00.000

Rapporto esplicativo relativo all'avamprogetto di modifica della legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)

Compendio

Gli importanti progressi tecnologici compiuti negli ultimi anni nel campo delle telecomunicazioni, in particolare per quanto riguarda Internet, aprono agli utenti un ampio spazio di libertà che offre molteplici possibilità di interazione e consente di scambiare in modo semplice e rapido un'ingente quantità di informazioni a costi relativamente bassi e con discrezione. Nella grande maggioranza dei casi questo spazio di libertà è utilizzato con consapevolezza sia dai privati sia dalle imprese. Tuttavia, è anche sfruttato a fini riprovevoli. Infatti, le nuove tecnologie attualmente a disposizione del grande pubblico, in particolare quelle di Internet (ad esempio la telefonia via Internet), possono essere utilizzate, allo stesso modo dei mezzi di comunicazione classici, per commettere reati soprattutto nel settore della pornografia infantile, della criminalità organizzata e degli stupefacenti. L'accesso a queste nuove tecnologie può facilitare la commissione di tali reati. È dunque essenziale dotarsi di strumenti per proteggersi e lottare contro la delinquenza, senza però pregiudicare gli incontestabili effetti positivi di queste tecnologie. L'obiettivo principale della revisione della legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) è quello di permettere di sorvegliare le persone seriamente sospettate di commettere reati gravi. Occorre inoltre garantire l'ordine e la sicurezza pubblici con il fine ultimo di proteggere i cittadini e rendere sicuro l'utilizzo di queste tecnologie. Si tratta dunque di lottare contro gli abusi, senza tuttavia sorvegliare chi tiene un comportamento conforme alla legge, esattamente come con la vecchia LSCPT: la libertà personale rimane dunque salvaguardata. Un altro obiettivo importante è la sorveglianza al di fuori di un procedimento penale per ritrovare una persona scomparsa, quando, viste le circostanze, si teme che la sua salute o la sua vita siano gravemente in pericolo.

La revisione si prefigge di adattare la LSCPT all'evoluzione tecnologica degli ultimi anni. Si tratta infatti di garantire che la sorveglianza non venga evitata utilizzando nuove tecnologie, né ora né nei prossimi anni. In sostanza, l'obiettivo non è quello di permettere di incrementare la sorveglianza, bensì di migliorarla.

Il Codice di diritto processuale penale (CPP), che è stato approvato dal Parlamento il 5 ottobre 2007 ed entrerà in vigore il 1° gennaio 2011, armonizza le disposizioni procedurali valide per la Confederazione e i Cantoni. Quelle contenute nella vecchia LSCPT sono quindi state abrogate e trasposte nel CPP. L'obiettivo perseguito dalla revisione della LSCPT ha reso necessarie modifiche e integrazioni non solo delle disposizioni di tale legge, ma anche delle disposizioni procedurali relative alla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, che sono state inserite nel nuovo CPP.

La revisione modifica la struttura della LSCPT e introduce una sistematica migliore, soprattutto per evitare le ripetizioni ed eliminare le disposizioni che non dovrebbero figurare in un legge, bensì in un'ordinanza. Alcuni articoli vengono precisati e completati. La numerazione degli articoli è nuova.

La revisione proposta prevede una definizione più precisa ed esauriente delle persone sottoposte alla LSCPT, ossia dei soggetti che effettuano la sorveglianza (della corrispondenza postale e del traffico delle telecomunicazioni) in virtù di detta legge. Inoltre, per quanto riguarda la gestione del sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni

da parte del servizio incaricato della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, dipendente dalla Confederazione (Servizio), la revisione proposta introduce nella LSCPT disposizioni che soddisfano i requisiti esistenti in materia di protezione dei dati. Si garantisce poi la possibilità di ricorrere alla sorveglianza per ricercare una persona condannata a una pena detentiva o a una misura privativa della libertà in base a una sentenza passata in giudicato. Si chiariscono e si completano i compiti attribuiti al Servizio e gli obblighi dei soggetti sottoposti alla LSCPT. In particolare si permette di installare nei sistemi di comunicazione determinati programmi informatici che rendono possibile la sorveglianza. Il periodo per il quale le autorità inquirenti possono richiedere retroattivamente i cosiddetti dati secondari viene aumentato da sei a dodici mesi e, di conseguenza, viene prolungata di altrettanto anche la durata della conservazione obbligatoria di tali dati. La nuova LSCPT propone anche un adattamento delle norme in materia di salvaguardia del segreto professionale nell'ambito della sorveglianza. Conformemente a quanto previsto dalla LSCPT nella versione derivante dal Programma di consolidamento (PCon) 2011-2013 posto in consultazione il 14 aprile 2010 dal Consiglio federale, la nuova legge non prevede più un'indennità a favore di soggetti che effettuano la sorveglianza in virtù di detta legge – in particolare i fornitori di servizi di telecomunicazione – per le attività svolte nell'ambito della sorveglianza (cfr. n. 1.4.6). Vengono poi introdotte nuove disposizioni penali applicabili ai soggetti sottoposti alla LSCPT che non rispettano i loro obblighi e una disposizione concernente la sorveglianza amministrativa. Infine, l'avamprogetto disciplina i rimedi giuridici contro le decisioni del Servizio e specifica i ricorsi ammissibili.

Indice

1 Punti essenziali del progetto

1.1 Situazione iniziale

Negli ultimi anni le telecomunicazioni, e in particolare Internet, hanno conosciuto importanti progressi tecnologici, aprendo agli utenti un ampio spazio di libertà che offre molteplici possibilità di interazione e consente di scambiare in modo semplice e rapido un'ingente quantità di informazioni a costi relativamente bassi e con discrezione. Nella grande maggioranza dei casi questo spazio di libertà è utilizzato con consapevolezza dai singoli e dalle imprese. Tuttavia, è anche sfruttato da delinquenti con fini riprovevoli. Infatti, le nuove tecnologie attualmente a disposizione del grande pubblico, in particolare quelle di Internet (ad esempio la telefonia via Internet), possono essere utilizzate, allo stesso modo dei mezzi di comunicazione classici, per commettere reati soprattutto nel settore della pornografia infantile, della criminalità organizzata e degli stupefacenti. Queste nuove tecnologie possono facilitare la commissione di reati ed è dunque essenziale dotarsi di strumenti per proteggersi e lottare contro la delinquenza, senza però pregiudicare gli incontestabili effetti positivi di tali tecnologie. L'obiettivo principale della revisione della legge federale del 6 ottobre 2000[1] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) è quello di permettere di sorvegliare le persone seriamente sospettate di commettere reati gravi. Occorre inoltre garantire l'ordine e la sicurezza pubblici con il fine ultimo di proteggere i cittadini e rendere sicuro l'utilizzo di queste tecnologie. Si tratta dunque di lottare contro gli abusi, senza tuttavia sorvegliare chi tiene un comportamento conforme alla legge, esattamente come con la vecchia LSCPT: la libertà personale rimane dunque salvaguardata. Un altro obiettivo importante è quello di poter effettuare la sorveglianza al di fuori di un procedimento penale per ritrovare una persona scomparsa, quando, alla luce delle circostanze, si teme che la sua salute o la sua vita siano gravemente in pericolo.

L’evoluzione tecnologica rende più difficile la sorveglianza del traffico delle telecomunicazioni, in particolare nell’ambito della telefonia via Internet. Al fine di adattare la LSCPT all’evoluzione tecnologica degli ultimi anni, è necessario aggiungere alcuni strumenti a quelli attualmente previsti. È infatti indispensabile evitare, ora come nei prossimi anni, che la sorveglianza venga neutralizzata utilizzando nuove tecnologie. In sostanza, l’obiettivo non è quello di permettere di incrementare la sorveglianza, bensì di migliorarla.

Per garantire la certezza del diritto, è sorta la necessità di specificare in modo più dettagliato ed esauriente le persone sottoposte alla LSCPT, ossia i soggetti che effettuano la sorveglianza (della corrispondenza postale e del traffico delle telecomunicazioni) in virtù di detta legge (soggetti LSCPT). Per quanto riguarda la gestione del sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni da parte del servizio incaricato della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, dipendente dalla Confederazione (Servizio), è emersa inoltre la necessità di introdurre nella LSCPT disposizioni che soddisfino i requisiti esistenti in materia di protezione dei dati. È poi apparso necessario precisare e completare i compiti attribuiti al Servizio e gli obblighi dei soggetti LSCPT.

[1] RS **780.1**

È stata inoltre espressa l'esigenza di poter ricorrere alla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni per ricercare una persona condannata a una pena detentiva o a una misura privativa della libertà in base a una sentenza passata in giudicato.

È anche stato chiesto di aumentare il periodo per il quale le autorità inquirenti possono richiedere retroattivamente i cosiddetti dati secondari e quindi di prolungare anche la durata della conservazione obbligatoria di tali dati.

Sono state inoltre adattate le norme in materia di salvaguardia del segreto professionale nell'ambito della sorveglianza, in particolare nel caso di collegamenti diretti.

È stata pure sollecitata l'introduzione nella LSCPT di una normativa relativa al trattamento dei dati ottenuti dalla sorveglianza disposta e di disposizioni penali applicabili ai soggetti LSCPT che non rispettano i loro obblighi.

Si è infine ritenuto opportuno prendere in considerazione l'inserimento nella LSCPT di una disposizione sulla sorveglianza amministrativa e di un'altra sui rimedi giuridici contro le decisioni del Servizio.

Questi aspetti saranno affrontati in dettaglio nei capitoli successivi (cfr. n. 1.4 e 2).

1.2 Oggetto della nuova legge

L'oggetto della nuova legge corrisponde essenzialmente a quello della legge attualmente in vigore. La nuova LSCPT si prefigge di permettere e disciplinare la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, compreso Internet, in particolare nel contesto di un procedimento penale. Seppure con qualche modifica, la sorveglianza resta possibile anche al di fuori di un procedimento penale (cfr. n. 1.4 e 2). L'obiettivo principale della nuova LSCPT è quello di adattare la legge vigente all'evoluzione tecnologica degli ultimi anni, affinché quest'ultima non impedisca, né ora né nei prossimi anni, la sorveglianza. Lo scopo non è quindi quello di incrementare la sorveglianza, bensì di migliorarla.

La nuova LSCPT specifica meglio, rispetto alla legge vigente, i soggetti cui si applica e i loro obblighi, nonché i compiti del Servizio. Contiene disposizioni che soddisfano i requisiti in materia di protezione dei dati per l'utilizzo da parte del Servizio del sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni. Disciplina inoltre per la prima volta esplicitamente l'installazione nei sistemi di comunicazione di determinati programmi informatici ai fini della sorveglianza.

Conformemente a quanto previsto dalla LSCPT nella versione derivante dal Programma di consolidamento (PCon) 2011-2013[2] posto in consultazione il 14 aprile 2010 dal Consiglio federale, la nuova legge non prevede più un'indennità a favore dei soggetti che effettuano la sorveglianza, in particolare dei fornitori di servizi di telecomunicazione, per le attività svolte in tale ambito. Infine, come novità, la nuova LSCPT statuisce le conseguenze penali e amministrative per i soggetti rientranti nel suo campo di applicazione personale che non rispettano i loro obblighi.

La struttura della LSCPT è stata cambiata, lo schema è più logico e sono state eliminate le ripetizioni. Il sistema previsto, invece, non è stato modificato nei suoi tratti

[2] http://www.admin.ch/ch/f/gg/pc/documents/1854/Vorlage.pdf

fondamentali. Lo stesso dicasi per la struttura e il contenuto degli articoli, che tuttavia sono stati precisati e completati. Nuova è la numerazione degli articoli. In considerazione di quanto precede, saranno commentate in maniera più approfondita solo le modifiche introdotte nella nuova LSCPT.

1.3 Genesi dell'avamprogetto

In marzo 2006, il Consiglio federale ha incaricato il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e della comunicazione (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 indica 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 le disposizioni legali necessarie.

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

1.4 Principali modifiche proposte

1.4.1 Campo d'applicazione

Il campo d'applicazione materiale della nuova LSCPT (art. 1 AP) dev'essere precisato rispetto alla legge attualmente in vigore. Infatti occorre soprattutto tenere conto del ruolo sempre più importante ricoperto da qualche anno da Internet, che costituisce un mezzo di telecomunicazione particolare.

Anche il campo d'applicazione personale della LSCPT (art. 2 AP) dev'essere precisato e completato. Non bisogna infatti dimenticare che, oltre ai fornitori di servizi postali o di telecomunicazione, anche altri soggetti, tra cui i fornitori di accesso a Internet (*access provider*), possono trovarsi in possesso di dati che potrebbero risultare importanti per le autorità inquirenti nella lotta contro la delinquenza. Ciò vale in particolare per i (semplici) *service provider* o *hosting provider*.

1.4.2 Trattamento dei dati personali

La sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni potrebbe riguardare dati sensibili. È quindi opportuno inserire le disposizioni relative al trattamento di tali dati in una legge formale e non soltanto in un'ordinanza. A tal fine, nella nuova LSCPT sono state introdotte disposizioni che soddisfano i requisiti in materia di protezione dei dati per l'utilizzo da parte del Servizio del sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni (sez. 2 art. 6-13 AP). Tali disposizioni riprendono in

parte gli articoli 7-10 dell'ordinanza del 31 ottobre 2001[3] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT). Ciononostante il contenuto degli articoli 6-13 AP è essenzialmente nuovo.

Dal punto di vista della protezione dei dati, il nuovo sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni utilizzato dal Servizio, l'Interception System Schweiz (ISS), completamente operativo per l'entrata in vigore della nuova LSCPT, sarà nettamente migliore rispetto al sistema attuale. Infatti, mentre adesso i dati ottenuti nell'ambito della sorveglianza del traffico delle telecomunicazioni e registrati presso il Servizio sono messi a disposizione delle autorità competenti mediante l'invio per posta dei supporti di dati e dei documenti, con il nuovo sistema tali dati saranno messi a disposizione essenzialmente per mezzo di un diritto d'accesso al sistema informatico gestito dal Servizio, salvo in caso di problemi tecnici (art. 9 cpv. 5 AP). In questo modo potranno essere evitati molti dei rischi relativi alla protezione dei dati insiti nel sistema attuale, come per esempio la perdita (durante l'invio o presso il destinatario) dei dati, le molteplici copie dei dati e la loro conservazione senza grandi precauzioni. Un ulteriore elemento a favore del cambiamento di sistema è il continuo aumento, dovuto all'evoluzione tecnologica, della quantità di dati ottenuti nell'ambito della sorveglianza – con la conseguenza che la loro trasmissione postale su supporti di dati e documenti diventa sempre più problematica e rischiosa. Inoltre, in seguito al rapido progresso tecnologico, è sempre più difficile leggere a lungo termine i supporti di dati (materiale di lettura difficilmente disponibile e condizioni di conservazione sfavorevoli), problema che può essere in gran parte risolto affidando al Servizio la conservazione centralizzata dei dati, potenzialmente per un lungo periodo. A sostegno del cambiamento vi è per di più il fatto che, con il sistema in essere, ogni Cantone deve dotarsi di strumenti costosi per poter trattare i dati ricevuti, con i relativi svantaggi economici. Una volta che, grazie al nuovo sistema, i dati ottenuti nell'ambito della sorveglianza in linea di massima saranno comunicati soltanto grazie a un diritto d'accesso al sistema informatico gestito dal Servizio, i dati dovranno rimanere registrati in tale sistema per un determinato periodo (art. 11 AP).

Il passaggio al nuovo sistema comporterà costi supplementari per la Confederazione. Tali costi appaiono tuttavia accettabili, se si considerano i miglioramenti apportati e l'esiguità dei costi connessi alla sorveglianza rispetto alla totalità dei costi del perseguimento penale. Le risorse economiche supplementari per l'introduzione del nuovo sistema sono già previsti (decisione del Consiglio federale del 17 giugno 2009).

1.4.3 Sorveglianza al di fuori di un procedimento penale

Le disposizioni relative alla sorveglianza al di fuori di un procedimento penale (art. 27-29 AP) vanno completate, in particolare prevedendo che si possa ricorrere alla sorveglianza per ricercare una persona condannata a una pena detentiva o a una misura privativa della libertà in base a una sentenza passata in giudicato (art. 28 AP).

1.4.4 Compiti del Servizio

L'evoluzione tecnologica degli ultimi anni rende necessario un adattamento dei compiti del Servizio nell'ambito della sorveglianza del traffico delle telecomunicazioni (art. 16-18 AP). I compiti vanno precisati e completati, anche per motivi ine-

[3] RS **780.11**

renti alla certezza del diritto. Un'ordinanza attribuirà al Servizio nuovi compiti, segnatamente nell'ambito della sorveglianza della comunicazione via Internet e in particolare della telefonia via Internet.

1.4.5 Prestazioni nell'ambito della sorveglianza del traffico delle telecomunicazioni da parte dei soggetti LSCPT

Come corollario a quanto previsto per i compiti del Servizio (cfr. n. 1.4.4), vanno precisate e completate anche le prestazioni dei soggetti LSCPT nell'ambito della sorveglianza del traffico delle telecomunicazioni (art. 20-25 AP).

Le prestazioni supplementari, richieste in particolare ai soggetti LSCPT, compresi i fornitori di accesso a Internet, sono dovute soprattutto all'evoluzione tecnologica della comunicazione via Internet e in particolare della telefonia via Internet; un'evoluzione da cui detti soggetti traggono profitto anche economicamente. Soprattutto considerati gli sviluppi tecnologici della comunicazione via Internet, una sorveglianza efficiente richiede che tali soggetti siano obbligati a collaborare all'installazione di determinati programmi informatici nei sistemi di comunicazione per rendere possibile la sorveglianza in conformità con gli articoli 270bis del Codice di diritto processuale penale (CPP)[4] e 70*a*^{bis} PPM[5] (art. 21 cpv. 4 AP). In generale occorre che questi soggetti si attivino maggiormente (art. 21-25 AP), al fine di anticipare i problemi che potrebbero sorgere nell'ambito della futura sorveglianza.

Per consentire un perseguimento più efficace dei reati, si prevede inoltre di estendere da sei a dodici mesi il periodo di conservazione obbligatoria dei cosiddetti dati secondari nell'ambito del traffico delle telecomunicazioni, compreso Internet (art. 23 AP). Questa modifica è soprattutto una conseguenza dell'adozione parziale da parte del Parlamento della mozione 06.3170 presentata da Rolf Schweiger, che chiedeva, tra l'altro, una simile estensione della durata di conservazione di detti dati. La richiesta era motivata dalla constatazione che il periodo durante il quale i dati devono essere conservati, ossia sei mesi, è per esperienza troppo breve per permettere alle autorità di fare ricerche fruttuose, in quanto nel momento in cui l'autorità ordina la sorveglianza, i dati secondari sono spesso già stati cancellati. Poiché questo problema si pone non soltanto nell'ambito del traffico delle telecomunicazioni, ma anche in quello della corrispondenza postale, è logico che l'estensione del periodo di conservazione si applichi anche ai dati secondari della corrispondenza postale (art. 19 cpv. 2 AP). Quanto all'estensione da sei a dodici mesi del periodo per il quale i dati possono essere richiesti con effetto retroattivo (art. 273 cpv. 3 CPP[6] e art. 70*d* cpv. 3 PPM[7]), si tratta del corrispettivo dell'estensione della durata di conservazione dei dati, e quindi valgono le stesse considerazioni e le stesse ragioni di efficacia.

1.4.6 Soppressione dell'indennità corrisposta ai soggetti LSCPT per le prestazioni di sorveglianza fornite

Il 14 aprile 2010 il Consiglio federale ha posto in consultazione il Programma di consolidamento (PCon) 2011-2013[8], che ha lo scopo di sgravare le finanze della Confederazione. La soppressione dell'indennità prevista per i soggetti che effettuano la sorveglianza in virtù della LSCPT è una misura che rientra in tale programma. Si

4 RS ... (FF **2007** 6327)
5 RS **322.1**
6 RS ... (FF **2007** 6327)
7 RS **322.1**
8 http://www.admin.ch/ch/d/gg/pc/documents/1854/Vorlage.pdf

tratta dell'indennità di cui all'articolo 16 capoverso 1 secondo periodo LSCPT, corrisposta ai soggetti LSCPT, in particolare ai fornitori dei servizi di telecomunicazione, a copertura delle spese sostenute per la sorveglianza (art. 30 cpv. 1 AP). Il presente avamprogetto tiene già conto di tale soppressione. Va inoltre precisato che anche altre considerazioni di ordine giuridico fanno propendere per un'eliminazione. I dati che devono essere forniti dai soggetti LSCPT nell'ambito della sorveglianza sottostanno, infatti, come quelli che devono essere forniti dalle banche, all'obbligo di edizione (*Editionspflicht*), che non prevede il versamento di un'indennità. Il versamento di un'indennità è contrario al sistema del diritto penale. Non sembra opportuno accordare ai soggetti LSCPT un'indennità per la sorveglianza, dal momento che è nel loro interesse evitare reati commessi per loro tramite.

Rimane per contro immutato l'emolumento corrisposto al Servizio dall'autorità che ha ordinato la sorveglianza (autorità ordinante).

Per ulteriori dettagli si rimanda all'articolo 30 AP e al numero 3.1 del presente rapporto esplicativo.

1.4.7 Disposizioni penali

Nella nuova LSCPT sono state introdotte alcune disposizioni penali (art. 31 AP) per sanzionare in modo efficace i soggetti LSCPT che non rispettano gli obblighi loro imposti, adottando una condotta atta a ostacolare la sorveglianza impartita. A tale proposito è opportuno precisare che fondamentalmente queste sanzioni non sono indirizzate ai principali fornitori di servizi di telecomunicazione attivi sul mercato svizzero, che in genere sono consapevoli dei loro obblighi.

In realtà si tratta soprattutto di prevedere una sanzione per l'inosservanza degli ordini del Servizio (art. 31 cpv. 1 lett. a AP), analoga a quella prevista dall'articolo 292 del Codice penale (CP)[9], che in questo caso non avrebbe un sufficiente potere deterrente, soprattutto se si considera il risparmio che un soggetto LSCPT potrebbe realizzare se non eseguisse un ordine di sorveglianza del Servizio basato su un corrispondente ordine dell'autorità competente, in pratica del pubblico ministero. Sebbene questo meccanismo abbia ovviamente anche lo scopo secondario di incentivare i soggetti LSCPT a eseguire gli ordini del Servizio nel più breve tempo possibile, non impedisce loro di contestarli in conformità con le disposizioni della procedura federale. Ciononostante va ricordato che tali soggetti non possono opporsi a una decisione del Servizio di procedere a una sorveglianza contestando la legalità dell'ordine di sorveglianza su cui si fonda detta decisione (cfr. n. 1.4.9). Le regole per la verifica della validità dell'ordine del Servizio da parte del giudice penale incaricato del perseguimento per violazione dell'articolo 31 capoverso 1 lettera a AP sono le stesse di quelle sviluppate dalla dottrina[10] e dalla giurisprudenza in caso di violazione dell'articolo 292 CP[11].

Basandosi in particolare sulla mozione 06.3170 di Rolf Schweiger, parzialmente adottata dal Parlamento, si è infine deciso – sempre al fine di permettere un'esecuzione efficace della sorveglianza – di prevedere una disposizione penale (art. 31 cpv. 1 lett. b AP) che sanzioni la violazione dell'obbligo di conservare i cosiddetti dati secondari nell'ambito del traffico delle telecomunicazioni (art. 23 AP). Oltre al

9 RS **311.0**
10 Bernard Corboz, *Les infractions en droit suisse*, vol. II, 2002, n. 11-16 ad art. 292 CP.
11 RS **311.0**

fatto che la sanzione prevista dall'articolo 292 CP[12] non è sufficientemente severa per punire la violazione in questione, non consente neppure di impedire una tale condotta. Detto articolo si applica infatti quando non vengono forniti dati esistenti di cui un'autorità ordina la consegna, ma non quando i dati sono già stati distrutti prima che sia emesso l'ordine e nemmeno quando i dati non sono stati raccolti o conservati affatto. Per coerenza, la nuova disposizione deve applicarsi anche alla violazione dell'obbligo di conservare i cosiddetti dati secondari nell'ambito della corrispondenza postale (art. 19 cpv. 2 AP).

1.4.8 Vigilanza

È opportuno assicurarsi che soltanto i soggetti LSCPT che rispettano la legislazione in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni siano liberi di operare sul mercato svizzero, ovviamente nei limiti imposti dalla legge. La nuova disposizione sulla vigilanza amministrativa dei soggetti LSCPT (art. 33 AP) – che rende l'articolo 58 della legge del 30 aprile 1997[13] sulle telecomunicazioni (LTC) in parte applicabile per analogia – si prefigge di realizzare tale obiettivo e permette al Servizio di emettere un'ingiunzione in caso di violazione della legislazione in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

L'articolo 33 AP instaura dunque un sistema di sanzioni amministrative distinto, complementare al sistema delle sanzioni penali.

1.4.9 Rimedi giuridici

Le considerazioni che seguono non riguardano i rimedi giuridici a disposizione delle persone sorvegliate o implicate, secondo le modalità previste dall'articolo 279 capoverso 3 del CPP[14], bensì i rimedi giuridici riconosciuti ai soggetti LSCPT contro le decisioni del Servizio.

La LSCPT attualmente in vigore non specifica i rimedi giuridici riconosciuti ai soggetti LSCPT contro le decisioni generiche del Servizio e contro le decisioni di sorveglianza fondate su un corrispondente ordine dell'autorità competente. Solo l'articolo 32 OSCPT[15] attribuisce a tali soggetti il diritto di ricorrere contro una decisione di sorveglianza del Servizio. Dalla giurisprudenza[16] e dalla dottrina[17] si evince tuttavia che, nel quadro di un tale ricorso, questi soggetti possono invocare solamente questioni di ordine tecnico o organizzativo connesse all'esecuzione della misura di sorveglianza disposta, sostenendo che tale sorveglianza richiederebbe mezzi tecnici o conoscenze di cui non dispongono. L'avamprogetto riprende questa regolamentazione (art. 34 cpv. 2 secondo periodo). Nel loro ricorso i soggetti LSCPT potranno quindi far valere che, allo stato attuale della tecnica, la sorveglianza loro ordinata è oggettivamente impossibile da effettuare. A questo proposito è opportuno rilevare che, considerata la normativa proposta, è altamente improbabile che il Servizio trasmetta a un soggetto LSCPT operante nel traffico delle telecomunicazioni un ordine di sorveglianza non eseguibile dal punto di vista tecnico. Il

12 RS **311.0**
13 RS **784.10**
14 RS ... (FF **2007** 6327)
15 RS **780.11**
16 DTF **130** II 249, consid. 2.2.2 e 2.2.3.
17 Thomas Hansjakob, *Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*, 2a ed., San Gallo, 2006, n. 3 ad art. 32 OSCPT.

Servizio ha infatti soprattutto il compito di verificare che l'ordine di sorveglianza trasmessogli dall'autorità ordinante possa essere eseguito in termini tecnici; in caso contrario deve informare l'autorità ordinante e l'autorità autorizzante (art. 16 lett. a AP). Nel quadro della normativa esposta, il Servizio ha la possibilità di imporre al soggetto LSCPT che si oppone all'esecuzione della misura di sorveglianza adducendo questioni di ordine tecnico o organizzativo di adottare (entro un determinato termine) i provvedimenti necessari per poter effettuare in futuro il tipo di sorveglianza in questione[18]. Tale decisione potrà a sua volta essere impugnata in conformità con le disposizioni generali sull'organizzazione giudiziaria federale (art. 34 cpv. 1 AP).

Stando alla giurisprudenza[19] e alla dottrina[20], i cui dettami sono ripresi nell'articolo 34 AP, i soggetti LSCPT non sono legittimati a ricorrere contro una decisione del Servizio di trasmettere dati contestando la legalità dell'ordine di sorveglianza debitamente approvato dall'autorità penale competente. Questo regime è giustificato, in quanto non vi è un rapporto diretto tra l'autorità penale ordinante e i soggetti LSCPT, in particolare i fornitori di servizi di telecomunicazione. Questi ultimi ricevono infatti il mandato di sorveglianza direttamente dal Servizio, a cui sono legati da un rapporto di diritto amministrativo indipendente dalla procedura penale. In questo settore il Servizio svolge dunque solo un ruolo di intermediario tra le autorità ordinanti e autorizzanti da una parte e i soggetti LSCPT dall'altra. Non dispone quindi di alcun potere di verifica materiale vincolante per le autorità menzionate. È compito esclusivo dell'autorità autorizzante verificare la legalità della misura ordinata e, se del caso, opporsi alla sua esecuzione se la considera illegale[21]. In virtù della giurisprudenza[22] e della dottrina[23] precedentemente menzionate, la possibilità di contestare la legalità di un ordine di sorveglianza è riservata unicamente alle persone sorvegliate o implicate, secondo le modalità previste dall'articolo 279 capoverso 3 CPP[24]. Il fatto che non sembri praticabile informare dell'ordine di sorveglianza tutte le persone interessate da un tipo di sorveglianza rivolta contro ignoti (p.es. «*Kopfschaltungen*») o un numero indeterminato di persone (p.es. «*Antennensuchläufe*»), non significa che si debba permettere ai soggetti LSCPT, e in particolare ai fornitori di servizi di telecomunicazione, di impugnare, eccezion fatta per la restrizione citata, una decisione del Servizio che impone loro un mandato di sorveglianza. Infatti, le persone interessate dai tipi di sorveglianza di cui sopra non sono né indagati, né terzi sorvegliati ai sensi dell'articolo 270 lettera b CPP[25] e neppure persone che hanno utilizzato lo stesso collegamento dell'indagato o del terzo sorvegliato sempre ai sensi dell'art. 270 lett. b CPP[26]. Di conseguenza, per applicazione inversa dell'articolo 279 CPP[27], non devono essere informate della sorveglianza ordinata dall'autorità penale e non possono ricorrere contro tale misura. D'altro canto sarebbe inutile informare tali persone, dato che la maggior parte delle informazioni in questione non è rilevante per il procedimento e, in virtù dell'artico-

18 Sentenza del TAF del 10 marzo 2009, A-2336/2008, consid. 7.4.
19 DTF **130** II 249, consid. 2.2.2 e 2.2.3.
20 Thomas Hansjakob, op. cit., n. 3 ad art. 32 OSCPT.
21 DTF **130** II 249, consid. 2.2.2 e 2.2.3.
22 DTF **130** II 249, consid. 2.2.2 e 2.2.3.
23 Thomas Hansjakob, op. cit., n. 3 ad art. 32 OSCPT.
24 RS ... (FF **2007** 6327)
25 RS ... (FF **2007** 6327)
26 RS ... (FF **2007** 6327)
27 RS ... (FF **2007** 6327)

lo 276 capoverso 1 CPP[28], non viene nemmeno inserita nel fascicolo, per cui l'ingerenza nella sfera privata è irrilevante[29].

Per motivi di chiarezza e di certezza del diritto, è auspicabile introdurre nella LSCPT un'apposita disposizione (art. 34 AP) che sancisca nel senso sopra esposto i rimedi giuridici contro le decisioni del Servizio, riconosciuti ai soggetti LSCPT.

Non vi è motivo d'introdurre nella LSCPT – per non ritardare l'esecuzione di una misura di sorveglianza disposta – una disposizione che preveda in maniera generale e assoluta l'assenza di effetto sospensivo dei ricorsi presentati dai soggetti LSCPT contro una decisione di sorveglianza del Servizio. Infatti, in primo luogo, conformemente all'articolo 55 capoverso 2 della legge federale del 20 dicembre 1968[30] sulla procedura amministrativa, il Servizio può sempre prevedere che un ricorso contro la propria decisione non abbia effetto sospensivo e l'autorità di ricorso può annullare l'effetto sospensivo una volta depositato il ricorso. In secondo luogo, le sanzioni penali (cfr. n. 1.4.7) e amministrative (cfr. n. 1.4.8) previste sono sufficienti per dissuadere i soggetti LSCPT desiderosi di ritardare l'esecuzione di una misura di sorveglianza dal depositare un ricorso dilatorio. In terzo luogo, quando un fornitore di servizi di telecomunicazione afferma di non essere in grado di effettuare la sorveglianza disposta, quest'ultima può, se del caso, essere affidata al Servizio o a un terzo a spese del fornitore in questione (art. 24 AP), fatto che del resto può anch'esso avere un effetto deterrente.

1.5 Diritto comparato

I Paesi confinanti con la Svizzera hanno adottato regimi di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni simili a quello proposto dall'avamprogetto. In particolare è ammessa anche la sorveglianza della telefonia via Internet. Tuttavia si riscontrano alcune differenze nelle modalità rispetto alla regolamentazione prevista nell'avamprogetto. Il diritto tedesco stabilisce, per esempio, che i dati corrispondenti a quelli che in Svizzera vengono chiamati dati secondari siano conservati dai fornitori di servizi di telecomunicazione per sei mesi e non per dodici come proposto dall'avamprogetto al posto degli attuali sei mesi (cfr. art. 23 AP e relativo commento).

2 Commento ai singoli articoli

2.1 Sezione 1: Disposizioni generali

Art. 1 Campo di applicazione materiale

Il *capoverso 1* definisce il campo di applicazione materiale della LSCPT. Non sono state apportate modifiche sostanziali rispetto alla LSCPT attualmente in vigore. Sebbene la cosa sia implicita e riconosciuta, per ragioni di chiarezza il nuovo testo

[28] RS ... (FF **2007** 6327)
[29] Cfr. messaggio del 1° luglio 1998 concernente la LSCPT, FF *1998* 3350.
[30] RS **172.021**

specifica che il traffico Internet, compresi in particolare la corrispondenza per posta elettronica[31] e la telefonia via Internet, è un tipo particolare di traffico delle telecomunicazioni ai sensi della definizione di cui agli articoli 2 e 3 lettera c LTC[32]. Pertanto è inutile ripetere, ogni volta che la legge parla di traffico delle telecomunicazioni, che il concetto comprende anche il traffico Internet, poiché è sottinteso.

Il *capoverso 1 lettera a* è stato modificato sopprimendo il riferimento al carattere federale o cantonale del procedimento penale, superfluo dopo l'entrata in vigore del CPP[33], il quale si applicherà ai procedimenti sia federali sia cantonali e prevede la possibilità di sorvegliare la corrispondenza postale e il traffico delle telecomunicazioni nel quadro di tali procedimenti.

Il *capoverso 1 lettera b* non ha subito cambiamenti rispetto all'attuale LSCPT.

Il riferimento al salvataggio contenuto nell'attuale *capoverso 1 lettera c* LSCPT può essere soppresso, poiché tale obiettivo si evince dalla volontà di cercare una persona dispersa (art. 27 AP).

Il *capoverso 1 lettera d* prevede l'applicabilità della LSCPT a un caso attualmente non previsto, ossia alla ricerca di una persona condannata a una pena detentiva o a una misura privativa della libertà sulla base di una sentenza passata in giudicato (art. 28 AP).

Vanno adeguate le disposizioni del *capoverso 2* in merito alle informazioni sul traffico dei pagamenti, retto dalla legge del 30 aprile 1997[34] sulle poste, dato che i rimandi dell'attuale LSCPT non sono più corretti. Infatti, l'obbligo di testimoniare sarà disciplinato dal CPP[35], non appena questo entrerà in vigore; è palese per cui non occorre specificarlo. L'obbligo di informare le autorità è retto dagli articoli 284 e 285 CPP[36], essendo la Posta considerata un «istituto analogo» a una banca ai sensi dell'articolo 284 CPP, vista la sua attività nell'ambito del traffico dei pagamenti. È opportuno inserire un rimando, dato che tale qualifica non è scontata.

Art. 2 Campo di applicazione personale

Parallelamente all'attuale articolo 1 capoverso 2, l'*articolo 2* specifica il campo d'applicazione personale della LSCPT, ossia i soggetti che vi sono sottoposti, cui sono attribuiti degli obblighi e che effettuano la sorveglianza in virtù di tale legge. In via preliminare è opportuno precisare che la LSCPT non si applica più unicamente agli enti, ma in generale a tutti i soggetti, siano essi persone fisiche o enti, e indipendentemente dal fatto che questi ultimi siano persone giuridiche o entità statali.

Il *capoverso 1* è stato riformulato rispetto all'attuale articolo 1 capoverso 2 per permettere alle autorità inquirenti di ottenere i dati della comunicazione rilevanti per il procedimento anche da soggetti che non rientrano nel campo d'applicazione dell'attuale LSCPT. I soggetti in questione sono, ad esempio, i servizi liberi postali (servizi di corriere, di posta rapida ecc.; art. 10 dell'Ordinanza del 26 novembre 2003[37] sulle poste) e gli *hosting provider* in Internet, che non devono

31 Bernard Corboz, op. cit., n. 6 ad art. 321ter CP.
32 RS **784.10**
33 RS ... (FF **2007** 6327)
34 RS **783.0**
35 RS ... (FF **2007** 6327)
36 RS ... (FF **2007** 6327)
37 RS **783.01**

né disporre di una concessione né adempiere un obbligo di notificazione[38]. Tuttavia, per circoscrivere l'insieme dei soggetti LSCPT è opportuno limitare nel *capoverso 1* il campo d'applicazione personale della legge ai soggetti di cui alle *lettere a e b* che esercitano la loro attività a titolo professionale, indipendentemente dal fatto che lavorino a tempo pieno o a tempo parziale, dietro remunerazione o gratuitamente. Non sono dunque incaricati di effettuare la sorveglianza i soggetti che esercitano la loro attività come passatempo. Se si tratta di un'attività svolta nel settore del traffico delle telecomunicazioni a titolo non professionale si applica il capoverso 2 e gli obblighi da rispettare sono quelli menzionati nell'articolo 26 AP. I soggetti che rientrano nel campo di applicazione personale della LSCPT ai sensi del capoverso 1 sono sottoposti a tale legge e tenuti a effettuare la sorveglianza; nel testo di legge sono definiti globalmente «soggetti che eseguono la sorveglianza (della corrispondenza postale e del traffico delle telecomunicazioni) in virtù della presente legge» o, più raramente, da espressioni in sostanza identiche. Nel settore del traffico delle telecomunicazioni, tale espressione comprende non solo i fornitori di servizi di telecomunicazione di cui al *capoverso 1 lettera a*, ma anche le persone di cui al *capoverso 1 lettera b*. Riassumendo, sono incaricati di effettuare la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni in virtù della LSCPT i soggetti che, cumulativamente, incorporano una delle qualità menzionate al capoverso 1 lettera a e b ed esercitano la loro attività a titolo professionale.

Il *capoverso 1 lettera a* riprende l'attuale articolo 1 capoverso 2 e lo modifica specificando, per ragioni di chiarezza, che, così come il traffico Internet è un tipo particolare di traffico delle telecomunicazioni, anche i fornitori di accesso a Internet (*Internet-Anbieter/Zugangsvermittler*) costituiscono un tipo particolare di fornitori di servizi di telecomunicazione. Pertanto è inutile ripetere, ogni volta che la legge parla di fornitori di servizi di telecomunicazione, che il concetto comprende anche i fornitori di accesso a Internet, poiché è sottinteso. La nozione di fornitore di servizi di telecomunicazione è definita dagli articoli 2 e 3 lettere b e c della legge del 30 aprile 1997[39] sulle telecomunicazioni (LTC). I fornitori di servizi di telecomunicazione si impegnano a trasferire per conto di terzi le informazioni previste dagli articoli precitati. Sono ad esempio fornitori di servizi di telecomunicazione i grandi operatori attivi sul mercato svizzero che permettono agli utenti di telefonare per mezzo di un telefono fisso o mobile o di accedere a Internet. Va da sé che, poiché esercitano la loro attività a titolo professionale, questi fornitori sono tenuti a effettuare la sorveglianza del traffico delle telecomunicazioni anche nell'ipotesi in cui forniscano i loro servizi gratuitamente.

Il *capoverso 1 lettera b* ha lo scopo di permettere espressamente alle autorità inquirenti di ottenere i dati della comunicazione rilevanti per il procedimento penale in corso da soggetti che non sono veri e propri fornitori di servizi postali o di telecomunicazione ai sensi degli articoli 2 e 3 lettere b e c LTC[40], ma che svolgono un ruolo di intermediari nel processo di corrispondenza in questione, poiché in un determinato momento si trovano in possesso dei relativi dati. Si tratta, per esempio, degli *hosting provider* in Internet (che siano privati, organizzazioni o imprese), anche per i servizi di corrispondenza elettronica (per esempio casella di posta elettronica) che mettono a disposizione di terzi. Sono considerati come tali anche i rivenditori (privati o meno) di carte SIM prepagate distribuite da società che forni-

38 Thomas Hansjakob, op. cit., n. 24 ad art. 1 LSCPT.
39 RS **784.10**
40 RS **784.10**

scono servizi di telecomunicazione. Lo stesso dicasi per le persone (private o meno) che ricevono da parte di fornitori di servizi di telecomunicazione i dati della comunicazione in outsourcing. Questi soggetti sono tenuti ad effettuare la sorveglianza del traffico delle telecomunicazioni se esercitano la loro attività a titolo professionale, anche se forniscono i loro servizi a titolo gratuito.

Gli Internet caffè, le scuole di qualsiasi genere, gli hotel, i ristoranti, gli ospedali e i privati che mettono per esempio la loro rete Wi-Fi a disposizione dei loro clienti o di terzi perché possano connettersi a Internet non sono considerati fornitori di servizi di telecomunicazione di cui al capoverso 1 lettera a o persone di cui al capoverso 1 lettera b. Non sono dunque tenuti ad effettuare personalmente la sorveglianza del traffico delle telecomunicazioni. Questo non significa, però, che i fornitori di accesso a Internet dei soggetti precitati non possano effettuare una sorveglianza efficace del traffico delle telecomunicazioni (cfr. anche commento dell'art. 22 AP).

Il capoverso 2 riprende l'attuale articolo 1 capoverso 4 LSCPT, aggiungendo i soggetti menzionati al capoverso 1 che non esercitano la loro attività a titolo professionale e che pertanto non sono tenuti a effettuare la sorveglianza del traffico delle telecomunicazioni. Questa aggiunta è giustificata dal fatto che è comunque essenziale permettere la sorveglianza nel caso di specie.

Art. 3 Servizio di sorveglianza

L'*articolo 3* riprende in sostanza l'attuale articolo 2 LSCPT.

Oltre ai compiti attribuitigli dal presente avamprogetto, il Servizio ha in particolare la facoltà – e non l'obbligo – di fornire alle autorità e ai soggetti che effettuano la sorveglianza in virtù della LSCPT consulenza tecnica in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (cfr. anche il commento all'art. 15 AP).

Art. 4 Trattamento dei dati personali

L'*articolo 4* ricalca l'attuale articolo 7 capoverso 1 OSCPT[41], adeguandone il campo d'applicazione personale in base all'articolo 2 capoverso 1 lettera b AP. I dettagli relativi alle modalità di trattamento rimangono invece disciplinati nell'ordinanza summenzionata.

Art. 5 Segreto postale e delle telecomunicazioni

L'*articolo 5* riprende sostanzialmente gli articoli 12 capoverso 3 e 15 capoverso 7 della LSCPT attuale.

41 RS **780.11**

2.2 Sezione 2: Sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni

Art. 6 Principio

L'*articolo 6* riprende in sostanza il capoverso 1 dell'attuale articolo 8 OSCPT[42].

Il sistema gestito dal Servizio non contiene i dati raccolti nel corso della sorveglianza della corrispondenza postale, poiché questi sono direttamente trasmessi all'autorità che ha ordinato la sorveglianza, conformemente all'articolo 9 AP.

Art. 7 Scopo del sistema di trattamento

Cfr. commento relativo al numero 1.4.2.

Art. 8 Contenuto del sistema di trattamento

I dati menzionati all'*articolo 8* sono quelli ottenibili nell'ambito della sorveglianza. Possono fornire varie informazioni come, per esempio, il contenuto delle conversazioni telefoniche della persona sorvegliata, il contenuto delle sue comunicazioni via Internet o il luogo in cui si trova.

Art. 9 Accesso al sistema di trattamento

La disposizione del *capoverso 1* rispecchia la situazione attuale. L'autorità che ha ordinato la sorveglianza può accedere, sotto riserva del capoverso 2, soltanto ai dati contenuti nel sistema che sono stati raccolti nel corso della sorveglianza e non a tutti i dati conservati nel sistema. In base a questa normativa, per esempio, anche le forze di polizia che lavorano a un caso possono accedere ai relativi dati se hanno l'autorizzazione del pubblico ministero che dirige le operazioni, ha ordinato la sorveglianza e ha accesso ai dati raccolti in tale ambito. Ma ciò è possibile soltanto se il pubblico ministero concede la propria autorizzazione e solo per i dati da questi indicati, in applicazione del principio della proporzionalità. Un poliziotto può, per esempio, essere autorizzato a consultare soltanto i dati che indicano quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto, e i dati relativi alle comunicazioni e alla fatturazione, ma non le comunicazioni di tale persona.

La disposizione prevista dal *capoverso 2* permette di evitare che l'autorità che ha ordinato sorveglianza e le persone da questa designate accedano a dati di cui non hanno più bisogno. Richiede inoltre un comportamento attivo da parte dell'autorità che ha ordinato la sorveglianza affinché, decorsa una determinata scadenza, possa mantenere l'accesso a dati di cui ha ancora bisogno. In caso contrario l'accesso ai dati viene bloccato. Il Servizio deve avvertire l'autorità che ha ordinato la sorveglianza che il diritto di accesso ai dati raccolti nel corso della sorveglianza sta per scadere per permetterle, se necessario, di depositare in tempo una richiesta di proroga della scadenza per non perdere tale facoltà. Una decisione diversa porrebbe

[42] RS **780.11**

problemi pratici nella gestione dei dati e implicherebbe un ulteriore lavoro amministrativo inutile.

Il *capoverso 3* ha lo scopo di permettere al Servizio di sapere se un'autorità diversa da quella che ha ordinato la sorveglianza, che lo contatta per accedere in rete ai dati raccolti nel corso della sorveglianza (cfr. cpv. 4), ha il diritto di accedere ai dati. Appositamente non si parla di «istanze», ma di «autorità» successivamente incaricate del caso, poiché ci si riferisce sia al caso in cui la sorveglianza sia stata ordinata dalla polizia per ritrovare una persona scomparsa sia al caso in cui l'autorità successiva sia un corpo di polizia diverso (p.es. perché le ricerche si svolgono in un Cantone diverso da quello a cui appartiene il corpo di polizia che ha ordinato la sorveglianza).

Per il *capoverso 4* cfr. commento, per analogia, dei capoversi 1-3.

Per il *capoverso 5* cfr. commento del numero 1.4.2.

Art. 10 Diritto di consultare gli atti e diritto di accedere ai dati

Tutti i diritti previsti dal *capoverso 1* sono retti dal CPP[43].

Il *capoverso 2* prevede le ipotesi in cui la domanda di assistenza giudiziaria sia una domanda d'estradizione e in cui la domanda verta su un altro caso di assistenza giudiziaria. Il diritto di consultare gli atti e il diritto di accedere ai dati dell'interessato raccolti nel corso dell'esecuzione di una domanda di estradizione (art. 1 cpv. 1 lett. b) sono retti dall'articolo 18*a* capoverso 4 della legge federale del 20 marzo 1981[44] sull'assistenza internazionale in materia penale (AIMP), dagli articoli 26 e 27 della legge federale del 20 dicembre 1968[45] sulla procedura amministrativa (PA), applicabile in virtù dell'articolo 12 capoverso 1 primo periodo AIMP[46] e dagli articoli 8 e 9 della legge federale del 19 giugno 1992[47] sulla protezione dei dati (LPD). L'articolo 18*a* capoverso 4 AIMP[48] è introdotto dal CPP[49]. Negli altri casi di assistenza giudiziaria (art. 1 cpv. 1 lett. b) questi diritti sono retti dagli articoli 18*a* capoverso 4 e 80*b* AIMP[50], dall'articolo 9 della legge federale del 3 ottobre 1975[51] relativa al Trattato conchiuso con gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale e dall'articolo 46 della legge federale del 22 giugno 2001[52] sulla cooperazione con la Corte penale internazionale (LCPI), nonché dagli articoli 8 e 9 LPD[53] se l'autorità incaricata della domanda di assistenza giudiziaria è un'autorità della Confederazione oppure dal diritto cantonale se tale autorità è il pubblico ministero di un Cantone. Va sottolineato che la legge federale del 21 dicembre 1995[54] concernente la cooperazione con i tribunali internazionali incaricati del perseguimento penale delle violazioni gravi del diritto internazionale umanitario (art. 2) e le Convenzioni internazionali stipulate dalla Svizzera in materia

43 RS ... (FF **2007** 6327)
44 RS **351.1**
45 RS **172.021**
46 RS **351.1**
47 RS **235.1**
48 RS **351.1**
49 RS ... (FF **2007** 6327)
50 RS **351.1**
51 RS **351.93**
52 RS **351.6**
53 RS **235.1**
54 RS **351.20**

di assistenza giudiziaria internazionale con altri Stati (p.es. con il Canada e il Brasile) prevedono l'applicazione dell'AIMP[55], in particolare degli articoli 18*a* capoverso 4 e 80*b*. Se l'autorità incaricata della domanda di assistenza giudiziaria è il pubblico ministero di un Cantone, l'articolo 37 capoverso 1 LPD[56] si applica in via sussidiaria al diritto d'accesso ai dati raccolti nel corso della sorveglianza, a meno che il diritto cantonale non assicuri un livello di protezione adeguato. L'autorità interpellata nell'ambito dell'esercizio del diritto di consultare gli atti o del diritto di accedere ai dati deve essere in grado, nell'ipotesi in cui tali diritti siano limitati e nella misura in cui sia necessario, di rispondere alla domanda in questione in modo da non rivelare informazioni coperte dal segreto d'ufficio.

Il *capoverso 3* rinvia al diritto cantonale. A tale proposito va precisato che l'articolo 37 capoverso 1 LPD[57] si applica in via sussidiaria al diritto di accesso ai dati raccolti nel corso della sorveglianza se il diritto cantonale non assicura un livello di protezione adeguato.

La disposizione prevista dal *capoverso 4* rende esplicito che il Servizio, pur essendo in possesso dei dati, non ricopre il ruolo di detentore della collezione di dati, che spetta, conformemente all'articolo 13 AP, alle autorità che hanno accesso al sistema di trattamento in virtù dell'articolo 9 AP.

Art. 11 Termine di conservazione dei dati

In virtù del *capoverso 1 secondo periodo*, l'autorità incaricata del caso deve comunicare al Servizio il termine di prescrizione dell'azione penale al fine di permettere a quest'ultimo di adempiere al proprio obbligo d'informazione previsto dal capoverso 5 (cfr. relativo commento). Tale comunicazione è importante, poiché il termine di prescrizione dell'azione penale varia a seconda della pena prevista per il reato in questione e che per conoscere tale reato bisogna avere accesso al contenuto del fascicolo penale, una facoltà che il Servizio non ha.

La durata massima di conservazione dei dati nel sistema di trattamento di cui al *capoverso 2* è giustificata in particolare dal fatto che spesso le procedure di assistenza giudiziaria hanno tempi lunghi. La durata corrisponde al termine massimo di prescrizione dell'azione penale secondo il diritto svizzero (se si escludono i reati imprescrittibili), anche se il reato in questione può essere imprescrittibile nel diritto dello Stato richiedente.

La durata massima di conservazione dei dati nel sistema di trattamento di cui al *capoverso 3* è giustificata in particolare dal fatto che è in gioco il bene giuridico più prezioso, ossia la vita umana, e dal fatto che una persona può risultare scomparsa durante un periodo molto lungo.

In virtù del *capoverso 4 secondo periodo*, nel caso di dati raccolti nel corso della ricerca di persone condannate a una pena privativa della libertà, l'autorità incaricata del caso deve comunicare al Servizio la scadenza del termine di prescrizione della pena (*cpv. 4 primo periodo*), al fine di permettere al Servizio di adempiere al proprio obbligo d'informazione previsto dal capoverso 5 (cfr. relativo commento). Tale comunicazione è importante, poiché il termine di prescrizione della pena varia a seconda della pena pronunciata e che per conoscere tale pena bisogna avere accesso

55 RS **351.1**
56 RS **235.1**
57 RS **235.1**

al contenuto del fascicolo penale, una facoltà che il Servizio non ha. Per quanto concerne la durata massima di conservazione dei dati nel sistema di trattamento di cui al *capoverso 4 terzo periodo*, essa è giustificata in particolare dal fatto che è in gioco il bene giuridico più prezioso, ossia la vita umana. È necessario precisare che una misura privativa della libertà non cade in prescrizione, a differenza di quanto avviene per una pena privativa della libertà.

In base al tenore del *capoverso 5*, l'autorità incaricata del caso oppure, se non vi è più un'autorità incaricata del caso, l'ultima che lo è stata o quella successiva, deve in via di principio chiedere il trasferimento dei dati in questione per rispettare le disposizioni relative alla conservazione degli atti (art. 103 cpv. 1 CPP[58]) o le regole applicabili all'archiviazione. In effetti è plausibile il caso in cui i dati debbano essere cancellati dal sistema in virtù dei capoversi 1-4, pur dovendo rimanere ancora conservati nel fascicolo in virtù dell'articolo 103 capoverso 1 CPP[59] al fine di rispettare il requisito di prescrizione della pena menzionato in tale disposizione. Inoltre, non è compito del Servizio ma dell'autorità incaricata del caso oppure, se non vi è più un'autorità incaricata del caso, dell'ultima ad esserlo stata o di quella successiva adottare le misure necessarie per rispettare le disposizioni in materia di archiviazione. A tale proposito si applicano le disposizioni della collettività (Confederazione o Cantoni) a cui appartiene l'autorità che ha ordinato la sorveglianza in questione, visto che è questa autorità, facente parte di tale collettività, che ricopre il ruolo di detentore della collezione di dati raccolti nel corso della sorveglianza di sua competenza. Una volta che i dati sono stati trasferiti all'autorità competente, il Servizio li distrugge nel sistema di trattamento. Lo stesso vale per i dati il cui trasferimento non è stato richiesto alla scadenza del termine di conservazione. Per evitare che il trasferimento dei dati non venga richiesto per errore (dimenticanza) alla scadenza del termine di conservazione nel sistema di trattamento – cosa che può comportare la perdita irreversibile di dati che devono invece ancora essere conservati in virtù dell'articolo 103 capoverso 1 CPP[60] o delle disposizioni applicabili in materia di protezione dei dati –, il Servizio ha il dovere di segnalare la prossima scadenza del termine di conservazione dei dati contenuti nel suo sistema di trattamento. Nelle ipotesi previste dal capoverso 1 e dal capoverso 4 primo periodo, a tal fine è indispensabile che il Servizio possa contare sulla comunicazione dell'autorità incaricata del caso (cfr. commento relativo al cpv. 1 e al cpv. 4 primo periodo). Questa soluzione «centralizzata» sembra preferibile a quella che obbligherebbe tutte le autorità incaricate di fascicoli contenenti dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni a contattare il Servizio prima della scadenza del termine. In effetti questa seconda alternativa imporrebbe alla Confederazione e ai singoli Cantoni di organizzarsi per non dimenticare la scadenza del termine, aumentando il rischio che l'intento fallisca. Per facilitare il compito del Servizio, la Confederazione e i singoli Cantoni devono designare l'autorità che il Servizio deve avvisare. Infatti non si può pretendere che il Servizio debba cercare, dopo molti anni, l'autorità incaricata del caso, l'ultima a esserlo stata o quella successiva. Sarebbe troppo complicato se si considera il gran numero di autorità che possono essere competenti per i fascicoli contenenti dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni.

58 RS ... (FF **2007** 6327)
59 RS ... (FF **2007** 6327)
60 RS ... (FF **2007** 6327)

Art. 12 Sicurezza

La disposizione prevista dal *primo periodo* è giustificata dal fatto che il Servizio – pur non essendo il detentore della collezione di dati (cfr. commento relativo all'art. 13 AP) – è in possesso dei dati, contenuti nel sistema di trattamento da esso gestito.

Il *terzo periodo* riprende il capoverso 2 dell'attuale art. 9 OSCPT[61]. Il campo di applicazione personale è stato completato in base all'articolo 2 capoverso 1 lettera b AP.

Art. 13 Responsabilità

L'*articolo 13* stabilisce che il ruolo di detentore della collezione di dati è ricoperto dalle autorità che hanno accesso al sistema, e non dal Servizio, che è soltanto in possesso dei dati contenuti nel sistema di trattamento (cfr. commento relativo all'art. 12 AP).

2.3 Sezione 3: Compiti del Servizio

Art. 14 Informazioni sui collegamenti di telecomunicazione

L'*articolo 14* riprende in sostanza l'attuale articolo 14 capoverso 2 LSCPT. I collegamenti di telecomunicazione in questione comprendono anche i collegamenti Internet (cfr. anche il commento relativo all'art. 1 cpv. 1 AP).

Art. 15 Compiti generali nell'ambito della sorveglianza

L'*articolo 15* elenca i compiti del Servizio nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, ripresi dagli attuali articoli 11 e 13 LSCPT. Contrariamente alla LSCPT in vigore, nella nuova versione sono stati eliminati gli articoli relativi a compiti specifici del Servizio nell'ambito della sorveglianza postale, mentre sono previsti compiti specifici per la sorveglianza del traffico delle telecomunicazioni (cfr. commento relativo all'art. 16 AP).

La *lettera a* riprende in sostanza gli attuali articoli 11 capoverso 1 lettera a e 13 capoverso 1 lettera a LSCPT.

La *lettera b* riassume essenzialmente gli attuali articoli 11 capoverso 1 lettera b e 13 capoverso 1 lettera b LSCPT e tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP: gli ordini del Servizio non sono dunque indirizzati solamente ai fornitori di servizi postali e di telecomunicazione, ma anche alle persone specificate all'articolo 2 capoverso 1 lettera b. Il compito di controllare l'esecuzione della sorveglianza è stato inserito al solo scopo di sottolineare il ruolo di intermediario tra le autorità penali e i soggetti LSCPT svolto dal Servizio.

La *lettera c* ricalca in sostanza l'attuale articolo 13 capoverso 1 lettera f LSCPT, applicabile alla sorveglianza della corrispondenza del traffico delle telecomunicazioni. Questo compito è esteso alla sorveglianza della corrispondenza postale, in

61 RS **780.11**

quanto indicato anche in tale ambito. La disposizione va messa in relazione con l'articolo 271 capoverso 1, modificato dal presente avamprogetto, e con l'articolo 274 capoverso 4 lettera a CPP[62], nonché con l'articolo 70*b* capoverso 1, modificato anch'essi dal presente avamprogetto, e con l'articolo 70*e* capoverso 4 lettera a PPM[63]. Tali articoli stabiliscono il regime applicabile alla sorveglianza quando occorre proteggere informazioni coperte dal segreto professionale di cui le autorità inquirenti non devono venire a conoscenza (cfr. commento all'art. 271 CPP[64]). Il Servizio adotta le disposizioni necessarie per permettere l'attuazione dei provvedimenti decisi nel quadro degli articoli citati, ma non procede, per esempio, alla cernita dei dati menzionata in tali articoli (art. 271 cpv. 1 CPP[65] e art. 70*b* cpv. 1 PPM[66]).

La *lettera d* riassume gli attuali articoli 11 capoverso 1 lettera d e 13 capoverso 1 lettera g LSCPT.

La *lettera e* riassume gli attuali articoli 11 capoverso 1 lettera c e 13 capoverso 1 lettera h LSCPT.

I compiti di cui all'attuale articolo 13 capoverso 2 lettere a-d LSCPT non sono ripresi nell'articolo 15 AP, poiché non devono più essere svolti dal Servizio o non sono più previsti, sia perché mancano i mezzi sia perché non sono più necessari. Nemmeno il testo degli attuali articoli 11 capoverso 2 primo periodo e 13 capoverso 2 lettera e LSCPT è stato ripreso nell'articolo 15, in quanto superfluo dal momento che prevede solo la possibilità – e non l'obbligo – del Servizio di fornire alle autorità e ai soggetti LSCPT consulenza in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Nonostante questa soppressione, il Servizio mantiene la facoltà di fornire consulenza alle autorità e ai soggetti menzionati.

I compiti del Servizio di cui all'attuale articolo 11 LSCPT che non sono stati inseriti nell'articolo 15 AP saranno trasferiti nell'OSCPT[67]. Per quanto riguarda, invece, i compiti del Servizio di cui all'attuale articolo 13 LSCPT non ripresi nell'articolo 15 AP si rimanda al commento relativo all'articolo 16 AP.

Art. 16 Compiti nell'ambito della sorveglianza del traffico delle telecomunicazioni

L'*articolo 16* elenca i compiti del Servizio specificamente previsti per la sorveglianza disposta nell'ambito del traffico delle telecomunicazioni, esclusa quindi la corrispondenza postale.

Il compito di cui alla *lettera a* del Servizio è stato inserito allo scopo di evitare che il Servizio trasmetta a un soggetto LSCPT operante nel settore del traffico delle telecomunicazioni un ordine di sorveglianza che ritiene ineseguibile dal punto di vista tecnico o la cui esecuzione comporta notevoli difficoltà, senza aver prima informato l'autorità ordinante e l'autorità autorizzante delle difficoltà riscontrate. Questo meccanismo serve in particolare a rendere l'autorità ordinante e l'autorità autorizzante maggiormente coscienti della presunta impossibilità o difficoltà. L'autorità ordinante

62 RS ... (FF **2007** 6327)
63 RS **322.1**
64 RS ... (FF **2007** 6327)
65 RS ... (FF **2007** 6327)
66 RS **322.1**
67 RS **780.11**

e l'autorità autorizzante possono – senza esservi obbligate – tenere conto di tale avvertimento per, eventualmente, revocare la sorveglianza impartita oppure non autorizzarla. Adottando questo meccanismo è possibile in particolare evitare le complicazioni derivanti da un eventuale ricorso contro la decisione del Servizio in seguito all'impossibilità tecnica di effettuare la sorveglianza (art. 34 cpv. 2 AP, cfr. n. 1.4.9). Va precisato che il Servizio non determina la fattibilità tecnica della sorveglianza considerando gli strumenti tecnici a disposizione del soggetto incaricato di attuare la decisone, ma in base allo stato della tecnica nel momento in la sorveglianza va effettuata (cfr. art. 34 cpv. 2 e n. 1.4.9). Il meccanismo proposto permette inoltre alle autorità precitate di tenere conto delle notevoli difficoltà legate all'eventuale esecuzione della sorveglianza impartita. Si considerano difficoltà notevoli costi manifestamente sproporzionati per l'esecuzione della sorveglianza oppure problemi di ordine legale. Il termine entro il quale il Servizio deve informare l'autorità ordinante e l'autorità autorizzante del fatto che non è tecnicamente possibile effettuare la sorveglianza sarà fissato in un'ordinanza. Tale termine dovrà ovviamente essere particolarmente breve, in modo da premettere all'autorità ordinante, se necessario, di emettere in tempi brevi un nuovo ordine.

La *lettera b* ricalca essenzialmente l'attuale articolo 15 capoverso 2 primo periodo LSCPT e lo completa sulla base del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b.

La *lettera c* riprende in sostanza il testo dell'attuale articolo 13 capoverso 1 lettera c LSCPT e lo completa sulla base del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b. Il testo è stato adattato al funzionamento del nuovo sistema di sorveglianza ISS, nel quale i dati ottenuti dalla sorveglianza non sono più messi a disposizione delle autorità interessate tramite invio postale dei supporti di dati e dei documenti, ma grazie a un diritto di accesso al sistema informatico utilizzato dal Servizio (cfr. n. 1.4.2).

La *lettera d* modifica e integra il testo dell'attuale articolo 13 capoverso 1 lettera d LSCPT, che verte sul collegamento diretto (*Direktschaltung*), una modalità particolare di esecuzione della sorveglianza, ammessa solo in casi eccezionali. Nel sistema in essere, i dati ottenuti nell'ambito della sorveglianza disposta passano di regola attraverso il Servizio (che funge da intermediario tra i soggetti incaricati di effettuare la sorveglianza e le autorità ordinanti) e sono registrati nel suo sistema informatico. La stessa procedura viene adottata anche per la cosiddetta sorveglianza in tempo reale (*Echtzeit-Überwachung*), cioè non retroattiva (*rückwirkende Überwachung*). Da questo punto di vista il nuovo sistema di sorveglianza ISS funzionerà nello stesso modo (cfr. n. 1.4.2 e art. 16 lett. c ed e AP). Quando la sorveglianza disposta viene effettuata ricorrendo al collegamento diretto, il soggetto incaricato trasferisce i dati raccolti direttamente all'autorità interessata, senza passare dal Servizio, che dunque non registra i dati nel suo sistema. I dati sono invece registrati dall'autorità destinataria. La lettera d stabilisce le condizioni alle quali è consentito ricorrere alla procedura di collegamento diretto: si tratta di situazioni in cui il Servizio non è in grado, per ragioni tecniche, di svolgere il ruolo di intermediario, attribuitogli dalla legge, tra i soggetti che eseguono la sorveglianza e le autorità ordinanti. Sono fatti salvi l'artico-

lo 271 capoverso 2 CPP[68] e l'articolo 70*b* capoverso 2 PPM[69], nella versione introdotta dal CPP[70]. Tale impiego restrittivo del collegamento diretto non diminuirà l'efficacia del lavoro delle autorità inquirenti, ossia non sarà causa di ritardi. Infatti i dati ottenuti nell'ambito della sorveglianza in tempo reale, vale a dire senza collegamento diretto, saranno messi a disposizione delle autorità interessate immediatamente, con solo qualche frazione di secondo di ritardo, per mezzo del sistema informatico utilizzato dal Servizio. La lettera d tiene inoltre conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b.

La *lettera e* riprende essenzialmente l'attuale articolo 13 capoverso 1 lettera e LSCPT e tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b. Inoltre, per meglio specificare il concetto di dati secondari e garantire l'omogeneità terminologica nel CPP[71] (nonché nella PPM[72] nella versione introdotta dal CPP[73]) e nella futura LSCPT, l'espressione che designa i dati secondari è stata sostituita con quella, in sostanza identica, utilizzata nell'articolo 273 capoverso 1 lettere a e b CPP[74] (e nell'art. 70*d* cpv. 1 lett. a e b PPM[75] nella versione introdotta dal CPP[76]). I dati secondari nell'ambito del traffico delle telecomunicazioni sono quindi designati come «i dati che consentono di individuare quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione». La lettera e è stata inoltre adattata al funzionamento del nuovo sistema di sorveglianza ISS, nel quale i dati ottenuti dalla sorveglianza non sono più messi a disposizione delle autorità interessate tramite invio postale dei supporti di dati e dei documenti, ma grazie a un diritto di accesso al sistema informatico utilizzato dal Servizio (cfr. n. 1.4.2).

L'ordine previsto alla *lettera f*, che il Servizio può impartire al soggetto incaricato di effettuare la sorveglianza del traffico delle telecomunicazioni, di trasmettergli unicamente determinati dati del flusso di dati è ammesso solo previo consenso dell'autorità ordinante. Si tratta, per esempio, di fornire esclusivamente i dati relativi al traffico Internet o alla telefonia via Internet, selezionandoli dal flusso di dati in analisi. In linea di massima, l'autorità ordinante avanzerà una tale richiesta solo se non desidera consultare altri dati o se è tecnicamente necessario per l'analisi corretta dei dati, dal momento che la quantità di materiale potrebbe essere tale da rendere i dati difficili, se non addirittura impossibili, da utilizzare. Per garantire la trasparenza necessaria alla valutazione oggettiva del materiale probatorio, negli atti giudiziari si dovrà, se del caso, menzionare il fatto che i dati riportati costituiscono solo una parte del flusso di dati. Il compito del Servizio di esigere la consegna di una parte soltanto del flusso di dati è complementare all'obbligo dei soggetti LSCPT di cui all'articolo 21 capoverso 3 secondo periodo AP. Inoltre, non deve essere confuso con la

68 RS ... (FF **2007** 6327)
69 RS **322.1**
70 RS ... (FF **2007** 6327)
71 RS ... (FF **2007** 6327)
72 RS **322.1**
73 RS ... (FF **2007** 6327)
74 RS ... (FF **2007** 6327)
75 RS **322.1**
76 RS ... (FF **2007** 6327)

possibilità riconosciuta al Servizio di mettere a disposizione dell'autorità ordinante, su richiesta di quest'ultima, solo una parte dei dati ottenuti dal soggetto incaricato di effettuare la sorveglianza. Infine si è tenuto conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b.

I compiti del Servizio di cui all'attuale articolo 13 LSCPT che non sono stati ripresi nell'articolo 16 AP sono stati inseriti nell'articolo 15 AP, a meno che non siano stati soppressi (cfr. commento relativo all'art. 15 AP) o trasferiti nell'OSCPT[77].

Art. 17 Controllo della qualità

L'*articolo 17* mira a garantire una corretta esecuzione della sorveglianza disposta.

Il *capoverso 1* consente al Servizio di adottare misure di controllo per rimediare a eventuali problemi riscontrati dall'autorità inquirente coinvolta o dal Servizio stesso, riguardo ai dati forniti dai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della LSCPT, soprattutto riguardo alla qualità dei dati. Un problema simile potrebbe verificarsi, per ipotesi, quando l'autorità inquirente constata che i cosiddetti dati secondari ottenuti nell'ambito di una sorveglianza retroattiva indicano comunicazioni che non figurano nelle registrazioni delle conversazioni effettuate nel quadro della sorveglianza in tempo reale. L'obiettivo di questa disposizione è anche quello di permettere al Servizio di anticipare tali situazioni effettuando controlli a titolo preventivo, al fine di garantire che nessun problema pregiudichi il corretto funzionamento della sorveglianza.

Secondo il *capoverso 2*, se il Servizio deve venire a conoscenza del contenuto dei dati per effettuare i controlli citati, la protezione dei dati gli impone di ottenere prima l'autorizzazione dell'autorità ordinante. Infatti il Servizio non ha alcun diritto di venire a conoscenza del contenuto dei dati, anche se sono in suo possesso perché registrati nel suo sistema informatico. L'autorizzazione non è invece richiesta se il Servizio è in grado di effettuare i controlli senza venire a conoscenza dei dati in questione.

Art. 18 Certificazione

Il compito del Servizio, di cui all'*articolo 18*, è teso a garantire che i fornitori di servizi di telecomunicazione possano eseguire senza difficoltà gli incarichi di sorveglianza loro assegnati.

Questo compito ha per corollario la possibilità per i fornitori di servizi di telecomunicazione di ottenere una certificazione a dimostrazione della loro capacità di eseguire correttamente le misure di sorveglianza per le quali hanno ottenuto la certificazione. Dal momento che i grandi fornitori di servizi di telecomunicazione operanti sul mercato svizzero – di cui si avvale la maggior parte degli utenti – dispongono di norma della tecnologia e del personale necessari per effettuare correttamente le misure di sorveglianza ordinate, è opportuno prevedere nell'articolo 18 AP solo la possibilità e non l'obbligo di certificazione, a differenza di quanto previsto dall'articolo 24 AP (cfr. relativo commento). Il Servizio procede alla certificazione secondo le proprie modalità, a spese dei fornitori di servizi di telecomunicazione. I test pos-

[77] RS **780.11**

sono quindi essere effettuati direttamente dal Servizio oppure da terzi; in quest'ultimo caso il Servizio si limita a verificare il verbale di certificazione e i risultati dei test effettuati per stabilire se accordare o meno la certificazione. La possibilità di affidare i test a terzi è giustificata dalla notevole mole di lavoro che richiedono, che potrebbe essere incompatibile con le risorse di personale del Servizio.

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

Art. 19

Il *capoverso 1* si fonda sull'attuale articolo 12 capoverso 1 LSCPT. Tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, attribuendo gli obblighi menzionati non soltanto ai fornitori di servizi postali, ma anche alle persone indicate all'articolo 2 capoverso 1 lettera b AP.

Il *capoverso 2*, che trae spunto dall'attuale articolo 12 capoverso 2 LSCPT, verte sul periodo di conservazione dei cosiddetti dati secondari nell'ambito della corrispondenza postale. Per meglio specificare il concetto di dati secondari e garantire l'omogeneità terminologica nel CPP[78] (nonché nella PPM[79] nella versione introdotta dal CPP[80]) e nella futura LSCPT, l'espressione che designa i dati secondari è stata sostituita con quella, in sostanza identica, utilizzata nell'articolo 273 capoverso 1 lettere a e b CPP[81] (e nell'art. 70*d* cpv. 1 lett. a e b PPM[82] nella versione introdotta dal CPP[83]). I dati secondari nell'ambito della corrispondenza postale sono quindi designati come «i dati che consentono di individuare quando e con quali persone la persona sorvegliata è stata o è in contatto postale e i dati relativi alle comunicazioni e alla fatturazione». L'estensione da sei a dodici mesi della durata di conservazione dei dati secondari nell'ambito delle corrispondenza postale è una conseguenza dell'adozione parziale da parte del Parlamento della mozione 06.3170 presentata da Rolf Schweiger, che chiedeva, tra l'altro, una simile estensione della durata di conservazione dei dati secondari del traffico delle telecomunicazioni, compreso Internet (art. 23 AP). La problematica sollevata nella mozione si pone in effetti non solo per i dati secondari del traffico delle telecomunicazioni, ma anche per quelli della corrispondenza postale. È dunque logico che l'estensione del periodo di conservazione si applichi anche ai dati secondari della corrispondenza postale (cfr. 1.4.5).

L'attuale articolo 12 capoverso 3 LSCPT è ripreso in sostanza all'articolo 5 AP.

78 RS ... (FF **2007** 6327)
79 RS **322.1**
80 RS ... (FF **2007** 6327)
81 RS ... (FF **2007** 6327)
82 RS **322.1**
83 RS ... (FF **2007** 6327)

2.5 Sezione 5: Obblighi nell'ambito della sorveglianza del traffico delle telecomunicazioni

Art. 20 Informazioni sui collegamenti di telecomunicazione

L'*articolo 20* riprende essenzialmente l'attuale articolo 14 LSCPT. I collegamenti di telecomunicazione menzionati comprendono anche i collegamenti Internet (cfr. commento all'art. 1 cpv. 1 AP). Il periodo iniziale del *capoverso 1* è uguale a quello del capoverso 1 dell'attuale articolo 14 LSCPT e tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, attribuendo gli obblighi elencati non soltanto ai fornitori di servizi di telecomunicazione, ma anche alle persone indicate all'articolo 2 capoverso 1 lettera b. Ciò permette di includere anche la categoria dei rivenditori, per esempio quelli di carte SIM. A differenza delle comunicazioni e dei dati cosiddetti secondari, le informazioni menzionate all'articolo 20 non sono coperte dal segreto delle telecomunicazioni e dunque possono essere comunicate nel quadro di una procedura semplificata[84]. La loro comunicazione non deve quindi avvenire nell'ambito di una procedura soggetta alle condizioni restrittive dell'articolo 269 CPP[85], in particolare all'elenco di reati menzionato al capoverso 2 di tale articolo[86]. Queste informazioni sono molto importanti per l'avanzamento delle indagini[87], che possono, a seconda del loro esito, permettere di ordinare la sorveglianza alle rigide condizioni dell'articolo 269 CPP[88].

Il *capoverso 1 lettera a* riprende l'attuale articolo 14 capoverso 1 lettera a LSCPT, aggiungendo il nome e la data di nascita, che sono elementi identificativi classici, anche per le autorità e ai fini di cui all'articolo 20 AP.

Il *capoverso 1 lettera b* riprende l'attuale articolo 14 capoverso 1 lettera b LSCPT.

Il *capoverso 1 lettera c* riprende l'attuale articolo 14 capoverso 1 lettera c LSCPT, utilizzando tuttavia la forma plurale. Se s'intende sorvegliare una persona è infatti utile conoscere tutti i tipi di collegamenti (p.es. telefono fisso, mobile e Internet) di cui dispone, e non soltanto un tipo di collegamento. Ciò permette di determinare con cognizione di causa quale tipo di collegamento deve essere sottoposto a sorveglianza. Occorre inoltre evitare di dover interrogare i fornitori di servizi di telecomunicazione tante volte quanti sono i tipi di collegamenti di cui dispone la persona in oggetto.

Il *capoverso 2* ricalca in sostanza l'attuale articolo 15 capoverso 5^{bis} LSCPT e tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, attribuendo gli obblighi menzionati non soltanto ai fornitori di servizi di telecomunicazione, ma anche alle persone indicate all'articolo 2 capoverso 1 lettera b. Ciò permette di includere anche i rivenditori, per esempio quelli di carte SIM prepagate. Il capoverso 2 estende inoltre al settore di Internet l'obbligo di informare imposto ai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della LSCPT. Tale obbligo, che attualmente riguarda esclusivamente le carte SIM prepagate nel settore della telefonia mobile, in futuro interesserà anche le carte «wireless» prepagate nel settore di Internet. Per permettere ai

84 Cfr. il messaggio del 1° luglio 1998 relativo alla LSCPT attuale, FF **1998** 3319, pag. 3350.
85 RS ... (FF **2007** 6327)
86 Thomas HANSJAKOB, op. cit. n. 1-4 e 23 ad art. 14 LSCPT.
87 Cfr. il messaggio del 1° luglio 1998 relativo alla LSCPT attuale, FF **1998** 3319, pag. 3350.
88 RS ... (FF **2007** 6327)

soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della LSCPT di adempiere all'obbligo di informare anche nel settore di Internet, l'obbligo di controllo e di registrazione applicabile alle carte SIM prepagate, inserito nell'OSCPT[89] (art. 19*a*), andrà esteso anche alle carte «wireless» prepagate. Va precisato che l'obbligo di informare riguarda soltanto le informazioni ottenute al momento della registrazione, che i soggetti LSCPT sono tenuti a effettuare prima di consegnare carte SIM prepagate o carte «wireless» prepagate all'avvio di un rapporto commerciale (*Erstregistrierung*), e non i dati riguardanti persone che potrebbero entrare in possesso di dette carte in seguito. Pertanto i soggetti LSCPT devono essere in grado di fornire, durante il periodo indicato, unicamente le informazioni che hanno dovuto richiedere al momento della vendita delle carte (*Erstregistrierung*), e non i dati relativi a eventuali futuri acquirenti, visto che una registrazione successiva di tali dati non è obbligatoria. Statuire diversamente significherebbe imporre ai rivenditori formalità eccessive e un lavoro amministrativo sproporzionato (cfr. anche il commento relativo all'art. 6*a* LTC[90]). Va inoltre sottolineato che il capoverso 2 non limita la portata del successivo capoverso 3 dell'articolo 20 AP; i soggetti di cui al capoverso 2 devono infatti rispettare anche l'obbligo specificato al capoverso 3.

Il *capoverso 3* riprende e integra l'attuale articolo 14 capoverso 4 LSCPT e tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, attribuendo gli obblighi menzionati non soltanto ai fornitori di servizi di telecomunicazione, ma anche alle persone indicate all'articolo 2 capoverso 1 lettera b. Per motivi di coerenza con il ruolo di intermediario attribuito al Servizio, si esplicita che le informazioni vanno fornite al Servizio e non, come nell'attuale LSCPT, all'autorità competente[91].

Il *capoverso 4* ricalca l'attuale articolo 14 capoverso 3 LSCPT e lo integra con i periodi finali degli attuali capoversi 5 e 6 dell'articolo 15 LSCPT.

Art. 21 Obblighi connessi all'esecuzione della sorveglianza

Il *capoverso 1* riprende in sostanza l'attuale articolo 15 capoverso 1 LSCPT e lo completa sulla base del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, attribuendo gli obblighi menzionati non soltanto ai fornitori di servizi di telecomunicazione, ma anche alle persone indicate all'articolo 2 capoverso 1 lettera b. Inoltre, per meglio specificare il concetto di dati secondari e garantire l'omogeneità terminologica nel CPP[92] (nonché nella PPM[93] nella versione introdotta dal CPP[94]) e nella futura LSCPT, l'espressione che designa i dati secondari è stata sostituita con quella, in sostanza identica, utilizzata nell'articolo 273 capoverso 1 lettere a e b CPP[95] (e nell'art. 70*d* cpv. 1 lett. a e b PPM[96] nella versione introdotta dal CPP[97]). I dati secondari nell'ambito del traffico delle telecomunicazioni sono quindi designati come «i dati che consentono di individuare quando e con

89 RS **780.11**
90 RS **784.10**
91 Thomas Hansjakob, op. cit., n. 24 ad art. 14 LSCPT.
92 RS ... (FF **2007** 6327)
93 RS **322.1**
94 RS ... (FF **2007** 6327)
95 RS ... (FF **2007** 6327)
96 RS **322.1**
97 RS ... (FF **2007** 6327)

quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione». Il rinvio all'articolo 16 lettera d AP mette in evidenza il fatto che, nel caso di una sorveglianza mediante collegamento diretto, i dati raccolti vengono trasmessi, in via eccezionale, direttamente al servizio di polizia designato dall'autorità ordinante e non al Servizio, che di norma svolge il ruolo di intermediario.

Il *capoverso 2* ricalca in sostanza l'attuale articolo 15 capoverso 4 LSCPT e tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, attribuendo gli obblighi menzionati non soltanto ai fornitori di servizi di telecomunicazione, ma anche alle persone indicate all'articolo 2 capoverso 1 lettera b. Inoltre, per meglio specificare il concetto di dati secondari e garantire l'omogeneità terminologica nel CPP[98] (nonché nella PPM[99] nella versione introdotta dal CPP[100]) e nella futura LSCPT, l'espressione che designa i dati secondari è stata sostituita con quella, in sostanza identica, utilizzata nell'articolo 273 capoverso 1 lettere a e b CPP[101] (e nell'art. 70*d* cpv. 1 lett. a e b PPM[102] nella versione introdotta dal CPP[103]). I dati secondari nell'ambito del traffico delle telecomunicazioni sono quindi designati come «i dati che consentono di individuare quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione».

Il *capoverso 3* impone ai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della LSCPT di trasmettere al Servizio, su sua richiesta, soltanto una parte del flusso di dati. Quest'obbligo è complementare al compito del Servizio menzionato nell'articolo 16 lettera f AP. Il trasferimento di una parte soltanto anziché dell'intero flusso di dati può causare lavoro supplementare ai soggetti LSCPT, per la selezione che comporta; pertanto è opportuno adottare una base legale che preveda espressamente tale alternativa. Inoltre, questa possibilità non va confusa con quella riconosciuta al Servizio di mettere a disposizione dell'autorità ordinante, su richiesta di quest'ultima, solo una parte dei dati ricevuti dal soggetto incaricato di effettuare la sorveglianza. Per ulteriori dettagli si rimanda al commento relativo all'articolo 16 lettera f AP. Il capoverso 3 tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b.

Il *capoverso 4* descrive gli obblighi specifici dei soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della LSCPT nell'attuazione della procedura di sorveglianza prevista dagli articoli 270bis CPP[104] e 70*a*^{bis} PPM[105], introdotti dal presente avamprogetto. Tale procedura consiste nell'accedere al sistema informatico sorvegliato per inserirvi uno o più programmi informatici al fine di consentire, da una parte, l'intercettazione e, dall'altra, la lettura dei dati decifrati (cfr. commento relativo all'art. 270bis CPP[106]). Nel quadro di tale procedura, i sog-

98 RS ... (FF **2007** 6327)
99 RS **322.1**
100 RS ... (FF **2007** 6327)
101 RS ... (FF **2007** 6327)
102 RS **322.1**
103 RS ... (FF **2007** 6327)
104 RS ... (FF **2007** 6327)
105 RS **322.1**
106 RS ... (FF **2007** 6327)

getti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della LSCPT devono, all'occorrenza, fornire al Servizio un aiuto particolare che esula dai loro obblighi ordinari, quando le peculiarità della modalità di sorveglianza lo richiedono. Tale aiuto è previsto solo nel caso in cui sia tecnicamente necessario per la corretta esecuzione della sorveglianza. Il capoverso 4 tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di accesso a Internet, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b. Ciò permette di includere anche chi tratta dati nell'ambito di un incarico di esternalizzazione conferito dai fornitori di servizi di telecomunicazione.

Il *capoverso 5* riprende in sostanza l'attuale articolo 15 capoverso 2 secondo periodo LSCPT e lo completa sulla base del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, attribuendo gli obblighi menzionati non soltanto ai fornitori di servizi di telecomunicazione, ma anche alle persone indicate all'articolo 2 capoverso 1 lettera b.

Art. 22 Identificazione degli utenti Internet

L'*articolo 22* prevede l'obbligo a carico dei soggetti LSCPT di adottare le misure tecniche necessarie per identificare chi accede a Internet per loro tramite. Quest'obbligo si applica a tutte le modalità di accesso, nei limiti imposti dall'articolo 20 capoverso 2 AP. L'articolo 22 integra inoltre l'articolo 20 capoverso 3 AP, è rivolto soprattutto ai fornitori di accesso a Internet (*Internet-Anbieter/Zugangsvermittler*) e trova applicazione in particolare per il caso in cui gli utenti accedono a Internet per mezzo di una rete senza fili (wireless LAN, WLAN, wireless local area network; hotspot, Wi-Fi, ecc.). Questo articolo si applica soprattutto nel caso in cui la rete di un Internet caffè, di una scuola, di un comune, di un albergo, di un ristornate, di un ospedale o di un privato sia messa a disposizione di terzi (p.es. i clienti di un albergo) perché possano accedere a Internet, sia a pagamento che gratuitamente (cfr. anche commento relativo all'art. 2 cpv. 1 AP). In questo caso il fornitore di accesso a Internet (*Internet-Anbieter/Zugangsvermittler*) delle istituzioni, degli organismi e delle persone precitati (p.es. l'albergo) deve essere in grado di identificare tali terzi ovvero i computer personali di questi ultimi che si sono connessi a Internet per mezzo della rete in oggetto. L'identificazione può aver luogo in diversi modi. Spetta al fornitore di servizi di telecomunicazione in questione adottare le misure necessarie, se necessario con l'appoggio del «titolare» della rete Internet (p.es l'albergo), per adempiere al suo obbligo d'identificazione. L'identificazione può, per esempio, avvenire attraverso un telefono cellulare (indipendentemente dal fatto che l'acceso a Internet sia gratuito o a pagamento): il terzo che desidera connettersi a Internet deve prima comunicare il proprio numero di telefonia mobile e poi riceve, nell'arco di qualche secondo, una password che gli permette di connettersi. In questo modo, grazie al numero del cellulare, il fornitore di servizi di telecomunicazione è in grado di contribuire all'identificazione della persona che accede a Internet per suo tramite. L'articolo 22 tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di accesso a Internet, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b. Ciò permette di includere anche gli esterni che trattano i dati su un incarico dei fornitori di servizi di telecomunicazione. A tale proposito si rimanda anche al commento relativo all'articolo 2 capoverso 1 AP.

Art. 23 Conservazione dei dati

L'*articolo 23*, che si ispira all'attuale articolo 15 capoverso 3 LSCPT, verte sul periodo di conservazione dei cosiddetti dati secondari nell'ambito del traffico delle telecomunicazioni. Per meglio specificare il concetto di dati secondari e garantire l'omogeneità terminologica nel CPP[107] (nonché nella PPM[108] nella versione introdotta dal CPP[109]) e nella futura LSCPT, l'espressione che designa i dati secondari è stata sostituita con quella, in sostanza identica, utilizzata nell'articolo 273 capoverso 1 lettere a e b CPP[110] (e nell'art. 70*d* cpv. 1 lett. a e b PPM[111] nella versione introdotta dal CPP[112]). I dati secondari nell'ambito del traffico delle telecomunicazioni sono quindi designati come «i dati che consentono di individuare quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione». L'estensione da sei a dodici mesi della durata di conservazione dei dati secondari del traffico delle telecomunicazioni, compreso Internet, è una conseguenza dell'adozione parziale da parte del Parlamento della mozione 06.3170 presentata da Rolf Schweiger (cfr. n. 1.4.5). Allo stesso modo viene estesa la durata di conservazione dei dati secondari nell'ambito della corrispondenza postale (cfr. commento relativo all'art. 19 cpv. 2 AP). L'articolo 23 tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di accesso a Internet, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b.

Art. 24 Certificazione

In base all'*articolo 24 primo periodo*, l'assunzione delle spese da parte dei fornitori di servizi di telecomunicazione che non richiedono la certificazione e quindi devono ricorrere a terzi o al Servizio per garantire la corretta esecuzione della sorveglianza è da considerarsi la contropartita per il carattere facoltativo della certificazione (cfr. commento relativo all'art. 18 AP). Questa disposizione intende incentivare i fornitori a farsi rilasciare la certificazione ai sensi dell'articolo 18 AP. Tuttavia, nel caso indicato all'*articolo 24 secondo periodo*, i fornitori di servizi di telecomunicazione non hanno più, a differenza della situazione prevista dall'articolo 18 AP, la possibilità di scegliere se richiedere la certificazione: sono obbligati a farlo secondo le modalità dell'articolo 18 AP per dimostrare la loro idoneità a eseguire correttamente eventuali future misure di sorveglianza.

Art. 25 Informazioni relative alle tecnologie e ai servizi

Come l'articolo 24 AP, l'*articolo 25* mira a garantire una corretta esecuzione della sorveglianza ordinata. Si tratta in particolare di consentire al Servizio di anticipare le difficoltà che potrebbero insorgere nel quadro dei futuri incarichi di sorveglianza, anziché limitarsi a rimediare ai problemi che dovessero emergere nel corso dell'esecuzione della sorveglianza. L'articolo 25 serve inoltre ad adottare senza indugio le misure necessarie per permettere, all'occorrenza, al Consiglio federale di fissare in

107 RS ... (FF **2007** 6327)
108 RS **322.1**
109 RS ... (FF **2007** 6327)
110 RS ... (FF **2007** 6327)
111 RS **322.1**
112 RS ... (FF **2007** 6327)

un'ordinanza, in virtù dell'articolo 30 capoverso 2 secondo periodo AP, un importo forfettario quale emolumento per l'esecuzione di un nuovo tipo di sorveglianza, che non rientra tra quelli già previsti dalla stessa ordinanza. A tale proposito va menzionato l'articolo 4 dell'ordinanza del 7 aprile 2004 sulle tasse e indennità nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni[113], emanata sulla base dell'attuale LSCPT (cfr. commento relativo all'art. 30 AP): se la modalità di sorveglianza non è prevista nell'ordinanza, l'emolumento che l'autorità ordinante deve versare al Servizio non è fissato su base forfettaria, bensì è calcolato in funzione del tempo e dei mezzi tecnici impiegati dal Servizio («*nach Aufwand*»)[114]. In considerazione degli obiettivi perseguiti dall'articolo 25, l'obbligo di informare sussiste indipendentemente dal fatto che la tecnologia o il servizio sia stato sviluppato dal soggetto LSCPT o da terzi. L'articolo 25 tiene conto del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b.

Art. 26 Gestori di reti di telecomunicazione interne e di centralini privati e soggetti di cui all'articolo 2 capoverso 1 che non esercitano la loro attività nell'ambito del traffico delle telecomunicazioni a titolo professionale

L'*articolo 26* riprende l'attuale articolo 15 capoverso 8 LSCPT e lo completa in base al contenuto dell'articolo 2 capoverso 2 AP.

2.6 Sezione 6: Sorveglianza al di fuori di un procedimento penale

Art. 27 Ricerca in casi urgenti

L'*articolo 27* riunisce in sostanza gli attuali articoli 3*a*, 6 lettera d, 8 capoverso 5 e 9 capoverso 1bis LSCPT, inseriti nell'attuale articolo 3 LSCPT in seguito all'introduzione della legge federale sull'organizzazione delle autorità penali della Confederazione[115]. Il testo dell'articolo 3 è ripreso nell'articolo 27 AP. Per motivi di chiarezza si precisa esplicitamente che la sorveglianza può ovviamente riguardare la localizzazione della persona in questione. Questa norma non va inserita nel CPP[116], dal momento che non si applica ai procedimenti penali in corso. Questo tipo di sorveglianza si limita ai dati indicanti quando e con quali collegamenti di telecomunicazione la persona sorvegliata stabilisce o ha stabilito un contatto e ai dati relativi al traffico, ossia ai cosiddetti dati secondari, e alla localizzazione della persona sorvegliata. Non può per contro vertere sulle comunicazioni, ossia sul contenuto delle conversazioni. In caso di necessità, in conformità con il principio costituzionale della proporzionalità, è possibile sorvegliare un collegamento che non appartenga al disperso, ma a un terzo non implicato. Questa misura è indicata in particolare quando si ha motivo di ritenere che la persona dispersa utilizzi il collegamento di tale terzo.

113 RS **780.115.1**
114 Decisione del Tribunale federale del 20 marzo 2007, 1A.255/2006, consid. 3.4 e 3.5.
115 RS ... (FF **2008** 7093)
116 RS ... (FF **2007** 6327)

Art. 28 Ricerca di persone condannate

L'*articolo 28* prevede la possibilità di avvalersi della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni per ritrovare una persona condannata a una pena detentiva o a una misura privativa della libertà in base a una sentenza passata in giudicato. È opportuno inserire questa possibilità, soprattutto perché è già prevista nell'ambito dell'assistenza penale internazionale[117] in virtù dell'articolo 18*a* capoverso 1 della legge federale del 20 marzo 1981[118] sull'assistenza internazionale in materia penale. Al pari della disposizione dell'articolo 27 AP, anche questa norma non va inserita nel CPP[119], poiché non si applica ai procedimenti penali in corso, bensì a quelli già conclusi. Come previsto in sostanza dagli articoli 269 capoverso 1 lettera c CPP[120] e 27 capoverso 2 lettera a AP, questa misura di sorveglianza è sussidiaria agli altri provvedimenti adottati per trovare il ricercato. Contrariamente al caso previsto dall'articolo 27 AP, la sorveglianza non si limita ai dati secondari, ma può riguardare anche le conversazioni atte a fornire informazioni sul luogo in cui si trova la persona condannata o soggetta alla misura privativa della libertà.

Art. 29 Procedura

L'*articolo 29* stabilisce la procedura applicabile nei casi previsti dagli articoli 27 e 28 AP.

Per quanto riguarda la procedura, il *capoverso 1* rinvia, per analogia, agli articoli 271-279 CPP[121]. Visto che nel caso previsto dall'articolo 28 AP si è in presenza di una sentenza passata in giudicato e non soltanto di gravi sospetti di reato, non vi è motivo di subordinare la sorveglianza alle condizioni supplementari di cui all'articolo 269 capoverso 1 lettere a e b CPP[122], ossia la commissione di uno dei reati specificati nell'articolo 269 capoverso 2 CPP e la gravità del reato.

Il *capoverso 2* attribuisce la competenza di disporre e autorizzare la sorveglianza descritta negli articoli 27 e 28 AP. Nell'ambito dell'assistenza penale internazionale, la questione è disciplinata dall'articolo 18*a* della legge federale del 20 marzo 1981[123] sull'assistenza internazionale in materia penale, nella versione modificata dal CPP[124]. In virtù dell'articolo 18*a* capoverso 1 di tale legge, in tale ambito l'emanazione dell'ordine di sorveglianza per determinare il luogo di soggiorno di una persona perseguita compete all'Ufficio federale di giustizia.

117 Thomas Hansjakob, op. cit., n. 8 ad art. 1 LSCPT.
118 RS **351.1**
119 RS ... (FF **2007** 6327)
120 RS ... (FF **2007** 6327)
121 RS ... (FF **2007** 6327)
122 RS ... (FF **2007** 6327)
123 RS **351.1**
124 RS ... (FF **2007** 6327)

2.7 Sezione 7: Spese ed emolumenti

Art. 30

Il *capoverso 1* riprende l'attuale articolo 16 capoverso 1 LSCPT nella versione derivante dal Programma di consolidamento (PCon) 2011-2013[125], posto in consultazione dal Consiglio federale il 14 aprile 2010 e che sopprime l'indennità per i soggetti LSCPT (cfr. n. 1.4.6). Il capoverso 1 completa inoltre il testo sulla base del nuovo campo d'applicazione personale di cui all'articolo 2 capoverso 1 lettera b AP, precisando che la disposizione non riguarda soltanto i fornitori di servizi postali e di telecomunicazione, ma anche le persone indicate all'articolo 2 capoverso 1 lettera b AP. Non si prevede nemmeno il versamento di un'indennità ai soggetti LSCPT in relazione ai loro obblighi derivanti dall'articolo 21 capoverso 4 AP.

Il *capoverso 2* primo periodo precisa espressamente, per motivi di chiarezza, che l'autorità ordinante deve versare un emolumento per le prestazioni di sorveglianza fornite dal Servizio. Il capoverso 2 secondo periodo riprende l'articolo 16 capoverso 2 LSCPT nella versione derivante dal Programma di consolidamento (PCon) 2011-2013[126] (cfr. n. 1.4.6), che è la disposizione su cui si fonda l'ordinanza del Consiglio federale che fissa tali emolumenti[127] in funzione del tipo di sorveglianza. Non viene più fatta menzione delle indennità, poiché il loro versamento non è più previsto al capoverso 1. Il Consiglio federale dovrà in particolare disciplinare, in detta ordinanza, l'emolumento da versare al Servizio dall'autorità che ha ordinato la sorveglianza prevista dall'articolo 270bis CPP[128] o dall'articolo 70*d*^{bis} PPM[129]. Nel fissare l'ammontare dell'emolumento previsto per ciascun tipo di sorveglianza, il Consiglio federale deciderà in quale percentuale il totale degli emolumenti versati deve coprire le spese di funzionamento del Servizio.

Nel sistema che prevede il versamento di un'indennità appropriata ai soggetti LSCPT, l'autorità ordinante versa al Servizio un ammontare a titolo di emolumento. Successivamente quest'ultimo versa – a seconda del tipo di sorveglianza – tutta o parte di tale somma a titolo d'indennità al soggetto che ha effettuata la sorveglianza, e tiene l'eventuale differenza come corrispettivo per le prestazioni fornite all'autorità ordinante[130]. Nel sistema dell'articolo 16 capoverso 1 della LSCPT nella versione derivante dal Programma di consolidamento (PCon) 2011-2013[131] (cfr. n. 1.4.6) e nel sistema corrispondente della futura LSCPT, che invece non prevedono più un'indennità per i soggetti LSCPT, l'ammontare che l'autorità ordinante versa al Servizio a titolo di emolumento non comprende più la quota corrispondente a detta indennità.

A completamento occorre ancora menzionare che l'ammontare versato al Servizio dall'autorità ordinante a titolo di emolumento costituisce una spesa procedurale, più precisamente un disborso, che tale autorità può, nel rispetto delle regole procedurali,

125 http://www.admin.ch/ch/i/gg/pc/documents/1854/Vorlage.pdf
126 http://www.admin.ch/ch/i/gg/pc/documents/1854/Vorlage.pdf
127 RS **780.115.1**
128 RS ... (FF **2007** 6327)
129 RS **322.1**
130 RS **780.115.1**
131 http://www.admin.ch/ch/i/gg/pc/documents/1854/Vorlage.pdf

in tutto o in parte addebitare a terzi, in particolare all'imputato condannato (art. 422, 425 e 426 CPP[132]).

2.8 Sezione 8: Disposizioni penali

Art. 31 Contravvenzioni

Le contravvenzioni previste all'*articolo 31* possono essere commesse, stando all'articolo 2 AP, da privati o, stando al capoverso 4 dell'articolo 25 AP, da imprese che rientrano nel campo d'applicazione personale della LSCPT secondo l'articolo 2 AP.

La multa massima prevista dal *capoverso 1* per chi commette intenzionalmente i reati previsti alle lettere a e b è superiore all'importo massimo previsto dall'articolo 106 capoverso 1 CP[133], che è pari a 10 000 franchi. In determinati casi, tale cifra è infatti troppo bassa per dissuadere dal commettere i reati menzionati, considerati i risparmi che possono essere realizzati assumendo la condotta vietata.

Il riferimento alla punibilità del tentativo e della complicità, inserito nel *capoverso 2*, è reso necessario dall'articolo 105 capoverso 2 CP[134].

Anche la multa massima prevista dal *capoverso 3* per chi commette un reato per negligenza è superiore all'importo massimo previsto all'articolo 106 capoverso 1 CP[135]. In determinati casi anche questa cifra è infatti troppo bassa se si considerano le gravi ripercussioni che la condotta vietata può avere su importanti indagini in corso.

Il *capoverso 4* permette di punire, oltre agli individui di cui al capoverso 1, anche le imprese che rientrano nel campo d'applicazione personale secondo l'articolo 2 AP e commettono i reati di cui alle lettere a e b del capoverso 1. L'applicazione dell'articolo 102 capoversi 1, 3 e 4 CP[136] è esclusa in virtù dell'articolo 105 CP, dal momento che i reati di cui alle lettere a e b del capoverso 1 sono contravvenzioni. Per conseguire l'obiettivo prefissato è pertanto opportuno prevedere espressamente l'applicazione per analogia dell'articolo 102 capoversi 1, 3 e 4 CP[137] e dell'articolo 112 CPP[138], che sostituirà l'articolo 102*a* CP[139] con l'entrata in vigore del CPP[140]. Tuttavia, l'importo massimo della multa è stato fissato a un milione di franchi, perché i cinque milioni di franchi previsti dall'articolo 102 capoverso 1 CP[141] per crimini e delitti sembrano troppi per i reati in questione.

Per ulteriori dettagli in merito all'articolo 31 si rimanda al numero 1.4.7.

132 RS ... (FF **2007** 6327)
133 RS **311.0**
134 RS **311.0**
135 RS **311.0**
136 RS **311.0**
137 RS **311.0**
138 RS ... (FF **2007** 6327)
139 RS **311.0**
140 RS ... (FF **2007** 6327)
141 RS **311.0**

Art. 32 Giurisdizione

L'*articolo 32* non attribuisce a un'autorità amministrativa federale la competenza di perseguire e giudicare eventuali reati. La legge federale del 22 marzo 1974[142] sul diritto penale amministrativo non è infatti applicabile. Come di norma, la competenza in materia spetta quindi ai Cantoni.

2.9 Sezione 9: Vigilanza e rimedi giuridici

Art. 33 Vigilanza

Il *capoverso 1* corrisponde all'articolo 58 capoverso 1 LTC[143]. Spetta al Servizio ricoprire il ruolo di autorità di vigilanza nell'ambito della corrispondenza postale e del traffico delle telecomunicazioni, poiché ha maggiore dimestichezza con la materia e le norme applicabili.

Il *capoverso 2* corrisponde all'articolo 58 capoverso 2 lettera a LTC[144]. Elenca i provvedimenti 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, l'articolo permette al Servizio di pronunciare un'ingiunzione a rimediare alla violazione constata o ad adottare misure atte a prevenire qualsiasi recidiva. Il destinatario dell'ingiunzione dovrà informare il Servizio sulle misure adottate. Il *secondo periodo* è una disposizione analoga all'articolo 58 capoverso 5 LTC[145]. Oltre a pronunciare le misure menzionate, il Servizio può presentare una denuncia penale fondandosi sull'articolo 31 AP. Occorre precisare che, come attualmente, in caso di violazione del diritto in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni si potranno ancora pronunciare misure più incisive rispetto a quelle di competenza del Servizio in virtù del capoverso 2. L'adozione di tali misure spetta tuttavia al Dipartimento federale dell'ambiente, dei trasporti, dell'energia e della comunicazione, per la corrispondenza postale, e all'Ufficio federale delle comunicazioni e alla Commissione federale delle comunicazioni, per il traffico delle telecomunicazioni. Come attualmente, l'Ufficio federale delle comunicazioni e la Commissione federale delle comunicazioni possono intervenire in virtù degli articoli 58 e 60 della LTC[146] e il Servizio informa queste autorità sulle violazioni che ha constatato, al fine di permettere loro di adottare, se necessario, le suddette misure.

Per ulteriori dettagli in merito all'articolo 33 si rimanda al numero 1.4.8.

Art. 34 Rimedi giuridici

Il *capoverso 1* è la disposizione generale che regge il ricorso contro le decisioni adottate dal Servizio, in particolare quelle che fissano gli emolumenti (cfr. anche il commento relativo all'art. 30 AP).

142 RS **313.0**
143 RS **784.10**
144 RS **784.10**
145 RS **784.10**
146 RS **784.10**

Il *capoverso 2* è una disposizione speciale rispetto al capoverso 1 AP. Riguarda infatti i ricorsi contro particolari decisioni del Servizio, ossia quelle fondate su un ordine di sorveglianza dell'autorità competente. A differenza delle decisioni di cui al capoverso 1, le eccezioni invocabili contro tali decisioni sono limitate.

Per ulteriori dettagli in merito all'articolo 34 si rimanda al numero 1.4.9.

2.10 Sezione 10: Disposizioni finali

Art. 35 Esecuzione

L'*articolo 35* attribuisce al Consiglio federale la competenza di emanare le disposizioni di esecuzione della nuova LSCPT. Attribuisce inoltre una competenza simile ai Cantoni, con particolare riferimento all'articolo 29 capoverso 2 AP.

Art. 36 Abrogazione e modifica del diritto vigente

L'allegato a cui fa riferimento l'*articolo 36* prevede in sostanza al numero I che l'attuale LSCPT[147] sia abrogata all'entrata in vigore della nuova LSCPT, che infatti non modifica la LSCPT attuale, ma la sostituisce.

Il numero II dell'allegato a cui rinvia l'articolo 36 indica le leggi modificate, senza essere abrogate, all'entrata in vigore della nuova LSCPT come segue:

Codice di diritto processuale penale svizzero del 5 ottobre 2007[148]

Art. 269 cpv. 2 lett. a

Il 1° gennaio 1984 è entrata in vigore per la Svizzera la Convenzione del 25 ottobre 1980[149] sugli aspetti civili del rapimento internazionale di minori. Tale Convenzione obbliga la Svizzera a localizzare un minore trasferito o trattenuto illecitamente, adottando tutti i provvedimenti idonei a tal fine (art. 7 lett. a della Convenzione). Fa parte di tali provvedimenti anche il perseguimento penale per sottrazione di minorenne (art. 220 CP[150]) del genitore che ha sottratto un figlio. Attualmente, nell'ambito di una procedura penale sono disponibili varie misure istruttorie e coercitive volte anch'esse a localizzare il genitore che ha sottratto un figlio (come p.es. la sorveglianza delle carte di credito o le perquisizioni). Non è tuttavia ancora prevista la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, dato che la fattispecie della sottrazione di minorenne (art. 220 CP[151]) non figura nell'elenco delle infrazioni per il cui perseguimento può essere ordinata tale misura. Tale svista non è stata corretta nemmeno con l'adozione della legge federale del 21 dicembre 2007[152] sul rapimento internazionale dei minori e sulle Convenzioni dell'Aia sulla protezione dei minori e degli adulti. Si coglie

147 RU
148 RS ... (FF **2007** 6327)
149 RS **0.211.230.02**
150 RS **311.0**
151 RS **311.0**
152 RS **211.222.32**

pertanto l'occasione di rimediare a questa dimenticanza completando l'*articolo 269 capoverso 2 lettera a* CPP.

Art. 270 lett. b n. 1 (testo francese)

Il testo francese attuale 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 adattato.

Art. 270bis Intercettazione e decodificazione di dati *(nuovo)*

Il *capoverso 1* costituisce la base legale esplicita per impiegare, su ordine del pubblico ministero, strumenti di sorveglianza particolari che consentono di accedere al sistema informatico sorvegliato per installarvi uno o più programmi informatici speciali in grado da una parte di intercettare e dall'altra di leggere i dati. Se sono rispettate le condizioni specificate nell'articolo 270bis, sussiste un motivo legale a giustificazione di tale tipo di sorveglianza, che altrimenti potrebbe rientrare nell'articolo 143bis CP[153]; a tali condizioni una simile sorveglianza è quindi lecita (art. 14 CP[154]).

Tale metodo riveste una particolare importanza nell'ambito della sorveglianza della telefonia via Internet (Voice over IP [VoIP]), e più precisamente della telefonia via Internet del tipo *peer-to-peer*, che mette in comunicazione due computer, visto che i dati comunicati e intercettati sono criptati e, dunque, illeggibili e inutilizzabili. Il metodo consiste nell'installare un programma speciale nel computer sorvegliato per accedere ai dati scambiati decodificandoli. Risulta indicato pure nel caso in cui sia 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 questa situazione, infatti, solo l'installazione di un programma nel computer portatile o nel telefono cellulare consente di intercettare la comunicazione, anche se non è criptata. Se nei due casi descritti il programma non è in grado di funzionare perché il computer sorvegliato è dotato di un antivirus che lo neutralizza, la procedura di sorveglianza di cui all'*articolo 270bis* permette di installare nel computer sorvegliato un ulteriore programma che elude l'antivirus e consente al primo programma di funzionare lo stesso, intercettando e leggendo i dati.

La procedura di sorveglianza di cui all'*articolo 270bis* richiede un intervento più invasivo delle altre procedure, che permettono di ricavare le informazioni semplicemente attingendo ai dati registrati o deviando il traffico. Il metodo previsto dall'articolo 270bis, invece, richiede di penetrare attivamente nel sistema informatico sorvegliato per ottenere le informazioni. Viste le peculiarità di tale meccanismo, il suo impiego non costituisce una semplice questione tecnica, per cui non è disciplinato nella nuova LSCPT, ma nel CPP[155]. Tuttavia, gli obblighi specifici dei soggetti

153 RS **311.0**
154 RS **311.0**
155 RS ... (FF **2007** 6327)

LSCPT (art. 2 cpv. 1 AP) nell'attuare la sorveglianza prevista dall'articolo 270bis sono inseriti nella nuova LSCPT all'articolo 21 capoverso 4 AP.

Questo meccanismo di sorveglianza consente di accedere a tutto il sistema informatico in cui è installato il programma informatico e dunque anche a dati che non rientrano nei motivi che giustificano la sorveglianza, quali per esempio corrispondenza, foto o filmati facenti parte della sfera privata o intima. Per evitare che vengano consultati dati non pertinenti, l'ultimo periodo del *capoverso 1* esige che il pubblico ministero indichi il tipo di dati che desidera ottenere per mezzo della sorveglianza ordinata.

Occorre sottolineare che, considerate le caratteristiche esposte, tale metodo di sorveglianza è sussidiario ad altre misure di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Ciò si giustifica per il fatto che tale metodo è più invasivo rispetto alle altre misure di sorveglianza. Il ricorso a tale metodo di sorveglianza è quindi possibile soltanto a condizioni supplementari severe (rispetto a quelle menzionate all'articolo 269 del CPP[156]), ossia se le altre misure di sorveglianza adottate non hanno avuto successo oppure se non avrebbero alcuna possibilità di successo o renderebbero la sorveglianza troppo difficile. L'esistenza di queste condizioni dovrà essere verificata dall'autorità abilitata ad autorizzare la sorveglianza (cpv. 2 e art. 274 CPP[157]). Occorre inoltre ricordare che il ricorso alle altre misure di sorveglianza è già sussidiario rispetto alle misure d'istruzione tradizionali (art. 269 cpv. 1 lett. c CPP[158]), il che conferisce un carattere di «duplice sussidiarietà» al metodo di sorveglianza previsto dall'*articolo 270bis* rispetto a dette misure d'istruzione tradizionali. Quanto illustrato permette di garantire che il metodo di sorveglianza in questione sarà utilizzato soltanto se effettivamente necessario. A tal fine non è invece necessario limitare l'uso di tale metodo di sorveglianza a un catalogo di reati più ristretto rispetto a quello dell'articolo 269 capoverso 2 CPP[159]. Infatti, tutti i reati menzionati in detto articolo possono, in un caso concreto, presentare una gravità che giustifica il ricorso a tale metodo di sorveglianza. Inoltre l'articolo 269 capoverso 1 lettera b CPP[160] richiede già che il reato presenti una gravità particolare per poter ricorrere a una misura di sorveglianza della corrispondenza postale e del traffico delle comunicazioni, il che vale in particolare anche per il metodo di sorveglianza in questione.

La persona nel cui sistema informatico vengono installati uno o più programmi informatici al fine di permettere la sorveglianza ordinata sarà avvertita dell'installazione di tale/i programma/i secondo l'articolo 279 CPP[161].

Il *capoverso 2* prevede che, come tutte le misure di sorveglianza ordinate, anche quella di cui al capoverso 1 sia soggetta all'autorizzazione del giudice dei provvedimenti coercitivi. Le peculiarità del metodo di sorveglianza in questione richiedono, inoltre, l'esplicita autorizzazione del giudice dei provvedimenti coercitivi conformemente all'articolo 274 capoverso 4 lettera c CPP[162] (nuova disposizione introdotta dalla nuova LSCPT).

156 RS ... (FF **2007** 6327)
157 RS ... (FF **2007** 6327)
158 RS ... (FF **2007** 6327)
159 RS ... (FF **2007** 6327)
160 RS ... (FF **2007** 6327)
161 RS ... (FF **2007** 6327)
162 RS ... (FF **2007** 6327)

Art. 270ter Impiego di dispositivi di localizzazione *(nuovo)*

Il *capoverso 1* costituisce la base legale esplicita per l'impiego, da parte della polizia e su ordine del pubblico ministero, di dispositivi particolari al fine di garantire la sicurezza pubblica. Questi dispositivi servono a individuare dati specifici che consentono di identificare l'apparecchio di telefonia mobile utilizzato, come per esempio, il numero d'identificazione internazionale dell'apparecchio (numero IMEI) o il numero della scheda d'identificazione dell'utente (numero SIM), e per localizzare gli apparecchi di telefonia mobile.

L'«IMSI-catcher» è un particolare dispositivo che rientra tra quelli previsti dal capoverso 1 e permette di simulare l'interazione tra la stazione di riferimento di una rete di telefonia mobile e gli apparecchi di telefonia mobile che si trovano 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 riferimento. In questo modo è possibile individuare il numero d'identificazione internazionale dell'utente (numero IMSI) fino ad allora sconosciuto.

Il Servizio e i fornitori di servizi di telecomunicazione non assumono rispettivamente né compiti né obblighi particolari nell'attuazione di tale metodo di sorveglianza, il quale va distinto in particolare dalla sorveglianza volta a ottenere dai fornitori di servizi di telecomunicazione i dati relativi alle chiamate di 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. Viste le peculiarità del metodo di sorveglianza previsto dall'articolo 270ter, il suo impiego non va disciplinato nella nuova LSCPT, ma nel CPP[163].

I dispositivi di cui al capoverso 1, utilizzati dalla polizia, possono interferire con le telecomunicazioni. Il capoverso 1 prevede quindi che non sono ammessi senza previa autorizzazione dell'Ufficio federale delle comunicazioni, che si fonda sull'articolo 32*a* LTC[164] e sull'articolo 49 e seguenti dell'ordinanza del 9 marzo 2007[165] sulla gestione delle frequenze e sulle concessioni di radiocomunicazione. In pratica, per ottenere l'autorizzazione, l'autorità che desidera utilizzare un dispositivo di cui al capoverso 1 deve presentare una domanda all'Ufficio federale delle comunicazioni, indicando i parametri tecnici del dispositivo. L'Ufficio decide se sono soddisfatte le condizioni per l'autorizzazione e in particolare se l'utilizzo del dispositivo non leda eccessivamente, in termini di efficacia delle telecomunicazioni, altri interessi pubblici o di terzi. L'Ufficio valuta il pericolo di interferenze nelle telecomunicazioni e in particolare nelle reti di telefonia mobile dovute all'impiego del dispositivo in questione. Una volta ottenuta l'autorizzazione, il dispositivo può essere utilizzato nell'ambito della sorveglianza senza che l'Ufficio debba rinnovare l'autorizzazione per ogni nuova sorveglianza.

Il *capoverso 2* prevede che, come tutte le misure di sorveglianza disposte, anche quella specificata nel capoverso 1 debba essere soggetta all'autorizzazione del giudice dei provvedimenti coercitivi. Le peculiarità del metodo di sorveglianza richiedono, inoltre, l'espressa autorizzazione del giudice dei provvedimenti coercitivi con-

163 RS ... (FF **2007** 6327)
164 RS **784.10**
165 RS **784.102.1**

formemente all'articolo 274 capoverso 4 lettera c CPP[166] (nuova disposizione introdotta dalla nuova LSCPT).

Art. 271 cpv. 1 e 2

I capoversi 1 e 2 dell'*articolo 271* sono stati riformulati.

Il *capoverso 1* si ispira al capoverso 1 in vigore. Per ragioni di chiarezza, tuttavia, in considerazione del funzionamento dell'attuale sistema gestito dal Servizio, il *primo periodo* del capoverso 1 in vigore è stato integrato in modo da stabilire esplicitamente che, nel caso di cui al capoverso 1 e al fine di salvaguardare il segreto professionale, le autorità inquirenti non possono accedere direttamente alle informazioni raccolte nell'ambito della sorveglianza effettuata, contrariamente a quanto avviene di norma. Dunque è solo dopo la cernita dei dati prevista dal capoverso 1 che le autorità inquirenti possono venire a conoscenza delle informazioni che non sono state scartate. Ovviamente, la necessità di una cernita implica che la sorveglianza non può essere effettuata avvalendosi di un collegamento diretto (cfr. commento relativo al cpv. 2).

Il *capoverso 2* riprende in sostanza l'attuale capoverso 2. Spiega tuttavia il caso previsto da quest'ultimo da un altro punto di vista più logico, poiché il capoverso 2 deve essere considerato come 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 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 effettuata con un collegamento diretto (*Direktschaltung*). Le caratteristiche del collegamento diretto – da non confondere con la sorveglianza in tempo reale (*Echtzeit-Überwachung*) – rendono infatti materialmente impossibile la cernita prevista dal capoverso 1 (cfr. commento relativo all'art. 16 lett. d AP). Va precisato che, in base al *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[167].

Art. 273 cpv. 3

L'*articolo 273 capoverso 3* estende da sei a dodici mesi il periodo per il quale i cosiddetti dati secondari possono essere richiesti con effetto retroattivo. 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. 2 e art. 23 AP). Per ulteriori dettagli si rimanda al numero 1.4.5.

Art. 274 cpv. 4 lett. c e d (nuove)

L'*articolo 274 capoverso 4 lettera c* rinvia al metodo di sorveglianza di cui all'articolo 270bis CPP[168], una disposizione introdotta dalla nuova LSCPT. Le peculiarità di

166 RS ... (FF **2007** 6327)
167 RS ... (FF **2007** 6327)
168 RS ... (FF **2007** 6327)

tale metodo (cfr. commento all'art. 270bis CPP[169]) richiedono l'autorizzazione esplicita del giudice dei provvedimenti coercitivi come previsto dalla presente disposizione.

L'*articolo 274 capoverso 4 lettera d* rinvia al metodo di sorveglianza di cui all'articolo 270ter CPP[170], una disposizione introdotta dalla nuova LSCPT. Le peculiarità di tale metodo (cfr. commento all'art. 270ter CPP[171]) richiedono l'esplicita autorizzazione del giudice dei provvedimenti coercitivi come previsto dalla presente disposizione.

Art. 278 cpv. 1bis

Il rimando contenuto nell'*articolo 278 capoverso 1bis*, una disposizione introdotta dalla legge federale sull'organizzazione delle autorità penali della Confederazione[172], deve essere modificato e completato. Il rinvio all'attuale articolo 3 LSCPT[173] va sostituito con il rinvio all'articolo 27 della nuova LSCPT (cfr. commento relativo all'art. 27 AP). È inoltre opportuno rinviare anche all'articolo 28 della nuova LSCPT, dal momento che esso, come l'articolo 27, non contempla i procedimenti penali in corso (cfr. commento relativo all'art. 28 AP) e che anche in una situazione del genere sono possibili scoperte casuali.

Procedura penale militare del 23 marzo 1979[174]

Art. 70a lett. b n. 1 (testo francese)

Il commento relativo all'articolo 270 lettera b numero 1 CPP[175] si applica per analogia all'*articolo 70a lettera b numero 1*, una disposizione introdotta dal CPP[176].

Art. 70abis Intercettazione e decodificazione di dati *(nuovo)*

Il commento relativo all'articolo 270bis CPP[177] si applica per analogia all'*articolo 70abis*. L'*articolo 70e capoverso 4 lettera c*, una disposizione introdotta dalla nuova LSCPT, è l'equivalente nella PPM[178] dell'articolo 274 capoverso 4 lettera c CPP[179].

Art. 70ater Impiego di dispositivi di localizzazione *(nuovo)*

Il commento relativo all'articolo 270ter CPP[180] si applica per analogia all'*articolo 70ater*. L'*articolo 70e capoverso 4 lettera d*, una disposizione introdotta dalla

169 RS ... (FF **2007** 6327)
170 RS ... (FF **2007** 6327)
171 RS ... (FF **2007** 6327)
172 RS ... (FF **2008** 7093)
173 RS **780.1**
174 RS **322.1**
175 RS ... (FF **2007** 6327)
176 RS ... (FF **2007** 6327)
177 RS ... (FF **2007** 6327)
178 RS **322.1**
179 RS ... (FF **2007** 6327)
180 RS ... (FF **2007** 6327)

nuova LSCPT, è l'equivalente nella PPM[181] dell'articolo 274 capoverso 4 lettera d CPP[182].

Art. 70b

Il commento all'articolo 271 capoversi 1 e 2 CPP[183] si applica per analogia all'*articolo 70b capoversi 1 e 2*, nuove disposizioni introdotte dal CPP[184]. Il rinvio all'articolo 75 lettere a e c nell'*articolo 70b capoverso 3*, anch'esso una disposizione introdotta dal CPP[185], è rimpiazzato dal rinvio all'articolo 75 lettera b, cui corrispondono gli articoli 170-173 CPP[186] menzionati nell'articolo 271 CPP. Va pertanto tracciato un parallelismo tra quest'ultimo e l'articolo 70*b*.

Art. 70d cpv. 3

L'*articolo 70d capoverso 3*, una disposizione introdotta dal CPP[187], estende da sei a dodici mesi il periodo per il quale i cosiddetti dati secondari possono essere richiesti con effetto retroattivo. 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. 2 e art. 23 AP). Per ulteriori dettagli si rimanda al numero 1.4.5.

Art. 70e cpv. 4 lett. c e d (nuove)

L'*articolo 70e capoverso 4 lettera c* rinvia al metodo di sorveglianza di cui all'articolo 70*a*^{bis} PPM[188], una disposizione introdotta dalla nuova LSCPT. Le peculiarità di tale metodo (cfr. commento all'art. 70*a*^{bis} PPM[189]) richiedono l'esplicita autorizzazione del giudice dei provvedimenti coercitivi come previsto dalla presente disposizione.

L'*articolo 70e capoverso 4 lettera d* rinvia al metodo di sorveglianza di cui all'articolo 70*a*^{bis} PPM[190], una disposizione introdotta dalla nuova LSCPT. Le peculiarità di tale metodo (cfr. commento all'art. 70*a*^{ter} PPM[191]) richiedono l'esplicita autorizzazione del giudice dei provvedimenti coercitivi come previsto dalla presente disposizione.

Legge del 30 aprile 1997[192] sulle telecomunicazioni

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

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

181 RS **322.1**
182 RS ... (FF **2007** 6327)
183 RS ... (FF **2007** 6327)
184 RS ... (FF **2007** 6327)
185 RS ... (FF **2007** 6327)
186 RS ... (FF **2007** 6327)
187 RS ... (FF **2007** 6327)
188 RS **322.1**
189 RS **322.1**
190 RS **322.1**
191 RS **322.1**
192 RS **784.10**

indicate. In tal modo si evita di dover fondare tale obbligo su un'interpretazione estensiva dell'articolo 20 capoverso 2 AP. Lo scopo 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 e di schede «wireless» prepagate.

Per ragioni pratiche, l'obbligo menzionato si limita alla situazione in cui i clienti dei fornitori di servizi di telecomunicazione hanno, al momento dell'avvio e della registrazione del rapporto commerciale (cfr. commento relativo all'art. 20 cpv. 2 AP), utilizzato l'identità di una persona inesistente o che non ha acconsentito all'avvio di tale rapporto. Una situazione del genere si può verificare nel caso in cui il controllo preliminare non si sia svolto conformemente a quanto prescritto (cfr. commento relativo all'art. 20 cpv. 2 AP). 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 qualora, sebbene il controllo dell'identità sia stato effettuato come prescritto, i clienti in questione non dovessero più corrispondere a quelli registrati all'avvio del rapporto commerciale. Un telefono cellulare munito di carta SIM prepagata può, infatti, essere per esempio 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.

Art. 37 Disposizioni transitorie

L'*articolo 37* non prevede disposizioni transitorie particolari. La nuova LSCPT si applica nella sua totalità sin dall'entrata in vigore, anche alle sorveglianze in corso ordinate prima di tale data.

Art. 38 Referendum ed entrata in vigore

Il *capoverso 1* precisa che la nuova LSCPT sottostà a referendum.

Il *capoverso 2* precisa che il Consiglio federale decide la data dell'entrata in vigore della nuova LSCPT.

3 Ripercussioni finanziarie e sull'effettivo del personale

3.1 Ripercussioni per la Confederazione

I nuovi compiti attribuiti esplicitamente al Servizio genereranno costi supplementari per la Confederazione, anche nell'ambito del personale. Tale aumento deve ovviamente essere considerato in rapporto al miglioramento apportato dalla nuova LSCPT nel perseguimento dei reati. Spetta al Consiglio federale decidere se tali costi supplementari devono essere compensati – in virtù del Programma di consolidamento

(PCon) 2011-2013[193], che il Consiglio federale ha posto in consultazione il 14 aprile 2010 (cfr. n. 1.4.6), e, soprattutto, della moratoria delle spese adottata dal Consiglio federale il 30 settembre 2009 – oppure se ciò non è necessario. In caso affermativo si tratterà di definire le modalità. È in particolare ipotizzabile una compensazione interna al DFGP in termini di personale o un aumento degli emolumenti (cfr. il commento all'art. 30 cpv. 2 AP).

L'effetto dell'avamprogetto sulle finanze della Confederazione, sotto il profilo del personale del Servizio e dei suoi costi di funzionamento, è stimato come segue:

- gli articoli 6-13 AP implicano un aumento di 6,0 posti e di 2,5 milioni di franchi all'anno a titolo di costi d'esercizio (inclusi i costi del personale) e un investimento di 1,6 milioni di franchi. Tali cifre sono in primo luogo legate al funzionamento operativo del nuovo sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni utilizzato dal Servizio. Tale sistema dovrà infatti permettere la conservazione di una grande quantità di dati in condizioni ottimali e a lungo termine. La ripercussione stimata sulle finanze della Confederazione è anche legata ai compiti di gestione assunti dal Servizio, in particolare per quanto riguarda l'amministrazione degli accessi ai dati contenuti nel sistema e il controllo del termine di conservazione di tali dati. Va sottolineato che le presenti informazioni tengono conto dei risparmi derivanti dal passaggio al nuovo sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni;
- l'articolo 17 AP implica un aumento di 0,50 posti e di 100 000 franchi all'anno a titolo di costi d'esercizio (inclusi i costi del personale);
- gli articoli 18 e 24 AP implicano un aumento di 3,50 posti e di 700 000 franchi all'anno a titolo di costi d'esercizio (inclusi i costi del personale);
- l'articolo 21 capoverso 4 AP implica un aumento di 2,50 posti e di 900 000 franchi all'anno a titolo di costi d'esercizio (inclusi i costi del personale);
- l'articolo 23 AP implica un aumento di 0,25 posti, di 750 000 franchi all'anno a titolo di costi d'esercizio (compresi i costi del personale) e un investimento di 100 000 franchi, dato che il Servizio registra i dati che i soggetti LSCPT dovranno ora conservare per dodici mesi e non più per sei;
- l'articolo 25 AP implica un aumento di 1 posto e di 200 000 franchi all'anno a titolo di costi d'esercizio (compresi i costi del personale);
- l'articolo 28 AP implica un aumento di 0,25 posti e di 50 000 franchi all'anno a titolo di costi d'esercizio (compresi i costi del personale).

Riassumendo, le suddette ripercussioni del presente avamprogetto sono stimate come segue:

- aumento di 14 posti di lavoro;
- 1,7 milioni di franchi di spese d'investimento
- aumento di 5,2 milioni di franchi all'anno delle spese d'esercizio, comprese quelle per il personale.

Occorre ricordare che tale stima si fonda su una situazione che tiene già conto delle ripercussioni – positive per le finanze della Confederazione – derivanti

[193] http://www.admin.ch/ch/i/gg/pc/documents/1854/Vorlage.pdf

dall'abolizione dell'indennità per i soggetti LSCPT. Tale abolizione è infatti una misura che fa parte del Programma di consolidamento (PCon) 2011-2013[194], che il Consiglio federale ha posto in consultazione il 14 aprile 2010 (cfr. n. 1.4.6).

È necessario precisare, a titolo di osservazione, che l'acquisto del nuovo sistema di trattamento dei dati raccolti in occasione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni gestito dal Servizio non è retto dal presente avamproggetto. Le risorse supplementari per l'introduzione del nuovo sistema sono già previste (decisione del Consiglio federale del 17 giugno 2009).

3.2 Ripercussioni per i Cantoni

L'evoluzione futura dei costi della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni potrà ripercuotersi sugli emolumenti.

Il passaggio al nuovo sistema informatico per il trattamento dei dati raccolti nell'ambito della sorveglianza del traffico delle telecomunicazioni comporterà, per i Cantoni, una riduzione dei costi per l'attrezzatura (cfr. n. 1.4.2). Per quanto riguarda gli emolumenti si veda il commento in merito all'articolo 30 AP.

3.3 Ripercussioni sull'economia

Il presente avamprogetto genererà costi supplementari per i soggetti LSCPT, ossia per chi effettua la sorveglianza in virtù di detta legge. Per quanto concerne in particolare i fornitori di servizi di telecomunicazione, tale aumento va tuttavia relativizzato dato che il costo della sorveglianza rappresenta una quota limitata del loro fatturato. L'aumento va relativizzato considerando anche la maggiore efficacia del perseguimento dei reati consentita dalla nuova LSCPT.

4 Programma di legislatura

Il presente avamprogetto non è previsto nel messaggio del 23 gennaio 2008[195] sul programma di legislatura 2007-2011 né nel decreto federale del 18 settembre 2008[196] sul programma di legislatura 2007-2011. Ciò è dovuto al fatto che al momento dell'elaborazione del messaggio sul programma di legislatura 2007-2011, l'avamprogetto non era abbastanza avanzato per esservi compreso.

194 http://www.admin.ch/ch/i/gg/pc/documents/1854/Vorlage.pdf
195 FF **2008** 597
196 FF **2008** 7469

5 Aspetti giuridici

La nuova LSCPT si fonda sugli articoli 92 capoverso 1 e 123 capoverso 1 della Costituzione federale[197], 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.

Prevede deleghe in ambito legislativo al Consiglio federale e ai Cantoni.

La nuova LSCPT non pone problemi per quanto riguarda il diritto internazionale.

[197] RS **101**