dei diversi interessi in gioco e delle diverse questioni che si pongono; devono invece essere graduati i rimedi giuridici.

Il diritto di ricorso delle persone assoggettate alla LSCPT, in particolare dei fornitori di servizi di telecomunicazione, è quindi escluso per tutti gli aspetti della procedura penale, poiché a tale riguardo non hanno un interesse giuridicamente protetto. Tale è per esempio il caso quando sussistono gravi sospetti in virtù dell'articolo 269 capoverso 1 lettera a CPP o 70 capoverso 1 lettera a PPM, oppure se le condizioni per la sorveglianza del collegamento di telecomunicazione di un terzo secondo l'articolo 270 lettera b CPP o 70*a* lettera b PPM sono adempite. Queste questioni hanno soltanto un'incidenza indiretta sui fornitori di servizi di telecomunicazione.

Il *capoverso 2* esprime in modo esplicito quanto esposto sopra e in ogni modo vale in virtù delle regole generali di procedura. È tuttavia ragionevole conservare questa disposizione che chiarisce espressamente un punto importante per la pratica in materia di perseguimento penale e di diritto amministrativo.

Tenuto conto in particolare della situazione d'urgenza in cui vanno eseguite le sorveglianze, il *capoverso 3 primo periodo* prevede in deroga all'articolo 55 capoverso 1 PA – in principio applicabile in virtù del rinvio dell'articolo 37 LTAF – che il ricorso non ha effetto sospensivo, salvo che la decisione del Servizio concerna una prestazione pecuniaria (p. es. in materia di indennità o di emolumenti), poiché occorre partire dal presupposto secondo cui in questo caso non vi è urgenza. Affinché il ricorso non abbia effetto sospensivo, non occorre quindi che il Servizio lo ritiri secondo l'articolo 55 capoverso 2 PA. Come l'articolo 55 capoverso 3 PA, il *capoverso 3 secondo periodo* prevede tuttavia che l'autorità di ricorso può restituire al ricorso l'effetto sospensivo. Peraltro, un ricorso retto dalla procedura penale non ha in linea di massima effetto sospensivo (art. 387 CPP) poiché la sorveglianza si prefigge di ottenere prove, operazione che in regola generale non deve essere in alcun modo differita.

70 RS **173.32**

2.12 Sezione 12: Disposizioni finali

Art. 43 Esecuzione

L'*articolo 43* attribuisce al nostro Consiglio la competenza di emanare le disposizioni esecutive della nuova LSCPT. Prevede parimenti la medesima competenza per i Cantoni facendo in particolare riferimento all'articolo 37 capoverso 3.

Art. 44 Abrogazione e modifica del diritto vigente

Nell'allegato, a cui si riferisce l'*articolo 44*, la cifra I dispone sostanzialmente che la legge federale del 6 ottobre 2000[71] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni è abrogata con l'entrata in vigore della nuova LSCPT. Infatti quest'ultima non modifica la LSCPT vigente, ma la sostituisce.

La cifra II, a cui fa riferimento l'*articolo 44,* menziona le leggi che sono modificate.

Art. 45 Disposizioni transitorie

In linea di massima le disposizioni transitorie sono volte a consentire che il nuovo diritto sostituisca il più in fretta possibile il diritto vigente, così da beneficiare il più celermente possibile dei vantaggi del nuovo diritto, ritenuto migliore di quello vigente. Oggetto delle disposizioni prese in considerazione sono le sorveglianze secondo la presente legge (ossia quelle previste dall'art. 269 CPP e pure rette dalla LSCPT) e i ricorsi contro le sorveglianze sempre secondo la presente legge. È così possibile operare una distinzione con le sorveglianze rette esclusivamente dal CPP (segnatamente quelle effettuate mediante IMSI-catcher [art. 269bis CPP] e GovWare [art. 269ter]) e i ricorsi contro siffatte sorveglianze che sono oggetto delle disposizioni transitorie previste dal CPP.

Il *capoverso 1* si rifà all'articolo 448 capoverso 1 CPP, senza però riprendere integralmente tale disciplina. Stando alla regolamentazione proposta, all'esecuzione delle sorveglianze si applicherà il diritto vigente nel momento preso in considerazione. Il nuovo diritto non si applicherà dunque prima della sua entrata in vigore, neppure se la sorveglianza è ancora in corso. Con l'entrata in vigore del nuovo diritto non si torna quindi su misure già eseguite. Va da sé che il rispetto del principio della non retroattività impone che il nuovo diritto non si applichi alle sorveglianze già attuate al momento della sua entrata in vigore. Se invece una sorveglianza è in corso, il nuovo diritto si applicherà dalla sua entrata in vigore al prosieguo della sorveglianza. Ciò consentirà di beneficiare già a questo stadio dei vantaggi del nuovo diritto senza complicare eccessivamente l'esecuzione della sorveglianza in corso. Il nuovo diritto si applicherà dunque alle sorveglianze ordinate dopo la sua entrata in vigore.

Il *capoverso 2* si rifà all'articolo 453 capoverso 1 CPP, senza riprenderne tuttavia per intero il tenore. I ricorsi vengono trattati secondo il diritto applicabile in prima istanza; ciò si giustifica in quanto nell'ambito del ricorso s'intende determinare se in prima istanza il diritto è stato applicato correttamente.

Il *capoverso 3* concerne l'estensione da 6 a 12 mesi della durata di conservazione dei dati secondari postali e delle telecomunicazioni. I dati secondari, il cui termine di

71 RU **2001** 3096, **2003** 2133 3043, **2004** 2149 3693, **2006** 2197 5437, **2007** 921 5437

conservazione di 6 mesi previsto dal diritto previgente non è ancora scaduto al momento dell'entrata in vigore della presente legge, vanno conservati per 12 mesi conformemente a quanto prevede il nuovo diritto, e ciò a decorrere dall'inizio del termine della loro conservazione secondo il diritto previgente. *A contrario*, i dati secondari il cui termine di conservazione di 6 mesi previsto dal diritto vigente è scaduto nel momento dell'entrata in vigore del nuovo diritto, non vanno conservati più a lungo.

Il *capoverso 4* riguarda la soppressione del termine di due anni – previsto dalla LSCPT vigente – dopo l'inizio della pertinente relazione commerciale, termine durante il quale le informazioni in questione devono essere disponibili. Le informazioni per le quali, al momento dell'entrata in vigore della nuova legge, non è ancora scaduto il termine di due anni previsto dal diritto previgente devono poter essere fornite a tempo indeterminato conformemente alla nuova legge. *A contrario*, le informazioni per le quali il termine di due anni del diritto previgente è scaduto al momento dell'entrata in vigore del nuovo diritto non devono più essere fornite.

Il *capoverso 5* prevede un disciplinamento molto semplice: è infatti applicabile il diritto vigente nel momento in cui la sorveglianza è stata ordinata. In questo contesto il momento in cui una sorveglianza (già ordinata) è stata all'occorrenza prorogata è irrilevante. Quanto precede implica in particolare che le indennità e gli emolumenti per una sorveglianza in corso nel momento dell'entrata in vigore della nuova legge sono retti dal diritto previgente.

Art. 46 Referendum ed entrata in vigore

L'*articolo 46* disciplina il referendum e l'entrata in vigore.

Codice di procedura penale[72]

Art. 269 cpv. 2 lett. a

L'esperienza insegna che gli strumenti attuali – inclusa la ricerca d'emergenza (art. 35 D-LSCPT) – non bastano a localizzare un minore illecitamente trasportato o trattenuto. Una sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, ossia una misura suscettibile di contribuire al ritrovamento del bambino, non può essere disposta dato che la sottrazione di minorenne (art. 220 CP) non figura nell'elenco dei reati per il cui perseguimento può essere ordinata tale misura. Per tale motivo occorre completare l'*articolo 269 capoverso 2 lettera a CPP con un rinvio all'articolo 220 CP.*

Art. 269bis (nuovo) Utilizzazione di speciali dispositivi tecnici per la sorveglianza del traffico delle telecomunicazioni

L'*articolo 269bis* contiene una base legale esplicita che consente al pubblico ministero di fare un uso più ampio di speciali dispositivi di sorveglianza quali gli IMSI-catcher, segnatamente per identificare apparecchi mobili di comunicazione e i loro utenti. Il concetto di apparecchi mobili di comunicazione non comprende soltanto gli apparecchi di telefonia mobile bensì segnatamente anche i laptop e i notebook dotati

72 RS **312.0**

di carte SIM per la trasmissione di dati mediante la rete di telefonia mobile. Tale nuova base legale consente inoltre di impiegare gli IMSI-catcher per ascoltare (e registrare) le comunicazioni nonché per localizzare tali apparecchi o i loro utenti. Le autorità inquirenti che oggigiorno ricorrono a tali dispositivi si fondano sull'articolo 280 lettere a e c CPP. Il citato complemento relativo all'identificazione è indispensabile per il perseguimento dei reati e inoltre è giustificato dal fatto che l'identificazione lede la sfera privata degli utenti meno delle succitate misure legittime, come la localizzazione e l'ascolto delle conversazioni[73]. L'IMSI-catcher consente di simulare gli effetti tra la stazione di base di una rete di telefonia mobile e gli apparecchi di telefonia mobile ubicati all'interno del suo campo. Gli apparecchi notificano la loro presenza all'IMSI-catcher ed eseguono la procedura di identificazione come farebbero con qualsiasi altra stazione di base di una rete. In questo modo è possibile individuare senza l'intervento dell'operatore di telefonia mobile il numero della scheda d'identificazione dell'utente (numero SIM) o il numero d'identificazione internazionale (numero IMSI o numero IMEI), sino ad allora ignoto, di una data persona o apparecchiatura, di localizzare gli apparecchi in una determinata zona o persino di ascoltare le conversazioni telefoniche[74].

Un numero piuttosto consistente di partecipanti alla procedura di consultazione, in particolare i Cantoni e le organizzazioni che rappresentano le autorità di perseguimento penale, è favorevole all'istituzione di una base legale che consenta l'impiego di dispositivi del tipo IMSI-catcher nel senso di cui sopra. Il Partito ecologista svizzero (I Verdi) nonché alcune organizzazioni di tutela dei consumatori e di utenti di Internet invece vi si oppone. In particolare quest'ultimi interpellati fanno notare che l'IMSI-catcher non soltanto consente di identificare il telefono mobile di un singolo utente, ma anche di deviare (e disturbare) le comunicazioni su una rete di telefonia mobile di tutte le persone, sospette o meno, che si trovano nei dintorni dell'utente in questione. Vi è pure stato chi si è interrogato sulla correttezza della classificazione sistematica della misura di sorveglianza presa in considerazione (art. 269 e segg. CPP o art. 280 e seg. CPP).

La classificazione sistematica dell'impiego di dispositivi tecnici quali gli IMSI-catcher tiene conto di quanto richiesto al numero 2 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander 10.3877 (Revisione della LSCPT), secondo cui nessun aspetto inerente al perseguimento penale deve figurare nella LSCPT. Nell'ottica della sistematica, l'utilizzazione di dispositivi tecnici del tipo IMSI-catcher è retta esclusivamente dagli articoli 269 e seguenti CPP, e non dagli articoli 280 e seguente CPP. Attualmente l'impiego di tali metodi di sorveglianza non richiede né la collaborazione di un fornitore di servizi di telecomunicazione né un intervento particolare del Servizio in relazione con l'utilizzazione di siffatti dispositivi di sorveglianza (nessun ordine di sorveglianza gli deve dunque pervenire). Tuttavia si tratta di ottenere dati del traffico delle telecomunicazioni, motivo per cui tale disposizione deve figurare nella sede summenzionata[75].

Tale metodo di sorveglianza va in particolare distinto dalla sorveglianza volta a ottenere dai fornitori di servizi di telecomunicazione i dati relativi alle chiamate di

73 Sophie de Saussure, op. cit., n. 45–56 e 70.
74 Sylvain Métille, op. cit., n. 25.
75 Sophie de Saussure, op. cit., n. 16, 20 e 41–44; di diverso parere Sylvain Métille, op. cit., n. 26 e 40.

telefonia mobile transitate, in un determinato lasso di tempo, attraverso le loro antenne, che coprono un luogo delimitato da determinate coordinate geografiche e che possono dunque servire a localizzare un telefono cellulare e la persona che lo utilizza. Occorre precisare che gli articoli 269–279 CPP si applicano all'impiego di dispositivi tecnici di sorveglianza ai sensi dell'articolo 269bis CPP, se questa norma non stabilisce altrimenti. Ciò implica segnatamente che l'impiego di un cosiddetto IMSI-catcher ordinato dal pubblico ministero sottostà all'approvazione del giudice dei provvedimenti coercitivi.

Dalla *lettera a* risulta dunque che i reati per i quali entra in linea di conto una sorveglianza del traffico delle telecomunicazioni mediante dispositivi tecnici quali gli IMSI-catcher sono i medesimi per i quali è possibile ricorrere a una sorveglianza di tipo tradizionale ai sensi dell'articolo 269 CPP.

La *lettera b* prevede che il ricorso a dispositivi tecnici quali gli IMSI-catcher, tenuto conto delle loro caratteristiche tecniche e visto che sono in grado di interferire con le telecomunicazioni, costituisce un metodo di sorveglianza sussidiario. L'impiego di siffatti dispositivi deve limitarsi a colmare le lacune esistenti attualmente nell'ambito dei metodi tradizionali di sorveglianza; infatti tali dispositivi non sono destinati a rimpiazzare i metodi attualmente in uso per sorvegliare il traffico delle telecomunicazioni ai sensi dell'articolo 269 CPP[76].

Considerato che tali dispostivi possono interferire con le telecomunicazioni, la *lettera c* prevede che un loro impiego è ammesso soltanto previa autorizzazione dell'Ufficio federale delle comunicazioni (UFCOM) – e non del giudice dei provvedimenti coercitivi – retta dagli articoli 32*a* e 34 capoverso 1ter LTC, dall'articolo 6 capoverso 4 dell'ordinanza del 14 giugno 2002[77] sugli impianti di telecomunicazione (OIT) e dagli articoli 49 e seguenti dell'ordinanza del 9 marzo 2007[78] sulla gestione delle frequenze e sulle concessioni di radiocomunicazione (OGC). In pratica, per ottenere l'autorizzazione, l'autorità che vuole utilizzare un tale dispositivo, deve presentare una pertinente domanda all'UFCOM, indicando tutti i parametri tecnici del dispositivo. L'UFCOM determina se sono soddisfatte le condizioni per il rilascio di un'autorizzazione, in particolare se l'utilizzo del dispositivo non leda eccessivamente, in termini di efficacia delle telecomunicazioni, altri interessi pubblici o di terzi. L'UFCOM valuta dunque il pericolo di interferenze nelle telecomunicazioni, segnatamente nelle reti di telefonia mobile, dovute all'impiego del dispositivo in questione[79]. Le autorizzazioni dell'UFCOM sono concesse a un utente specifico per l'impiego di un certo numero di dispositivi di tipo determinato. Una volta ottenuta l'autorizzazione, il dispositivo può essere utilizzato nell'ambito della sorveglianza senza che tale ufficio debba rinnovare l'autorizzazione per ogni nuova sorveglianza.

Art. 269ter (nuovo) Utilizzazione di speciali programmi informatici per la sorveglianza del traffico delle telecomunicazioni

L'*articolo 269ter* intende consentire al pubblico ministero di ordinare nel contesto di un procedimento penale, a condizioni molto severe, l'utilizzazione di speciali programmi informatici comunemente denominati «government software» (GovWare).

76 Sophie de Saussure, op. cit., n. 72.
77 RS **784.101.2**
78 RS **784.102.1**
79 Per maggiori ragguagli sulle interferenze che gli IMSI-catcher possono cagionare nonché sulle autorizzazioni dell'UFCOM, cfr. Sophie de Saussure, op. cit., n. 57–59.

Si tratta cioè di introdurre in un sistema di trattamento dei dati tali programmi informatici per intercettare e leggere il contenuto delle comunicazioni e i dati secondari. Spetta alla polizia svolgere tale compito su ordine del pubblico ministero. Tale metodo non richiede dunque la collaborazione di un fornitore di servizi di telecomunicazione. Per quanto concerne il Servizio, esso non è chiamato a svolgere alcun ruolo particolare nell'impiego di un GovWare; non occorre pertanto fargli pervenire un ordine di sorveglianza. Beninteso tale programma viene introdotto all'insaputa del detentore del sistema di trattamento dei dati. Per «sistema di trattamento dei dati», s'intende un'apparecchiatura che consente il traffico delle telecomunicazioni, mediante telefonia o in altro modo, come gli ordinatori, i telefoni portatili o fissi, nonché i tablet elettronici. Un GovWare viene impiegato esclusivamente nell'ambito di un procedimento penale; tale metodo di sorveglianza non può dunque essere utilizzato a titolo preventivo. I GovWare vengono sovente impropriamente detti «cavalli di Troia». In realtà, oltre al fatto che un GovWare viene utilizzato – a differenza del cavallo di Troia – per uno scopo legale, ossia per la lotta contro la criminalità, l'obiettivo non è la propagazione del programma in questione come nel caso di un cavallo di Troia, bensì consentire al pubblico ministero di sorvegliare un apparecchio specifico o una data persona[80].

Il GovWare è particolarmente utile per leggere comunicazioni effettuate con la telefonia via Internet (Voice over IP [VoIP]), e più precisamente della telefonia via Internet del tipo peer-to-peer[81]; infatti nel caso di questo tipo di telefonia i dati comunicati e intercettati sono criptati e senza l'impiego di un GovWare risulterebbero dunque illeggibili e inutilizzabili. Tale metodo di sorveglianza è pure utile nel caso in cui è impossibile intercettare una comunicazione, anche non criptata, senza farvi ricorso come, ad esempio, nel caso di uno scambio di messaggi istantanei avviato da un computer portatile o da un telefono cellulare muniti di diverse carte SIM DATAS prepagate. In questi casi, infatti, soltanto l'installazione di un programma nel computer portatile o nel telefono cellulare consente di intercettare la comunicazione, anche se non è criptata.

Sotto il profilo tecnico i GovWare consentono di accedere all'insieme delle informazioni private (p. es. documenti, foto), ossia anche a dati facenti parte della sfera intima, salvate sul computer. Mediante i GovWare si devono tuttavia poter ottenere soltanto dati del traffico summenzionato (dati acustici e ottici), di cui fanno parte anche le comunicazioni via Internet; i dati relativi alla telefonia via Internet e alla corrispondenza via e-mail rivestono un interesse particolare (cfr. anche il commento all'art. 1 capoverso 1 D-LSCPT). Giuridicamente tale limitazione esclude segnatamente la perquisizione online mediante GovWare di un sistema di trattamento dei dati.

I pareri divergono sull'ammissibilità, in virtù dell'articolo 280 CPP, in particolare le lettere a e b, dell'impiego di GovWare nel senso evocato in precedenza[82]. La dottri-

80 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 3.

81 Sylvain Métille, op. cit., n. 30 cfr. Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 7 e Sylvain Métille, op. cit., n. 30.

82 Annegret Katzenstein in: Basler Kommentar, Schweizerische Strafprozessordnung, Basilea 2011, n. 16 ad art. 280 CPP; Thomas Hansjakob in: Kommentar zur Schweizerischen Strafprozessordnung, Zurigo/Basilea/Ginevra, n. 2 ad art. 280 CPP; Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 16 e 30; Sylvain Métille, op. cit., n. 37.

na prevalente ritiene che tale impiego non sia ammesso. Taluni autori sono del parere che l'impiego di GovWare sia possibile soltanto interpretando in modo molto estensivo l'articolo 280 CPP. Sinora il Tribunale federale non si è ancora espresso esplicitamente al riguardo. A tal proposito va precisato che le autorità di perseguimento penale (Confederazione e Cantoni) hanno fatto ricorso a GovWare soltanto sporadicamente, fondandosi sulle disposizioni della procedura penale vigente prima dell'entrata in vigore il 1° gennaio 2011 del nuovo CPP, in particolare sull'articolo 66 capoverso 2 della legge federale del 15 giugno 1934 sulla procedura penale o su codici di procedura penale cantonali abrogati. La PGF, su mandato del MPC e dopo aver ottenuto l'autorizzazione del Tribunale penale federale, ha fatto capo ai GovWare in quattro procedimenti relativi a differenti categorie di reati. Tali normative si limitavano a consentire l'impiego di apparecchi tecnici di sorveglianza senza fornire particolari precisazioni sullo scopo perseguito da tale utilizzo. Dette disposizioni consentivano tuttavia il ricorso ai GovWare, interpretando in maniera estensiva il concetto di « apparecchi tecnici di sorveglianza », con un'interpretazione meno estensiva di quella necessaria per fondare una siffatta sorveglianza sull'articolo 280 CPP. Nell'ambito dei lavori concernenti il CPP, si era tuttavia ritenuto che dette regolamentazioni non erano in grado di soddisfare l'esigenza di precisione richiesta dalle norme che limitano i diritti fondamentali; si tenta di ovviare al problema con l'articolo 280 CPP[83]. Pertanto, visto quanto precede, per fare ricorso ai GovWare è necessario creare una base legale esplicita nel senso di cui sopra. Ciò si giustifica anche poiché una siffatta base legale deve costituire il giustificativo legale (art. 14 CP) per un comportamento che altrimenti soggiace all'articolo 143bis CP (accesso indebito a un sistema per l'elaborazione di dati).

Durante la consultazione sull'avamprogetto sono stati espressi pareri contrastanti in merito al principio di una disposizione sulla possibilità di fare ricorso ai GovWare per la sorveglianza del traffico delle telecomunicazioni. Un certo numero di Cantoni e di organizzazioni attive nell'ambito del perseguimento penale si è detto favorevole a tale eventualità, mentre il Partito ecologista svizzero (I Verdi) come pure le organizzazioni di tutela dei consumatori e di utenti di Internet la respingono. La maggioranza dei fornitori di servizi di telecomunicazione, come anche molti privati, ha espresso parecchie riserve. È in particolare stato posto il quesito dell'opportunità di autorizzare questo tipo di sorveglianza molto incisiva e potenzialmente in grado di perquisire «online» l'intero sistema per l'elaborazione di dati. È pure stato osservato che l'introduzione di siffatti programmi informatici in un computer comporta rischi troppo rilevanti per la sicurezza informatica (lacuna nel sistema di sicurezza che prima o poi potrebbe venir sfruttata anche dai criminali, uso abusivo da parte di criminali, rischi per il computer nel quale è stato istallato il GovWare, rischi per l'intera rete informatica) nonché per l'affidabilità e l'integrità dei mezzi di prova (p. es. modifica dei dati da parte del GovWare). È pure stata sottolineata l'impossibilità di prevedere l'interazione tra GovWare e gli altri elementi del sistema di trattamento dei dati nel quale viene introdotto; sussiste inoltre l'eventualità che tali software danneggino un numero relativamente elevato di sistemi di trattamento dei dati sia in Svizzera sia all'estero e ci si interroga in merito alla responsabilità (segnatamente della Confederazione) per coprire i danni cagionati. Inoltre vi è chi ha messo in dubbio l'efficacia di questo metodo di sorveglianza e ha osservato che, considerate le caratteristiche di siffatto metodo, e vista la notevole ingerenza nei

83 Messaggio del 21 dicembre 2005 concernente l'unificazione del diritto processuale penale, FF **2006** 989 1155.

diritti fondamentali dell'interessato che ne deriva, andrebbe impiegato soltanto in relazione con una determinata categoria di reati (molto gravi) previsti dall'articolo 269 capoverso 2 CPP. Ci si è pure chiesti se la classificazione sistematica di tale misura di sorveglianza sia da ritenere corretta (art. 269 segg. CPP o art. 280 e 281 CPP).

Secondo il parere degli specialisti di polizia interpellati, i timori espressi in merito ai GovWare sono infondati. I GovWare restano in permanenza sotto il controllo delle autorità inquirenti (polizia sottoposta al pubblico ministero). A dipendenza della situazione, il GovWare è introdotto in modo piuttosto semplice fisicamente e in modo diretto nell'apparecchio target (computer) dalla polizia su ordine del pubblico ministero, accedendo ai locali in cui si trova l'apparecchio oppure – anche se si rivela essere più complicato da attuare – a distanza, per esempio ricorrendo alla messaggeria elettronica, operazione che potrebbe comportare la necessità di eludere l'intervento di un antivirus. Il GovWare in questione è specialmente concepito e configurato per il computer interessato tenendo conto degli ordini del pubblico ministero sulle informazioni ricercate (p. es. telefonia via Internet, esclusi i siti consultati o le immagini ottenute mediante la webcam integrata nel computer). Tale configurazione su misura rende arduo nonché molto oneroso ricorrere a un GovWare. Di regola l'impiego efficace e mirato di un GovWare necessita preliminarmente l'attuazione di una sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni di tipo tradizionale ai sensi dell'articolo 269 CPP, come pure un'analisi dell'ambiente sociale della persona interessata (in particolare nel caso in cui svariate persone condividono la medesima connessione a Internet), al fine di evitare di sorvegliare il traffico delle telecomunicazioni di una persona diversa dall'interessato. Il GovWare è dunque in grado di effettuare esattamente quello che gli si chiede di fare e nulla più di questo. Esso trasmette i dati ottenuti su un server utilizzato dalle autorità di perseguimento penale mediante il collegamento della persona oggetto di sorveglianza. La polizia, operando sotto il controllo del pubblico ministero, può attivare il funzionamento del programma, prolungarlo previa approvazione del giudice dei provvedimenti coercitivi nonché disattivarlo – nel caso in cui la sua disattivazione automatica non sia stata prevista –, senza che il GovWare si propaghi. La polizia, sempre operando sotto il controllo del pubblico ministero e con l'approvazione del giudice dei provvedimenti coercitivi, può estendere una sorveglianza in corso ad altri tipi di dati diversi da quelli inizialmente sottoposti a sorveglianza. Il funzionamento del GovWare dipende dunque dalla sua configurazione. Il programma può e deve essere configurato in modo tale da consentire di ottenere solamente i dati del traffico delle telecomunicazioni senza che sia possibile accedere all'insieme dei dati contenuti nel computer preso di mira, ciò che esclude la messa in atto di una perquisizione online di tale apparecchio. Un'azienda esterna, responsabile della configurazione del GovWare, non è in grado di accedere ai dati ottenuti durante la sorveglianza. Alla stessa stregua, la persona titolare del server utilizzato dall'autorità inquirente per attuare la sorveglianza mediante un GovWare non è in grado di leggere i dati ottenuti, essendo infatti soltanto in condizione di rilevare il trasferimento di dati. Le caratteristiche del GovWare, specialmente la circostanza che esso viene elaborato su misura per l'apparecchio interessato e che il suo impiego è limitato nel tempo, implica che soltanto difficilmente potrebbe venir copiato e integrato poi in un altro computer. Dirottare un GovWare richiederebbe infatti approfondite conoscenze e molto tempo. Sarebbe inoltre molto più agevole per un malintenzionato procurarsi per un importo decisamente modico un «cavallo di Troia» già disponibile sul mercato. Per di più, il ricorso a un GovWare

non rappresenta un pericolo per la rete visto che non implica la manipolazione degli elementi che compongono quest'ultima.

Gli specialisti contattati giungono alla conclusione che non è possibile produrre e mantenere dei GovWare in grado di funzionare correttamente in tutte le situazioni, ossia senza condizionare altri programmi o funzioni; essi precisano tuttavia che, secondo i test effettuati, è possibile impiegare siffatti programmi senza che si verifichino danni riscontrabili immediatamente. Sotto il profilo tecnico, il ricorso al programma utilizzato dalle autorità di perseguimento penale non può (ancora) probabilmente venire limitato alla sola sorveglianza della comunicazione: l'accesso furtivo reso possibile dal GovWare consente tecnicamente agli inquirenti di accedere all'insieme dei dati e delle informazioni contenute nel computer; qualsivoglia dato sul sistema o sull'utente può essere copiato, modificato, cancellato o aggiunto all'insaputa del detentore dell'apparecchio. Tale accesso furtivo provoca inoltre una falla nel sistema del computer che può venir sfruttata anche da terzi[84].

Per raggiungere l'obiettivo principale della revisione della LSCPT, che non consiste nell'estendere la sorveglianza bensì nell'adeguarne i metodi all'evoluzione tecnica nel settore delle telecomunicazioni, il nostro Collegio è del parere che sia indispensabile consentire alle autorità inquirenti di utilizzare i GovWare. La decisione contraria indebolirebbe notevolmente l'efficacia della lotta contro la criminalità. Una forma di criptaggio che non può essere soppressa dai fornitori di servizi di telecomunicazione impedisce in effetti la sorveglianza del traffico delle telecomunicazioni con le misure di sorveglianza classiche poiché i dati così ottenuti sono illeggibili. Questo genere di criptaggio è già oggi utilizzato in particolare nell'ambito della telefonia via Internet, molto diffusa e in continua espansione a scapito della telefonia classica. Queste falle della sorveglianza sono note ai delinquenti che ne approfittano. Il ricorso ai GovWare consente di ovviare a questo problema: infatti invece di deviare i dati durante la loro trasmissione, come nel caso delle misure di sorveglianza della corrispondenza o del traffico delle telecomunicazioni classiche, i GovWare permettono d'intercettare i dati alla fonte, prima che siano criptati[85]. Inoltre con la progressiva estensione nei prossimi anni dei nuovi elementi d'indirizzo (indirizzi IPv6), la sorveglianza delle comunicazioni via Internet, compresa la telefonia via Internet, sarà notevolmente complicata o diverrà impossibile da realizzare con le misure di sorveglianza del traffico delle telecomunicazioni classiche di cui all'articolo 269 CPP. In effetti, questo nuovo sistema agevola l'utilizzazione di protocolli di criptaggio come per esempio l'IPSec. Inoltre, vi è attualmente un incremento della tendenza a criptare le comunicazioni (p. es. https). Ne risulta dunque che il criptaggio si espanderà considerevolmente. Il ricorso ai GovWare consente di evitare che la sorveglianza sia elusa grazie a Internet e al criptaggio dei dati. Considerato quanto precede, non consentire alle autorità inquirenti di far capo ai GovWare significherebbe limitare notevolmente la sorveglianza della telefonia via Internet e, più in generale, la sorveglianza, attualmente possibile dal profilo tecnico, del traffico via Internet, il che sarebbe inconciliabile con l'obbiettivo della revisione della LSCPT in corso.

84 Sabine Gless, Strafverfolgung im Internet, Revue Pénale Suisse, vol. 130 [2012], pag. 12, 17 seg.; Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 2 seg. (in particolare nota 5) e 10.

85 Cfr. per maggiori ragguagli Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 5–9

In considerazione di quanto precede e dopo aver ponderato i diversi interessi, il nostro Consiglio ha deciso di proporre nel presente disegno la creazione di una base legale esplicita che consenta l'impiego di GovWare alle autorità inquirenti. Proponiamo che il ricorso ai GovWare sia consentito soltanto per il perseguimento dei reati di cui all'articolo 286 capoverso 2 CPP, e non di tutti i reati menzionati nel catalogo più esteso dell'articolo 269 capoverso 2 CPP, applicabile alle misure di sorveglianza tradizionali del traffico delle telecomunicazioni (cfr. cpv. 1 lett. b e il pertinente commento). Inoltre il nostro Collegio propone che l'impiego dei GovWare sia sussidiario alle altre misure di sorveglianza classiche del traffico delle telecomunicazioni; beninteso va fatto salvo il principio della proporzionalità (cfr. cpv. 1 lett. c e il pertinente commento). Sotto il profilo giuridico occorre pertanto garantire che la sorveglianza si limiti ai dati relativi alla comunicazione. Le regole proposte intendono fornire questa garanzia, menzionando come campo di applicazione materiale dei GovWare il «contenuto delle comunicazioni e i dati secondari delle telecomunicazioni»; la perquisizione online è vietata[86]. È pure escluso che il GovWare utilizzi la webcam o il microfono per scopi diversi dalla sorveglianza del traffico delle telecomunicazioni (cfr. cpv. 3 e il pertinente commento). Solide garanzie legali consentono inoltre di proteggere ogni interessato contro gli abusi potenziali risultanti all'impiego di GovWare. Infatti per poter impiegare i GovWare è previsto che l'autorità competente (giudice dei provvedimenti coercitivi) approvi l'ordine di sorveglianza (art. 274 CPP). Di sopraggiunta le informazioni ottenute in violazione dei limiti applicabili, per esempio nell'ambito di una perquisizione online, e non connesse con dati concernenti esclusivamente il traffico delle telecomunicazioni non possono in alcun caso essere impiegate come mezzo di prova e vanno distrutte (cpv. 3 e art. 141 cpv. 1 e art. 277 CPP). Inoltre, l'interessato può presentare ricorso contro la sorveglianza mediante GovWare ordinata nei suoi confronti (art. 279).

Il ricorso ai GovWare nel senso illustrato sopra è da preferire alle alternative teoricamente possibili e in grado di perseguire il medesimo scopo. Ipotizzabile sarebbe istituire un obbligo dei fornitori di servizi Internet, che consentono la telefonia via Internet, di fornire alle autorità inquirenti, tramite il Servizio, i dati, segnatamente quelli di comunicazione, delle persone che ricorrono al loro programma per comunicare telefonicamente via Internet, operando un'analogia con l'obbligo dei fornitori di servizi di telecomunicazione. Tuttavia un siffatto obbligo sarebbe molto difficile se non addirittura impossibile da attuare nella pratica. In particolare non terrebbe conto dell'offerta di alcuni fornitori di servizi Internet, ossia un programma scaricabile gratuitamente da Internet e che consente di telefonare (in modo criptato) via Internet, mettendo in comunicazione gli ordinatori (peer-to-peer), senza passare da una centrale gestita da un fornitore di servizi Internet, con la conseguenza che quest'ultimo non è in possesso dei dati menzionati sopra e non può dunque fornirli alle autorità inquirenti. Tale obbligo non terrebbe neppure conto della circostanza che la maggioranza di questo tipo di fornitori di servizi Internet risiede all'estero rendendo dunque la sua portata del tutto vana. Un'altra alternativa all'impiego dei GovWare potrebbe consistere nell'obbligare tutte le imprese, che consentono di criptare il traffico delle telecomunicazioni, a fornire le loro chiavi di criptaggio al fine di essere in grado di decriptare queste comunicazioni. Tale obbligo non può tuttavia ignorare che anche detti fornitori di servizi Internet hanno la loro sede prevalentemente all'estero, la qual cosa lo svuoterebbe di senso.

86 Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 21.

Il disciplinamento dell'impiego di GovWare nel CPP e non nella LSCPT accoglie quanto richiesto al numero 2 delle mozioni Schmid-Federer 10.3831 (Revisione della LSCPT), Eichenberger 10.3876 (Revisione della LSCPT) e (von Rotz) Schwander 10.3877 (Revisione della LSCPT), secondo cui gli aspetti inerenti al perseguimento penale non devono figurare nella LSCPT. Per quanto concerne la classificazione sistematica in seno al CPP di tale disciplinamento, due sezioni entrano in linea di conto: quella relativa alla «sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni» (art. 269 segg. CPP) e quella relativa alla «sorveglianza mediante apparecchi tecnici di sorveglianza» (art. 280 seg. CPP). A tal proposito va osservato quanto segue: impiegando un GovWare, si penetra in un sistema di trattamento dei dati (computer) e lo si manipola, ciò che non è il caso con le misure di sorveglianza di cui all'articolo 269 CPP, con le quali ci si limita a «deviare» i dati al momento della loro trasmissione o a richiederli a un fornitore di servizi (di telecomunicazione). Inoltre l'utilizzazione di un GovWare non necessita della collaborazione di un fornitore di servizi di telecomunicazione e quest'ultimo non svolge alcun ruolo particolare in tale contesto. Sotto il profilo della sistematica, la base legale che consente di ricorrere ai GovWare va comunque inserita negli articoli 269 e seguenti CPP, e non negli articoli 280 e seguenti CPP. Ciò in considerazione del fatto che il loro impiego si limita unicamente alla sorveglianza del traffico delle telecomunicazioni, e non deve consentire anche la sorveglianza, per esempio, di una stanza mediante la webcam del computer. Va precisato che gli articoli 269–279 CPP si applicano all'impiego di GovWare ai sensi dell'articolo 269ter CPP, salvo disposizioni contrarie previste in tale norma.

Il *capoverso 1 lettera a* non rinvia all'articolo 269 capoverso 2 CPP visto che i reati per i quali è possibile una sorveglianza del traffico delle telecomunicazioni mediante GovWare sono diversi da quelli per i quali è ammessa una sorveglianza tradizionale retta dall'articolo 269 CPP (cfr. lett. b e il relativo commento).

Tenuto conto della natura particolarmente aggressiva della sorveglianza mediante GovWare, il nostro Collegio, accogliendo alcune critiche formulate in occasione della procedura di consultazione, propone quanto segue: contrariamente a quanto prevedeva l'avamprogetto, è consentito fare ricorso ai GovWare soltanto per i reati menzionati nell'elenco di cui all'articolo 286 capoverso 2 CPP, applicabile all'inchiesta mascherata, e non per tutti quei reati menzionati nell'elenco più esteso di cui all'articolo 269 capoverso 2 CPP, applicabile alle misure di sorveglianza classiche della corrispondenza postale e del traffico delle telecomunicazioni. Tuttavia tale restrizione, formulata nel *capoverso 1 lettera b*, non è incontestata. In particolare si rileva che, quando l'impiego di un GovWare si rende necessario, l'ingerenza nei diritti fondamentali dell'interessato è più grave rispetto a quando si ricorre a una sorveglianza attuata mediante la procedura convenzionale, ossia tramite un fornitore di servizi di telecomunicazione ai sensi degli articoli 269 e seguenti CPP; infatti si ritiene[87] che se ne dovrebbe tenere conto nell'applicazione del principio della proporzionalità ai sensi dell'articolo 269 capoverso 1 lettera b CPP. La restrizione citata implica segnatamente che se, nell'ambito di una sorveglianza mediante GovWare, vengono raccolte informazioni relative a reati che figurano nel catalogo dell'articolo 269 capoverso 2 CPP, ma non in quello dell'articolo 286 capoverso 2 CPP, esse non potranno essere utilizzate (art. 141 cpv. 1 e 278 CPP).

87 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 25.

Sempre in considerazione della natura dell'impiego dei GovWare, il *capoverso 1 lettera c* dispone che l'utilizzo di GovWare è sussidiario alle misure tradizionali di sorveglianza del traffico delle telecomunicazioni di cui all'articolo 269 CPP, dato che queste ultime sono già sussidiarie rispetto alle operazioni d'inchiesta classiche (art. 269 cpv. 1 lett. c CPP). Beninteso va fatto salvo il principio della proporzionalità (art. 269 cpv. 1 CPP). Così facendo è possibile garantire che questo tipo di sorveglianza sarà utilizzato soltanto se veramente necessario. Inoltre va evidenziato che l'elevato costo per l'impiego di un GovWare impone che esso venga utilizzato con particolare attenzione. In tale contesto è opportuno rammentare che per impiegare efficacemente un GovWare deve in linea di massima essere preceduto dall'impiego di una misura tradizionale di sorveglianza del traffico delle telecomunicazioni.

L'obbligo del pubblico ministero, discendente dal *capoverso 2 lettera a*, di indicare nell'ordine di sorveglianza quale tipo di dati vuole ottenere, contribuisce al controllo (da parte del giudice dei provvedimenti coercitivi) del rispetto del divieto di tentare di ottenere dati diversi da quelli concernenti esclusivamente il traffico delle telecomunicazioni[88], in particolare mediante una perquisizione online (cfr. cpv. 3 e il pertinente commento).

Per quanto concerne l'obbligo del pubblico ministero, previsto dal *capoverso 2 lettera b,* di indicare nell'ordine di sorveglianza se sia necessario penetrare in un locale non accessibile al pubblico per introdurre nel sistema di trattamento dei dati interessato gli speciali programmi informatici, esso intende rendere attento il giudice dei provvedimenti coercitivi a questa modalità di esecuzione, affinché possa all'occorrenza autorizzarla esplicitamente conformemente all'articolo 274 capoverso 4 lettera c CPP (cfr. anche il commento dell'art. 274 cpv. 4 lett. c CPP).

Il *capoverso 3* esclude in particolare che si possano utilizzare i mezzi di prova ottenuti in occasione della perquisizione online di un sistema di trattamento dei dati mediante un GovWare che consente di accedere all'integralità dei dati potenzialmente facenti parte della sfera intima, contenuti nel computer interessato. Pure escluso è l'utilizzo dei mezzi di prova ottenuti mediante un GovWare dalla webcam o dal microfono integrati in un computer per scopi diversi dalla sorveglianza del traffico delle telecomunicazioni, ad esempio per sorvegliare una stanza. Infatti secondo il capoverso 1, i GovWare possono essere impiegati soltanto per ottenere dati che riguardano il traffico delle telecomunicazioni. Una perquisizione online appare dunque già esclusa dall'articolo 247 CPP, secondo cui l'interessato deve essere messo al corrente della perquisizione visto che l'impiego di un GovWare ha senso soltanto all'insaputa della persona interessata. L'obbligo del pubblico ministero, previsto dal capoverso 2 lettera a, di indicare nell'ordine di sorveglianza il tipo di dati ricercati contribuisce al controllo del rispetto del divieto di raccogliere dati diversi da quelli riguardanti esclusivamente il traffico delle telecomunicazioni, segnatamente mediante una perquisizione online[89]. I dati raccolti in violazione di tale divieto non possono essere utilizzati (art. 141 cpv. 1 e 277 CPP)[90].

Il postulato della Commissione degli affari giuridici del Consiglio nazionale 11.4042 (Sorveglianza tramite cavalli di Troia [1]) incarica il nostro Collegio di esaminare la necessità di adeguare la normativa vigente riguardante l'utilizzo di GovWare e di

88 Sylvain Métille, op. cit., n. 33 e 38.
89 Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, Jusletter 5.12.2011, n. 21; Sylvain Métille, op. cit., n. 35 e 40.
90 Sylvain Métille, op. cit., n. 33 e 38.

stilare un pertinente rapporto. Per quanto concerne invece il postulato della Commissione degli affari giuridici del Consiglio nazionale 11.4043 (Sorveglianza tramite cavalli di Troia [2]), esso ci incarica di stilare un rapporto sull'utilizzo degli strumenti di sorveglianza elettronica, in particolare i «cavalli di Troia», nonché sulle basi legali e le condizioni generali del loro impiego. Tale rapporto deve illustrare la situazione a livello federale e, all'occorrenza, cantonale. Le argomentazioni esposte in precedenza rispondono alle richieste formulate da questi postulati.

Art. 270, frase introduttiva e lett. b n. 1

Adeguamenti di natura terminologica sono attuati nella *frase introduttiva* e nella *lettera b numero 1* per tenere conto dei nuovi concetti utilizzati nel disegno della LSCPT. La nozione di «collegamento», a dipendenza del contesto, è sostituita con la nozione di «servizio» o di «corrispondenza» (cfr. il commento dell'art. 17 D-LSCPT).

Il testo francese vigente contempla soltanto la ricezione di invii postali e di comunicazioni da parte dell'imputato tramite l'indirizzo postale o il collegamento di telecomunicazione di terzi. Il testo è troppo restrittivo e deve includere anche la spedizione di invii postali e di comunicazioni da parte dell'imputato tramite l'indirizzo postale o il collegamento di telecomunicazione di terzi, come si evince dalla versione tedesca e da quella italiana. Il testo francese è stato dunque opportunamente adeguato.

Art. 271

L'*articolo 271* è precisato e completato.

Si propone di non riprendere la versione del *capoverso 1* posto in consultazione e di mantenere la formulazione attuale completandola (cfr. *infra*). Infatti quest'ultima è chiara, mentre quella posta in consultazione potrebbe indurre a pensare che neppure la valutazione dei dati, che in seguito alla cernita non sono stati scartati, può essere effettuata dalle autorità di perseguimento penale. La cernita potrà svolgersi sotto la direzione di un giudice, con l'impiego di misure tecniche che consentano, ad esempio, di conservare soltanto la corrispondenza con determinati corrispondenti o collegamenti selezionati. Non vi è motivo di conservare nel fascicolo informazioni che non hanno alcun nesso con l'inchiesta e che sono sottoposte al segreto professionale. Il *capoverso 1* va dunque completato e deve prevedere, esattamente come fa il capoverso 3, sia la distruzione di tali dati sia il divieto di utilizzarli.

Il *capoverso 2* si rifà all'attuale capoverso 2. Il caso previsto da quest'ultimo è tuttavia contemplato da un punto di vista più logico, poiché il *capoverso 2* deve stabilire un'eccezione rispetto al capoverso 1, che sancisce il principio della necessità della cernita delle informazioni raccolte nell'ambito della sorveglianza. Se sono soddisfatte le condizioni cumulative del capoverso 2, la cernita menzionata al capoverso 1 non deve essere effettuata. Nella fattispecie, ciò significa che, da una parte, le autorità inquirenti possono accedere direttamente alle informazioni raccolte servendosi del sistema informatico gestito dal Servizio e che, dall'altra, la sorveglianza può essere eseguita con un collegamento diretto. Le caratteristiche del collegamento diretto – da non confondere con la sorveglianza in tempo reale – rendono infatti materialmente impossibile la cernita prevista dal capoverso 1. Per ulteriori dettagli si rinvia all'articolo 17 lettera c D-LSCPT e al pertinente commento. Si rammenta che,

ai sensi del *capoverso 2 lettera a*, il collegamento diretto è possibile solo se la persona vincolata dal segreto professionale è sorvegliata in quanto imputato e non in quanto terzo ai sensi dell'articolo 270 lettera b CPP. *Secondo* quanto fatto valere a giusto titolo durante la consultazione, l'interesse dei clienti, dei pazienti ecc., alla protezione del segreto professionale sussiste sia nel caso del *capoverso 2* sia in quelli dei capoversi 1 e 3. Visto che la fattispecie del *capoverso 2* è un caso particolare della situazione di cui al capoverso 1, le informazioni senza un nesso diretto con l'indagine e sottoposte al segreto professionale non vanno conservate nel fascicolo; esse vanno distrutte e il loro utilizzo è vietato conformemente a quanto previsto dal capoverso 1.

Il *capoverso 3* è integrato in modo da tenere meglio conto di quanto avviene nella realtà. Alla stessa stregua del capoverso 1 occorre evitare che le autorità di perseguimento penale vengano a conoscenza di informazioni coperte dal segreto professionale. La cernita svolta sotto la direzione di un giudice concerne esclusivamente informazioni raccolte durante la sorveglianza di invii e comunicazioni con le persone menzionate agli articoli 170–173 CPP. Le informazioni riguardanti comunicazioni con persone che non presentano tali caratteristiche non sono oggetto di siffatta cernita[91].

Art. 272 cpv. 2, primo periodo, e cpv. 3

Adeguamenti di carattere terminologico; si veda in merito il commento all'articolo 270, frase introduttiva e lettera b numero 1.

Art. 273 Identificazione degli utenti, localizzazione e caratteristiche tecniche della corrispondenza

La *rubrica* di questa disposizione è adeguata al suo tenore.

La nozione di dati secondari secondo il *capoverso 1* viene semplificata rispetto a quella vigente, senza modificare il suo tenore materiale (cfr. commento agli art. 19 cpv. 1 lett. b e 26 cpv. 1 lett. b D-LSCPT). Va rilevato che l'informazione relativa alla durata della corrispondenza («per quanto tempo») è rilevante soltanto per il traffico delle telecomunicazioni, e non per gli invii postali (cfr. il tenore dell'art. 19 cpv. 1 lett. b D-LSCPT).

Il *capoverso 3* estende da sei a dodici mesi il periodo durante il quale è possibile chiedere con effetto retroattivo i cosiddetti dati secondari. Questa estensione mira a un perseguimento più efficace dei reati e ha come corollario l'estensione della durata di conservazione dei dati secondari (art. 19 cpv. 4 e art. 26 cpv. 5 D-LSCPT). Per ulteriori dettagli si rinvia al commento riguardante gli articoli 19 capoverso 4 e 26 capoverso 5 D-LSCPT.

91 Laurence Aellen/Frédéric Hainard, Secret professionnel et surveillance des télécommunications, Jusletter 23.3.2009, n. 21 segg.; Nathalie Zufferey/Jean-Luc Bacher, Commentaire romand: Code de procédure pénale suisse, Basilea 2011, n. 18 ad art. 271 CPP.

Art. 274 cpv. 4

L'*articolo 274 capoverso 4 lettera a* è adeguato alla nuova versione dell'articolo 271.

L'autorizzazione esplicita prevista dall'*articolo 274 capoverso 4 lettera b* trova la sua giustificazione nel carattere particolarmente aggressivo del fatto di penetrare in un locale non accessibile al pubblico all'insaputa dell'interessato per introdurre un GovWare nel sistema di trattamento dei dati (ad es. computer) che si trova in quel locale. Un GovWare può venir introdotto in un sistema di trattamento dei dati anche a distanza per esempio attraverso una e-mail (cfr. pure il commento dell'art. 269ter). Affinché il giudice dei provvedimenti coercitivi sia messo al corrente di questa modalità d'esecuzione, il pubblico ministero sarà tenuto a indicarlo conformemente all'articolo 269ter capoverso 2 lettera b (cfr. pure il commento dell'art. 269ter cpv. 2 lett. b).

Art. 278 cpv. 1bis

Il rinvio che figura nell'*articolo 278 capoverso 1bis* è modificato e completato. Il rinvio all'articolo 3 della LSCPT vigente è sostituito con il rinvio all'articolo 35 D-LSCPT. Occorre inoltre rinviare anche all'articolo 36 D-LSCPT, dal momento che esso, come l'articolo 35 D-LSCPT, non contempla i procedimenti penali in corso (cfr. commento dell'art. 36 D-LSCPT) e che anche in una situazione del genere sono possibili scoperte casuali.

Art. 279 cpv. 3, primo periodo

Adeguamenti di carattere terminologico; si veda in merito il commento dell'articolo 270, frase introduttiva e lettera b numero 1.

Procedura penale militare del 23 marzo 1979[92]

Art. 70bis (nuovo) Utilizzazione di speciali dispositivi tecnici per la sorveglianza del traffico delle telecomunicazioni

Si veda per analogia il commento dell'articolo 269bis CPP.

Art. 70ter (nuovo) Utilizzazione di speciali programmi informatici per la sorveglianza del traffico delle telecomunicazioni

Si veda, per analogia, il commento dell'articolo 269ter CPP, salvo per quanto concerne il capoverso 1 lettera b riguardante la limitazione dell'elenco dei reati (e le relative motivazioni). Infatti, conformemente al rinvio contenuto all'articolo 73*a* capoverso 1 lettera a PPM, l'elenco applicabile all'inchiesta mascherata è in linea di massima il medesimo di quello applicabile alla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, fatto tuttavia salvo l'articolo 73*a* capoverso 2 PPM, il cui rinvio all'articolo 286 capoverso 2 CPP va ripreso per motivi di coerenza al *capoverso 2bis*.

92 RS **322.1**

Art. 70a, frase introduttiva e lett. b n. 1

Il commento relativo all'articolo 270, frase introduttiva e lettera b numero 1 CPP *si applica per analogia all'articolo 70a, frase introduttiva e lettera b numero 1*.

Art. 70b

L'*articolo 70b* è precisato e completato.

Invece della versione del *capoverso 1* posta in consultazione, si propone di mantenere la formulazione attuale integrandola (cfr. *infra*). Infatti quest'ultima è chiara mentre quella posta in consultazione potrebbe indurre a pensare che neppure la valutazione dei dati, che in seguito alla cernita non sono stati scartati, può essere effettuata dal giudice d'istruzione. La cernita potrà invece svolgersi sotto la direzione del presidente del tribunale militare con l'impiego di misure tecniche che consentano, ad esempio, di conservare soltanto la corrispondenza passata con determinati corrispondenti o collegamenti selezionati. Non vi è motivo di conservare nel fascicolo informazioni che non hanno alcun nesso con l'inchiesta e che sono sottoposte al segreto professionale. Il *capoverso 1* va dunque completato prevedendo, esattamente come lo fa il capoverso 3, sia la distruzione di tali informazioni sia il divieto di utilizzarle.

Il commento relativo all'articolo 271 capoverso 2 CPP si applica per analogia all'*articolo 70b capoverso 2*.

Il commento dell'articolo 271 capoverso 3 CPP si applica per analogia all'*articolo 70b capoverso 3*.

Per il resto il rinvio all'articolo 75 lettere a e c nell'*articolo 70b capoverso 3* è rimpiazzato dal rinvio all'articolo 75 lettera b, cui corrispondono gli articoli 170–173 CPP menzionati nell'articolo 271 CPP; va infatti tracciato un parallelismo tra quest'ultimo e l'*articolo 70b*.

Art. 70c cpv. 2, primo periodo, e 3

Adeguamenti di carattere terminologico; si veda in merito il commento all'articolo 70*a*, frase introduttiva e lettera b numero 1.

Art. 70d Identificazione degli utenti, localizzazione e caratteristiche tecniche della corrispondenza

Il commento relativo all'articolo 273, rubrica, e capoversi 1 e 3 CPP *si applica* per analogia all'*articolo 70d, rubrica, e capoversi 1 e 3*.

Art. 70e cpv. 4

Si veda per analogia il commento dell'articolo 274 capoverso 4 CPP.

Art. 70k Reclamo

Adeguamenti di carattere terminologico; si veda in merito il commento dell'articolo 70*a*, frase introduttiva e lettera b numero 1.

Legge del 30 aprile 1997[93] sulle telecomunicazioni

Art. 6a (nuovo) Blocco dell'accesso ai servizi di telecomunicazione

L'*articolo 6a* impone espressamente ai fornitori di servizi di telecomunicazione di bloccare l'accesso alla telefonia mobile e a Internet in presenza delle condizioni indicate. In tal modo si evita di dover fondare tale obbligo su un'interpretazione estensiva dell'articolo 21 D-LSCPT. Lo scopo di tale obbligo è di contribuire a identificare le persone che accedono alla telefonia mobile o a Internet senza aver sottoscritto un abbonamento, ad esempio per mezzo di carte SIM prepagate, di schede «wireless» prepagate e di mezzi che consentono l'accesso alla rete della telefonia fissa. È in particolare basandosi sulle informazioni ottenute dalle autorità penali, segnatamente dalle autorità di perseguimento penale, che i fornitori di servizi di telecomunicazione procedono al pertinente blocco dell'accesso. Non spetta al Servizio contattare l'UFCOM o tali fornitori affinché questi ultimi effettuino il blocco in questione. Le autorità inquirenti informano tuttavia il Servizio in merito alle circostanze che hanno condotto a un siffatto blocco, affinché quest'ultimo possa verificare se i fornitori di servizi di telecomunicazione hanno attuato le misure per aggiornare il sistema di comunicazione delle domande di informazioni sui servizi di telecomunicazione (cfr. il commento all'art. 21 D-LSCPT). Se tale non fosse il caso, si possono applicare gli articoli 39–41 D-LSCPT.

Per ragioni pratiche, l'obbligo menzionato in precedenza si limita alla situazione in cui un cliente di un fornitore di servizi di telecomunicazione, al momento dell'avvio e della registrazione del rapporto commerciale (cfr. commento all'art. 21 D-LSCPT), ha utilizzato l'identità di una persona inesistente o che non ha acconsentito all'avvio di tale rapporto, o alla situazione in cui il cliente al momento dell'avvio della relazione ha presentato un documento non conforme alle esigenze dell'articolo 23 D-LSCPT, ossia a situazioni che si possono verificare nel caso in cui il controllo preliminare non si sia svolto conformemente a quanto prescritto (cfr. commento dell'art. 23 D-LSCPT). Sarebbe invece eccessivo, anche dal punto di vista dell'ingerenza nella sfera della libertà personale, esigere il blocco dell'accesso alla telefonia mobile e a Internet, sebbene il controllo dell'identità sia stato effettuato come prescritto, nel caso in cui i clienti non dovessero più corrispondere a quelli registrati all'avvio del rapporto commerciale. Un telefono cellulare munito di carta SIM prepagata può, infatti, essere prestato a un conoscente per un periodo più o meno lungo in un contesto del tutto normale, cioè senza che l'apparecchio sia per forza utilizzato a fini illegali. Una regolamentazione più restrittiva imporrebbe, inoltre, ai clienti l'obbligo di aggiornare i dati relativi al rapporto commerciale e ai fornitori di servizi di telecomunicazione l'obbligo di controllare e registrare i clienti che subentrano a quelli registrati inizialmente, il che comporterebbe formalità eccessive e un onere amministrativo ingestibile.

93 RS **784.10**

3 Ripercussioni

3.1 Per la Confederazione

Conformemente all'articolo 38 capoverso 4 D-LSCPT, il Consiglio federale fissa le indennità e gli emolumenti.

I costi che il Servizio dovrà sopportare nell'espletamento delle proprie mansioni legali sono finanziati dagli emolumenti. Visto che oggigiorno il Servizio non riesce a coprire integralmente i propri costi (tasso di copertura per il 2012 pari al 54 %), è inevitabile che la Confederazione debba accollarsi costi effettivi supplementari nel caso in cui il nostro Consiglio rinunciasse ad aumentare in modo sensibile il grado di copertura. Occorre chiedersi se sia opportuno mantenere l'attuale (basso) tasso di copertura dei costi, tenuto conto che il perseguimento penale spetta ai Cantoni.

L'aumento del fabbisogno finanziario e di personale va tuttavia posto in relazione con il miglioramento che la nuova LSCPT comporterà per il perseguimento dei reati.

Le ripercussioni finanziarie del presente disegno, per quel che riguarda il personale del Servizio e i suoi costi di gestione e di investimento, è stimato come segue:

- l'articolo 2 lettere b–f D-LSCPT opera una distinzione dei diversi fornitori di servizi di telecomunicazione con obblighi diversi e comporta un numero molto più elevato di soggetti sottoposti agli obblighi. Il numero di interlocutori del Servizio, che attualmente si aggira sulla cinquantina di fornitori attivi, aumenterà verosimilmente a 150–200. Il Servizio dovrà quindi farsi carico di una maggiore mole di lavoro, che si tradurrà anche in un aumento delle sue attività di picchetto. L'articolo 5 D-LSCPT prevede inoltre che il Servizio sia rappresentato in seno all'organo consultivo che il DFGP può istituire. Tali fattori implicano la necessità di creare un nuovo posto a tempo pieno, costi di gestione supplementari pari a 300 000 franchi all'anno come pure un investimento una tantum pari a 150 000 franchi (in particolare per ampliare e adeguare la rete);
- gli articoli 6–14 D-LSCPT implicano un aumento degli effettivi di 4 posti a tempo pieno, 2,15 milioni di franchi all'anno per costi d'esercizio e 1,6 milioni di franchi per costi d'investimento. Tali cifre sono anzitutto legate alla gestione del nuovo sistema informatico per la conservazione dei dati raccolti nell'ambito delle misure di sorveglianza. Il sistema dovrà infatti garantire la conservazione sicura, a lungo termine e in condizioni ottimali, di una grande quantità di dati. Vi si aggiunga inoltre la messa a disposizione di interfacce con i sistemi informatici delle autorità inquirenti. Gli oneri supplementari tengono segnatamente conto dei costi per l'acquisizione di una nuova infrastruttura, per l'ammortamento di componenti del sistema attuale, per i costi della rete, della rete informatica e delle licenze, dei contratti di assistenza e manutenzione nonché per l'attuazione delle direttive in materia di sicurezza;
- l'articolo 15 capoverso 2 D-LSCPT, l'articolo 16 D-LSCPT e l'articolo 18 D-LSCPT estendono le prestazioni fornite dal Servizio relative alle informazioni e attribuiscono a quest'ultimo nuovi compiti nell'ambito della formazione e dell'attività tecnica nonché nell'ambito del controllo della qualità. Ciò implica la creazione di 3 posti di lavoro a tempo pieno, come pure costi d'esercizio pari a 800 000 franchi all'anno e investimenti pari a 600 000

franchi, per poter da un canto creare e gestire i mezzi necessari alla formazione e, dall'altro, poter attuare i controlli di qualità richiesti;

– i nuovi compiti del Servizio inerenti alla sorveglianza del traffico delle telecomunicazioni, in particolare quelli risultanti dagli articoli 26 capoverso 2, 32 e 33 D-LSCPT implicano la creazione di 4 posti di lavoro a tempo pieno, ai quali si aggiungeranno costi d'esercizio annuali per 500 000 franchi e investimenti una tantum pari a 700 000 franchi. Le disposizioni menzionate in precedenza richiedono un trasferimento degli obblighi da determinati fornitori di servizi di telecomunicazione al Servizio (è il caso dei fornitori che sono stati dispensati integralmente o in parte dai loro obblighi ma sono tenuti a tollerare una sorveglianza da parte del Servizio). A tal fine quest'ultimo deve infatti prevedere le pertinenti infrastrutture di sorveglianza, fornire un maggior numero di prestazioni di supporto esterno, procedere a degli adeguamenti dei sistemi informatici ed effettuare installazioni presso i fornitori di servizi di telecomunicazione interessati. Occorre inoltre tenere conto di un fabbisogno accresciuto di formazione dei collaboratori del Servizio;

– gli articoli 40 e 41 D-LSCPT attribuiscono competenze al Servizio inerenti al diritto in materia di sorveglianza e al diritto penale amministrativo che implicano la creazione di un posto a tempo pieno.

Riassumendo, le ripercussioni finanziarie e in materia di personale del disegno sono stimate come segue:

– creazione di 13 nuovi posti di lavoro a tempo pieno;

– 3,05 milioni di franchi per costi d'investimento;

– aumento di 3,75 milioni di franchi all'anno dei costi d'esercizio (esclusi quelli per il personale).

Occorre ricordare che questa stima dei costi tiene conto soltanto del finanziamento delle misure previste dal profilo qualitativo. Non è invece ancora possibile stimare le eventuali ripercussioni finanziarie derivanti da un aumento quantitativo delle misure di sorveglianza, che potrebbe in teoria risultare da un'estensione del campo di applicazione.

3.2 Per i Cantoni

L'evoluzione futura dei costi della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni si ripercuoterà sull'ammontare degli emolumenti.

Il passaggio al nuovo sistema informatico del Servizio per il trattamento dei dati può comportare, per i Cantoni, una riduzione dei costi per l'attrezzatura. Tuttavia, l'aumento dei costi per la Confederazione determinato dall'allungamento dei termini di conservazione dei dati presso il Servizio può incidere sugli emolumenti versati dalle autorità di perseguimento penale, in particolare da quelle dei Cantoni (cfr. n. 2.2). Per quanto riguarda gli emolumenti si veda il commento in merito all'articolo 38 D-LSCPT.

3.3 Ripercussioni economiche

Il presente disegno genererà costi supplementari per le persone obbligate a collaborare ai sensi della LSCPT. Tuttavia, in particolare per quanto concerne i fornitori di servizi di telecomunicazione, tale aumento va relativizzato dato che il costo della sorveglianza rappresenta una quota molto limitata della loro cifra d'affari. L'aumento va relativizzato anche in considerazione del fatto che la nuova LSCPT permetterà di perseguire i reati con maggiore efficacia. A tal proposito va rammentato che ai sensi dell'articolo 26 capoverso 6 D-LSCPT il nostro Collegio potrà dispensare da alcuni obblighi legali i fornitori di servizi di telecomunicazione, in particolare quelli che offrono servizi di scarsa importanza economica o che operano nel settore dell'educazione, ciò che comporterà una diminuzione dei costi a loro carico.

4 Programma di legislatura

Il presente disegno è annunciato nel messaggio del 25 gennaio 2012[94] sul programma di legislatura 2011–2015.

5 Aspetti giuridici

La nuova LSCPT si fonda sugli articoli 92 capoverso 1 e 123 capoverso 1 della Costituzione federale, che attribuiscono alla Confederazione la competenza rispettivamente in materia di servizi postali e di telecomunicazione e in materia di legislazione relativa al diritto penale e alla procedura penale.

La nuova LSCPT non pone problemi per quanto riguarda il diritto costituzionale e nell'ottica del diritto internazionale.

L'articolo 13 capoverso 1 Cost., l'articolo 8 paragrafo 1 CEDU e l'articolo 17 paragrafo 1 del Patto internazionale del 16 dicembre 1966[95] relativo ai diritti civili e politici garantiscono il segreto postale e delle telecomunicazioni, ossia il diritto alla protezione della corrispondenza nonché delle relazioni stabilite mediante la corrispondenza postale e il traffico delle telecomunicazioni. Tale diritto è un aspetto rilevante della protezione della sfera privata. La sorveglianza della corrispondenza e delle relazioni stabilite mediante la posta e le telecomunicazioni costituisce una lesione grave dei diritti fondamentali. Secondo l'articolo 36 Cost. e l'articolo 8 CEDU la restrizione di un diritto fondamentale deve avere una base legale, essere giustificata da un interesse pubblico ed essere proporzionata allo scopo. Inoltre i diritti fondamentali sono intangibili nella loro essenza. Le misure di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni vanno quindi precisate in una legge in senso formale. In linea di principio un'ingerenza grave richiede una base legale in senso formale chiara e precisa. La comprensibilità della legge esige che la sua formulazione sia sufficientemente precisa, affinché i soggetti di diritto interessati siano in grado di prevedere le conseguenze di un determinato

94 FF **2012** 305
95 RS **0.103.2**

atto e possano all'occorrenza rivolgersi a uno specialista[96]. Le garanzie minime legali contro l'abuso di potere che ai sensi dell'articolo 8 CEDU la legge deve prevedere sono le seguenti: la natura dei reati che possono fondare un ordine di sorveglianza, la definizione delle categorie di persone che possono essere oggetto di sorveglianza, la limitazione temporale dell'esecuzione della misura, la procedura da seguire per l'esame, l'utilizzazione e la conservazione dei dati raccolti, le misure precauzionali da adottare per trasmettere i dati ad altre parti e le condizioni alle quali si possono o si devono cancellare o distruggere le registrazioni[97]. La nuova LSCPT soddisfa le condizioni menzionate poc'anzi.

Sono parimenti soddisfatte le esigenze della Convenzione del Consiglio d'Europa del 23 novembre 2001[98] sulla cibercriminalità.

La nuova LSCPT contiene deleghe legislative al Consiglio federale e ai Cantoni.

96 DTF **123** I 112, consid. 7a.
97 Cfr. anche le sentenze della corte EDU *Kopp vs Svizzera* del 25 marzo 1998, par. 64 e 72, Raccolta 1998-II e *Liberty e altri vs Regno Unito* del 1 ottobre 2008, ricorso n. 58243/00, par 59 segg. (con ulteriori rinvii).
98 RS **0.311.43**