Rapporto esplicativo Progetto marzo 2017

concernente la revisione totale dell'ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT; RS 780.11)

A. Situazione iniziale

La revisione totale della legge federale del 6 ottobre 2000[1] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) rende necessaria la revisione totale delle ordinanze d'esecuzione e dunque anche dell'ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT).

Il progetto di revisione dell'OSCPT è suddiviso in quattro capitoli: disposizioni generali, corrispondenza postale, traffico delle telecomunicazioni e disposizioni finali. Descrive i singoli diritti e doveri in modo molto dettagliato, poiché è stata auspicata una maggiore certezza del diritto. Il progetto di ordinanza non distingue più, ad esempio, soltanto tra forme di sorveglianza in tempo reale e forme di sorveglianza retroattiva, ma è articolato in modo da prevedere per ogni servizio offerto disposizioni specifiche che ne descrivono, se del caso, la sorveglianza in tempo reale e quella retroattiva. Ne consegue che sono descritte in modo molto dettagliato anche i presupposti per ogni tipo di informazione o sorveglianza.

Oltre all'auspicata certezza del diritto, la densità normativa ha l'obiettivo di standardizzare il più possibile i tipi di informazioni e di sorveglianza nell'ambito del traffico delle telecomunicazioni, favorendo in tal modo le procedure automatiche.

Un'ulteriore differenza rispetto all'ordinanza vigente è inoltre la rinuncia alla distinzione tra servizi di telecomunicazione a commutazione di circuito (CS) e quelli a commutazione di pacchetto (PS). Una tale distinzione non è più conforme alle nuove tecnologie, grazie alle quali, ad esempio, si usa sempre più spesso Internet per telefonare. Nella nuova ordinanza le singole forme di sorveglianza sono invece suddivise in sorveglianza di servizi di accesso alla rete (sezione 8 e art. 60) e sorveglianza delle applicazioni (sezione 9 e art. 61-63).

Inoltre, nell'ambito della revisione totale della legge è stata ampliata la cerchia delle persone obbligate a collaborare. In virtù della legislazione vigente non è ad esempio possibile imporre i doveri legati alla sorveglianza ai fornitori di servizi di telecomunicazione esenti dall'obbligo di notifica e ai fornitori di servizi di comunicazione derivati operanti su Internet senza essere fornitori di accesso a Internet. In virtù dell'articolo 2 lettera c nLSCPT, i fornitori di servizi di comunicazione derivati sono ora inclusi nel campo d'applicazione personale. Si tratta di fornitori i cui servizi si basano su servizi di telecomunicazione e che permettono ai loro utenti una comunicazione unilaterale (p. es. caricare un documento) o multilaterale (p. es e-mail, instant messaging o chat). Inoltre, in futuro il campo d'applicazione personale nell'ambito della sorveglianza del traffico delle telecomunicazioni non sarà più legato all'obbligo di notifica sancito

[1] RS **780.1;** per il testo in votazione cfr. FF **2016** 1675 (nLSCPT)

dall'articolo 4 della legge sulle telecomunicazioni[2]. In tal modo il campo d'applicazione contempla anche i fornitori che secondo il diritto vigente non sono sottoposti all'obbligo di notifica.

Visto questo disciplinamento ci si potrebbe aspettare un aumento del numero delle persone obbligate a collaborare e tenute a mettere attivamente in pratica gli obblighi di informazione e di sorveglianza; tuttavia molto probabilmente il loro numero diminuirà. Ciò è dovuto al fatto che la nuova ordinanza permette al Consiglio federale di sollevare i fornitori di servizi di telecomunicazione da determinati obblighi di sorveglianza se forniscono servizi di esigua importanza economica o nel settore dell'educazione (cfr. il commento all'art. 49). Ai fornitori di servizi di comunicazione derivati, che sono tenuti in linea di massima a tollerare la sorveglianza, possono invece essere imposti obblighi più estesi di informazione e di sorveglianza qualora offrano servizi di grande importanza economica o li forniscano a un gran numero di utenti. Tuttavia, giacché le condizioni sono molto severe, ci saranno pochi fornitori di servizi di comunicazione derivati che dovranno svolgere attivamente attività di sorveglianza (cfr. il commento all'art. 50) e molti fornitori di servizi di telecomunicazione che fino ad ora sono stati sottoposti a questo obbligo non lo saranno più. La maggior parte dei fornitori di servizi di comunicazione derivati e dei fornitori di servizi di telecomunicazione saranno soltanto tenuti a tollerare eventuali sorveglianze effettuate dal servizio di sorveglianza della corrispondenza postale e del traffico delle comunicazioni (Servizio SCPT) o da persone da esso incaricate. A tale scopo devono permettere senza indugio l'accesso alle loro installazioni, fornire le informazioni necessarie all'esecuzione della sorveglianza, sopprimere i criptaggi da loro effettuati e consegnare i metadati a loro disposizione (per il termine *metadati* si veda il commento introduttivo alla sezione 10 del capitolo 3). Inoltre, con la revisione totale è stata espressamente concessa la possibilità a determinati servizi federali di presentare una domanda d'informazione o di inoltrare un incarico di sorveglianza al Servizio SCPT (cfr. il commento all'art. 1). La Segreteria di Stato dell'economia, ad esempio, potrà d'ora innanzi esercitare più facilmente il suo diritto di querela e combattere efficacemente le chiamate pubblicitarie indesiderate, poiché grazie alle nuove disposizioni potrà chiedere al Servizio SCPT informazioni sui relativi collegamenti di telecomunicazione. Anche il Servizio delle attività informative della Confederazione potrà procurarsi tutti i tipi di informazione tramite il Servizio SCPT.

Al fine di non pregiudicare il buon andamento della sorveglianza, la revisione totale prevede anche la valutazione della qualità delle informazioni e dei dati sulla sorveglianza trasmessi. Il presente progetto di revisione dell'ordinanza stabilisce il livello di qualità necessario e chi è tenuto ad assicurarlo (cfr. il commento all'art. 27). Il SCPT assume la funzione di autorità di vigilanza e in caso di mancata osservanza delle disposizioni legali, per esempio nello stabilire il livello di qualità, può infliggere sanzioni amministrative o addirittura penali ai fornitori coinvolti conformemente agli articoli 41 o 39 capoverso 1 lettera a nLSCPT.

Al fine di garantire la corretta esecuzione della sorveglianza del traffico delle telecomunicazioni e della trasmissione delle informazioni, sono inoltre sanciti nella legge i cosiddetti controlli di conformità (procedura di compliance) applicati dal Servizio SCPT. Si tratta della procedura tesa a verificare la disponibilità a

[2] RS **784.2**

informare e sorvegliare di un fornitore (art. 31-34 nLSCPT). Occorre soprattutto verificare che i fornitori che hanno l'obbligo di fornire informazioni o di eseguire la sorveglianza siano in grado di farlo (crf. il commento agli art. 29−32).

B. Commento ai singoli articoli

Capitolo 1: Disposizioni generali

Sezione 1: Introduzione

Art. 1 Oggetto e campo d'applicazione

L'*articolo 1 capoverso 1* corrisponde al vigente articolo 1 capoverso 1 OSCPT del 31 ottobre 2001[3] (stato al 1° gennaio 2012).

Il *capoverso 2* precisa il campo d'applicazione personale dell'articolo 2 nLSCPT. Come nell'articolo 1 OSCPT vigente sono indicati come destinatari le autorità che dispongono la sorveglianza (qui appresso: autorità disponenti) e quelle che dirigono i procedimenti (di norma i pubblici ministeri; *lett. a*) e le autorità d'approvazione (di norma il giudice dei provvedimenti coercitivi; *lett. b*). Sono state aggiunte le autorità di polizia federali, cantonali e comunali (*lett. c*), al fine di avere una lista esaustiva di tutti i servizi aventi diritto all'informazione. In seguito alle disposizioni dell'articolo 15 capoverso 2 lettera a e b nLSCPT, rispetto all'OSCPT del 31 ottobre 2001[4] l'elenco è stato inoltre integrato con il Servizio delle attività informative della Confederazione (SIC; *lett. d*) e con la Segreteria di Stato dell'economia (SECO; *lett. e*), in quanto anch'essi sono servizi aventi diritto all'informazione. A questi si aggiungono le autorità della Confederazione e dei Cantoni di cui all'articolo 15 capoverso 1 lettera c nLSCPT, che hanno bisogno di informazioni sui dati per il disbrigo di cause di diritto penale amministrativo (*lett. f*). Infine anche il Servizio SCPT (*lett. g*) rientra ovviamente nel campo d'applicazione dell'OSCPT.

Una delle modifiche più importanti della revisione totale della LSCPT è costituita dall'ampliamento della cerchia delle cosiddette **persone obbligate a collaborare**. Con ciò si intendono persone che sottostanno alla LSCPT e ai doveri che ne risultano, sia che si tratti di doveri attivi, come per esempio la cosiddetta disponibilità a sorvegliare (cfr. art. 32 nLSCPT), sia di doveri passivi, come l'obbligo di tollerare la sorveglianza (cfr. art. 26 cpv. 2 e 6, art. 27 cpv. 1 e 2, art. 28 e 29 nLSCPT). Nel capoverso 2 lettere h-m sono state inserite le seguenti categorie di persone obbligate a collaborare:

- *lettera h*: i fornitori di servizi postali (FSP) secondo la legge del 17 dicembre 2010[5] sulle poste (LPO)[6];

- *lettera i*: i fornitori di servizi di telecomunicazione (FST) secondo l'articolo 3 lettera b della legge sulle telecomunicazioni del 30 aprile 1997 (LTC)[7]

3 RS **780.11**
4 RS **780.11**
5 RS **783.0**
6 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT; commento all'art. 2 lett. a, FF **2013** 2283 2306.

- *lettera j*: i fornitori di servizi che si fondano su servizi di telecomunicazione e permettono una comunicazione unilaterale o multilaterale (fornitori di servizi di comunicazione derivati)[8];

- *lettera k*: i gestori di reti di telecomunicazione interne[9];

- *lettera l*: le persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazione[10];

- *lettera m*: i rivenditori professionali di carte o altri mezzi analoghi che consentono di accedere a una rete pubblica di telecomunicazione[11];

Art. 2 Termini e abbreviazioni

L'*articolo 2* rinvia all'allegato per la definizione di numerosi termini e per le abbreviazioni si basa sull'articolo 2 OSCPT del 31 ottobre 2001[12].

Sezione 2: Ordine di sorveglianza

Art. 3 Trasmissione al Servizio SCPT

L'*articolo 3 capoverso 1* disciplina i mezzi di trasmissione approvati per l'inoltro al Servizio SCPT, da parte delle autorità disponenti, degli ordini di sorveglianza nonché delle loro proroghe e revoche e per la comunicazione dei diritti d'accesso da concedere.

I diritti d'accesso al sistema di trattamento del Servizio SCPT valgono per le pertinenti misure di sorveglianza e i membri, designati dall'autorità disponente, delle autorità inquirenti che si occupano del caso in questione e devono trattare i dati nell'ambito dell'inchiesta penale. Di norma i diritti d'accesso sono gestiti su due livelli. Di solito ogni autorità di perseguimento penale coinvolta nelle misure di sorveglianza designa un responsabile per gli utenti con la funzione di amministratore dell'organizzazione (AO) che gestisce i diritti d'accesso per ogni misura di sorveglianza all'interno dell'organizzazione. Il Servizio SCPT autorizza l'AO ad adottare le misure di sorveglianza secondo le indicazioni dell'autorità disponente nell'ordine di sorveglianza (cfr. art. 47). L'AO dell'autorità di perseguimento penale così autorizzato gestisce autonomamente i diritti d'accesso alle singole attività di sorveglianza per i membri della propria organizzazione secondo le indicazioni dell'autorità disponente (cfr. art. 8 e 9 dell'ordinanza del xx.xx.xxxx[13] sul sistema di trattamento per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni [OST-SCPT).

7 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. b, FF **2013** 2283 2306.
8 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. c, FF **2013** 2283 2307.
9 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. c, FF **2013** 2283 2308.
10 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. c, FF **2013** 2283 2308.
11 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. c, FF **2013** 2283 2308.
12 RS **780.11**
13 RS **XX.XXX**

In alternativa un'autorità di perseguimento penale può chiedere al Servizio SCPT di occuparsi della gestione degli utenti per ogni misura di sorveglianza. In tal caso quest'ultimo gestisce i diritti d'accesso dei singoli utenti alle misure di sorveglianza secondo le indicazioni dell'ordine di sorveglianza dell'autorità disponente (cfr. art. 47).

Qualora siano necessarie delle modifiche in merito alle misure di sorveglianza (p. es modificare o aggiungere una forma di sorveglianza, modificare l'elemento d'indirizzo sorvegliato a causa di una svista delle autorità di perseguimento penale), l'autorità disponente deve inoltrare un nuovo ordine di sorveglianza soggetto ad emolumento al Servizio SCPT. La modifica dei diritti d'accesso non genera nuovi emolumenti.

Fanno ad esempio parte dei «mezzi di trasmissione sicuri approvati dal Servizio SCPT» di cui alla *lettera a* un'interfaccia elettronica per gli ordini conforme agli standard ETSI o le soluzioni di cifratura per le e-mail usate dal Servizio SCPT. Le corrispondenti disposizioni sono emanate nell'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT; cfr. anche il commento all'art. 70).

La *lettera b* permette la trasmissione dell'ordine per posta o telefax al Servizio SCPT, ma soltanto se motivi tecnici impediscono la trasmissione conformemente alla lettera a. Le autorità di perseguimento penale devono pertanto innanzitutto adoperarsi affinché l'ordine sia trasmesso conformemente alla lettera a.

La *lettera c* stabilisce che, in caso di ordine telefonico, ammissibile soltanto in casi urgenti (p. es. ricerche di emergenza, ordini al di fuori degli orari d'ufficio), occorre inoltrare successivamente l'ordine con un mezzo di trasmissione conforme alla lettera a o b.

Secondo il *capoverso 2* il Servizio SPCT può sostituire il mezzo di trasmissione di cui al capoverso 1 lettera a con un accesso in linea al proprio sistema di trattamento. Ciò agevola molto gli inoltri delle autorità disponenti al Servizio SCPT; spetterà a quest'ultimo decidere il momento a partire dal quale gli ordini potranno essere trasmessi soltanto attraverso l'accesso in linea.

Art. 4 Esecuzione della sorveglianza

L'*articolo 4* corrisponde essenzialmente all'articolo 17 capoversi 1 e 6 dell'OSCPT in vigore[14] e disciplina l'esecuzione della sorveglianza.

Il *capoverso 1* corrisponde alla disposizione vigente.

Se a seguito di problemi di esercizio la persona obbligata a collaborare è impossibilitata ad adempiere i propri obblighi in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, secondo il capoverso 2 è tenuta a comunicarlo immediatamente al Servizio SCPT e a motivare successivamente tale inadempienza per scritto. I problemi di esercizio comprendono sia motivi tecnici sia motivi organizzativi. Tali problemi possono avere conseguenze (p. es. art. 33 cpv. 5 e art. 34 cpv. 1 LSCPT).

È importante che le persone obbligate a collaborare informino immediatamente il Servizio SCPT sui problemi in merito ad attività di sorveglianza e agli ordini di

14 RS **780.11**

sorveglianza, per i quali il tempo è un fattore decisivo. Pertanto la comunicazione va fatta immediatamente per telefono al Servizio SCPT. Nel caso in cui non fosse in grado di evadere un ordine di sorveglianza o di adempiere all'obbligo di svolgere attività di sorveglianza in tempo reale, la persona obbligata a collaborare deve contattare, durante gli orari d'ufficio, il centralino oppure, al di fuori degli orari d'ufficio, il numero di picchetto del settore competente del Servizio SCPT. Il giorno successivo la persona obbligata a cooperare deve notificare per scritto il guasto al Servizio SCPT menzionandone la durata, descrivendo il problema, fornendo una panoramica cronologica delle misure prese e illustrando lo stato attuale del problema. Se fino ad allora il guasto non è stato riparato, dopo l'eliminazione del guasto deve inoltrare al Servizio SCPT una pertinente notifica.

Nel caso di un simile guasto e indipendentemente dalla causa del problema, secondo il *capoverso 3* la persona obbligata a collaborare è tenuta a memorizzare, per il lasso di tempo indicato nelle prescrizioni tecniche del DFGP, e successivamente consegnare senza indugio almeno i metadati della sorveglianza in tempo reale (per il termine *metadati della sorveglianza in tempo reale* si veda il commento introduttivo alla sezione 10 del capitolo 3). Se i metadati della sorveglianza in tempo reale non dovessero più essere disponibili o se dovessero essere incompleti, la persona tenuta a collaborare deve consegnare senza indugio i corrispondenti metadati della sorveglianza retroattiva conformemente alle direttive del Servizio SCPT (per il termine *metadati della sorveglianza retroattiva* si veda il commento introduttivo alla sezione 10 del capitolo 3).

Art. 5 Salvaguardia del segreto d'ufficio e professionale

L'*articolo 5* corrisponde agli articoli 17 capoverso 2 (sorveglianza dei servizi telefonici) e 25 capoverso 2 (sorveglianza di Internet) dell'OSCPT in vigore[15] e intende salvaguardare il segreto d'ufficio e quello professionale. Questa disposizione disciplina soltanto il caso in cui il Servizio SCPT constata che la sorveglianza coinvolge una persona tenuta al segreto d'ufficio o professionale senza che siano stati presi provvedimenti secondo gli articoli 271 CPP o 70*b* PPM (*lettere a e b*).

Secondo l'articolo 16 lettera e nLSCPT, il Servizio SCPT attua i provvedimenti per la salvaguardia del segreto d'ufficio e di quello professionale disposti dall'autorità d'approvazione. «Questo compito è stato esteso alla sorveglianza della corrispondenza postale, la qual cosa ha […] pienamente senso in questo settore. Questa disposizione va posta in relazione con gli articoli 271 e 274 capoverso 4 lettera a CPP nonché con gli articoli 70*b* e 70*e* cpv. 4 lett. a PPM. Questi articoli indicano il regime applicabile alla sorveglianza nel caso in cui sia necessario tutelare un segreto professionale di cui l'autorità di perseguimento penale non deve prendere atto. Il Servizio prende i provvedimenti necessari per porre in essere le misure decise nel quadro dei succitati articoli; ma non esegue da sé la cernita menzionatavi (art. 271 cpv. 1 CPP e art. 70*b* cpv. 1 PPM)»[16].

Secondo gli articoli 15 lettere j e k (corrispondenza postale) e 47 lettere k e l (traffico delle telecomunicazioni) l'ordine di sorveglianza trasmesso al Servizio SCPT deve contenere l'indicazione delle persone tenute al segreto d'ufficio o

15 RS **780.11**

16 FF **2013** 2283 2324; v. anche le spiegazioni del messaggio concernente la LSCPT relative agli art. 271 CPP e 70*b* PPM.

professionale in virtù degli articoli 271 CPP o 70*b* PPM e dei provvedimenti per la loro tutela (cfr. anche l'articolo 9 capoverso 2 lettera i secondo il quale il fascicolo relativo alla sorveglianza contiene anche le misure speciali di protezione).

Secondo la nLSCPT, oltre che a un esame formale, il Servizio SCPT può sottoporre gli ordini di sorveglianza ricevuti a un esame materiale sotto il profilo del diritto amministrativo[17]. Nell'ambito di tale esame il Servizio SCPT potrebbe formulare una pertinente constatazione, ad esempio quando la denominazione professionale è indizio di una professione che sottostà al segreto professionale e non è stata disposta nessuna cernita.

Se per esempio deve essere sorvegliato un medico, che è sottoposto al segreto medico, senza che siano state allestite misure conformemente agli articoli 271 CPP o 70*b* PPM, il Servizio SCPT effettua la sorveglianza, ma l'autorità disponente non ottiene l'accesso ai dati registrati. L'autorità disponente e l'autorità d'approvazione ne sono informate. L'autorità d'approvazione può approvare la sorveglianza a condizione che sia effettuata una cernita secondo gli articoli 271 capoverso 1 e 274 capoverso 4 lettera a CPP o secondo gli articoli 70*b* e 70*e* capoverso 4 lettera a PPM. Può designare un responsabile che passa previamente in rassegna i dati e effettua una cernita. Una volta designato un responsabile, il Servizio SCPT gli concede l'autorizzazione e/o l'accesso ai dati nel sistema di trattamento. Successivamente, l'autorità d'approvazione comunica al Servizio SCPT a quali dati potrà accedere l'autorità disponente. Se è ordinata una cernita, l'autorità d'approvazione trasmette periodicamente al Servizio SCPT un pertinente elenco e quest'ultimo procede alla cernita nel sistema di trattamento. Ciò significa che le autorità disponenti ricevono accesso ai dati selezionati dall'autorità d'approvazione e il Servizio SCPT distrugge i dati rimanenti[18]. Questa procedura si applica durante l'intero periodo di sorveglianza.

La *lettera c* stabilisce che quanto detto in precedenza si applica per analogia al Servizio delle attività informative della Confederazione (SIC) in quanto autorità che dispone la sorveglianza. In tal caso l'autorità d'approvazione è il Tribunale amministrativo federale.

Art. 6 Obbligo del segreto

L'*articolo 6* corrisponde agli articoli 17 capoverso 7 e 25 capoverso 7 dell'OSCPT vigente[19] e disciplina l'obbligo del segreto.

L'obbligo del segreto è di particolare importanza per il successo delle misure di sorveglianza e delle informazioni nonché per la salvaguardia dei diritti della personalità degli interessati e non può essere violato in alcun modo. Né la persona sorvegliata né terzi non autorizzati possono ottenere direttamente o indirettamente indicazioni sulle attività di sorveglianza e sulle informazioni fornite (cfr. anche art. 320 CPP e l'art. 39 cpv. 1 lett. d nLSCPT).

17 FF **2013** 2283 2296; n. 1.4.5.
18 FF **2006** 989 1152
19 RS **780.11**

Art. 7 Selezione tecnica dei dati (cernita)

L'*articolo 7* precisa l'articolo 17 lettera g LSCPT.

La cernita prevista si distingue da quella di cui agli articoli 271 CPP e 70*b* PPM in riferimento alla tutela del segreto d'ufficio e di quello professionale (cfr. il commento all'art. 5).

Con selezione tecnica dei dati (cernita) si intende una riduzione, mediante procedura automatica e conformemente agli ordini documentati dell'autorità disponente, della quantità di dati da esaminare. L'autorità disponente può ordinare la cernita automatica dei dati risultanti dalla sorveglianza ad esempio per facilitare la valutazione di grandi quantità di dati. In tal modo i dati irrilevanti per le indagini, come ad esempio quelli di TV Internet, che non consentono alle autorità di perseguimento penale di acquisire ulteriori elementi, sono filtrati dal flusso di dati già prima del salvataggio nel sistema di trattamento.

Non sono contemplati i casi in cui molti terzi non coinvolti sono toccati da una misura di sorveglianza (p. es. quando il numero del centralino di un'azienda deve essere sorvegliato). Anche in questi casi il Servizio SCPT consulta le autorità che dispongono la sorveglianza (per analogia come all'art. 5).

Il Servizio SCPT effettua la cernita gratuitamente, a condizione che possa essere effettuata automaticamente e con un onere ragionevole. Per onere ragionevole si intende che il Servizio SCPT possa prendere le pertinenti misure nell'ambito delle risorse finanziarie, di personale e tecniche a sua disposizione. Se il Servizio SCPT constata che la cernita è tecnicamente impossibile o che non può essere effettuata con un onere ragionevole, lo comunica immediatamente e in modo fondato all'autorità disponente.

Le autorità di perseguimento penale sono responsabili della configurazione delle possibilità di cernita prestabilite dal Servizio SCPT. Quest'ultimo offre loro consulenza. Sono usate soltanto procedure automatizzate poiché la cernita è molto impegnativa sotto il profilo tecnico. Ogni altro tipo di cernita sarebbe complicato o impossibile[20]. Prima di ordinare una selezione tecnica dei dati, l'autorità disponente consulta il servizio SCPT in merito alla sua fattibilità.

Art. 8 Registrazione delle telefonate a scopo probatorio

L'*articolo 8 capoverso 1* permette al Servizio SCPT di registrare a scopi probatori le telefonate attinenti all'esecuzione dei suoi compiti, poiché le autorità disponenti trasmettono spesso per telefono un ordine di sorveglianza (p. es. in casi urgenti; cfr. art. 3 cpv. 1 lett. c) o le spiegazioni su un tale ordine. In passato ci sono stati casi isolati in cui in occasione di accertamenti successivi, i collaboratori del Servizio SCPT e le autorità disponenti hanno fatto dichiarazioni divergenti in merito alle misure di sorveglianza disposte telefonicamente. Nell'ambito delle indagini è necessario poter constatare i fatti in modo inequivocabile; perciò è importante avere a disposizione questi mezzi di prova.

Inoltre, secondo il diritto vigente sono già conservate tutte le comunicazioni *scritte* tra il Servizio SCPT, le autorità e le persone obbligate a collaborare (p. es. provvedimenti, decisioni, ordini di sorveglianza, corrispondenza, ecc.; cfr. art. 9

20 FF **2013** 2283 2326

[fascicolo relativo alla sorveglianza]). Il presente avamprogetto prevede lo stesso disciplinamento per le comunicazioni telefoniche.

La registrazione di telefonate riguarda i numeri di ufficio e di picchetto della gestione della sorveglianza del Servizio SCPT.

Soltanto il delegato alla protezione dei dati del Servizio SCPT può eseguire un'eventuale valutazione delle registrazioni (cpv. 2). Il Servizio SCPT può conservare le registrazioni soltanto per due anni e dopo lo scadere di tale termine devono essere distrutti (cpv. 3).

Art. 9 Fascicolo relativo alla sorveglianza

L'*articolo 9* descrive la documentazione del Servizio SCPT ed elenca in modo esaustivo il contenuto del fascicolo relativo alla sorveglianza.

Il *capoverso 1* obbliga il Servizio SCPT ad allestire un fascicolo per ogni ordine di sorveglianza; l'ordine può contenere varie misure di sorveglianza.

Il *capoverso 2* elenca i documenti compresi nel fascicolo relativo alla sorveglianza: l'ordine di sorveglianza e eventuali allegati, il mandato di sorveglianza trasmesso alle persone obbligate a collaborare, la conferma di trasmissione dell'incarico alle persone obbligate a collaborare, la conferma di esecuzione del mandato di sorveglianza (data e ora) da parte delle persone obbligate a collaborare, le decisioni dell'autorità competente sull'approvazione o sul rifiuto dell'ordine di sorveglianza nonché eventuali decisioni sul ricorso, gli eventuali ordini di proroga e le eventuali decisioni dell'autorità competente per l'approvazione, l'ordine di revoca della sorveglianza, l'eventuale corrispondenza relativa alla sorveglianza (e-mail ecc.), le misure speciali di protezione ordinate (p. es. la cernita) e i giustificativi contabili.

Questo fascicolo rappresenta anche la base per l'emolumento da riscuotere presso le autorità che dispongono la sorveglianza e per gli indennizzi da versare alle persone obbligate a collaborare. L'obiettivo è conservare in formato elettronico i fascicoli relativi alla sorveglianza e, laddove possibile, nel sistema di trattamento.

Il *capoverso 3* disciplina la conservazione dei dati della sorveglianza conformemente all'articolo 11 nLSCPT e la loro distruzione conformemente all'articolo 14 OST-SCPT.

Sezione 3: Orari d'ufficio e disciplinamento del servizio di picchetto

Art. 10 Orari d'ufficio ordinari e giorni festivi

L'*articolo 10* è nuovo e nel *capoverso 1* definisce gli orari d'ufficio ordinari, che corrispondono alla prassi corrente. Gli orari si riferiscono all'ora svizzera.

Il *capoverso 2* definisce i giorni festivi, che corrispondono a quelli di cui all'articolo 66 capoverso 2 dell'ordinanza del 3 luglio 2001[21] sul personale federale.

21 RS **172.220.111.3**

Art. 11 Prestazioni al di fuori degli orari d'ufficio ordinari

L'*articolo 11* è nuovo, ma corrisponde alla prassi corrente del Servizio SCPT e disciplina le prestazioni nell'ambito del servizio di picchetto del Servizio stesso e delle persone obbligate a collaborare. I mandati urgenti sono sbrigati durante il servizio di picchetto soltanto previo comunicazione telefonica al numero di picchetto del Servizio SCPT.

Il *capoverso 1* descrive le prestazioni del Servizio SCPT durante il servizio di picchetto.

Ne consegue che durante il servizio di picchetto non è in particolare possibile ottenere informazioni e sorveglianze speciali (cosiddetti casi speciali). Si tratta di informazioni o sorveglianze che non corrispondono ad alcun tipo di informazione o sorveglianza dell'ordinanza (cosiddette informazioni o sorveglianze non standardizzate); in merito si veda anche il commento agli articoli 22 e 25. Durante il servizio di picchetto il Servizio SCPT non può organizzare corsi di formazione e può fornire consulenza soltanto in modo limitato.

Il *capoverso 2* disciplina le prestazioni che le persone obbligate a collaborare forniscono al di fuori degli orari d'ufficio ordinari. Per motivi di proporzionalità sono sollevati da questi obblighi i FST con obblighi di sorveglianza ridotti (art. 49) e i fornitori di servizi di comunicazione derivati senza obblighi di sorveglianza supplementari (ossia coloro i quali non sono contemplati dall'art. 50) e pertanto le misure che devono attuare tali fornitori non possono essere eseguite durante il picchetto. Inoltre, non possono essere richieste e ottenute durante il picchetto le informazioni e sorveglianze speciali di cui all'*articolo 22*.

Sezione 4: Statistiche

Art. 12 Statistiche delle sorveglianza e delle informazioni

La LSCPT in vigore stabilisce che il Servizio SCPT tiene una statistica delle sorveglianze. In tale contesto, l'articolo 11 capoverso 1 lettera f della LSCPT in vigore è la base legale per la sorveglianza della corrispondenza postale e l'articolo 13 capoverso 1 lettera j della LSCPT in vigore è quella per la sorveglianza del traffico delle telecomunicazioni.

L'articolo 16 capoverso k nLSCPT è stato introdotto il 10 marzo 2014 dal Consiglio degli Stati e prevede che il Servizio SCPT tenga una statistica delle sorveglianze.

L'articolo 35 capoverso 3 (ricerca d'emergenza) e l'articolo 36 capoverso 2 nLSCPT (ricerca di condannati) contengono ulteriori disposizioni relative alla statistica, mentre l'OSCPT in vigore non contiene alcuna disposizione in merito. Sul sito del Servizio SCPT (https://www.li.admin.ch > Statistica) sono disponibili le statistiche dal 2010, che distinguono le misure di sorveglianza disposte in ambito penale dalla ricerca d'emergenza di persone scomparse.

Durante i lavori di revisione dell'OSCPT è emerso che occorre sancire la prassi corrente nell'ordinanza stessa, tenendo conto delle novità. In linea di principio è nell'interesse generale sapere quali tipi di sorveglianza sono effettuati ogni anno e in quale misura, nonché le spese connesse.

Secondo il *capoverso 1* le statistiche allestite dal Servizio SCPT devono essere pubblicate una volta all'anno sul sito Internet del Servizio SCPT (https://www.li.admin.ch), di norma a inizio anno. Le statistiche possono essere pubblicate anche su altri media (TV, radio, giornali ecc.).

Il *capoverso 2* stabilisce il contenuto delle statistiche. Le *lettere a-c* corrispondono alla prassi attuale. Alla *lettera c* è nuova unicamente la menzione della ricerca di condannati. Le *lettere d-f* contengono le novità. La *lettera b* menziona anche il Principato del Liechtenstein, giacché ai sensi dell'articolo 35 LSCPT può essere considerato un'autorità competente per disporre ricerche di emergenza (cfr. n. 3 dello scambio di note del 27 ottobre 2003[22]). Nel *capoverso 2* si è rinunciato a una disposizione sul numero delle sorveglianze non autorizzate (come richiesto da ANITA FETZ e STEFAN ENGLER il 10.03.2014; Boll. uff. 2014 S 112). Attualmente soltanto i giudici dei provvedimenti coercitivi sarebbero in grado di fornire tali statistiche. Il Servizio SCPT non ne è in grado, poiché viene soltanto a conoscenza delle misure di sorveglianza non autorizzate trasmessegli dal pubblico ministero prima della decisione del giudice dei provvedimenti coercitivi. Ma probabilmente c'è un numero non trascurabile di misure di sorveglianza respinte dal giudice dei provvedimenti coercitivi prima che giungano al Servizio SCPT, di cui quest'ultimo non può pertanto essere a conoscenza.

Il Servizio SCPT non è neppure in grado di dare informazioni sul successo delle misure di sorveglianza (cfr. domanda ALINE TREDE 15.5191 «Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Efficacia della conservazione dei dati» e la risposta del Consiglio federale del 16.03.2015).

Nella redazione dell'articolo 12 si è posta la questione se occorra conteggiare le sorveglianze disposte nell'anno in rassegna oppure soltanto quelle concluse. Si è infine deciso di dare seguito alla prassi corrente e conteggiare tutte le sorveglianze disposte nell'anno in rassegna. Tuttavia c'è un problema per il calcolo del termine (*cpv. 2 lett d*) delle sorveglianze che sono a cavallo tra due anni civili consecutivi. In questo caso è impossibile sapere all'inizio dell'anno la durata totale delle sorveglianze disposte l'anno precedente ma non ancora concluse. Questo problema deve essere risolto nella prassi.

Art. 13 Statistica delle misure di sorveglianza con apparecchi tecnici speciali e programmi informatici speciali

Per quanto riguarda l'uso di apparecchi tecnici speciali (p. es gli IMSI-catcher) e i programmi informatici speciali (cosiddetti «GovWare»), l'articolo 13 stabilisce le disposizioni d'esecuzione dei nuovi articoli 269*bis* capoverso 2 e 269*ter* capoverso 4 del Codice di procedura penale[23] (CPP) per i pubblici ministeri e dei nuovi articoli 70*bis* capoverso 2 e 70*ter* capoverso 4 del Codice penale militare del 23 marzo 1979[24] (PPM) per i giudici istruttori militari. Queste nuove disposizioni prevedono che il Consiglio federale disciplini i dettagli. In linea di massima dovrebbero trovarsi nelle disposizioni d'esecuzione del CPP o in quelle del PPM (p. es. nell'OGPM[25]). Tuttavia l'attuale diritto procedurale penale non dispone di alcuna ordinanza generale nell'ambito del procedimento penale. Allestire una

22 RS **0.780.151.41**
23 RS **312.0**
24 RS **322.1**
25 RS **322.2**

nuova ordinanza soltanto per questo scopo sarebbe inadeguato e sproporzionato. Considerando che gli apparecchi tecnici e i programmi informatici speciali sono legati in senso lato alla materia della sorveglianza disciplinata dalla LSCPT e dall'OSCPT e che è più efficiente centralizzare la pubblicazione di tali statistiche appare sensato assegnare al Servizio SCPT il compito di pubblicarle e integrare le pertinenti disposizioni nella OSCPT.

Le statistiche sono allestite dalle autorità cantonali di perseguimento penale, dai procuratori della Confederazione e dai giudici istruttori militari. Questi ultimi le trasmettono all'ufficio dell'uditore in capo. Pertanto il *capoverso 2* prevede che le diverse autorità devono trasmettere le statistiche al Servizio SCPT. Ciò significa che i pubblici ministeri dei Cantoni, il Ministero pubblico della Confederazione e l'ufficio dell'uditore in capo sono tenuti a consegnare le loro statistiche al Servizio SCPT. Occorre che la trasmissione avvenga nel primo trimestre dell'anno successivo di modo che il Servizio SCPT possa pubblicare tutte le statistiche in tempo utile.

Sono state espresse alcune riserve relative alla necessità della pubblicazione. Si temeva che la pubblicazione potesse compromettere il buon andamento delle indagini, giacché l'uso di apparecchi tecnici speciali per la sorveglianza ma soprattutto di GovWare è molto meno frequente delle normali misure di sorveglianza. Se si pubblicano le statistiche dei Cantoni, anche se in forma anonima, potrebbe essere possibile, soprattutto nei Cantoni piccoli, individuare il relativo procedimento penale. Tali considerazioni sono condivisibili. Pertanto il *capoverso 2* secondo periodo prevede che le statistiche non comprendano le misure di sorveglianza con apparecchi tecnici o programmi informatici speciali qualora queste siano ancora in corso. Le autorità cantonali preposte al perseguimento penale o il Ministero pubblico della Confederazione sono tenute a informare il Servizio SCPT in merito alla conclusione della misura di sorveglianza. In tal modo il Servizio SCPT ne può tenere conto nella statistica successiva. Secondo il capoverso 3 il Servizio SCPT pubblica annualmente le statistiche. Le indicazioni relative al Cantone dell'autorità disponente e quelle relative all'autorità della Confederazione non sono contenute nella statistica, proprio per eliminare il timore che tali informazioni possano pregiudicare le indagini.

Più difficile è la questione delle spese per l'impiego e l'uso di apparecchi tecnici speciali o programmi informatici speciali. Di norma tali programmi informatici si acquistano una volta sola e sono poi usati più volte in procedure diverse con i necessari adeguamenti. Inoltre sembra che singoli modelli di acquisto comportino diritti di licenza per ogni impiego. Ciò rende più difficile illustrare correttamente i costi. Occorrerebbe d'altronde considerare anche i costi difficilmente verificabili segnatamente per l'impiego del personale al fine di preparare il funzionamento di GovWare (polizia, informatici, traduttori ecc.). A causa di queste difficoltà si rinuncia a un'indicazione dei costi.

Capitolo 2: Corrispondenza postale

Art. 14 Obblighi dei FSP

L'*articolo 14* corrisponde essenzialmente all'articolo 14 dell'OSCPT del 31 ottobre 2001[26] e disciplina gli obblighi dei fornitori di servizi postali (FSP); si vedano anche gli articoli 19 (obblighi dei fornitori di servizi postali e 20 nLSCPT (informazioni precedenti un ordine di sorveglianza), il commento a quest'ultimo nel messaggio sulla nLSCPT[27] e il commento qui appresso all'articolo 16.

Art. 15 Ordine di sorveglianza della corrispondenza postale

L'*articolo 15* corrisponde essenzialmente all'articolo 11 dell'OSCPT del 31 ottobre 2001[28] e disciplina il contenuto dell'ordine di sorveglianza nel caso di una sorveglianza della corrispondenza postale (per il traffico delle telecomunicazioni cfr. il commento all'art. 47).

Per le *lettere j* e *k* si veda il commento all'articolo 5 (salvaguardia del segreto d'ufficio e professionale).

Art. 16 Tipi di sorveglianza

L'*articolo 16* corrisponde essenzialmente all'articolo 12 dell'OSCPT del 31 ottobre 2001[29] e disciplina i diversi tipi di sorveglianza della corrispondenza postale.

I dati da fornire dei singoli tipi di sorveglianza sono essenzialmente rimasti invariati. La sola novità è che nell'ambito della sorveglianza retroattiva occorre indicare, qualora possibile, anche il luogo da cui è stato spedito l'invio postale (cfr. lett. b n. 4). Va osservato che, come secondo il disciplinamento vigente, l'obbligo di memorizzare e consegnare metadati sussiste soltanto nel caso di invii postali con giustificativo di distribuzione. Ai sensi dell'ordinanza un giustificativo di distribuzione è dato sicuramente per prodotti come invii postali raccomandati e per pacchetti «track and trace». Se i FSP hanno raccolto altri dati, sono tenuti a consegnarli su richiesta (cfr. lett. c n. 2).

Occorre ancora menzionare che i servizi di comunicazione elettronica dei FSP rientrano nella sorveglianza del traffico delle telecomunicazioni, per esempio i servizi e-mail della posta quali PostMail.

Capitolo 3: Traffico delle telecomunicazioni

A causa del rapido progresso tecnico e delle diverse possibilità di applicazione a disposizione delle persone obbligate a collaborare, sono inadatti elenchi esaustivi dei numerosi servizi, opzioni e parametri relativi ai tipi di informazione e sorveglianza. L'ordinanza si limita pertanto a elencare esempi tipici.

26 RS **780.11**
27 FF **2013** 2327-2329
28 RS **780.11**
29 RS **780.11**

La nuova ordinanza è molto più dettagliata rispetto a quella precedente e dà così seguito alla richiesta di maggiore certezza del diritto.

Sezione 1: Disposizioni generali per informazioni e sorveglianze

Art. 17 Domande di informazioni

Occorre dapprima spiegare come vengono solitamente fornite le informazioni (p. es. per l'identificazione degli utenti). Di norma, il fornitore cerca, nei dati relativi agli utenti e nei metadati conservati, le indicazioni corrispondenti alla domanda d'informazioni nel periodo indicato. Quindi fornisce, conformemente alle richieste delle domande di informazioni, i dati sugli utenti e sui servizi di telecomunicazione o di comunicazione derivati da loro utilizzati.

Il *capoverso 1* stabilisce che le autorità autorizzate trasmettono le loro domande di informazioni tramite il sistema di trattamento e che anche le persone obbligate a collaborare sono in linea di principio tenute a trasmettere i dati alle autorità attraverso il sistema di trattamento. In tal modo tutte le altre vie di trasmissione (p. es per posta elettronica, per lettera, telefonicamente o con un fax) sono ammissibili soltanto se il sistema di trattamento non è disponibile, ad esempio per motivi tecnici, oppure se si tratta di un'eccezione di cui all'articolo 18 capoverso 3 o 4.

Secondo il *capoverso 2*, nella domanda di informazioni occorre indicare il numero massimo di pacchetti dati da consegnare. Il sistema di trasmissione è impostato in modo tale che non possa essere superato un limite massimo. Si tratta di impedire che l'autorità disponente riceva troppi risultati, il che si potrebbero ripercuotere sulle sue spese. È inoltre necessario proteggere il sistema d'informazione dal sovraccarico ed evitare consultazioni collettive non specifiche. I risultati della domanda di informazioni sono considerati pacchetti dati.

Art. 18 Obblighi per la trasmissione di informazioni

Analogamente all'articolo 48 per gli obblighi di sorveglianza, il *capoverso 1* stabilisce che i FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari (art. 21) devono essere in grado di fornire le informazioni richieste (art. 33−46).

Le informazioni di cui alle sezioni 4 e 5 del capitolo 3 (art. 33−41) vengono in linea di massima fornite tramite un'interfaccia elettronica del sistema di trattamento in una procedura automatizzata. Alcuni tipi di informazione (art. 42-46) possono tuttavia essere forniti anche manualmente (*cpv. 2 secondo periodo*). Anche in questo caso, seppure non automaticamente, la risposta alla domanda d'informazioni è fornita mediante il sistema di trattamento.

Secondo il *capoverso 3* i FST con obblighi di sorveglianza ridotti ai sensi dell'articolo 49, possono fornire le informazioni anche per scritto, senza ricorrere all'interfaccia del sistema di trattamento. Questo perché molti FST appartenenti a questa categoria non dispongono di una simile interfaccia.

Il *capoverso 4* precisa che i fornitori di servizi di comunicazione derivati senza obblighi di informazione supplementari (quelli che non soddisfano le condizioni di cui all'art. 21) e i gestori di reti di telecomunicazione interne (art. 1 cpv. 2 lett. k) non sono tenuti a fornire le informazioni di cui agli articoli 33–46. Essi forniscono per scritto le informazioni di cui dispongono.

Se il numero di pacchetti dati trovati supera il valore massimo indicato nella domanda di informazioni, il fornitore comunica soltanto il numero dei risultati trovati, senza trasmettere alcun dato (*cpv. 5*). L'autorità richiedente può successivamente presentare una nuova domanda di informazioni con criteri più specifici e/o con un valore maggiore per quanto riguarda il numero massimo di pacchetti dati da consegnare, sempreché tale valore non superi il limite massimo previsto dal sistema di trattamento. Qualora avesse bisogno di un numero di pacchetti dati che supera il limite massimo consentito dal sistema di trattamento, l'autorità richiedente deve presentare al Servizio SCPT una domanda di informazioni particolari ai sensi dell'articolo 22 capoverso 1.

Art. 19 Identificazione degli utenti

L'*articolo 19* corrisponde all'articolo 19*a* dell'OSCPT del 31 ottobre 2001[30] e apporta le precisazioni necessarie, basandosi segnatamente sulle norme di delega generale al Consiglio federale di cui agli articoli 21 capoverso 1 lettera d, 22 capoverso 2 e 23 capoverso 1 nLSCPT[31].

Il *capoverso 1* prevede che i fornitori di servizi di telecomunicazione o di servizi di comunicazione derivati identifichino gli utenti con i mezzi adeguati.

Il *capoverso 2* prevede che per i servizi di telefonia mobile i fornitori devono verificare l'identità degli utenti per mezzo di un passaporto, una carta d'identità o una carta di soggiorno ai sensi degli articoli 71 e 71*a* dell'ordinanza del 24 ottobre 2007[32] sull'ammissione, il soggiorno e l'attività lucrativa (OASA). Con «attivazione» si intende il momento a partire dal quale un utente può usufruire del servizio, ad esempio l'attivazione del profilo nel caso di strumenti di accesso già attivi al momento della sua consegna o di una embedded SIM inserita all'interno del dispositivo. Il termine *mezzo di accesso* è la forma abbreviata per «mezzo che consente l'accesso al servizio di telecomunicazione» (art. 21 cpv. 1 lett. e LSCPT).

Per i servizi di telefonia mobile è imperativo verificare l'identità del cliente per mezzo di un documento di legittimazione. Ciò corrisponde al disciplinamento in vigore per i servizi di telefonia mobile prepagati (prepaid), il quale è ora esteso esplicitamente anche agli abbonamenti. Nella prassi i fornitori di servizi di telefonia mobile chiedono già da molto tempo un documento di identità al cliente che stipula un abbonamento. Le disposizioni per verificare l'identità dei clienti sono più severe per i servizi di telefonia mobile rispetto agli altri servizi perché sono particolarmente diffusi e altri servizi possono svolgere identificazioni indirette sulla base di questi dati.

I dati personali devono essere rilevati in base al documento d'identità presentato (art. 23 cpv. 1 nLSCPT). I fornitori di servizi di telecomunicazione, i fornitori di

30 RS **780.11**
31 Cfr. Messaggio concernente la LSCPT del 27 febbraio 2013, FF **2013** 2283 2331
32 RS **142.201**

servizi di comunicazione derivati con obblighi supplementari ai sensi dell'articolo 21 e i rivenditori ai sensi dell'articolo 2 lettera f nLSCPT devono garantire che il rilevamento dei dati personali avvenga correttamente in base al documento presentato; la verifica si fonda sulla copia del documento d'identità. I dati non presenti sul documento d'identità (p. es l'indirizzo) devono essere rilevati in base alle indicazioni del cliente. I dati rilevati in occasione della registrazione e la copia elettronica del documento devono essere trasmessi dal rivenditore al fornitore ai cui servizi il mezzo rivenduto permette di accedere. Se il cliente o il fornitore modificano i dati (p. es nuovo indirizzo di fatturazione) è necessario memorizzare anche questi. Non sussiste tuttavia l'obbligo di una verifica e di un aggiornamento costante dei dati. È per contro importante che il fornitore conservi i dati raccolti al momento del rilevamento per tutta la durata della relazione commerciale nonché per sei mesi dopo la loro conclusione (cfr. art. 21 cpv. 2 nLSCPT).

Altre misure si sono rese necessarie perché in passato ci sono state numerose registrazioni false di dati degli utenti. La copia del documento d'identità sembra attualmente il mezzo più indicato per prevenire queste registrazioni false; finora non sono state individuate altre soluzioni. Sono eventualmente possibili altre opzioni come la SuisseID, l'identità elettronica (eID) o simili (cfr. legge federale del 19 dicembre 2003[33] sui servizi di certificazione nel campo della firma elettronica [Legge sulla firma elettronica, FiEle] e la futura legge sull'identità elettronica[34]) (cfr. art. 23 cpv. 1 nLSCPT).

Non occorre per forza copiare il documento d'identità e conservarlo in forma cartacea. Tuttavia nel sistema del fornitore deve esserci una copia elettronica ben leggibile del documento d'identità (cpv. 2 secondo periodo), non importa se fotografata o scannerizzata (cfr. art. 23 cpv. 1 nLSCPT).

Il *capoverso 3* precisa i dati che devono essere registrati nel caso di persone fisiche. I dati necessari (cognome, nome, data di nascita, tipo di documento d'identità e numero, indirizzo) sono già previsti nell'articolo 19*a* dell'OSCPT del 31 ottobre 2001[35] e corrispondono alla prassi attuale. Secondo la nuova ordinanza occorrerà indicare anche la professione, qualora nota (art. 21 cpv. 1 lett. a nLSCPT).

Il *capoverso 4* elenca i dati che devono essere registrati per le persone giuridiche. Per «persona fisica responsabile» ai sensi della lettera c s'intende una persona autorizzata a firmare secondo l'iscrizione nel registro di commercio. Tale persona non è obbligatoriamente la persona responsabile secondo il diritto delle obbligazioni e può essere una persona diversa da quella che usufruisce del servizio di telefonia mobile (p. es. un collaboratore). Per tale persona sono sufficienti cognome e nome (*lett. d*).

Il *capoverso 5* obbliga i FST, i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari e i rivenditori a rilevare ulteriori dati sui clienti che non hanno stipulato un abbonamento (prepaid). Esso non riguarda invece i venditori di semplici schede telefoniche che permettono di telefonare senza denaro dalle cabine telefoniche (p. es. «taxcard» dotate di un credito e vendute

33 RS **943.03**
34 https://www.egovernment.ch/it/umsetzung/schwerpunktplan/elektronische-identitat/
35 RS **780.11**

all'edicola)[36]. Secondo l'articolo 1 lettera b dell'ordinanza del 9 marzo 2007[37] sui servizi di telecomunicazione un cliente è una persona fisica o giuridica che ha concluso con un fornitore di servizi di telecomunicazione un contratto sulla fruizione di tali servizi. Lo stesso vale per analogia per i servizi di comunicazione derivati. Il rilevamento di questi ulteriori dati è necessario per poter capire chi ha effettuato eventuali registrazioni false (cfr. anche la disposizione penale dell'art. 39 cpv. 1 lett. c nLSCPT).

Art. 20 Termine di conservazione

L'*articolo 20* contiene le disposizioni d'esecuzione degli articoli 21 capoverso 2 (informazioni sui servizi di telecomunicazione) e 22 capoverso 2 nLSCPT (informazioni per identificare gli autori di reati commessi via Internet).

Il *capoverso 1* prevede che tutti i dati sui servizi di telecomunicazione e quelli per l'identificazione degli autori di reati commessi via Internet devono essere in linea di massima conservati e trasmessi elettronicamente finché dura la relazione commerciale, nonché durante sei mesi dopo il suo termine. Dei *dati sui servizi di telecomunicazione* fanno parte anche i dati personali di cui all'articolo 19 capoversi 1−3.

In esecuzione degli articoli 21 capoverso 2 secondo periodo e 22 capoverso 2 secondo periodo nLSCPT, il *capoverso 2* indica i dati da conservare e da trasmettere soltanto per sei mesi, affinché non sorgano contraddizioni con il termine di conservazione di cui all'articolo 26 capoverso 5 nLSCPT. Tale termine di conservazione è un termine più breve rispetto a quello del capoverso 1. I dati in questione sono l'elenco degli identificatori dell'apparecchio (p. es. IMEI, indirizzo IP; cfr art. 34 cpv. 1 lett. d e art. 39 cpv. 1 lett. d) nonché i dati di cui agli articoli 35 capoverso 1, 36 capoverso 1 e 37 capoverso 1.

Si vedano anche le disposizioni transitorie previste dall'articolo 45 capoverso 3 nLSCPT.

Art. 21 Fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari

I servizi di comunicazione derivati sono sempre più utilizzati e pertanto ne aumenta l'importanza. Nell'ambito della sorveglianza del traffico delle telecomunicazioni, i comuni fornitori di servizi di comunicazione derivati hanno obblighi meno estesi. Sono soltanto tenuti a tollerare la sorveglianza e a consegnare i dati a loro disposizione necessari per lo svolgimento della stessa. Tuttavia se un reato è commesso tramite Internet può succedere che questo obbligo minimo non sia sufficiente. Pertanto nell'articolo 22 capoverso 4 nLSCPT il legislatore ha attribuito al Consiglio federale la competenza di prevedere obblighi di informazione più estesi anche per i fornitori di servizi di comunicazione derivati. Gli obblighi da osservare sono quelli previsti per i FST. Pertanto i fornitori di servizi di comunicazione derivati sottoposti a obblighi più estesi devono adempiere tutti gli obblighi di cui all'articolo 22 capoverso 1 e 2 nLSCPT.

36 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, FF **2013** 2283 2308.
37 RS **784.101.1**

Il *capoverso 1* concretizza le condizioni che devono essere soddisfatte affinché un fornitore di servizi di comunicazione derivati abbia obblighi di informazione più estesi. Un fornitore ha obblighi di informazione più estesi se ha dovuto espletare 50 mandati di informazione negli ultimi 12 mesi (data di riferimento 30 giugno) o se ha raggiunto un fatturato annuo di 100 milioni di franchi per due esercizi consecutivi. Il secondo criterio è ulteriormente precisato in quanto sono soggetti a obblighi supplementari soltanto i fornitori la cui attività commerciale consiste in gran parte nel fornire servizi di comunicazione derivati e i cui servizi vengono utilizzati da almeno 5000 utenti. Giacché, ai fini della tutela delle PMI svizzere, i valori soglia sono molto alti, saranno relativamente pochi i fornitori di servizi di comunicazione derivati soggetti a obblighi di informazione supplementari.

Il *capoverso 2* contempla i gruppi di imprese. Se un fornitore controlla una o più imprese soggette all'obbligo di presentare i conti, per il calcolo dei valori di cui al capoverso 1 lettere a e b, il fornitore e le imprese controllate sono considerate un'unità. La disposizione rinvia all'articolo 963 capoverso 1 e 2 del Codice delle obbligazioni (CO), che va applicato per analogia. Va detto che la società madre e le imprese controllate sono considerate un'unità soltanto per quanto riguarda i servizi di comunicazione da loro offerti.

Il *capoverso 3* prevede che i fornitori che non raggiungono più oppure superano i valori soglia di cui al capoverso 1 lettera a o b ne informino il Servizio SCPT. A tal fine il Servizio SCPT mette a disposizione strumenti di comunicazione adeguati.

Secondo il *capoverso 4* il fornitore che adempie le condizioni di cui al capoverso 1 deve garantire rispettivamente entro due ed entro dodici mesi la memorizzazione dei dati necessari per fornire le informazioni e la disponibilità a fornire informazioni. Il termine decorre dal momento in cui il fornitore constata di adempiere le condizioni di cui al capoverso 1 lettera a o b. Il Servizio SCPT sostiene i fornitori nell'adempimento dei loro obblighi prestando loro consulenza.

Art. 22 Informazioni e sorveglianze particolari

Tutti i tipi comuni di informazioni e di sorveglianza sono menzionati negli articoli 23 e 24 e rispettivamente nelle sezioni 4−6 (art. 33−46) e 8−11 (art. 52−68) del 3° capitolo.

Le informazioni e le sorveglianze non espressamente elencate nella presente ordinanza e, temporaneamente, le sorveglianze di cui agli articoli 58 e 59 sono le cosiddette misure speciali, effettuate dal Servizio SCPT o dalle persone da esso incaricate. Ciò corrisponde alla prassi attuale secondo gli articoli 17 capoverso 5 e 25 capoverso 5 dell'OSCPT del 31 ottobre 2001[38]. Queste disposizioni sono state introdotte con la modifica del 23 novembre 2011 (in vigore dal 1° gennaio 2012) per disciplinare in via separata la facoltà del Servizio SCPT di ordinare ai FST l'esecuzione di misure di sorveglianza che, pur non figurando esplicitamente nell'ordinanza, sono state ordinate dalle autorità di perseguimento penale e approvate dai giudici dei provvedimenti coercitivi. Secondo la decisione del Tribunale amministrativo federale del 23 giugno 2011 (A-8267/2010), i FST interessati devono tollerare l'esecuzione di simili misure di sorveglianza mettendo a disposizione del Servizio le interfacce già esistenti. Lo stesso vale quando terzi

38 RS **780.11**

sono stati coinvolti dal fornitore come persone ausiliarie per l'esecuzione delle domande d'informazioni e delle sorveglianze (*cpv. 2*).

I fornitori devono tollerare anche l'accesso agli impianti (art. 51), in particolare devono mettere a disposizione gratuitamente gli accessi esistenti alle reti di comunicazioni pubbliche.

Art. 23 Tipi di informazioni

L'*articolo 23* offre una panoramica sommaria dei diversi tipi di informazioni, disciplinati più dettagliatamente nelle sezioni 4−6 del capitolo 3 (art. 33−46). Per tipo di informazioni s'intende un tipo di domanda e di rilascio delle informazioni di cui agli articoli 21 e 22 LSCPT in relazione a servizi di telecomunicazione o servizi di comunicazione derivati.

I tipi di informazioni di cui agli articoli 33−40 si distinguono per l'alta densità normativa, il che è necessario affinché possano essere trattati automaticamente. Corrispondono sostanzialmente alle attuali informazioni semplici A0. Dato che sono molto numerose, il trattamento automatizzato di simili domande di informazioni è imprescindibile (181 835 domande nel 2015[39]).

L'automatizzazione richiede regole precise, soprattutto per quanto riguarda i singoli parametri e i tipi di dati. Queste regole sono fissate nell'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT; art. 31 cpv. 3 nLSCPT).

Oltre ai tipi di informazioni fortemente formalizzati ci sono altre informazioni (art. 40−46) che possono essere fornite anche mediante una procedura manuale.

Tutte le informazioni hanno in comune che le autorità legittimate secondo l'articolo 15 nLSCPT possono presentare una richiesta al Servizio SCPT, che la trasmette alle persone obbligate a collaborare. Queste ultime trasmettono le informazioni richieste al Servizio SCPT, che inoltra i risultati all'autorità richiedente. Se tecnicamente possibile, le richieste di informazione e i risultati sono trasmessi in forma automatizzata mediante il sistema di informazione del Servizio SCPT.

Nella nuova ordinanza i tipi di informazioni sono strutturati secondo la norma ETSI TS 102 657 e sono suddivisi per categorie di servizi. Tali categorie sono predefinite dalla norma ETSI. Giacché i prodotti dei fornitori possono comprendere diverse categorie di servizi (p. es. abbonamento di telefonia mobile con le categorie di servizi accesso alla rete nonché servizi di telefonia e multimedia), nella prassi, per poter ottenere informazioni su tutti i servizi, occorre presentare una domanda per ogni tipo di informazioni.

Le categorie più frequenti nelle domande di informazioni, ossia i *servizi di accesso alla rete* e i *servizi di telefonia e multimedia*, sono suddivise in «informazioni sui partecipanti» (art. 33 e 38) e «informazioni sui servizi» (art. 34 e 39). Tale suddivisione corrisponde all'incirca alle precedenti informazioni A0 e A1 ed è volta a limitare il numero di informazioni per ogni tipo di informazioni, al fine di facilitare e velocizzare il trattamento automatizzato.

39 Statistica del Servizio SCPT: https://www.li.admin.ch/it/temi/statistica

Per le categorie di servizi meno spesso oggetto di domande di informazioni, quali i *servizi di posta elettronica* nonché *altri servizi di telecomunicazione o servizi di comunicazione derivati,* si è rinunciato a questa suddivisione.

Per la categoria *servizi di accesso alla rete* si aggiungono tre ulteriori tipi specifici di informazioni (art. 35−37) volti ad identificare gli utenti in caso di reati commessi via Internet (art. 22 nLSCPT).

Art. 24 Tipi di sorveglianza

L'*articolo 24* offre una breve panoramica sui diversi tipi di sorveglianza, disciplinati in modo più dettagliato nelle sezioni 8−11 del capitolo 3 (art. 52−68). Per tipo di sorveglianza s'intende un tipo di sorveglianza di uno o più servizi di telecomunicazione o di comunicazione derivati (art. 31 cpv. 1 nLSCPT) precisato nella presente ordinanza. Si distingue tra sorveglianza in tempo reale (cpv. 1), sorveglianza retroattiva (cpv. 2) nonché ricerche d'emergenza e ricerche di condannati (cpv. 4).

I tipi di sorveglianza in tempo reale sono strutturati in modo tale che per le categorie di servizi più importanti le autorità di perseguimento penale potranno in futuro chiedere la trasmissione in tempo reale dei metadati oppure la trasmissione in tempo reale dei contenuti e dei metadati completi (cpv. 1). In tal modo s'intende creare la possibilità di graduare la gravità dell'ingerenza nei diritti fondamentali.

I dati relativi al contenuto (p. es conversazioni, testi di posta elettronica e allegati) possono essere ottenuti soltanto nell'ambito di una sorveglianza in tempo reale. Invece nel caso di sorveglianze retroattive (metadati della sorveglianza retroattiva, detti anche metadati delle telecomunicazioni) i dati relativi al contenuto non sono né registrati né trasmessi (per il termine metadati si veda anche il commento introduttivo alla sezione 10 del capitolo 3).

La sorveglianza del traffico delle telecomunicazioni è strutturata in modo tale che per le categorie di servizi più importanti sono definiti tipi di sorveglianza specifici. Si tiene così conto sia del principio di determinatezza che degli standard internazionali. Le categorie di servizi sono suddivise in servizi di accesso alla rete e applicazioni (in inglese: application). Fanno parte delle applicazioni i servizi di telefonia e multimedia, i servizi di posta elettronica nonché i servizi di telecomunicazione e i servizi di comunicazione derivati.

In passato per la telefonia l'accesso alla rete e l'applicazione erano identici (collegamento telefonico). Pertanto di norma bastava sorvegliare il collegamento. Tuttavia in seguito al progresso tecnologico ci sono sempre più servizi di comunicazione per i quali l'accesso può essere quasi di qualsiasi tipo. Per tali servizi sorvegliare l'accesso alla rete (collegamento) avrebbe scarso successo, tanto più se il fornitore, le apparecchiature terminali o i client criptano la comunicazione. La telefonia nomade tramite Internet (VoIP) è un buon esempio: i dati di accesso dell'utente possono ad esempio essere memorizzati in un'applicazione mobile sullo smartphone. L'utente può usare lo smartphone con un accesso a internet qualsiasi (p. es. in albergo, in ufficio, all'aeroporto) e grazie all'applicazione mobile può usufruire di servizi di telefonia tramite Internet. Dato che le autorità di perseguimento penale non possono sapere quali accessi a Internet userà l'utente sorvegliato e vista la molteplicità degli accessi a disposizione (p. es. reti wireless), è più efficiente svolgere la sorveglianza presso i fornitori delle applicazioni (nel presente esempio presso i fornitori dei servizi di telefonia tramite Internet). In

questo modo sono sorvegliate tutte le comunicazioni svoltesi attraverso il servizio di telefonia tramite Internet, indipendentemente dall'accesso alla rete usato dalla persona sorvegliata. Inoltre, il fornitore è tenuto a eliminare eventuali criptaggi. In tal modo le autorità di perseguimento penale possono esaminare i contenuti delle comunicazioni sorvegliate.

Visto che i prodotti dei fornitori possono comprendere diverse categorie di servizi (p. es. gli abbonamenti di telefonia mobile possono comprendere le categorie servizi di accesso alla rete e servizi di telefonia e multimedia), per una sorveglianza completa può essere necessario ordinare diversi tipi di sorveglianza per lo stesso identificativo di destinazione. Va inoltre osservato che i prodotti di telecomunicazione possono contenere diverse offerte di servizi differenti appartenenti a diversi tipi di sorveglianza. Quando ad esempio si intende sorvegliare totalmente uno smartphone in tempo reale (contenuto e metadati) l'autorità deve ordinare due sorveglianze (la prima del tipo RT_16_NA_CC_IRI per l'accesso a Internet e la seconda del tipo RT_18_TEL_CC_IRI per il servizio di telefonia mobile). Questa suddivisione ha un motivo amministrativo e uno tecnico. Dal punto di vista amministrativo, come finora l'autorità disponente deve poter ordinare separatamente le sorveglianze dei singoli servizi di telecomunicazione, a seconda delle necessità delle indagini. Sotto il profilo tecnico la sorveglianza dell'accesso a Internet da rete mobile si differenzia in linea di massima dalla sorveglianza dell'applicazione della telefonia mobile. Con la suddivisione in due tipi di sorveglianza diversi, si tiene conto delle divere procedure per l'attivazione e l'esecuzione delle sorveglianze da parte delle persone obbligate a collaborare.

Art. 25 Rinuncia alla standardizzazione

Per standardizzazione di un tipo di informazione o di sorveglianza da parte del DFGP si intende la regolamentazione dei suoi dettagli tecnici e amministrativi nell'OE-SCPT (per il termine tipo di informazione si veda il commento all'art. 23 e per tipo di sorveglianza il commenti all'art. 24). Le premesse per tale standardizzazione sono da una parte l'esistenza di standard internazionali e dall'altra la fattibilità e l'adeguatezza della loro attuazione nella pratica. Qualora al momento dell'entrata in vigore della presente ordinanza, per determinati tipi non ci fossero ancora queste premesse, il DFGP rinuncerà in un primo momento alla loro standardizzazione.

Secondo l'articolo 31 capoverso 3 nLSCPT il DFGP stesso determina i tipi «usuali», ossia i tipi adatti alla standardizzazione. I tipi definiti dal Consiglio federale e quelli standardizzati dal DFGP non devono essere strettamente connessi, affinché il secondo disponga di un certo margine di manovra per ampliare, ridurre o modificare la cerchia dei tipi standardizzati, senza che sia necessaria una revisione dell'OSCPT.

Sezione 2: Garanzia della qualità

Art. 26 Collegamenti diretti per motivi tecnici

L'*articolo 26* disciplina il caso in cui per motivi tecnici il Servizio SCPT non può ricevere e memorizzare nel sistema di trattamento i dati delle misure di sorveglianza. In tal caso occorre prevedere la possibilità che la persona obbligata a collaborare trasmetta i dati risultanti dalla sorveglianza direttamente all'autorità

interessata senza passare attraverso il Servizio SCPT (collegamento diretto ai sensi degli art. 17 lett. c e 26 cpv. 1 frase introduttiva nLSCPT). I dati non sono pertanto registrati nel sistema di trattamento gestito dal Servizio SCPT e spetta invece all'autorità interessata registrarli.

Se il Servizio SCPT constata che il collegamento diretto è necessario per motivi tecnici, informa le persone obbligate a collaborare, l'autorità disponente e l'autorità da designata quest'ultima. Per effettuare un collegamento diretto, le persone obbligate a collaborare devono essere in grado di inoltrare i dati risultanti dalla sorveglianza direttamente alle autorità di perseguimento penale e le autorità di perseguimento penale devono essere in grado di ricevere questi dati dalle persone obbligate a collaborare.

La disposizione non si pronuncia in merito al tempo a disposizione dei fornitori e delle autorità di perseguimento penale per prepararsi, in caso di necessità, ad attuare tale collegamento diretto. In termini realistici è ipotizzabile che abbiano bisogno di vari mesi. Il Servizio SCPT presta d'altronde consulenza alle persone obbligate a collaborare e alle autorità di perseguimento penale.

Analogamente a quanto accade per una misura di sorveglianza effettuata attraverso il sistema di trattamento del Servizio SCPT, occorre trasmettere il mandato di sorveglianza al Servizio SCPT. Questi lo trasmette alle persone obbligate a collaborare, sottolineando che per motivi tecnici occorre trasmettere i dati della sorveglianza non attraverso il sistema di trattamento del Servizio SCPT, ma direttamente all'autorità designata. Nel contempo informa della procedura anche l'autorità coinvolta. La persona obbligata a collaborare conferma al Servizio SCPT di aver ricevuto il mandato e lo informa se è in grado o meno di svolgere autonomamente il collegamento diretto. Anche l'autorità interessata è tenuta a informare il Servizio SCPT se è in grado di ricevere direttamente i dati risultanti dalla sorveglianza. Se sia la persona obbligata a collaborare che l'autorità di perseguimento penale confermano che è possibile effettuare un collegamento diretto, la persona obbligata a collaborare svolge la sorveglianza da sé oppure la fa svolgere a terzi e conferma al Servizio SCPT che il mandato è stato eseguito (in merito all'esecuzione di un mandato di sorveglianza cfr. l'articolo 11 OE-SCPT nonché il pertinente commento del relativo rapporto esplicativo).

Per la trasmissione dei dati mediante un collegamento diretto vengono applicate le stesse specifiche d'interfaccia che per la trasmissione attraverso il sistema di trattamento del Servizio SCPT. Analogamente a quanto accade per una misura di sorveglianza trasmessa attraverso il sistema di trattamento del Servizio SCPT, un collegamento diretto può rimanere attivo fino a quando stabilito dall'autorità disponente; vi è inoltre la possibilità della proroga. Un collegamento diretto esistente non può essere trasferito nel sistema di trattamento del Servizio SCPT; in tal caso è necessario che l'autorità ordini una nuova sorveglianza di cui il Servizio SCPT incarica la persona obbligata a collaborare. Il nuovo ordine è inoltre soggetto agli emolumenti e alle indennità usuali.

Il collegamento diretto sottostà alle restrizioni di cui agli articoli 271 CPP e 70*b* PPM (cfr. art. 271 cpv. 2 CPP e art. 70*b* cpv. 2 PPM e messaggio del 27 febbraio 2013 concernente la LSCPT, FF **2013** 2283 2375).

Art. 27 Qualità dei dati trasmessi

Per non pregiudicare il buon andamento della sorveglianza, occorre, tra le altre cose, garantire la qualità dei dati trasmessi. Pertanto la presente disposizione definisce i requisiti posti alla qualità dei dati trasmessi ovvero le condizioni che devono essere soddisfatte affinché la qualità sia garantita.

Secondo il *capoverso 1* la qualità dei dati trasmessi è garantita se l'intercettazione dei dati soddisfa i requisiti stabiliti dal Dipartimento (lett. a), avviene senza perdita di dati e interruzioni (lett. b), i dati della sorveglianza o le informazioni trasmessi corrispondono al mandato di sorveglianza o alla domanda di informazioni (lett. c). Pertanto è sufficiente che l'intercettazione dei dati avvenga senza perdite e senza interruzione. Se i dati a disposizione delle persone obbligate a collaborare sono incompleti, la qualità è garantita se tali dati sono trasmessi senza perdita e interruzioni. Può quindi essere trasmesso soltanto ciò che si trova nella rete della persona obbligata a collaborare. La qualità dei dati risultanti dalla sorveglianza non può essere migliore rispetto a quella dei medesimi presso i servizi sorvegliati. Allo stesso modo la qualità delle informazioni non può essere migliore rispetto a quella delle informazioni relative agli utenti e dei metadati rilevati e memorizzati conformemente alle regole.

I *capoversi 2 e 3* disciplinano le responsabilità per quanto attiene alla garanzia della qualità. La persona obbligata a collaborare è responsabile della qualità delle informazioni e dei dati risultanti dalla sorveglianza e il Servizio SCPT la sostiene fornendole consulenza. La persona obbligata a collaborare resta responsabile della qualità anche se ha conferito a terzi il compito di eseguire la sorveglianza.

Se constatano lacune nella qualità dei dati trasmessi, la persona obbligata a collaborare e il Servizio SCPT si informano reciprocamente senza indugio (*cpv. 4*). Se le lacune riguardano in particolare prestazioni effettuate durante il servizio di picchetto (cfr. art. 11), deve esserne informato immediatamente per telefono il relativo servizio di contatto. È anche possibile che siano le autorità di perseguimento penale a constatare lacune della qualità. In questo caso l'autorità di perseguimento penale deve comunicare la lacuna al Servizio SCPT, che successivamente ne informa la persona obbligata a collaborare.

Sia il Servizio SCPT che le persone obbligate a collaborare effettuano un monitoraggio ai fini del controllo della qualità.

I dettagli sono disciplinati nella OE-SCPT.

In caso di guasti, le persone obbligate a collaborare e il Servizio SCPT li analizzano senza indugio e informano esaustivamente e il più rapidamente possibile la controparte in merito ai risultati dell'analisi. Se il guasto si verifica presso le persone obbligate a collaborare, queste sono tenute a segnalarlo per scritto al Servizio SCPT, indicandone con precisione la durata e la natura e fornendo una panoramica cronologica dei provvedimenti disposti e dello stato del problema. Il guasto deve essere segnalato al più tardi il giorno lavorativo successivo. Inoltre, la persona obbligata a collaborare deve comunicare il più rapidamente possibile al Servizio SCPT la presumibile durata del guasto. Fanno parte delle informazioni esaustive da trasmettere alla controparte anche i singoli risultati degli accertamenti e i relativi dati. Questi servono a cementare i risultati delle analisi ed eventualmente alla controparte per le sue analisi. Il Servizio SCPT sente la persona obbligate a collaborare e stabilisce di comune accordo il livello di gravità del problema (p. es: critico, grave, esiguo). La persona obbligata a

collaborare elimina la lacuna individuata entro il tempo indicato dal Dipartimento per i singoli livelli di gravità e informa, per scritto e alle scadenze regolari stabilite dal Dipartimento, il Servizio SCPT in merito agli ulteriori provvedimenti disposti e agli ultimi sviluppi concernenti lo stato del problema. Dopo aver riparato il guasto la persona obbligata a collaborare deve inviare senza indugio al Servizio SCPT una notificazione di avvenuta riparazione che completa ed eventualmente precisa i dati relativi alla comunicazione del guasto.

I metadati della sorveglianza in tempo reale vanno memorizzati e in seguito immediatamente trasmessi secondo le possibilità tecniche delle specifiche d'interfaccia. Se i metadati della sorveglianza in tempo reale non sono più disponibili o sono lacunosi, la persona obbligata a collaborare è tenuta a trasmettere senza indugio i corrispondenti metadati della sorveglianza retroattiva conformemente alle direttive impartite dal Servizio SCPT (cfr. art. 4 cpv. 3).

Art. 28 Collegamenti di collaudo

Secondo il *capoverso 1* si effettuano collegamenti di collaudo per garantire la qualità del trasferimento dei dati intercettati da parte delle persone obbligate a collaborare al Servizio SCPT e alle autorità di perseguimento penale (*lett. a*), per verificare la disponibilità a informare e sorvegliare delle persone obbligate a collaborare *(lett. b*), per testare il sistema di trattamento del Servizio SCPT (lett. c), a scopi di formazione (*lett. d*) e per creare dati di riferimento (*lett. e*).

Per *collegamento di collaudo* s'intende la sorveglianza tecnica di un servizio di comunicazione (p. es. abbonamento telefonico, carta SIM prepagata, telefono fisso) o di un servizio di comunicazione derivato (p. es. servizi di messaggistica, webmail) per gli scopi di cui al *capoverso 1*. I dispositivi e i software utilizzati a tal fine sono definiti *attrezzatura per i test;* può trattarsi ad esempio di apparecchiature terminali come gli smartphone o anche simulatori sotto forma di software utilizzati dall'organizzazione che effettua il test esclusivamente a tale scopo. In un collegamento di collaudo l'obbiettivo della sorveglianza è chiamato *target del test*. I dati usati o raccolti nell'ambito di un collegamento di collaudo (p. es. conversazioni telefoniche, SMS, traffico Internet) sono definiti *dati relativi ai test*. Tali dati sono usati o raccolti solamente per gli scopi di cui al capoverso 1. In tal modo si garantisce che tutti i partner che partecipano alla comunicazione oggetto del test di sorveglianza e le loro telecomunicazioni siano fittizi. I target del test, i dati relativi ai test e l'attrezzatura per i test sono a disposizione soltanto dei collaboratori del Servizio SCPT, delle persone obbligate a collaborare e delle autorità di perseguimento penale autorizzate a effettuare un collegamento di collaudo.

Poiché sono usati solo per collegamenti di collaudo, i dati relativi ai test non sottostanno al segreto delle telecomunicazioni. Per i collegamenti di collaudo non è pertanto necessaria l'autorizzazione dell'autorità giudiziaria competente e non devono essere neppure soddisfatti i requisiti dell'articolo 269 capoverso 1 CPP. Poiché per i collegamenti di collaudo non vi è un'autorità investita del procedimento, il Servizio SCPT può prendere conoscenza del contenuto dei dati relativi ai test senza doverne richiedere l'autorizzazione (art. 18 cpv. 2 nLSCPT).

Per i collegamenti di collaudo, il Servizio SCPT tiene un fascicolo relativo alla sorveglianza (art. 9) separato. Il Servizio SCPT registra soltanto i dati relativi al responsabile, alla sua unità organizzativa (nome e indirizzo), allo scopo di utilizzo

dei target del test e al nome delle persone autorizzate ad elaborare i dati relativi al test. I collegamenti di collaudo sono tuttavia protocollati in modo simile alle sorveglianze normali. Pertanto, anche nel caso di un collegamento di collaudo il Servizio SCPT protocolla il trattamento dei dati di tutti i target dei test.

Secondo il *capoverso 4* anche le autorità di perseguimento penale possono eseguire a proprie spese dei test ai fini della garanzia della qualità della trasmissione del traffico delle comunicazioni e a scopi di formazione. A tal fine devono presentare la relativa domanda al Servizio SCPT e versano i relativi emolumenti. Affinché possa chiedere un collegamento di collaudo, un'autorità di perseguimento penale deve indicare una persona e un supplente come responsabili per la gestione del target del test, dei servizi testati e delle attrezzature di test delle unità organizzative coinvolte e che hanno diritto a trasmettere al Servizio SCPT gli ordini necessari per i collegamenti di collaudo. A proprie spese significa che le autorità di perseguimento penale devono assumersi anche le indennità per i collegamenti di collaudo da versare alle persone obbligate a collaborare. Ciò significa che anche per lo svolgimento di collegamenti di collaudo devono versare al Servizio SCPT gli emolumenti, incluse le indennità previste per le persone obbligate a collaborare. Gli emolumenti e le indennità sono fissati nell'ordinanza sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OEm-SCPT). Le autorità di perseguimento penale possono trasferire i dati intercettati con i collegamenti di collaudo al sistema di trattamento gestito dal Servizio SCPT oppure direttamente a sé stesse (cfr. commento all'articolo 26 sul collegamento diretto). Ai collegamenti di collaudo delle autorità di perseguimento penale si applica per analogia l'articolo 18 capoverso 2 nLSCPT.

Al mandato di sorveglianza, il Servizio SCPT deve apporre un'annotazione che indichi che si tratta in realtà di un collegamento di collaudo. Se per creare dati relativi ai test ha bisogno delle persone obbligate a collaborare, il Servizio SCPT può incaricarle di tale compito (*cpv. 2*). Inoltre, la persona obbligata a collaborare deve mettere gratuitamente e permanentemente a disposizione del Servizio SCPT, su sua richiesta, i collegamenti di collaudo necessari e i servizi di telecomunicazione o i servizi di comunicazione derivati richiesti (*cpv. 3*). Ciò significa che le persone obbligate a collaborare sono tenute a finanziare in particolare gli emolumenti di base, gli emolumenti di attivazione, gli emolumenti ricorrenti nonché tutti i tipi di emolumenti legati alla comunicazione e all'utenza. La persona obbligata a collaborare mette ad esempio gratuitamente a disposizione del Servizio SCPT il numero necessario di schede SIM, attiva gratuitamente i servizi occorrenti e non conteggia alcun emolumento per il loro uso.

Le apparecchiature terminali non proprietarie, ossia i terminali usuali sul mercato, sono invece procurate e finanziate dal Servizio SCPT. Se tuttavia i servizi di telecomunicazione o i servizi di comunicazione derivati di una persona obbligata a collaborare richiedessero apparecchiature terminali di proprietà, essa è tenuta a metterle gratuitamente a disposizione del Servizio SCPT per i collegamenti di collaudo.

I collegamenti di collaudo effettuati su richiesta delle autorità di perseguimento penale devono seguire una procedura formale simile a quella per le sorveglianze usuali. L'autorità di perseguimento penale deve trasmettere la richiesta al Servizio SCPT e indicare per quanto tempo deve rimanere attivo il collegamento; tale durata non può superare 12 mesi. Il Servizio SCPT verifica se la richiesta soddisfa i suoi

requisiti e se è stata presentata da una persona che ne è autorizzata. Se i requisiti sono soddisfatti, il Servizio SCPT trasmette il mandato di sorveglianza alle persone obbligate a collaborare affinché quest'ultima attivi i collegamenti di collaudo. Anche in questo caso il Servizio SCPT deve apportare un'annotazione che indichi che si tratta di un collegamento di collaudo. Previo emolumento e su richiesta, le persone autorizzate presso l'autorità di perseguimento penale possono prorogare i collegamenti di collaudo al massimo per ulteriori 12 mesi. Al più tardi tre mesi prima della fine di un collegamento di collaudo, il Servizio SCPT invia una pertinente comunicazione alla persona autorizzata presso l'autorità di perseguimento penale. Il collegamento di collaudo rimane attivo se i requisiti per la proroga sono soddisfatti. In caso contrario il Servizio SCPT mette fine al collegamento trasmettendo il pertinente incarico alla persona obbligata a collaborare.

Sezione 3: Garanzia della disponibilità a informare e sorvegliare

Art. 29 Verifica della disponibilità a informare e sorvegliare

Ogni FST e ogni fornitore di servizi di comunicazione derivati con obblighi di informazione supplementari ai sensi dell'articolo 21 deve essere in grado (disponibilità a informare) di fornire o far fornire da terzi le informazioni di cui agli articoli 33-46 che concernono i servizi da esso offerti (cfr. art. 18).

Ogni FST e ogni fornitore di servizi di comunicazione derivati con obblighi di sorveglianza supplementari ai sensi dell'articolo 50 deve essere in grado (disponibilità a sorvegliare) di eseguire o far eseguire le sorveglianze di cui agli articoli 52-68 che concernono i servizi da esso offerti (cfr. art. 48). Sono escluse i FST con obblighi di sorveglianza ridotti ai sensi dell'articolo 49.

Per dimostrare la disponibilità a informare o a sorvegliare i fornitori summenzionati dovranno provare di essere in grado di fornire le informazioni fornite o eseguire le sorveglianze conformemente al diritto applicabile (*cpv. 1*).

Secondo il *capoverso 2* la prova è fornita se i test eseguiti secondo le prescrizioni del Servizio SCPT si sono conclusi positivamente (*lett. a*) e se il fornitore conferma in un questionario elaborato dal Servizio SCPT di soddisfare le prescrizioni relative alle informazioni e sorveglianze standardizzate per le quali la prova non può essere fornita mediante dei test. Giacché hanno la possibilità di delegare l'esecuzione dei loro obblighi di informazione e di sorveglianza a terzi, i fornitori possono prevedere che siano questi ultimi a fornire la prova della disponibilità a informare e sorvegliare. In questo caso, per la verifica della disponibilità a informare e sorvegliare si chiede anche al terzo di fornire la prova necessaria. È possibile che la prova possa essere fornita in collaborazione con il fornitore stesso. In ogni caso è il fornitore a essere responsabile della prova.

Conformemente al *capoverso 3*, nella verifica della disponibilità a informare e sorvegliare il Servizio SCPT svolge i seguenti compiti: dopo aver consultato il fornitore interessato fissa uno scadenzario vincolante per i test e definisce i casi che il fornitore deve testare; controlla i risultati dei test (*lett. a*), valuta i questionari (*lett. b*), verbalizza lo svolgimento della verifica (*lett. c*) e, una volta accertata la disponibilità a informare e sorvegliare dei fornitori, rilascia loro un attestato (*lett. d*). Il Servizio SCPT deve conservare i pertinenti verbali per la durata di validità dell'attestato e per i due anni successivi alla scadenza (*lett. e*). I

verbali possono fungere da mezzo di prova in caso di controversia ed essere di aiuto per la prossima verifica della disponibilità a informare e sorvegliare.

L'attestato certifica che per determinati tipi di informazione e sorveglianza il fornitore è in grado di eseguire l'intercettazione dei dati secondo le prescrizioni del Dipartimento e quindi di garantire la disponibilità ad informare e a sorvegliare.

Art. 30 Durata di validità dell'attestato

Se dalla verifica della disponibilità a informare e sorvegliare emerge che è in grado di eseguire i relativi mandati conformemente alle disposizioni, la persona obbligata a collaborare riceve un attestato (cfr. il commento all'art. 29).

Secondo il *capoverso 1* l'attestato è valido tre anni; per il calcolo del termine è determinante la data di rilascio dell'attestato del Servizio SCPT.

Secondo il *capoverso 2,* allo scadere della durata di validità il Servizio SCPT può prolungare l'attestato per ulteriori tre anni se la persona obbligata a collaborare certifica che dalla concessione dell'attestato non sono avvenuti cambiamenti che influiscono sulla trasmissione dei dati e sulla disponibilità a informare e sorvegliare. Per ottenere la proroga, la persona obbligata a collaborare deve presentare richiesta al Servizio SCPT e allegare le certificazioni menzionate.

Il *capoverso 3* prevede l'obbligo delle persone obbligate a collaborare di informare senza indugio il Servizio SCPT se constatano di non essere più in grado di informare e sorvegliare.

Art. 31 Procedura di collaudo

Questa disposizione conferisce al Dipartimento la competenza di disciplinare lo svolgimento della procedura per il collaudo dei sistemi tecnici e della procedura per la verifica della disponibilità a informare e sorvegliare (cfr. art. 31 cpv. 3 nLSCPT).

Art. 32 Annullamento dell'attestato della disponibilità a informare e sorvegliare

Se un FST o un fornitore di servizi di comunicazione derivati con obblighi di sorveglianza supplementari non è più in grado di fornire le informazioni o svolgere le sorveglianze che riguardano i servizi da esso offerti, il Servizio SCPT dichiara immediatamente nullo l'attestato relativo alla disponibilità a informare e sorvegliare. È possibile che il fornitore non sia più in grado di fornire le informazioni e/o di sorvegliare soltanto per quanto riguarda determinati servizi da esso offerti. In tal caso la dichiarazione di annullamento si riferisce solamente al servizio in questione e al tipo di informazione e/o di sorveglianza non più garantito e non agli altri servizi offerti dal fornitore. In un caso simile occorre allestire un attestato separato per quanto riguarda i servizi per i quali il fornitore garantisce la disponibilità a informare e sorvegliare. Se ce n'è bisogno si può ordinare anche in questo caso un'ulteriore verifica prima che venga allestito un eventuale attestato. L'attestato deve indicare chiaramente a quali servizi si riferisce. Se per quanto riguarda un servizio offerto è stata accertata la disponibilità di fornire informazioni ma non quella di sorvegliare, occorre indicarlo nell'attestato o nella dichiarazione di annullamento.

Il Servizio SCPT annulla l'attestato se il fornitore comunica che non sussiste più la disponibilità a informare e sorvegliare (*lett. a*), se si è a conoscenza di fatti per cui il fornitore non è in grado in uno o più casi di garantire la trasmissione dei dati e la disponibilità a informare e sorvegliare (*lett. b*) o se le dichiarazioni del fornitore su cui si basa l'attestato non corrispondono a verità (*lett. c*).

Sezione 4: Tipi di informazione per servizi di accesso alla rete

Art. 33 Tipo d'informazione IR_1_NA: informazioni su utenti di servizi di accesso alla rete

La presente disposizione definisce il tipo d'informazione standardizzato per le informazioni relative agli utenti dei servizi di accesso alla rete. Questo tipo d'informazione corrisponde essenzialmente alle informazioni attuali A0 e in parte A1 (*cpv. 2 lett. j e k*). Secondo la nuova ordinanza sarà possibile chiedere il numero d'identificazione delle imprese (*cpv. 2 lett. g*), l'identificativo dell'utente (*cpv. 2 lett. h*) e l'identificativo del servizio (*cpv. 2 lett. l*).

Con servizi di accesso alla rete si intendono i servizi di telecomunicazione che permettono l'accesso ai servizi di telecomunicazione pubblici come Internet in modo diretto (p. es. accesso a Internet DSL) o indiretto (p. es. Virtual Private Network, VPN). Per quanto riguarda il VPN occorre notare che tra l'accesso a Internet diretto del cliente VPN e il fornitore VPN vi è un tunnel VPN. I clienti VPN operano su Internet con un indirizzo IP del fornitore VPN e non con l'indirizzo IP loro assegnato dal fornitore di accesso diretto a Internet; ciò significa che gli accessi a Internet dei clienti VPN hanno come indirizzo di fonte un indirizzo IP del fornitore VPN. Soltanto i fornitori VPN possono vedere l'indirizzo IP dell'accesso diretto a Internet dei clienti VPN. Pertanto i fornitori VPN devono essere in grado di fornire informazioni sui loro utenti e i loro servizi.

Questo tipo di informazioni è strutturato secondo lo standard ETSI TS 102 657 e combina tutte le informazioni generali sugli utenti (generic subscriber info) con i dati più importanti sui loro servizi di accesso alla rete. È possibile richiedere ulteriori dati specifici sui servizi di accesso alla rete attraverso il tipo d'informazione IR_2_NA (*art. 34*).

Il presente articolo può essere spiegato con un esempio. La persona X usufruisce dei seguenti servizi del fornitore Y: tre abbonamenti di telefonia mobile (con telefonia e Internet), dieci carte prepagate (soltanto telefonia) e due servizi di accesso a Internet da rete fissa. L'autorità di perseguimento penale, che conosce il nome e l'indirizzo della persona X, vuole sapere i servizi di cui usufruisce presso il fornitore Y. A tal fine formula le domande di informazioni IR_1_NA (art. 33) e IR_6_TEL (art. 38). Il fornitore Y risponde al tipo d'informazione IR_1_NA (art. 33) con cinque risultati (considerati cinque pacchetti di dati, cfr. commenti all'art. 17 cpv. 2) e al tipo d'informazione IR_6_TEL (art. 38) con 13 risultati (anch'essi considerati 13 pacchetti di dati).

Il *capoverso 1* stabilisce le informazioni da fornire sugli utenti dei servizi di accesso alla rete (cfr. gli art. 21 cpv. 1 nLSCPT [informazioni sui servizi di telecomunicazione] e 22 cpv. 2 e 4 nLSCPT [informazioni per identificare gli autori di reati commessi via Internet]).

Secondo la *lettera a* occorre comunicare l'identificativo univoco (p. es. numero di cliente) nel caso in cui il fornitore ne abbia assegnato uno all'utente.

I dati identificativi della persona elencati nella *lettera b* sono spiegati in dettaglio all'articolo 19.

Qui appresso si commentano i singoli numeri della *lettera c*:

- l'«identificativo univoco che designa il fornitore» menzionato al *numero 1* indica un numero amministrativo che il Servizio SCPT conferisce al fornitore per identificarlo in modo univoco;

- l'«identificativo univoco del servizio» di cui al *numero 2* indica i servizi di telecomunicazione o i servizi di comunicazione derivati di cui ha fruito l'utente. Tale denominazione deve essere univoca almeno nell'ambito del fornitore (p. es. numero di telefono, nome utente, denominazione dei collegamenti senza filo a banda larga, indirizzo di posta elettronica);

- per *inizio* del «periodo di utilizzazione del servizio» (*n. 3*) si intende il momento (data e ora) dell'avvio della relazione commerciale, anche se eventualmente l'attivazione effettiva del servizio può essere avvenuta in seguito. È ad esempio possibile che una carta SIM prepagata sia acquistata e i relativi dati personali siano rilevati in un determinato giorno, ma che la carta stessa sia attivata soltanto alcuni giorni dopo. Per attivazione si intende pertanto che a partire da tale momento l'utente può usufruire del servizio. Se del caso va comunicato anche il momento dell'attivazione. La *fine* del servizio indica il momento a partire dal quale gli utenti non possono più usare il servizio in modo permanente. Il blocco temporaneo del servizio non vale come fine dello stesso. L'aggiunta «se del caso» significa che occorre trasmettere la *data della fine* soltanto quando l'utente non può più usare il servizio in modo permanente;

- secondo il *numero 4* possono essere trasmesse, in forma leggibile per gli umani, informazioni su opzioni supplementari o limitazioni del servizio di accesso alla rete, (p. es. «con indirizzo IP statico», «volume dei dati di massimo un GB»; cfr. standard ETSI TS 102 657, tabella E.2);

- gli indirizzi d'installazione dell'accesso fisso alla rete di cui al *numero 5* sono le indicazioni relative all'ubicazione di tali accessi come annotati dal fornitore;

- Per quanto riguarda lo stato del servizio, secondo il *numero 6* il fornitore può trasmettere le sue designazioni usuali, poiché una conversione nelle designazioni standard costituirebbe un onere eccessivo. Con periodo di validità si intende il periodo (data di inizio ed eventualmente data della fine) in cui è o era valido lo stato;

- Secondo il *numero 7* vanno forniti, se del caso, tutti gli indirizzi IP statici, i prefissi IP, i settori di indirizzi IP e le maschere di sottorete o le lunghezze di prefisso assegnati al servizio di accesso alla rete e il loro periodo di validità.

- Secondo il *numero 8*, nel caso di servizi di telecomunicazione prepagati, occorre comunicare, conformemente all'articolo 21 capoverso 1 lettera e nLSCPT e all'articolo 19 capoverso 1 della presenta ordinanza, il momento e il luogo della consegna, nonché nome e cognome della persona che gli ha consegnati.

- Secondo il *numero 9* occorre comunicare, se del caso, tutti i numeri delle carte SIM (ICCID) registrati dai fornitori in relazione con il servizio di accesso alla rete richiesto, con la loro data di attivazione o eventualmente di disattivazione.

- Secondo il *numero 10*, nel caso di servizi mobili va comunicato l'IMSI (International Mobile Subscriber Identity). Questo numero univoco a livello globale serve a identificare l'utente del servizio mobile nella rete.

- Secondo il *numero 11* occorre comunicare il tipo di servizio. In altre parole, va comunicato se si tratta di un servizio prepagato (prepaid) o di un abbonamento (postpaid).

- Secondo il *numero 12* va comunicato l'identificativo alternativo dell'utente per il servizio d'accesso alla rete. Questa informazione è necessaria soltanto se oltre all'identificativo univoco dell'utente di cui alla lettera a esiste anche un altro identificativo per il servizio di accesso alla rete.

Il *capoverso 2* elenca i criteri che deve contenere una domanda. Con tali criteri l'autorità di perseguimento penale presenta la domanda ai fornitori attraverso il sistema d'informazione del Servizio SCPT. Nella domanda d'informazioni è necessario indicare almeno un criterio. Se è usato un criterio di cui alle lettere a-d, occorre indicarne anche un altro (*lett. a–k*), di modo che la domanda sia sufficientemente precisa. I criteri di cui alle *lettere e–k* sono invece univoci, cosicché è sufficiente indicarne solo **uno**.

La *lettera a* riunisce il/i cognome/i e il/i nome/i in un criterio; ciò permette una combinazione libera per la domanda. Può infatti darsi che in occasione della registrazione, nome e cognome siano scambiati; inoltre, non è sempre chiaro quale sia il nome e quale il cognome (p. es. Thomas Peter) oppure vi sono casi in cui una persona ha più nomi o cognomi (p. es. Heydi Núñez Gómez).

Poiché non sempre esistono numeri civici, nella *lettera d* è inserita l'aggiunta «se del caso».

Nella *lettera i* gli indirizzi IP sono esclusi dal criterio poiché per la richiesta degli stessi sono a disposizioni i dati d'informazione IR_3_IP (art. 35), IR_4_IP(NAT) (art. 36) e IR_5_NAT (art. 37) (cfr. il commento agli art. 35-37).

Art. 34 Tipo di informazione IR_2_NA: informazioni su servizi di accesso alla rete

La presente disposizione definisce il tipo d'informazione standardizzato, basato sullo standard ETSI TS 102 657, per informazioni in merito ai servizi di accesso alla rete. In questo modo sono raccolti ulteriori dati di cui all'articolo 21 capoverso 1 lettera d nLSCPT.

Il *capoverso 1* elenca le informazioni da fornire e il *capoverso 2* i criteri che deve contenere la domanda.

Per il *capoverso 1 lettera d* occorre osservare che va consegnato l'elenco degli identificativi degli apparecchi **realmente utilizzati** durante il periodo a cui si riferisce la domanda di informazioni. Il fornitore deve evincere queste informazioni dai metadati memorizzati, senza tuttavia trasmettere questi ultimi (per il termine metadati si veda anche il commento introduttivo alla sezione 10 del capitolo 3). Ciò significa che dalla risposta non deve trasparire quando, come e dove sono stati utilizzati gli apparecchi.

Art. 35 Tipo di informazione IR_3_IP: Identificazione dell'utenza in caso di indirizzi IP assegnati univocamente

La presente disposizione definisce il tipo d'informazione standardizzato, basato sullo standard ETSI TS 102 657, per le informazioni volte all'identificazione dell'utente nel caso siano stati assegnati indirizzi IP univoci. Sono in tal modo raccolti i dati secondo l'articolo 22 capoverso 2 LSCPT. Il tipo d'informazione corrisponde alle informazioni in vigore A0.1 (indirizzo IP statico) e A0.2 (indirizzo IP dinamico). In questo tipo d'informazione tutte le domande sono uniformate secondo l'indirizzo IP, giacché non è possibile evincere da quest'ultimo se è o è stato assegnato univocamente. Se ciò non fosse, il fornitore lo comunica nella risposta e l'autorità richiedente può presentare una nuova domanda di informazioni del tipo IR_4_IP (NAT) (art. 36) in cui è tuttavia necessario indicare ulteriori criteri (cfr. il commento all'art. 36).

Il termine *indirizzi IP assegnati univocamente* significa che in qualsivoglia momento è apparso in Internet con tale indirizzo un solo utente. Ciò vale sia per gli indirizzi IP statici sia per gli indirizzi IP dinamici assegnati univocamente. Dato che, come già detto, non si vede se l'indirizzo IP è stato o è assegnato univocamente, soltanto il risultato di questo tipo di informazione può fare chiarezza. Nella domanda di informazioni è importante indicare un momento preciso, al secondo, visto che per gli indirizzi IP dinamici assegnati univocamente il momento dell'assegnazione può essere molto breve e si possono quindi ottenere risulti falsamente positivi. Occorre controllare che il fuso orario sia corretto, soprattutto per i dati temporali esteri.

Il fornitore svolge la ricerca per il momento richiesto con un intervallo di tolleranza di più o meno qualche secondo. Questo intervallo di tolleranza è necessario a causa delle possibili imprecisioni degli orologi del sistema e sarà definito nell'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT), nella quale saranno concretizzati anche i diversi passi per rispondere ad una simile domanda di informazioni.

Art. 36 Tipo di informazione IR_4_IP (NAT): identificazione dell'utenza in caso di indirizzi IP non assegnati univocamente (NAT)

Questo tipo d'informazione è nuovo e tratta un problema specifico legato all'identificazione degli utenti nel caso di indirizzi IP assegnati in modo non univoco. Si basa sullo standard ETSI TS 102 657. Con i cosiddetti Network Address Translation (NAT) diverse migliaia di utenti possono dividersi lo stesso indirizzo IP pubblico. Pertanto nel caso dei NAT l'identificazione degli utenti è possibile soltanto con un onere tecnico più elevato.

Carrier Grade NAT (cgNAT) significa Network Address Translation (NAT) al livello dei fornitori (carrier). Nella rete del fornitore di accesso agli utenti vengono assegnati indirizzi IP privati validi soltanto all'interno di detta rete. Quando gli utenti accedono a Internet tali indirizzi vengono tradotti in un indirizzo IP sorgente pubblico comune (diversi utenti si dividono contemporaneamente un indirizzo IP comune). Le numerose singole connessioni a Internet possono essere distinte grazie al numero di porta. Occorre che la traduzione dell'indirizzo avvenga per ogni pacchetto IP in entrata e in uscita. In caso di procedure non deterministiche l'apparecchio (router) crea delle tabelle di assegnazione e per ogni connessione Internet (contesto) memorizza il marcatempo, la fonte e la destinazione (l'indirizzo

IP e il numero di porta), il corrispondente indirizzo IP privato e numero di porta dell'utente nonché il tipo di protocollo di trasporto. In caso di procedure NAT deterministiche gli indirizzi e i numeri di porta sono tradotti per mezzo di un algoritmo. Successivamente possono nuovamente essere ritrasposti e quindi non è necessario che ai fini dell'identificazione dell'utente il fornitore dell'accesso memorizzi gli indirizzi IP e i numeri di porta di destinazione.

Già da parecchio tempo vengono usate procedure NAT per l'accesso a Internet da rete mobile (p. es. GPRS, UMTS, LTE). I motivi sono il numero ridotto di indirizzi IPv4 pubblici e misure di sicurezza quali ad esempio il cosiddetto topology hiding, che impedisce di dedurre dall'esterno la struttura della rete. Giacché oggi ci sono pochissimi indirizzi IPv4 pubblici ancora disponibili, i fornitori di accesso utilizzano sempre più spesso cgNAT anche per gli accessi a Internet da rete fissa.

A differenza dell'IPv4 per l'IPv6 vi sono sufficienti indirizzi a disposizione e si prevede che a lungo termine il cgNAT perderà importanza. Tuttavia al momento si osserva piuttosto una crescente importanza a causa delle scarse riserve di indirizzi IPv4 e del forte aumento del traffico di dati mobile (p. es smartphone, tablet).

Il *capoverso 1 lettera a* stabilisce le indicazioni da fornire in caso di identificazione dell'utente. Secondo la *lettera b* in caso di mancata identificazione occorre fornirne il motivo (p. es. nessun risultato, più risultati).

Il *capoverso 2* stabilisce le indicazioni che deve contenere la domanda di informazioni:

- l'indirizzo di IP sorgente pubblico (*lett. a*), ossia l'indirizzo IP pubblico usato in comune, visibile in Internet come originating IP;
- se necessario per l'identificazione, vale a dire nel caso di una procedura NAT, il numero di porta sorgente pubblico (*lett. b*), visibile in Internet come originating Port;

  (Osservazione: l'indirizzo IP sorgente privato e il numero di porta sorgente privato sono noti soltanto al fornitore dell'accesso);
- se necessario per l'identificazione, ossia nel caso di una procedure NAT non deterministica, l'indirizzo IP di destinazione pubblico, il numero di porta di destinazione e il tipo di protocollo di trasporto, ad esempio TCP, UDP (*lett. c-e*);
- l'indicazione della data e dell'ora (*lett. f*). L'indicazione deve essere esatta e i parametri di ricerca devono essere molto ristretti.

Riassumendo, per la procedura sono previste le seguenti tappe:

- 1ª tappa (fa parte dei lavori preliminari e non è parte di questo tipo di informazioni): IP history per l'account utente ricercato presso il gestore del servizio Internet (server).

- 2ª tappa: domanda di informazioni al fornitore di accesso a Internet (indicando i dettagli di connessione di un login concreto secondo l'IP history).

Dettagli sulla 1ª tappa: chiedere la cosiddetta IP history per uno specifico account utente presso il fornitore del server, ossia presso la «destinazione» (p. es. gestore di un blog, webmail o social network).

L'autorità di perseguimento penale riceve un protocollo di connessione con tutti i dati necessari per individuare gli accessi ad Internet, dai quali è stato effettuato

l'accesso all'account utente ricercato: sorgente della connessione (indirizzo IP + porta), server di destinazione (indirizzo IP + porta), marcatempo e tipo di protocollo. Grazie a queste indicazioni nella seconda tappa si potrà procedere all'identificazione dell'utente.

Dettagli sulla 2ª tappa: la ricerca per un accesso a Internet da rete mobile potrebbe ad esempio svolgersi come segue. In base a tre fino a sei indicazioni contenute nella domanda di informazioni, il fornitore di accesso cerca tra i dati NAT di traduzione da esso memorizzati l'indirizzo IP privato e il numero di porta (assegnati all'utente ricercato nel momento ricercato, ossia l'IP sorgente [IP/numero di porta privato]). Successivamente, in base all'indirizzo IP e al numero di porta privati trovati nonché al marcatempo, si cerca il MSISDN o l'IMSI dell'utente. Infine, in base al MSISDN o all'IMSI identificati, si cercano i dati personali dell'utente.

È possibile effettuare anche ricerche analoghe, ad esempio nel caso di Dual-Stack Lite (DS Lite).

Dalla pubblicazione della versione V1.14.1 dello standard ETSI TS 102 657 nel marzo 2014, esiste una struttura dei dati standardizzata per i dati NAT (allegato E.3 «ASN.1 definitions for network access services»).

Le sfide tecniche per memorizzare e richiedere i dati di traduzione NAT risultano dal fatto che i fornitori devono memorizzare grandi quantità di dati e garantire l'efficienza delle procedure di ricerca. Le numerose connessioni IP, che avvengono in contemporanea attraverso il router NAT, sono distinti grazie ai parametri descritti sopra. Di norma un singolo utente utilizza decine fino a centinaia di connessioni IP allo stesso tempo. I numeri di porta sorgente e i numeri di porta tradotti sono rilasciati e riassegnati ciclicamente. In caso di mancato utilizzo, la connessione Internet degli smartphone è ad esempio sospesa per risparmio di batteria. Pertanto, quando la connessione è riattivata, allo smartphone è assegnato un nuovo indirizzo IP (privato). Ne risulta un processo enormemente dinamico che genera grandi quantità di dati. Attualmente si stima che nelle grandi reti mobili svizzere vi siano circa un miliardo di procedure di traduzione NAT al giorno.

Le autorità di perseguimento penale devono essere consapevoli che con questo tipo d'informazione è possibile che non si ottenga alcun risultato o risultati ambigui, soprattutto se nella domanda non sono stati indicati tutti i parametri necessari. La precisione dei risultati può essere aumentata correlando ad esempio diverse domande. Di per sé il fatto che i fornitori memorizzino i dati NAT di traduzione non risolve il problema dell'identificazione degli utenti su Internet. Spesso i server di destinazione non memorizzano alcun numero di porta sorgente né un marcatempo preciso. A causa della notevole dinamicità delle procedure NAT, sono necessari dati per quanto possibile completi e precisi per evitare risultati falsamente positivi.

Infine va detto che, a seconda della procedura NAT, i fornitori di accesso devono memorizzare gli indirizzi IP di destinazione e i numeri di porta di tutti gli utenti soltanto per sei mesi, a condizione che si tratti di metadati ai sensi della nLSPTC o della OSPCT (art. 21 cpv. 2 secondo periodo nonché art. 22 cpv. 2 secondo periodo e cpv. 4 nLSCPT e art. 20 cpv. 2 OSCPT).

Art. 37 Tipo di informazione IR_5_NAT: informazioni su procedure di traduzione NAT

Questo nuovo tipo d'informazione, basato sullo standard ETSI TS 102 657, è finalizzato all'identificazione dell'utenza in caso di reati commessi via Internet, come previsto dall'articolo 22 nLSCPT.

Sono possibili due tipi di ricerca («prima» e «dopo» la procedura NAT sono da intendersi in senso temporale e dal punto di vista delle persone obbligate a collaborare):

- Ricerca 1

  Sono noti i dati **dopo** la traduzione NAT e si cercano quelli **prima**; ad esempio: si conoscono l'indirizzo IP sorgente pubblico e il numero di porta risultanti dalla traduzione NAT, si cerca l'indirizzo IP precendente alla stessa.
  Analogamente all'articolo 35, la domanda di informazioni su meccanismi di traduzione NAT deve contenere le seguenti indicazioni (*cpv. 2*):

  - l'indirizzo IP sorgente e il numero di porta dopo la traduzione NAT (*lett. a e b*), ad esempio l'indirizzo IP pubblico e il relativo numero di porta, visibili su Internet come «Source IP/port»;
  - il tipo di protocollo di trasporto, ad esempio TCP (*lett. e*);
  - l'indicazione di data e ora della traduzione NAT (*lett. f*);
  - qualora fosse necessario per l'identificazione (dipende dal tipo di procedura NAT), la domanda di informazioni deve indicare l'indirizzo IP di destinazione pubblico e il numero di porta di destinazione (*lett. c e d*) del server di destinazione.

- Ricerca 2

  Sono noti i dati **prima** dell'operazione NAT, si cercano quelli **dopo** la traduzione: si conosce ad esempio l'indirizzo IP **prima** della traduzione (p. es. indirizzo IP privato), si cerca l'indirizzo IP **dopo** la traduzione NAT (p. es. l'indirizzo IP sorgente pubblico).
  La domanda di informazioni su meccanismi di traduzione NAT deve contenere le seguenti indicazioni (*cpv. 2*):

  - l'indirizzo IP sorgente e il numero di porta prima della traduzione NAT (*lett. a e b*), ad esempio l'indirizzo IP privato del fornitore di accesso a Internet e il numero di porta;
  - il tipo di protocollo di trasporto, ad esempio TCP (*lett. e*);
  - l'indicazione di data e ora del meccanismo di traduzione NAT (*lett. f*);
  - qualora fosse necessario per l'identificazione (dipende dal tipo di procedura NAT), la domanda di informazioni deve indicare l'indirizzo IP di destinazione pubblico e il numero di porta di destinazione (*lett. c e d*) del server di destinazione.

Esempio di ricerca 1: se il tipo d'informazione IR_4_IP (NAT) di cui all'articolo 36 non produce risultati, è possibile che per identificare l'utenza debba essere tracciato ulteriormente l'indirizzo IP sorgente. Questo processo, noto come tracciamento (*backtracking*), è possibile soltanto se ogni persona obbligata a collaborare salva in modo preciso e completo tutte le informazioni delle rispettive

traduzioni NAT necessarie per l'identificazione. Quali siano queste informazioni nel singolo caso dipende dalla procedura usata dalla persona obbligata a collaborare. È anche possibile adottare una procedura più articolata (da NAT a NAT), inviando le domande di informazione a tutte le persone obbligate a collaborare che hanno eseguito una traduzione NAT per il collegamento Internet cercato.

Esempio di ricerca 2: nell'ambito della sorveglianza in tempo reale dell'accesso alla rete si rileva che la persona sorvegliata usa un determinato servizio di comunicazione derivato. I dati trasmessi tuttavia sono cifrati e l'identificativo dell'utente non è pertanto visibile; le autorità di perseguimento penale vorrebbero però conoscerlo. Presso il fornitore di servizi di comunicazione derivati, a causa della traduzione NAT del fornitore di accesso, è visibile un indirizzo IP sorgente (pubblico) diverso da quello (privato) assegnato all'utente sorvegliato e conosciuto dalle autorità di perseguimento penale grazie ai metadati della sorveglianza in tempo reale. Per poter identificare l'accesso in questione presso il fornitore del servizio di comunicazione derivato, l'indirizzo IP sorgente pubblico cercato e il numero di porta sorgente può essere chiesto al fornitore d'accesso mediante questo tipo di domanda indicando i dati di collegamento IP noti.

Sezione 5: Tipi di informazione per applicazioni

Art. 38 Tipo di informazione IR_6_TEL: informazioni su utenti di servizi di telefonia e multimedia

La disposizione definisce il tipo d'informazione standardizzato sugli utenti di servizi di telefonia e multimedia. Corrisponde in linea di massima alle attuali informazioni A0 e (in parte) A1 (*cpv. 2 lett. j e k*), con la differenza che ora è possibile indicare come criteri di ricerca il numero d'identificazione delle imprese (*cpv. 2 lett. g*), l'identificativo dell'utente (*cpv. 2 lett. h*) e l'identificativo del servizio (*cpv. 2 lett. l*).

Rientrano nei servizi di telefonia e multimedia, in particolare, i classici servizi telefonici analogici e digitali della rete fissa (p. es. POTS, ISDN), i servizi di telefonia mobile inclusi gli SMS e la segreteria vocale (p. es. GSM, UMTS), la telefonia Internet (p. es. VoIP), i servizi di telefonia multimediale di IMS (p. es. VoLTE, VoWLAN, presenza, RCS), la videotelefonia e le teleconferenze.

Questo tipo di informazione si basa sullo standard ETSI TS 102 657 e unisce i dati generici degli utenti (*generic subscriber info*) ai principali dati sui servizi di telefonia e multimedia da loro usati. Altri dati specifici su questo tipo di servizi possono essere richiesti con il tipo d'informazione IR_7_TEL (art. 39).

L'*articolo 38* si applica sia agli abbonamenti che alle offerte prepagate. Data l'analogia tra le disposizioni, si rimanda ai commenti all'articolo 33.

Analogamente all'articolo 33, il *capoverso 1* stabilisce le informazioni che devono essere fornite sugli utenti di servizi di telefonia e multimedia. I dati relativi al tipo di servizio (*n. 4*) servono a definire meglio il servizio. Nel caso dei servizi di telefonia e multimedia su rete fissa, per l'indirizzo di installazione dell'accesso alla rete e il suo periodo di validità (*n. 5*) vanno trasmessi i dati registrati presso il

fornitore (p. es. indirizzo dell'ubicazione). Dal momento che l'ubicazione dell'accesso può cambiare nel corso del tempo, va fornita la cronologia dei dati con, se del caso, le date di inizio e fine. Tuttavia, bisogna tener presente che non sempre i dati forniti corrispondono all'ubicazione effettiva dell'accesso, poiché in alcuni casi è possibile usare gli apparecchi forniti da una sede diversa, a insaputa del fornitore.

Il fornitore deve inoltre indicare, se del caso, l'elenco o il settore degli altri elementi di indirizzo registrati nell'ambito del servizio (*n. 7*) e le indicazioni sulla preselezione del fornitore di collegamenti (*n. 9*), vale a dire il *carrier selection code* preselezionato. Secondo l'articolo 9 capoverso 1 dell'ordinanza del 17 novembre 1997[40] della Commissione federale delle comunicazioni concernente la legge sulle telecomunicazioni, i fornitori di servizi telefonici pubblici su rete fissa devono offrire ai loro utenti la possibilità di scegliere liberamente, sia in modo prestabilito che per ogni chiamata, il loro fornitore di collegamenti nazionali e internazionali. Se il fornitore del servizio sorvegliato sa quale fornitore è stato preliminarmente scelto per le chiamate nazionali e internazionali, deve fornire tale informazione in adempimento della domanda di informazioni.

Analogamente all'articolo 33 capoverso 2, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e come vanno usati (cfr. il commento all'art. 33 cpv. 2).

Si distingue tra identificativi (*lett. h, j, k e l*) ed elementi d'indirizzo (*lett. i*): i primi definiscono univocamente il tipo di servizi di telefonia e multimedia, ma, contrariamente agli elementi di indirizzo, non servono a stabilire la comunicazione. Gli identificativi, come IMSI o IMPI, sono dati altamente confidenziali per i fornitori e hanno lo scopo di identificare l'utente all'interno della rete.

Dato che secondo l'articolo 23 dell'ordinanza del 6 ottobre 1997[41] concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT), un fornitore titolare di una serie di numeri può attribuire a sua volta numeri della serie («attribuzione subordinata») per la fornitura di un servizio di telecomunicazione, egli non dispone di norma dei dati aggiornati degli utenti di tali numeri. Nel rispondere a una domanda di informazioni, dovrà quindi indicare l'attribuzione subordinata nonché il nome e i dati di contatto (indirizzo e numero di telefono) del fornitore a cui ha ceduto il numero.

Art. 39 Tipo di informazione IR_7_TEL: informazioni su servizi di telefonia e multimedia

La disposizione definisce il tipo d'informazione standardizzato sui servizi di telefonia e multimedia, che corrisponde in linea di massima a quella che finora era l'informazione A1 (dati tecnici). La nozione di servizi di telefonia e multimedia è spiegata nel commento all'articolo 38.

Come nel caso dell'articolo 34, il *capoverso 1* stabilisce i dati da trasmettere quando sono richieste informazioni su servizi di telefonia e multimedia. Per quanto riguarda l'elenco degli identificativi degli apparecchi (*lett. d*) occorre tener presente che devono essere quelli effettivamente usati nel periodo in questione. Il fornitore deve estrapolare queste informazioni dai metadati memorizzati, senza

40 RS **784.101.112**
41 RS **784.104**

però trasmettere i metadati stessi. Ciò significa che dalla risposta non deve trasparire quando, come e dove gli apparecchi sono stati usati nel singolo caso. Va trasmessa, ad esempio, una lista degli IMEI degli apparecchi mobili effettivamente usati nel periodo in questione (indipendentemente dal tempo di utilizzo), senza indicare quando esattamente sono stati usate le apparecchiature terminali.

La durata di conservazione degli identificativi delle apparecchiatura terminali effettivamente usate (p. es. indirizzo MAC, IMEI) è limitata a sei mesi, poiché si tratta di metadati ai sensi dell'articolo 26 nLSCPT (art. 21 cpv. 2 secondo periodo nonché art. 22 cpv. 2 secondo periodo e cpv. 4 nLSCPT e art. 20 cpv. 2 OSCPT).

Analogamente all'articolo 34, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e come vanno usati (cfr. commento all'art. 34 cpv. 2).

Per i criteri di ricerca si distingue tra elementi d'indirizzo (*lett. a*) e identificativi (*lett. b, c ed e*).

Art. 40 Tipo di informazione IR_8_MSG: informazioni su utenti di servizi di posta elettronica

La disposizione definisce il tipo d'informazione standardizzato sugli utenti di servizi di posta elettronica, che corrisponde in linea di massima alle attuali informazioni A0 e (in parte) A1.

Data l'analogia tra le disposizioni, si rimanda ai commenti all'articolo 38. Anche in questo caso, il *capoverso 1* stabilisce quali informazioni devono essere fornite sugli utenti di servizi di posta elettronica.

Tra gli altri elementi d'indirizzo menzionati alla *lettera c numero 4* rientrano gli indirizzi alias. Questi sono indirizzi di posta elettronica supplementari che fanno parte di un unico account e che l'utente può creare, modificare e cancellare a piacere. Gli indirizzi alias, il cui numero massimo e la cui struttura sono stabiliti dal fornitore, sono collegati all'account principale, nella cui cartella di posta in entrata sono visualizzati i messaggi inviati a un indirizzo alias.

Nel caso del *numero 5*, vanno indicate, ad esempio, le mailing list. Si tratta di un gruppo di indirizzi di posta elettronica, chiamato anche lista di distribuzione, a cui è assegnato un indirizzo di posta elettronica proprio. I messaggi inviati all'indirizzo della mailing list sono inoltrati agli indirizzi di posta elettronica dei membri del gruppo, che possono a loro volta inviare messaggi usando l'indirizzo della mailing list come mittente.

La *lettera d* raggruppa invece altri elementi d'indirizzo, come indirizzi di posta elettronica o numeri di telefono, che di per sé non hanno nulla a che fare con il servizio considerato e che vengono ad esempio usati per resettare la password o inviare avvisi di sicurezza agli utenti.

Analogamente all'articolo 38, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e le relative modalità d'uso (cfr. il commento all'art. 38 cpv. 2).

Art. 41 Tipo di informazione IR_9_COM: informazioni su utenti di altri servizi di telecomunicazione o servizi di comunicazione derivati

La disposizione definisce il tipo d'informazione standardizzato sugli utenti di altri servizi di telecomunicazione o di comunicazione derivati. Anch'esso corrisponde in linea di massima alle attuali informazioni A0 e (in parte) A1, ma è ora introdotto

per questa categoria di servizi. Scopo della disposizione è di riunire tutti i servizi di telecomunicazione o di comunicazione derivati che sono già in esercizio, ma i cui standard ETSI sono ancora in elaborazione, nonché tutti i possibili servizi che saranno sviluppati in futuro. Si tratta, ad esempio, dei servizi di comunicazione nelle reti sociali e dei servizi cloud e proxy. I servizi cloud sono servizi di comunicazione derivati, quali i servizi per il salvataggio di dati e le applicazioni, che sono disponibili online e, a seconda delle risorse richieste, ospitati in centri di calcolo. Un servizio proxy è un'interfaccia di comunicazione all'interno di una rete. È usato per svolgere un servizio di intermediazione, in cui le richieste ricevute sono trasmesse tramite l'indirizzo del proxy stesso al punto terminale con cui crea un collegamento. I servizi proxy sono pertanto di rilievo ai fini dell'identificazione degli utenti in caso di reati.

Fanno parte di questa categoria anche i servizi di messaggeria. Si tratta di servizi per la trasmissione di comunicazioni o messaggi, indipendenti dai servizi di telefonia e multimedia e principalmente asincroni, quali la messaggistica istantanea, IMS messaging, le applicazioni per messaggistica e SMS di fornitori terzi (ovvero servizi SMS non forniti dal FST dell'utente). I servizi di messaggistica possono includere anche altre funzioni supplementari come la comunicazione multimediale, la trasmissione di dati e le informazioni di presenza (p. es. l'utente può visualizzare lo stato attuale ed eventualmente l'ubicazione di altri utenti).

Data l'analogia nella struttura delle disposizioni del presente articolo, si rimanda ai commenti agli articoli 38-40.

Anche in questo caso, il *capoverso 1* stabilisce quali informazioni devono essere fornite sugli utenti di servizi di telecomunicazione o servizi di comunicazione derivati.

Analogamente agli articoli 38-40, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e come vanno usati (cfr. commento all'art. 38 cpv. 2).

Sezione 6: Altri tipi di informazione

Art. 42 Tipo di informazione IR_10_PAY: informazioni sulle modalità di pagamento degli utenti di servizi di telecomunicazione e servizi di comunicazione derivati

La disposizione definisce il tipo d'informazione standardizzato sulle modalità di pagamento degli utenti di servizi di telecomunicazione e servizi di comunicazione derivati. Dal momento che non vi sono differenze significative tra le diverse modalità di pagamento, questo tipo di informazione – basato sul parametro ETSI PaymentDetails – include tutte le categorie di servizi.

Per quella che finora è l'informazione A1 (dati tecnici) sui codici di ricarica per i servizi prepagati, non esiste ancora un parametro ETSI adatto. Il tipo di informazione IR_10_PAY si applica, invece, sia ai servizi prepagati che agli abbonamenti e include nella ricerca tutte le modalità di pagamento di servizi di telecomunicazione e servizi di comunicazione derivati.

Il *capoverso 1* definisce i dati da trasmettere.

Secondo il *capoverso 2* le indicazioni di cui al capoverso 1 vanno fornite nella misura in cui il fornitore ne dispone. In caso di servizi gratuiti quali quelli di posta elettronica non sono disponibili informazioni sulle modalità di pagamento.

Il *capoverso 3* stabilisce i criteri di ricerca per il tipo di informazione e come vanno usati.

Art. 43 Tipo di informazione IR_11_ID: copia del documento di identità

L'articolo 19 definisce quali dati identificativi dell'utente devono essere registrati all'atto di vendita di carte prepagate o abbonamenti e di concessione di offerte gratuite. Per garantire la correttezza dei dati registrati e prevenire falsificazioni, le persone obbligate a collaborare devono conservare una copia del documento d'identità dell'utente. Le modalità di conservazione non sono precisate, si richiede semplicemente che la copia sia ben leggibile e che le persone obbligate a collaborare siano in grado di fornirla su richiesta. L'autorità che dispone la sorveglianza deve precisare nella domanda di informazioni il periodo e l'identificativo univoco dell'utente o del servizio a cui si riferisce la richiesta (*cpv. 2*). La copia del documento d'identità deve essere fornita per via elettronica.

Art. 44 Tipo di informazione IR_12_BILL: copia della fattura

Questo tipo d'informazione corrisponde all'attuale informazione A2 (dati di fatturazione; cfr. in particolare art. 21 cpv. 1 lett. d nLSCPT). Le persone obbligate a collaborare devono fornire copie elettroniche di tutta la documentazione di fatturazione disponibile in riferimento all'utente. È importante però che escludano i metadati. Sulle copie delle fatture non devono ad esempio apparire collegamenti; è sufficiente la pagina di riepilogo della fattura mensile con importo, numero cliente e indirizzo di fatturazione. L'autorità richiedente deve precisare nella domanda di informazioni il periodo e l'identificativo univoco dell'utente o del servizio a cui si riferisce la richiesta (*cpv. 2*).

Art. 45 Tipo di informazione IR_13_CONTRACT: copia del contratto

Questo tipo d'informazione corrisponde all'attuale informazione A2 (copia del contratto; cfr. in particolare art. 21 cpv. 1 lett. d nLSCPT). Nel caso di una richiesta di informazioni devono essere fornite le copie elettroniche di tutta la documentazione contrattuale disponibile o della documentazione equivalente. Poiché i contratti possono essere conclusi sia in forma scritta che orale, è possibile che non esista un contratto scritto. Con la disposizione non viene introdotto alcun obbligo della forma scritta per le persone obbligate a collaborare: se non è disponibile un contratto scritto, basterà ad esempio fornire solo uno screen shot del proprio sistema contente informazioni sulla relazione contrattuale. L'autorità che dispone la sorveglianza deve precisare nella domanda di informazioni il periodo e l'identificativo univoco dell'utente o del servizio a cui si riferisce la richiesta (*cpv. 2*).

Art. 46 Tipo di informazione IR_14_TECH: dati tecnici

La disposizione stabilisce che le persone obbligate a collaborare devono fornire informazioni sui dati tecnici dei sistemi di telecomunicazione e degli elementi di

rete (cfr. in particolare art. 21 cpv. 1 lett. d nLSCPT). Questo tipo d'informazione corrisponde all'attuale informazione A3.

Il *capoverso 1* riporta a titolo esemplificativo alcuni tipi di dati tecnici. Rientrano tra i dati tecnici dei sistemi di telecomunicazione e degli elementi di rete anche quelli relativi alle antenne radio o ai punti di accesso WLAN mobili, ad esempio aerei (compagnia aerea, codice del velivolo), treni (impresa ferroviaria e numero del treno), autobus (impresa di autobus e numero del veicolo) o a bordo di navi da crociera (società armatrice e nome della nave).

Il *capoverso 2* disciplina nel dettaglio i dati da fornire sull'ubicazione delle celle radio e dei punti di accesso WLAN; quelli indicati alle *lettere b e c* vanno trasmessi solo se disponibili.

Il *capoverso 3* stabilisce i criteri di ricerca per il tipo di informazione. La domanda di informazioni ne deve contenere almeno uno e l'autorità che dispone la sorveglianza deve precisare il periodo a cui si riferisce la richiesta e le informazioni di cui al capoverso 1 desiderate. In caso di domande per mezzo delle coordinate geografiche (*lett. a*), queste ultime vanno indicate con sufficiente precisione e riferite a un'unica ubicazione di elementi di rete. Il fornitore deve fornire le indicazioni desiderate per tutti gli elementi di rete che si trovano all'ubicazione designata. Non deve tuttavia svolgere una ricerca per zona di copertura per le coordinate geografiche indicate nella domanda. La ricerca per zona di copertura rientra nel tipo di sorveglianza AS_27_PREP_COV (art. 64).

Sezione 7: Disposizioni generali per la sorveglianza del traffico delle telecomunicazioni

Art. 47 Ordine di sorveglianza del traffico delle telecomunicazioni

La disposizione corrisponde essenzialmente all'articolo 15 dell'OSCPT del 31 ottobre 2001[42] e disciplina il contenuto dell'ordine di sorveglianza nel caso di una sorveglianza del traffico delle telecomunicazioni (per la corrispondenza postale cfr. il commento all'art. 15). Fatti salvi i diritti di accesso, non è possibile modificare un ordine di sorveglianza già quietanzato/confermato; modifiche sostanziali dell'ordine di sorveglianza (p. es. tipo o oggetto della sorveglianza) richiedono un nuovo ordine, soggetto agli emolumenti e alle indennità usuali.

Il *capoverso 1* elenca in modo esaustivo i dati che l'ordine di sorveglianza deve contenere.

Lettera a: il Servizio SCPT verifica dal punto di vista formale se l'autorità è autorizzata a ordinare la sorveglianza.

Lettera b: sulla base dei dati di cui alla lettera b dati, il Servizio SCPT assegna alle persone indicate i diritti di accesso ai dati della sorveglianza nel sistema di trattamento.

Lettera c: i dati di cui alla lettera c servono a verificare presso i FST o i fornitori di servizi di comunicazione derivati se vi è un collegamento tra l'applicazione o l'accesso Internet da sorvegliare e l'utente indicato.

42 RS **780.11**

Lettera d: il numero di riferimento e la denominazione della sorveglianza sono necessari per una corretta registrazione nel sistema di trattamento.

Lettera e: il Servizio SCPT verifica dal punto di vista formale se per il tipo di reato è possibile ordinare una sorveglianza ai sensi degli articoli 269 oppure 273 CPP.

Lettera f: l'autorità che dispone la sorveglianza comunica al Servizio SCPT i nomi delle persone obbligate a collaborare che devono eseguire la sorveglianza.

Lettera g: indicazione dei tipi di sorveglianza ordinati. Possono essere ordinati tipi di sorveglianza standardizzati o meno. In caso di dubbi, contraddizioni o emolumenti prevedibilmente elevati, il Servizio SCPT contatta l'autorità che ha disposto la sorveglianza.

Lettera h: l'autorità che ha disposto la sorveglianza comunica al Servizio SCPT gli elementi d'indirizzo da sorvegliare. In caso di dubbi, il Servizio SCPT contatta l'autorità che ha disposto la sorveglianza.

Lettera i: se la persona da sorvegliare cambia in rapida successione il collegamento di telecomunicazione, il giudice dei provvedimenti coercitivi può autorizzare, ai sensi dell'articolo 272 capoverso 2 CPP mediante un'autorizzazione di massima, la sorveglianza di tutti i collegamenti identificati utilizzati da tale persona, senza nuova approvazione per ogni singolo caso. La domanda concernente l'autorizzazione di massima va allegata all'ordine di sorveglianza.

Lettera j: l'autorità disponente deve indicare il periodo durante il quale va eseguita la sorveglianza, tenendo conto dei termini legali. Infatti, le sorveglianza in tempo reale possono essere ordinate per al massimo tre mesi e quelle retroattive per al massimo sei mesi.

Per le *lettere k e l* si veda il commento all'articolo 5. Va indicato se la sorveglianza interessa persone, ad esempio avvocati o medici, tenute al segreto d'ufficio o professionale secondo l'articolo 271 CPP o secondo l'articolo 70*b* PPM. In questo caso il Servizio SCPT deve provvedere a una cernita dei dati registrati nel corso della sorveglianza.

Il *capoverso 2* si riferisce a sorveglianze che richiedono indicazioni tecniche supplementari, ad esempio perché il tipo di sorveglianza non è standardizato o la trasmissione dei dati relativi alla sorveglianza non avviene mediante il sistema di trattamento del Servizio SCPT.

Art. 48 Obblighi di sorveglianza

Il *capoverso 1* definisce la cerchia delle persone obbligate a collaborare che possono essere incaricate dello svolgimento di una sorveglianza in tempo reale del traffico delle telecomunicazioni. Ai fornitori di servizi di telecomunicazione, si aggiungono ora i fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari ai sensi dell'articolo 50. La disposizione esclude invece esplicitamente i FST con obblighi di sorveglianza ridotti. I fornitori incaricati devono essere in grado di eseguire o far eseguire da terzi i tipi di sorveglianza previsti alle sezioni 8–12 del capitolo 3 (cfr. art. 32 nLSCPT).

Secondo il *capoverso 2*, la disponibilità alla sorveglianza va garantita a partire dall'inizio dell'esercizio commerciale di un servizio. Ciò significa che la procedura per la verifica della disponibilità a informare e sorvegliare va portata a termine prima della messa in esercizio (cfr. commento agli art. 29-32).

Il *capoverso 3* stabilisce che i fornitori devono garntire di essere in grado di ricevere ed eseguire entro i termini previsti gli incarichi di sorveglianza anche al di fuori degli orari di servizio ordinari di cui all'articolo 10. La definizione dei termini per l'esecuzione degli ordini di sorveglianza è delegata al DFGP, che li disciplina nell'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT).

Il *capoverso 4* disciplina il periodo di riferimento e gli elementi del traffico delle telecomunicazioni da sorvegliare. Il Servizio SCPT comunica alle persone obbligate a collaborare il periodo da sorvegliare stabilito dall'autorità che dispone la sorveglianza. A tal fine, nel caso della sorveglianza in tempo reale, invia loro un mandato di attivazione all'inizio della sorveglianza e uno di disattivazione al termine della stessa, mentre per la sorveglianza retroattiva invia soltanto un mandato di attivazione in cui è indicato il periodo di riferimento. Nel caso della sorveglianza in tempo reale, la persona obbligata a collaborare non sa quanto durerà l'incarico di sorveglianza, poiché la sua conclusione è comunicata soltanto con il mandato di disattivazione.

In linea di massima, la persona obbligata a collaborare deve garantire che possa essere sorvegliato l'intero traffico delle telecomunicazioni da essa controllato; deve però trasmettere soltanto il traffico delle telecomunicazioni proveniente da o destinato all'accesso alla rete sorvegliato e quello relativo all'applicazione sorvegliata o all'identificativo di destinazione sorvegliato (p. es. le chiamate da/a un numero di telefono di un servizio telefonico). Con «infrastruttura da essi controllata» si intende l'infrastruttura che la persona obbligata a collaborare possiede, affitta, amministra, esternalizza (outsorcing) o usa per contratto in un tipo particolare di diritto d'uso (p. es. MVNO). Quando viene usata un'infrastruttura straniera (p. es. roaming all'estero), la persona obbligata a collaborare deve sorvegliare il traffico delle telecomunicazioni soltanto nella misura in cui è in grado di controllarlo nell'ambito della gestione tecnica ordinaria. Nel caso venga usata un'infrastruttura nazionale di terzi, ad esempio nel caso di roaming nazionale, Mobile Virtual Network Operator (MVNO), la persona obbligata a collaborare deve garantire di poter eseguire o far eseguire da terzi la sorveglianza di tutto il traffico delle telecomunicazioni.

Una persona obbligata a collaborare deve quindi essere anche in grado di sorvegliare il traffico delle telecomunicazioni riguardante elementi d'indirizzo che non ha assegnato, che non si trovano nella sua rete o che non usano la sua rete (p. es. la sorveglianza di un numero di telefono straniero; cfr. art. 69).

Per quanto riguarda il roaming, vanno distinti outbound e inbound roaming.

1. Outbound roaming: la sorveglianza di un utente del fornitore incaricato che con la sua apparecchiatura terminale usa come ospite una rete terza. In questo caso sono possibili due scenari:

A) rete terza su territorio nazionale

B) rete terza all'estero

La differenza tra i due consiste nel fatto che nello scenario A il fornitore incaricato della sorveglianza deve sorvegliare o far sorvegliare da terzi l'intero traffico delle telecomunicazioni dei suoi utenti anche quando usano la rete terza, mentre nello scenario B deve semplicemente fare in modo che siano sorvegliati i metadati e i

contenuti che controlla nell'ambito della procedura operativa ordinaria (routing, segnalazione, cfr. anche art. 52 cpv. 1 lett. h) e ai quali può pertanto accedere.

2. Inbound roaming: la sorveglianza di un utente di un altro fornitore, che con la sua apparecchiatura terminale usa come ospite la rete della persona obbligata a collaborare. La sorveglianza in questo caso è possibile poiché l'utente si trova nella rete della persona obbligata a collaborare. Per motivi tecnici particolari può darsi, tuttavia, che non sia possibile trasmettere i contenuti della comunicazione in chiaro, ciò avviene ad esempio quando i dati sono protetti da cifratura durante la trasmissione tra l'utente terzo e la sua rete natia e la relativa chiave non è stata definita dalla persona obbligata a collaborare, che non può quindi rimuoverla. Un fornitore estero di reti mobili, ad esempio, che non è considerato una persona obbligata a cooperare ai sensi dell'articolo 2 nLSCPT e i cui clienti sono registrati in una rete svizzera soltanto come inbound-roamer, non sottostà invece ad obblighi secondo la LSCPT.

I dati della sorveglianza trasmessi devono corrispondere al traffico delle telecomunicazioni indicato nel mandato di sorveglianza. La persona obbligata a collaborare deve fornire assistenza al Servizio SCPT (cfr. cpv. 5).

Secondo il *capoverso 6*, se all'identificativo di destinazione sono associati altri identificativi, i fornitori devono garantire che anche questi siano sorvegliati nell'ambito del tipo di sorveglianza.

Infine il *capoverso 7* stabilisce che se al momento dell'attivazione di una sorveglianza in tempo reale l'oggetto della sorveglianza ha già iniziato una comunicazione, i relativi dati vanno trasmessi senza indugio

Art. 49 FST con obblighi di sorveglianza ridotti

In linea di massima, i FST devono essere in grado di eseguire o far eseguire da terzi i tipi di sorveglianza riguardanti i servizi da loro offerti (art. 32 nLSCPT) e devono pertanto disporre delle attrezzature necessarie per la sorveglianza del traffico delle telecomunicazioni. Non tutti i FST sono in grado di sostenere i costi di investimento richiesti per l'acquisto di tali attrezzature, in particolare tali costi creano difficoltà ai fornitori di piccole e medie dimensioni. Nell'articolo 26 capoverso 6 nLSCPT, il Legislatore ha pertanto attribuito al Consiglio federale la competenza di dispensare da alcuni obblighi legali i FST che offrono servizi di scarsa importanza economica o nel settore dell'istruzione. La deroga non si applica però all'obbligo legale minimo di tollerare una sorveglianza, sopprimere i criptaggi, garantire l'accesso ai propri impianti e trasmettere i metadati delle telecomunicazioni della persona sorvegliata (art. 26 cpv. 2 nLSCPT).

Il *capoverso 1* specifica le condizioni in base alle quali un FST deve rispettare soltanto l'obbligo legale minimo e ha quindi obblighi di sorveglianza ridotti. Ciò è il caso se offre i propri servizi di telecomunicazione soltanto nel settore dell'istruzione oppure se non raggiunge entrambi i seguenti valori: 10 incarichi di sorveglianza negli ultimi 12 mesi (data di riferimento: 30 giugno) o un fatturato annuo di meno di 100 milioni di franchi per due esercizi consecutivi. Il secondo criterio è ulteriormente circoscritto in quanto entra in linea di consto soltanto il fatturato realizzato con i servizi di telecomunicazione e i servizi di comunicazione derivati. I FST che offrono i propri servizi esclusivamente nel settore

dell'istruzione sottostanno soltanto all'obbligo legale minimo per il fatto stesso che operano solo in tale settore. Si presume che con l'applicazione di queste soglie il numero di FST tenuti alla sorveglianza attiva si ridurrà da circa 450 a circa 20-50. Nella prassi queste modifiche non porteranno comunque a lacune nella sorveglianza del traffico delle telecomunicazioni. Le sorveglianze possono infatti essere eseguite anche presso i FST con obblighi ridotti, poiché questi hanno l'obbligo di tollerare la sorveglianza e di collaborare. Il Servizio SCPT potrà quindi intraprendere i passi necessari per eseguire la sorveglianza (art. 17 lett. e nLSCPT).

Come all'articolo 21, il *capoverso 2* descrive il caso dei gruppi di imprese, in cui un fornitore controlla una o più imprese soggette all'obbligo di presentare i conti. Anche in questo caso il fornitore e le imprese controllate sono considerate un'unità, così da evitare i casi di abuso (per ulteriori spiegazioni si veda il commento all'art. 21).

I FST i cui obblighi di sorveglianza cambiano a causa del raggiungimento o non raggiungimento dei valori di cui al capoverso 1 o che non operano più soltanto nel settore dell'istruzione ne informano per scritto il Servizio SCPT entro tre mesi dalla chiusura dell'esercizio annuale e consegnano i giustificativi corrispondenti (*cpv. 3*).

Se dopo aver esaminato la documentazione, il Servizio SCPT giunge alla conclusione che il FST soddisfa le condizioni di cui al capoverso 1, lo comunica al FST interessato. A partire da quel momento decade l'obbligo della disponibilità a sorvegliare (cfr. *cpv. 4*).

Analogamente a quanto previsto dall'articolo 21 capoverso 4, il FST deve garantire la memorizzazione dei dati necessari per la sorveglianza e la disponibilità a sorvegliare rispettivamente entro 2 ed entro 12 mesi dal momento in cui il Servizio SCPT gli conferma di non essere più considerato un FST con obblighi di sorveglianza ridotti (*cpv. 5*).

Il Servizio SCPT adotta le decisioni necessarie (*cpv. 6*).

Art. 50 Fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari

Analogamente a quanto previsto per gli obblighi di notifica di cui all'articolo 22 nLSCPT, il Legislatore ha attribuito al Consiglio federale la competenza di imporre ai fornitori di servizi di comunicazione derivati obblighi di sorveglianza supplementari. Il presente articolo attua tale competenza.

La disposizione ha una struttura analoga all'articolo 21, in cui sono disciplinate le condizioni che prevedono obblighi di informazione supplementari per i fornitori di servizi di comunicazione derivati. L'unica differenza consiste nella condizione alternativa dei dieci incarichi di sorveglianza di cui alla lettera a. Data l'analogia tra le due disposizioni si rimanda al commento all'articolo 21.

Gli obblighi da osservare sono quelli previsti per i FST, ossia in particolare gli obblighi previsti dall'articolo 26 capoversi 1 e 3−5 nLSCPT: essere in grado di eseguire o far eseguire da terzi i tipi di sorveglianza standardizzati previsti alle sezioni 7−12 del capitolo 3 e conservare per sei mesi i metadati delle telecomunicazioni. Le disposizioni della nLSCPT che riguardano i fornitori di servizi di telecomunicazione si applicano per analogia ai fornitori di servizi di

comunicazione derivati con obblighi di sorveglianza supplementari (art. 27 cpv. 3 nLSCPT).

Art. 51 Accesso agli impianti

Il Servizio SCPT svolge o fa svolgere a terzi (art. 26 cpv. 2 e 6 nonché art. 34 nLSCPT) i mandati che, in virtù delle disposizioni legali o per mancanza di disponibilità a sorvegliare, non devono (p. es. i FST con obblighi di sorveglianza ridotti ai sensi dell'art. 49) o non sono in grado di eseguire attivamente le persone obbligate a collaborare. Per poterli eseguire, il Servizio SCPT o i terzi incaricati devono poter accedere agli impianti delle persone obbligate a collaborare.

Secondo il *capoverso 1*, garantire l'accesso agli impianti significa in particolare rendere possibile l'accesso a edifici, infrastrutture, apparecchi, linee, sistemi, reti e servizi. Le persone obbligate a collaborare devono mettere gratuitamente a disposizione del Servizio SCPT o dei suoi incaricati anche i loro accessi alle reti di telecomunicazione pubbliche (p. es. il collegamento Internet; *cpv. 2*). Se la persona obbligata a collaborare non dispone degli accessi alle reti di telecomunicazione pubbliche necessari allo svolgimento della sorveglianza, deve crearli nella misura in cui ciò sia ragionevolmente esigibile.

Sezione 8: Tipi di sorveglianza in tempo reale per i servizi di accesso alla rete

Art. 52 Tipo di sorveglianza RT_15_NA_IRI: sorveglianza in tempo reale dei metadati per i servizi di accesso alla rete

La disposizione definisce il tipo di sorveglianza in tempo reale standardizzato di un servizio di accesso alla rete (corrisponde all'attuale tipo di sorveglianza PS 2). Contrariamente all'articolo 53, il presente tipo di sorveglianza prevede soltanto la trasmissione dei metadati del traffico delle telecomunicazioni; è impiegato soprattutto nel caso degli accessi a Internet da rete mobile al fine di ottenere informazioni in tempo reale relative all'ubicazione dell'utente.

Questo tipo di sorveglianza non raccoglie in genere i metadati delle applicazioni; se ad esempio viene usato un servizio VoIP mediante l'accesso alla rete sorvegliato, i metadati dell'applicazione in questione non sono trasmessi. Per la trasmissione dei dati delle applicazioni è infatti previsto un apposito tipo di sorveglianza. Nel caso di messaggi MMS, ad esempio, nell'ambito del presente tipo di sorveglianza non vengono trasmessi i metadati specifici dell'MMS (che è un'applicazione), ma soltanto i metadati dell'accesso alla rete. I metadati e il contenuto specifici dei messaggi MMS possono tuttavia essere richiesti tramite il tipo di sorveglianza RT_16_NA_CC_IRI di cui all'articolo 53.

Il *capoverso 1* definisce i metadati del traffico delle telecomunicazioni, inviato o ricevuto tramite il servizio di accesso alla rete sorvegliato, che vanno trasmessi in tempo reale. Tra gli elementi di indirizzo menzionati alla *lettera e* rientra il numero di telefono assegnato a un collegamento DSL. Con «modifiche tecniche» (*lett. g*) si intendono gli eventi che modificano le caratteristiche tecniche dell'accesso alla rete sorvegliato o che influiscono sulla gestione della mobilità (p. es. *bearer modification* o *location update*). «Gestione tecnica ordinaria» (*lett. h*) indica invece che la gestione tecnica (p. es. segnalazione, roaming) per l'utente sotto

sorveglianza (target) non si differenzia in linea di massima da quella prevista per un utente non sorvegliato.

Il *capoverso 2* specifica i dati da includere nell'indicazione dell'ubicazione di cui al capoverso 1 lettera h. La persona obbligata a collaborare può in questo caso scegliere tra tre alternative, ma può trasmettere soltanto indicazioni verificate, cioè determinate dalla rete, dal momento che i dati sull'ubicazione che vengono da un'apparecchiatura terminale o da un'applicazione possono essere falsificati.

Conformemente alla *lettera a*, la persona obbligata a collaborare deve, tra le altre cose, comunicare la direzione di trasmissione della cella, ma soltanto nella misura in cui disponibile e corretta. Nel caso di antenne con più settori non può per esempio essere calcolato un valore medio della direzione di trasmissione, ma vanno comunicate le direzioni di trasmissione di ogni settore. Nel caso di una cella semplice, la direzione di trasmissione dell'antenna della cella indica l'angolo in gradi [°] tra il nord geografico e la trasmissione principale, invece per le celle complesse questo campo può contenere molteplici direzioni di trasmissione, mentre per le celle onnidirezionali (trasmissione equivalente in tutte le direzioni) questo campo resta vuoto.

La *lettera c* costituisce un'alternativa alle *lettere a* e *b*. La disposizione rimanda semplicemente agli standard internazionali vigenti o futuri che riguardano la comunicazione dell'ubicazione. Lo scopo è di evitare che l'ordinanza vada adeguata in casi di modifica degli standard internazionali o di introduzione di nuovi standard internazionali.

Art. 53 Tipo di sorveglianza RT_16_NA_CC_IRI: sorveglianza in tempo reale dei contenuti e dei metadati per i servizi di accesso alla rete

Il tipo di sorveglianza definito nell'*articolo 53* corrisponde all'attuale tipo PS 1. Nell'ambito di questo tipo di sorveglianza, la persona obbligata a collaborare deve intercettare in tempo reale l'intero traffico delle telecomunicazioni trasmesso (upload) o ricevuto (download) attraverso l'accesso alla rete sorvegliato, vale a dire sia i contenuti (communication content) sia i relativi metadati (IRI) elencati all'articolo 52.

Come spiegato nel commento all'articolo 48 capoverso 4, la persona obbligata a collaborare deve in linea di massima garantire che si possa sorvegliare l'intero traffico delle comunicazioni che si svolge attraverso l'infrastruttura da essa controllata. Deve tuttavia essere intercettato solo il traffico delle comunicazioni diretto al o proveniente dall'accesso alla rete sorvegliato. Nel caso venga usata un'infrastruttura nazionale di terzi, ad esempio nel caso di roaming nazionale, Mobile Virtual Network Operator (MVNO), la persona obbligata a collaborare deve garantire di poter eseguire o far eseguire da terzi l'intercettazione di tutto il traffico delle telecomunicazioni.

Quando viene usata un'infrastruttura straniera (p. es. roaming all'estero), la persona obbligata a collaborare deve sorvegliare il traffico delle telecomunicazioni soltanto nella misura in cui è in grado di controllarlo. Se tuttavia controlla l'infrastruttura straniera, la persona obbligata a collaborare deve trasmettere tutti i contenuti e i metadati della comunicazione sorvegliata.

Una particolarità è costituita dai servizi MMS associati a un servizio di telefonia mobile, poiché i dati sul contenuto di MMS non sono sorvegliati in quanto

applicazione (cfr. sezione 9), bensì nell'ambito del tipo di sorveglianza definito nel presente articolo. Secondo gli standard ETSI, i dati sul contenuto di comunicazioni MMS ricevute e inviate sono intercettati come parte del flusso di dati nell'ambito della sorveglianza dell'accesso. In altre parole, la sorveglianza degli MMS è automaticamente inclusa nella sorveglianza dell'accesso alla rete. Tuttavia nella sorveglianza in tempo reale dell'accesso alla rete, per le comunicazioni MMS non vengono trasmessi i relativi metadati.

A seconda del tipo di accesso alla rete (fisso o mobile) e della tecnologia, a questo tipo di sorveglianza si applicano i seguenti standard:

- accesso mobile alla rete (GPRS, UMTS, EPS (LTE), WLAN-Interworking): ETSI TS 101 671, TS 133 108, TS 102 232-1, TS 102 232-7,
- accesso fisso alla rete: ETSI TS 102 232-1, TS 102 232-3, TS 102 232-7.

Sezione 9: Tipi di sorveglianza in tempo reale per le applicazioni

Art. 54 Tipo di sorveglianza RT_17_TEL_IRI: sorveglianza in tempo reale dei metadati per i servizi di telefonia e multimedia

La disposizione definisce il tipo di sorveglianza in tempo reale standardizzato per i servizi di telefonia e multimedia (corrisponde ai tipi di sorveglianza attuali CS 2 e CS 3). Si può pertanto rinviare al commento all'articolo 55. Tuttavia, al contrario di quanto previsto dall'articolo 55, nell'ambito di un incarico di sorveglianza secondo l'articolo 54 vanno trasmessi in tempo reale soltanto i metadati del traffico delle comunicazioni, di cui fanno parte anche le indicazioni sull'ubicazione. L'unica eccezione è costituita dai contenuti degli SMS, che per ragioni tecniche possono essere compresi nei metadati in tempo reale e perciò sono trasmessi insieme a questi ultimi.

Il *capoverso 1* definisce i metadati che devono essere trasmessi in tempo reale. Le informazioni di cui alla lettera b sugli eventi di registrazione e le relative risposte si riferiscono ad esempio al metodo di richiesta SIP «REGISTER» (cfr. RFC 3261). Analogamente per evento di sottoscrizione s'intende ad esempio il metodo di richiesta SIP «SUBSCRIBE» (cfr. RFC 6665). Per «modifiche tecniche» di cui alla *lettera e* s'intendono gli eventi che modificano le caratteristiche tecniche dell'accesso alla rete sorvegliato o che influiscono sulla gestione della mobilità (p. es. *bearer modification* o *location update*). In caso di servizi mobili va trasmessa l'indicazione dell'ubicazione momentanea, specificata al capoverso 2, reperibile nel quadro della gestione tecnica ordinaria (lett. e n. 9). Per le spiegazioni relative all'indicazione dell'ubicazione si veda il commento all'articolo 52 capoverso 2.

Il fornitore del servizio di telefonia deve fornire i metadati anche per i collegamenti in uscita o i relativi tentativi effettuati per mezzo della libera scelta del fornitore (carrier selection).

Art. 55 Tipo di sorveglianza RT_18_TEL_CC_IRI: sorveglianza in tempo reale di contenuti e metadati per i servizi di telefonia e multimedia

Il tipo di sorveglianza definito nel presente articolo si basa sui tipi attuali CS 1, CS 2 e CS 3. La sorveglianza dei servizi di telefonia tradizionali a commutazione di circuito è tuttavia estesa ai servizi di telefonia e multimedia a commutazione di pacchetto. Dei servizi di telefonia e multimedia fanno parte anche i servizi convergenti, in particolare SMS, Voice Mail e RCS (per i termini e le abbreviazioni si veda l'allegato 1). Per *servizi convergenti* s'intendono tutte le applicazioni che la persona obbligata a collaborare fornisce all'utente in concomitanza con il o come parte del servizio di telefonia o multimedia, ad esempio il servizio di telefonia mobile con SMS, VoiceMail e RCS o il servizio di telefonia fissa con la telefonia mobile. I cosiddetti prodotti multiple-play, in cui vari servizi quali telefonia, accesso a Internet e TV sono offerti in un pacchetto, non sono tuttavia considerati servizi convergenti.

Un esempio noto di servizi di telefonia a commutazione di pacchetto è Voice over IP (VoIP), detta anche telefonia via Internet. Nell'ambito della telefonia mobile vanno menzionati soprattutto VoLTE (Voice over LTE, ossia telefonia mobile in reti 4G) e VoWLAN (telefonia mobile via Wireless LAN, cosiddetto non-3GPP access) e in quello dei servizi multimedia ViLTE (Video over LTE, ossia telefonia video in reti 4G).

I servizi di telefonia e multimedia sono di norma sorvegliati come applicazione e non all'accesso alla rete. Anche se nella telefonia mobile e nella telefonia a commutazione di circuito i fornitori dell'accesso (p. es. collegamento telefonico o accesso alla rete mobile) e dell'applicazione (servizio di telefonia) sono spesso identici, ciò non è più necessariamente così nel caso di servizi moderni quali VoIP. Anche nelle reti di telefonia tradizionali vi è una progressiva separazione dei collegamenti ed è possibile scegliere liberamente il fornitore del servizio (carrier selection; art. 9 dell'ordinanza del 17 novembre 1997[43] della Commissione federale delle comunicazioni concernente la legge sulle telecomunicazioni). Nel settore delle reti mobili nel caso di un Mobile Virtual Network Operator (MVNO) e del roaming il fornitore dell'accesso alla rete (Radio Access Network) e il fornitore del servizio non sono identici. Nel caso dell'IP Multimedia Subsystem (IMS) si può accedere alla rete anche attraverso le reti di fornitori terzi che non sono reti mobili (cosiddetti non-3GPP Access). Si tratta soltanto di alcuni esempi in cui il fornitore dell'accesso alla rete non è identico al fornitore del servizio dell'utente.

Nell'ambito di questo tipo di sorveglianza, la persona obbligata a collaborare deve trasmettere in tempo reale l'intero traffico delle telecomunicazioni effettuato per mezzo del servizio di telefonia e multimedia e dei servizi convergenti, vale a dire sia i contenuti (communication content) sia i relativi metadati (IRI) elencati all'articolo 54.

Il fornitore del servizio di telefonia deve fornire i metadati anche per i collegamenti in uscita o i relativi tentativi effettuati per mezzo della libera scelta del fornitore (carrier selection).

43 RS **784.101.112**

Art. 56 Tipo di sorveglianza RT_19_EMAIL_IRI: sorveglianza in tempo reale dei metadati per servizi di posta elettronica

Analogamente all'articolo 57 la disposizione definisce il tipo standardizzato della sorveglianza in tempo reale dei servizi di posta elettronica e corrisponde all'attuale tipo PS 4. Si può pertanto rinviare al commento del suddetto articolo. Secondo il diritto vigente un fornitore di servizi di posta elettronica è tuttavia tenuto a sorvegliare le e-mail soltanto se è nel contempo il fornitore dell'accesso a Internet (art. 15 cpv. 4 LSCPT del 6 ott. 2000[44]). Le nuove disposizioni eliminano questa restrizione. Tecnicamente la sorveglianza e la trasmissione dei dati si svolgerà unicamente secondo gli standard ETSI TS 102 232-2. La soluzione precedente, specifica alla Svizzera, sarà supportata soltanto durante un periodo transitorio (cfr. art. 73).

A differenza dell'articolo 57, nell'ambito di un incarico di sorveglianza secondo l'articolo 56 vanno trasmessi in tempo reale soltanto i metadati dell'account di posta elettronica sorvegliato, di cui fanno parte anche le informazioni sull'indirizzo SMTP. Nell'ambito del presente tipo di sorveglianza non possono essere trasmessi dati sul contenuto e pertanto neppure l'intestazione (header) del messaggio di posta elettronica con l'oggetto (subject).

Vanno sorvegliate sia le operazione del server mail, quali l'invio, la ricezione, il salvataggio dei messaggi nella mailbox, sia l'accesso di mail clients al mail server, ossia operazioni quali il login o il logout dell'utente nella mailbox o i relativi tentativi (*lett. a*), lo scaricamento di un'e-mail dalla mailbox o la sua cancellazione. I parametri più importanti dei metadati sono elencati nelle lettere a-d. Ne fanno parte anche le informazioni AAA senza la parola chiave (*lett. b*). Gli eventi per cui va generato un IRI sono illustrati in modo sommario alla *lettera d*. I dettagli sono disciplinati nello standard ETSI TS 102 232-2 e nell'allegato 1 dell'OE-SCPT. Va osservato che vanno sorvegliate anche le e-mail interne, ossia le mailbox servite dal medesimo server, nonché gli indirizzi alias e le mailing list dell'account di posta elettronica (per i termini «indirizzo alias» e «mailing list» cfr. il commento all'art. 40).

Art. 57 Tipo di sorveglianza RT_20_EMAIL_CC_IRI: sorveglianza in tempo reale di contenuto e metadati per servizi di posta elettronica

Il tipo di sorveglianza definito nel presente articolo corrisponde al tipo attuale PS 3. Vanno trasmessi in tempo reale sia i dati sul contenuto sia i metadati dell'account di posta elettronica sorvegliato (cfr. il commento all'art. 56). Il fornitore deve sopprimere i propri criptaggi (art. 26 cpv. 2 lett. c nLSCPT).

Art. 58 Tipo di sorveglianza RT_21_COM_IRI: sorveglianza in tempo reale di metadati per altri servizi di telecomunicazione o servizi di comunicazione derivati

Il tipo di sorveglianza definito nel presente articolo corrisponde in linea di massima al tipo attuale PS 4 (sorveglianza in tempo reale dei metadati di un'applicazione). Sono contemplati soprattutto i cosiddetti servizi Over the top (OTT), la cui

44 Cfr. anche FF **1998** III 3319 3356 ad art. 13 cpv. 3

definizione non è tuttavia sufficientemente precisa per distinguere nettamente questa categoria di servizi da quelle degli altri tipi di sorveglianza.

Fanno ad esempio parte di questa categoria i servizi di comunicazione nella cloud, mediante proxy o nelle reti sociali. Va osservato che per questo tipo di sorveglianza non esistono attualmente standard internazionali specifici. Le misure di sorveglianza di questo tipo saranno pertanto attuate e fatturate dal Servizio SCPT come misure di sorveglianza speciali (cosiddetti casi speciali). Il Servizio SCPT osserverà lo sviluppo degli standard internazionali e, se dovesse essere definito uno standard per questo tipo di sorveglianza, adeguerà tempestivamente le ordinanze d'esecuzione della LSCPT.

A differenza del tipo di sorveglianza RT_22_COM_CC_IRI (art. 59), con questo tipo di sorveglianza il fornitore del servizio deve trasmettere in tempo reale soltanto i metadati del traffico delle telecomunicazioni, e non i dati sul contenuto (cfr. anche la fine del commento all'art. 59). Le *lettere a-e* elencano sommariamente i metadati da trasmettere.

Art. 59 Tipo di sorveglianza RT_22_COM_CC_IRI: sorveglianza in tempo reale di contenuti e metadati per altri servizi di telecomunicazione o servizi di comunicazione derivati

Questo tipo di sorveglianza si fonda in linea di principio sull'attuale tipo PS 3 (sorveglianza in tempo reale di un'applicazione). I dati sul contenuto e i metadati possono essere sorvegliati e intercettati temporaneamente all'accesso alla rete oppure analogamente ai servizi di telefonia e multimedia (cfr. il commento all'art. 58).

Sezione 10: Tipi di sorveglianza retroattiva

Nel linguaggio specialistico, i metadati raccolti ai fini della sorveglianza retroattiva (art. 26 cpv. 4 nLSCPT) e dell'identificazione degli autori di reati commessi via Internet (art. 22 nLSCPT) sono designati con il termine «dati conservati» (retained data). Nel linguaggio comune si usano anche i termini dati registrati e dati preventivamente memorizzati, poiché vengono memorizzati preventivamente i metadati di tutti gli utenti. La nLSCPT usa l'espressione *i metadati delle telecomunicazioni passate conservati* (art. 26 cpv. 4 nLSCPT). Dato che la sorveglianza delle telecomunicazioni passate è designata con il termine *sorveglianza retroattiva*, vi è, come alternativa, anche l'espressione *metadati delle telecomunicazioni passate.* Nei commenti al capitolo 3, dedicato esclusivamente alle telecomunicazioni, si usa piuttosto la forma breve *dati marginali conservati*.

In virtù delle competenze che l'articolo 31 nLSCPT conferisce al Consiglio federale, nella *sezione 10* sono definiti i metadati che vanno conservati e trasmessi ai fini della sorveglianza retroattiva.

I metadati da conservare ai fini dell'identificazione degli autori di reati commessi via Internet (art. 22 nLSCPT) sono invece definiti nelle sezioni 4 e 5 del capitolo 3.

I metadati delle telecomunicazioni passate conservati, ossia i metadati della sorveglianza retroattiva, non sono identici ai metadati intercettati in occasione di una sorveglianza in tempo reale (IRI). Una sorveglianza in tempo reale fornisce ad esempio anche metadati che non sono correlati a comunicazioni o tentativi di comunicazione (p. es. location update). D'altra parte ci sono anche applicazioni (p. es. MMS) per le quali sono standardizzati specifici *metadati conservati*, ma non specifici metadati della sorveglianza in tempo reale (IRI).

Secondo il commento all'articolo 26 capoverso 1 lettera b nLSCPT del messaggio concernente la LSCPT del 27 febbraio 2013[45], non devono essere conservati soltanto i metadati delle comunicazioni, dei login o degli accessi alla rete effettivamente riusciti, bensì anche quelli dei relativi tentativi.

Nei servizi di telefonia o multimedia è considerato un tentativo di comunicazione la situazione in cui un collegamento è stato instaurato con successo, ma il destinatario non ha risposto oppure è intervenuto il gestore della rete. A titolo esemplificativo si possono menzionare due esempi: 1) Chi chiama seleziona un numero valido, fa squillare brevemente l'apparecchio del destinatario e poi riattacca; 2) Chi chiama seleziona un numero valido e la segreteria telefonica gli risponde che l'utente chiamato non è al momento raggiungibile. Se, invece, nel secondo esempio chi chiama viene deviato su una VoiceMail si considera che la comunicazione è avvenuta. Per contro la selezione di un numero incompleto o inesistente non è considerata né una comunicazione né un tentativo di comunicazione.

Nel caso dei servizi di posta elettronica e di messaggeria non ci sono pertanto tentativi di comunicazione, poiché l'invio di un'e-mail o di un messaggio a un mailserver o a un messagging server è considerato avvenuto anche nel caso in cui la successiva trasmissione al destinatario non dovesse riuscire. Non vi sono pertanto tentativi di comunicazione neppure nel caso di altri servizi di telecomunicazione e servizi di comunicazione derivati.

Nel caso del login o dell'accesso alla rete, un tentativo è dato quando l'autenticazione dell'utente è avvenuta con successo ma il login o l'accesso alla rete non è riuscito per altri motivi, ad esempio la mancanza di un credito in denaro.

I metadati dei tentativi di collegamento devono essere tuttavia conservati dalle persone obbligate a collaborare soltanto conformemente all'articolo 48 capoverso 4. Se per esempio sono interrotti tentativi di chiamata da altre reti prima che il segnale raggiunga la rete della persona obbligata a collaborare (in questo caso il telefono chiamato non squilla), quest'ultima non è in grado di conservare i relativi metadati poiché non ne è in possesso.

Può anche darsi che le comunicazioni o i tentativi di comunicazione contengano elementi di indirizzo incompleti o che ne manchino alcuni. Ad esempio, in caso di chiamate dall'estero il numero della persona che chiama potrebbe essere incompleto o mancare del tutto. In occasione di una sorveglianza retroattiva di questo numero straniero (identificativo di destinazione) i relativi metadati non si potrebbero trovare, poiché nei metadati conservati l'identificativo di destinazione risulterebbe incompleto o mancherebbe del tutto.

I *dati marginali conservati* si basano sullo standard ETSI TS 102 657 per tutti i tipi di sorveglianza retroattiva (art. 60-66).

45 FF **2013** 2283 2336.

Art. 60 Tipo di sorveglianza HD_23_NA: sorveglianza retroattiva dei metadati per i servizi di accesso alla rete

Il tipo di sorveglianza definito nel presente articolo corrisponde all'attuale tipo PS 5 e serve alla sorveglianza retroattiva di un accesso a Internet. Vanno trasmessi i metadati del traffico delle comunicazioni inviate o ricevute tramite il servizio di accesso alla rete sorvegliato. I dati marginali vanno conservati anche nel caso di tentativi di accesso. Per la nozione di tentativo di accesso alla rete si veda il commento introduttivo alla sezione 10 (cfr. sopra).

Le *lettere a–g* elencano i dati che le persone obbligate a collaborare devono conservare e trasmettere. Si tratta dei dati seguenti: la data e l'ora d'inizio dell'accesso alla rete o del relativo tentativo e della fine della sessione (*lett. a*), il tipo di accesso alla rete (*lett. b*), i dati di autenticazione, autorizzazione e accounting utilizzati (*lett. c*), gli indirizzi IP o i settori di indirizzi assegnati dal fornitore del servizio di accesso alla rete e la data e l'ora dell'assegnazione (*lett. d*) nonché gli elementi d'indirizzo del servizio di accesso alla rete (*lett. e*), di cui fanno ad esempio parte il numero del collegamento telefonico di un accesso DSL o il MSISDN per le reti mobili. Fanno inoltre parte di questi dati gli identificativi dei terminali (*lett. f*) e, se disponibile, il volume di dati caricato e scaricato durante una sessione (*lett. g*). In caso di sevizi mobili, oltre ai dati di cui alle lettere a-g, vanno trasmessi i dati relativi all'ubicazione a inizio e, se del caso, a fine sessione disponibili nel quadro della gestione tecnica ordinaria. Il significato dell'espressione «gestione tecnica ordinaria» è illustrato nel commento all'articolo 52 capoverso 1 lettera h. Per la trasmissione dei dati relativi all'ubicazione di cui alla lettera h, la persona obbligata a collaborare ha a disposizione tre varianti. Può tuttavia trasmettere solo dati verificati, ossia dati definiti dalla rete. Non vengono accettati dati relativi all'ubicazione provenienti dall'apparecchiatura terminale o da un'applicazione, poiché tali dati possono essere falsificati.

Art. 61 Tipo di sorveglianza HD_24_TEL: sorveglianza retroattiva dei metadati per i servizi di telefonia e multimedia

Il tipo di sorveglianza definito nel presente articolo si basa sul tipo attuale CS 4 (sorveglianza retroattiva di un servizio di telefonia) ed è stato esteso ai servizi multimedia. Serve alla sorveglianza retroattiva dei servizi di telefonia e multimedia, ossia alla raccolta dei metadati di questi servizi. I termini *servizi di telefonia e multimedia* nonché *servizi convergenti* sono illustrati nel commento all'articolo 55.

Il fornitore del servizio di telefonia deve fornire anche i metadati dei collegamenti e dei tentativi di collegamento che sono stati effettuati per mezzo della libera scelta del fornitore (carrier selection) descritta nel commento all'articolo 55. Nella sorveglianza retroattiva la persona obbligata a collaborare deve essere in grado di riconoscere la coincidenza di numeri E.164, anche qualora siano a disposizione in formati diversi (nazionale, internazionale).

Contrariamente alla sorveglianza in tempo reale, in cui i servizi MMS sono anch'essi sorvegliati all'accesso alla rete, retroattivamente tali servizi sono sorvegliati come applicazione nell'ambito del tipo di sorveglianza qui definito e non nell'ambito di una sorveglianza a sé stante.

Le *lettere a–d* elencano i dati che le persone obbligate a collaborare devono conservare e trasmettere. Nel commento introduttivo alla sezione 10 (cfr. sopra) abbiamo illustrato cosa s'intende per *tentativo di comunicazione* (*lett. b*). Nel caso di VoIP fa parte degli indirizzi disponibili di cui alla *lettera b numero 5* anche l'indirizzo del proxy SIP. Analogamente a quanto previsto dall'articolo 60, nel caso di servizi mobili vanno trasmessi i dati relativi all'ubicazione a inizio e, se del caso, a fine sessione reperibili nel quadro della gestione tecnica ordinaria (*lett. d*). Il significato dell'espressione «gestione tecnica ordinaria» è illustrato nel commento all'articolo 52 capoverso 1 lettera h.

Per la trasmissione dei dati relativi all'ubicazione secondo la *lettera d numero 1* la persona obbligata a collaborare ha a disposizione tre varianti. Può tuttavia trasmettere solo dati verificati, ossia dati determinati dalla rete. Non vengono accettati dati relativi all'ubicazione provenienti dall'apparecchiatura terminale o da un'applicazione, poiché tali dati possono essere falsificati.

Per altri servizi mobili (*lett. d n. 2*), ad esempio servizi nomadi quali VoIP, vanno conservati e trasmessi i dati relativi all'ubicazione dell'accesso ai servizi sorvegliati. I servizi nomadi possono essere utilizzati praticamente a ogni accesso a Internet e non sono pertanto legati a un'ubicazione. Le indicazioni relative all'ubicazione dell'accesso al servizio devono essere conservate e trasmesse solo se disponibili.

Art. 62 Tipo di sorveglianza HD_25_EMAIL: sorveglianza retroattiva di metadati per servizi di posta elettronica

Il tipo di sorveglianza definito nel presente articolo corrisponde all'attuale tipo PS 6 (sorveglianza retroattiva di un servizio di messaggistica elettronica asincrona). Le *lettere a* e *b* elencano i dati che le persone obbligate a collaborare devono conservare e trasmettere. Sono prioritari l'invio e la ricezione di un messaggio nonché il login alla e il logout dalla mailbox. Il download di un messaggio include anche il download parziale. Le informazioni sugli altri eventi vanno conservate e trasmesse solo se disponibili. Questo disciplinamento flessibile tiene conto del fatto che molti fornitori di servizi di posta elettronica gestiscono da parecchio tempo sistemi di sostegno alla sorveglianza degli eventi prioritari. Per sorvegliare gli altri eventi questi sistemi dovrebbero essere adeguati, il che non sarebbe proporzionato allo scopo. Se tuttavia sono a disposizione sistemi nuovi devono essere conservati e trasmessi tutti i dati di cui alle lettere a e b.

Art. 63 Tipo di sorveglianza HD_26_COM: sorveglianza retroattiva di metadati per altri servizi di telecomunicazione o servizi di comunicazione derivati

Il tipo di sorveglianza definito nel presente articolo è nuovo. Il progresso tecnologico e l'uso molto diffuso rendono tuttavia necessario estendere la sorveglianza retroattiva a questi nuovi servizi. Poiché per essi non sono ancora stati pubblicati standard ETSI, devono essere trasmessi solo i dati esistenti. Il formato della trasmissione dei dati si basa su servizi di telecomunicazione o servizi di comunicazione derivati analoghi, già standardizzati. Sono tuttavia ipotizzabili anche altri formati, qualora le persone obbligate a collaborare abbiano già

implementato processi e sistemi a tal fine, ad esempio in seguito a istruzioni di altri Stati.

Art. 64 Tipo di sorveglianza AS_27_PREP_COV: analisi della copertura di rete in vista di una ricerca per zona di copertura dell'antenna

Il tipo di sorveglianza definito nel presente articolo corrisponde all'attuale tipo CS 5 (analisi della rete nel corso di una ricerca per zona di copertura dell'antenna). Per preparare una ricerca per zona di copertura della rete, l'autorità disponente può chiedere al Servizio SCPT un elenco delle celle radio o dei punti di accesso WLAN (WLAN access points) che probabilmente coprivano una posizione geografico in un determinato momento (*cpv. 1*). La posizione geografica va indicata tramite coordinate o per mezzo di un indirizzo postale (cfr. il commento all'art. 67 lett. a n. 1). Altre indicazioni quali ad esempio l'ora possono contribuire a un'indicazione più chiara della posizione geografica. Non è tuttavia obbligatorio fornire altre indicazioni.

Il *capoverso 2* elenca le informazioni che il FST deve trasmettere al Servizio SCPT.

Art. 65 Tipo di sorveglianza AS_28_PREP_REF: comunicazioni o accessi alla rete di riferimento in vista di una ricerca per zona di copertura dell'antenna

Il tipo di sorveglianza definito nel presente articolo corrisponde all'attuale tipo CS 7 (analisi della rete mediante comunicazioni di riferimento delle autorità di perseguimento penale in vista di una ricerca per zona di copertura dell'antenna).

Analogamente all'articolo 64, il presente articolo serve a preparare una ricerca per zona di copertura. L'autorità disponente fornisce al Servizio SCPT un elenco di comunicazioni o accessi di riferimento al fine di determinare le celle radio o i punti di accesso WLAN (WLAN access points).

Il *capoverso 2* stabilisce le indicazioni che l'autorità disponente deve fornire al Servizio SCPT affinché l'ordine possa essere eseguito. I FST hanno bisogno di queste indicazioni per identificare le celle radio o i punti di accesso WLAN.

Il *capoverso 3* disciplina il modo in cui i FST devono perquisire i propri sistemi in base ai criteri di ricerca di cui al capoverso 2 e descrive le informazioni che devono fornire al Servizio SCPT.

Art. 66 Tipo di sorveglianza AS_29: ricerca per zona di copertura dell'antenna

Il tipo di sorveglianza definito nel presente articolo corrisponde all'attuale tipo CS 6 (ricerca per zona di copertura dell'antenna).

L'articolo elenca le indicazioni che deve fornire il FST.

Il *capoverso 1* definisce la portata della sorveglianza e limita la sua durata a un periodo di due ore per ordine. Questa durata massima corrisponde alla prassi attuale ed è stata fissata per minimizzare l'onere della sorveglianza, circoscrivere la quantità di dati mediante un limite temporale e tenere conto del principio della proporzionalità. Se le autorità di perseguimento penale sono interessate a una

sorveglianza più lunga devono suddividerla in più ordini di sorveglianza di due ore ciascuna. Gli emolumenti sono calcolati per ogni ordine di sorveglianza della durata di due ore e per cella radio. Il giudice dei provvedimenti coercitivi deve approvare ciascun ordine. Esempio: per le celle A, B e C deve essere effettuata una ricerca per zona di copertura dell'antenna presso il FST Y per un periodo di 5 ore. L'autorità di perseguimento penale ordina la ricerca con un totale di 9 ordini presso il Servizio SCPT nel modo seguente: gli ordini 1 e 2 di due ore ciascuno per la cella A e l'ordine 3 di un'ora sempre per la cella A; analogamente gli ordini 4, 5 e 6 per la cella B e 7, 8 e 9 per la cella C. Ne risultano emolumenti pari a nove volte l'emolumento per una ricerca per zona di copertura dell'antenna secondo l'ordinanza sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OEm-SCPT).

Secondo il *capoverso 2* i dati della sorveglianza di cui al capoverso 1 devono essere trasmessi nel modo stabilito dagli articoli 60 e 61, per cui si può rinviare ai pertinenti commenti.

Sezione 11: Ricerca d'emergenza e ricerca di condannati

Al di fuori di un procedimento penale, la nuova LSCPT permette la sorveglianza della corrispondenza postale per la ricerca d'emergenza (art. 35 cpv. 1 nLSCPT) o la ricerca di condannati (art. 36 cpv. 1 nLSCPT). La sorveglianza della corrispondenza postale nell'ambito di una ricerca d'emergenza o di condannati si distingue dalla sorveglianza nell'ambito di un procedimento penale soltanto in riferimento alla procedura per l'ordine e l'autorizzazione. Nell'ordinanza non è pertanto necessario definire tipi specifici di sorveglianza o regole speciali.

L'ordinanza prevede invece regole speciali per la sorveglianza del traffico delle telecomunicazioni per la ricerca d'emergenza (art. 35 nLSCPT) o di condannati (art. 36 nLSCPT) al di fuori di un procedimento penale. A differenza di quanto previsto per i tipi di sorveglianza ordinari, per la ricerca d'emergenza (art. 67) la sorveglianza dell'accesso e dell'applicazione sono riunite in un solo tipo. Infatti le ricerche d'emergenza devono avvenire rapidamente poiché si è in presenza di un grave pericolo per la salute o la vita della persona dispersa. Pertanto, l'ordine dell'autorità di perseguimento penale al Servizio SCPT e l'incarico di quest'ultimo alla persona obbligata a collaborare devono poter avvenire nel modo più semplice possibile. Inoltre, occorre raccogliere quanto prima tutte le informazioni disponibili sulla persona dispersa e quindi la persona obbligata a collaborare deve sorvegliare conformemente al tipo di sorveglianza ordinato tutti i servizi di telecomunicazione che fornisce in relazione all'identificativo di destinazione indicato.

Va precisato che, in virtù dell'articolo 35 capoverso 3 nLSCPT, nell'ambito di una ricerca d'emergenza si può ricorrere anche ad apparecchi tecnici secondo l'articolo 269bis CPP (p. es. IMSI-catcher) e che, in virtù dell'articolo 36 capoverso 2, è altresì possibile ricorrere ad apparecchi tecnici secondo l'articolo 269bis CPP (p. es. IMSI-catcher) o a programmi informatici speciali secondo l'articolo 269ter (p. es. GovWare) nell'ambito della ricerca di condannati.

Art. 67 Tipo di sorveglianza EP: ricerca d'emergenza

Il presente articolo sostituisce l'articolo 16*a* dell'OSCPT vigente che contempla la ricerca e il salvataggio di persone disperse. Nell'ambito della sorveglianza delle

telecomunicazioni per la ricerca d'emergenza, la nLSCPT permette anche la sorveglianza del contenuto delle comunicazioni (lett. b), mentre attualmente sono possibili soltanto il cosiddetto paging (lett. a), la sorveglianza in tempo reale dei metadati (lett. c) e la sorveglianza retroattiva (lett. d), tutti e tre mantenuti nella nuova ordinanza.

La *lettera a* descrive il tipo di sorveglianza «paging», che permette di determinare l'ultima attività (al massimo sei mesi prima) rilevata dalla persona obbligata a collaborare per l'apparecchiatura terminale mobile della persona dispersa. La *lettera a* elenca le indicazioni necessarie. L'*identificativo univoco della rete mobile* è costituito dal codice della telefonia mobile del Paese (Mobile Country Code, MCC) e dal codice della rete mobile (Mobile Network Code, MNC). I numeri 1-3 illustrano le possibili indicazioni necessarie per la localizzazione. La persona obbligata a collaborare deve localizzare l'ultima attività per mezzo di una delle indicazione di cui ai numeri 1-3. L'*indirizzo postale* di cui al *numero 1* può essere anche una descrizione geografica (p. es. numero civico e chilometro, NAP Comune) poiché non per tutte le antenne esistono indirizzi postali. Il campo previsto per *la direzione di trasmissione* può anche rimanere vuoto o contenere più direzioni o elementi. Nel caso di celle radio onnidirezionali (trasmissione uguale in tutte le direzioni) il campo rimane vuoto. Nel caso di celle radio complesse o specifiche, oltre alla direzione di trasmissione, il campo può ad esempio contenere anche i seguenti elementi: «inh» (inhouse = cella all'interno di un edificio) o «tun» (tunnel = la cella ha un ripetitore per coprire uno o più tunnel).

La lettera b descrive la sorveglianza in tempo reale del contenuto e dei metadati nell'ambito di una ricerca d'emergenza. L'autorità che dispone la sorveglianza trasmette al Servizio SCPT un ordine per ogni persona obbligata a collaborare e per ogni terminale cercato. Successivamente il Servizio SCPT trasmette il pertinente incarico alle persone obbligate a collaborare. Ogni persona obbligata a collaborare installa i tipi di sorveglianza pertinenti tra quelli di cui agli articoli 53 e 55, in modo tale che siano contemplati tutti i servizi da essa forniti per l'apparecchiatura terminale cercata. In tal modo si tiene conto dell'urgenza della ricerca d'emergenza, poiché si tratta di localizzare e trovare quanto prima la persona la cui vita o integrità fisica è in pericolo. Nel caso di una ricerca d'emergenza costerebbe troppo trasmettere un incarico per ogni servizio di telecomunicazione o di comunicazione derivato, come previsto per le sorveglianze ordinarie. Esempio: la persona obbligata a collaborare riceve un incarico per la ricerca d'emergenza del tipo EP_31_RT_CC_IRI (lett. b) per il MSISDN X. Se l'utente con il MSISDN X ha un abbonamento di telefonia mobile con accesso a Internet presso la persona obbligata a collaborare, quest'ultima installa per il servizio di telefonia una sorveglianza in tempo reale del tipo RT_18_TEL_CC_IRI e per l'accesso alla rete una sorveglianza in tempo reale del tipo RT_16_NA_CC_IRI. Anche nell'ambito della ricerca d'emergenza le sorveglianze in tempo reale restano attive fintanto che il Servizio LSCPT non trasmette alla persona obbligata a collaborare l'incarico di porvi fine.

La *lettera c* descrive la sorveglianza in tempo reale senza dati sul contenuto, ossia soltanto dei metadati, nell'ambito di una ricerca d'emergenza. Il modo di procedere è analogo a quanto illustrato alla *lettera b*. L'unica differenza è costituita dal fatto che ogni persona obbligata a collaborare installa i tipi di sorveglianza pertinenti tra quelli di cui agli articoli 52 e 54, di modo che siano contemplati tutti i servizi forniti per il terminale cercato.

La *lettera d* disciplina la ricerca d'emergenza retroattiva, ad esempio nel caso in cui l'apparecchio terminale non è più attivo. Il modo di procedere è analogo a quanto illustrato alla lettera b. L'unica differenza è costituita dal fatto che si tratta di una sorveglianza retroattiva, che ogni persona obbligata a collaborare installa il tipo di sorveglianza pertinenti tra quelli di cui agli articoli 60 e 61, di modo che siano contemplati tutti i servizi forniti per l'apparecchiatura terminale cercata. Inoltre nel caso della sorveglianza retroattiva non è necessario l'incarico di porvi fine.

Le indennità per le persone obbligate a collaborare si basano sul numero delle ricerche d'emergenza ordinate dall'autorità disponente per ogni apparecchiatura terminale cercata e non sul numero delle sorveglianze effettivamente svolte.

La *lettera e* permetterà in futuro anche la ricerca per zona di copertura dell'antenna (art. 66) e i relativi preparativi (art. 64 e 65) nell'ambito della ricerca d'emergenza.

Art. 68 Ricerca di condannati

Il presente articolo è nuovo e disciplina la ricerca di condannati prevista dall'articolo 36 nLSCPT. Il tipo di ordine di ricerca è costituito da un tipo di sorveglianza in tempo reale «contenuti e metadati» (*lett.* a), un tipo di sorveglianza in tempo reale «solo metadati» (*lett. b*) o un tipo di sorveglianza retroattiva (*lett. c*). I tipi di ricerca corrispondono esattamente ai tipi di sorveglianza e pertanto, a differenza della ricerca d'emergenza, nella ricerca di condannati non vengono riuniti diversi tipi di sorveglianza. Ai fini della distinzione nella statistica, nell'ordinare questo tipo di ricerche occorre indicare la menzione «ricerca di condannati». Se nell'ambito di una ricerca di condannati sono ordinati più tipi di sorveglianza, deve essere trasmesso un ordine per ciascun tipo. Si applica la regola usuale per gli emolumenti, secondo cui ogni tipo di sorveglianza ordinato per fornitore e per identificativo di destinazione è soggetto a emolumento (cfr. OEm-SCPT).

Sezione 12: Identificativi esterni alla rete

Art. 69

Analogamente a quanto previsto dagli articoli 16*b* e 24*c* dell'OSCPT vigente, l'articolo 69 disciplina la sorveglianza di identificativi esterni alla rete. Si tratta di identificativi che non sono amministrati dalla persona obbligata a collaborare o che non sono registrati nella sua rete.

L'articolo disciplina pertanto la sorveglianza relativa a elementi di indirizzo stranieri. Questi elementi sono standardizzati nell'applicazione, ma non nell'accesso alla rete. Inoltre vi sono delle limitazioni in riferimento agli identificativi di destinazione (p. es. nessun IMSI, nessun IMEI); limitazioni che sono disciplinate in dettaglio nell'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OA-SCPT). Per quanto riguarda gli elementi di indirizzo stranieri si rinvia al commento dell'articolo 31 nLSCPT nel messaggio del 27 febbraio 2013[46]

46 FF **2013** 2283 2346.

concernente la LSCPT. Contrariamente alla prassi vigente, nell'ordine e nel mandato di sorveglianza non occorre aggiungere una relativa annotazione. L'articolo 48 capoverso 4 disciplina in generale il traffico delle telecomunicazioni da sorvegliare.

Capitolo 4: Disposizioni finali

Art. 70 Prescrizioni organizzative, amministrative e tecniche

La disposizione corrisponde, all'articolo 33 dell'OSCPT del 31 ottobre 2001[47] ad eccezione delle modifiche necessarie.

Insieme all'articolo 31 capoverso 3 nLSCPT[48], l'articolo 70 costituisce la base legale per l'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE−SCPT). Per contro, l'ordinanza del DFGP sull'organo consultivo per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (organo consultivo) si fonda direttamente sulla nLSCPT e precisamente sull'articolo 5 capoverso 3 di tale legge.

In base all'articolo 70 il DFGP emana le necessarie prescrizioni tecniche, amministrative e organizzative per l'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Tali prescrizioni non sono destinate solamente ai fornitori di servizi di telecomunicazione e di servizi di comunicazione derivati, ma anche ai fornitori di servizi postali.

Secondo il diritto vigente, i dettagli tecnici e amministrativi sono disciplinati dalle direttive del Servizio SCPT (art. 33 cpv. 1bis OSCPT del 31 ott. 2001[49]; cfr. www.li.admin.ch)

Altre norme di delega al DFGP sono contenute negli articoli 31 (procedura di collaudo) 47 capoverso 2 (indicazioni tecniche nell'ordine di sorveglianza) e 27 capoverso 1 (requisiti della qualità dei dati trasmessi).

Il *secondo periodo* dell'articolo 70 precisa che il DFGP definisce i termini entro cui vanno consegnati i relativi dati.

Art. 71 Esecuzione

Il *capoverso 1* corrisponde sostanzialmente all'articolo 33 capoverso 2 dell'OSCPT del 31 ottobre 2001[50]. La disposizione sancisce che il Servizio SCPT può continuare a mettere a disposizione delle autorità che dispongono la sorveglianza e delle persone obbligate a collaborare le interfacce e i moduli elettronici. Per motivi di efficienza e per evitare errori vanno utilizzati esclusivamente le interfacce e i moduli elettronici del servizio SCPT.

47 RS **780.11**
48 FF **2013** 2283, 2347.
49 RS **780.11**
50 RS **780.11**

Il *capoverso 2* prevede che, in un secondo momento, i moduli elettronici possano essere sostituiti da un accesso online al sistema di trattamento del Servizio SCPT. Poiché non è stato ancora stabilito un termine preciso, il Servizio SCPT può decidere direttamente in merito al momento di tale sostituzione. Se non fosse possibile accedere online al sistema di trattamento oppure se tale accesso dovesse interrompersi per qualche ragione, andrebbero nuovamente utilizzati i moduli.

Art. 72 Abrogazione e modifica di altri atti normativi

Con l'entrata in vigore della presente ordinanza la OSCPT del 31 ottobre 2001 viene abrogata.

Nel contempo sono in parte modificate altre due ordinanze:

- l'ordinanza del 17 novembre 1999[51] sull'organizzazione del Dipartimento federale di giustizia e polizia (Org-DFGP), che subisce una modifica formale dell'articolo 25;

- l'ordinanza del 9 marzo 2007[52] sui servizi di telecomunicazione (OST), che viene modificato all'articolo 3 capoversi 1 lettera d e 2, nonché all'articolo 80.

Art. 73 Disposizioni transitorie

È necessario prevedere disposizioni transitorie affinché le persone obbligate a collaborare e il Servizio SCPT abbiano abbastanza tempo per introdurre le nuove disposizioni. Ciò permette di rinunciare a un'entrata in vigore scaglionata delle ordinanze d'esecuzione relative alla nLSCPT.

Il *capoverso 1* permette al Servizio SCPT di allestire le statistiche secondo il diritto anteriore fino alla messa in servizio delle componenti di sistema previste dalla prima fase del Programma di sviluppo e di esercizio del sistema di trattamento per la sorveglianza del traffico delle telecomunicazioni (sistema di trattamento) e dei sistemi d'informazione di polizia della Confederazione (programma STT)[53]. Gli attuali sistemi, soprattutto il CCIS, il cui contratto di assistenza non può più essere adeguato, non consentono di procedere al tipo di statistiche desiderato.

Secondo il *capoverso 2,* dopo che il Servizio SCPT ha messo in funzione l'interfaccia automatizzata per le informazioni, le persone obbligate a collaborare hanno altri sei mesi di tempo per adattare i propri sistemi e quindi fornire al Servizio SCPT le informazioni richieste tramite tale interfaccia.

Non tutti i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari di cui l'articolo 21 sono già in grado di fornire attualmente le informazioni conformemente ai nuovi tipi di informazioni. Pertanto sono tenuti ad adeguare i loro software o i loro sistemi. Per farlo il *capoverso 3* concede loro dodici mesi di tempo.

Ai FST e ai fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari ai sensi dell'articolo 50 che adeguano i propri sistemi affinché, come previsto dalla nuova legislazione, possano memorizzare e

51 RS **172.213.1**
52 RS **784.101.1**
53 FF **2015** 2543

trasmettere anche i metadati relativi ai *tentativi* di comunicazione e di login, è concesso un periodo transitorio di 24 mesi (*cpv. 3*).

I meccanismi e le procedure di intercetazione nell'ambito della sorveglianza della posta elettronica, propri della Svizzera e ormai obsoleti, non sono più contemplati dalla OE-SCPT. Il sistema di trattamento del Servizio SCPT li supporta ancora per un determinato periodo nel caso di sistemi operativi prima dell'entrata in vigore della presente ordinanza. Ai FST è concesso un periodo di 24 mesi per adeguare i propri sistemi per la sorveglianza della posta elettronica alle disposizioni della presente ordinanza e della OE-SCPT (*cpv. 4*).

Art. 74 Entrata in vigore

L'entrata in vigore della presente ordinanza è stata coordinata con quella della nLSCPT e delle altre ordinanze esecutive.

Si può rinunciare a un'entrata in vigore scaglionata.

Allegato

Tabella obblighi FSP/FST

Allegato al rapporto esplicativo OSCPT

		INFORMAZIONE			SORVEGLIANZA		
		LSCPT	OSCPT	Obblighi	LSCPT	OSCPT	Obblighi
Fornitori di servizi postali (FSP)		_____	_____	_____	19	14	
Fornitori di servizi di telecomunicazione (FST) Art. 2 lett. b nLSCPT	PICCOLI[54] (o settore educazione) Art. 26 cpv. 6 nLSCPT	21/22	18 cpv. 1 e 3 20 29 (compliance)	A	26 cpv. 2 e 6	49	B
	STANDARD	21/22	11 cpv. 2, 18 cpv. 1 e 2, 19, 20 29 (compliance) 73 (disp. trans.)	C	26 cpv. 1-5	11 cpv. 2 48 29 (compliance)	D
Fornitori di servizi di comunicazione derivati Art. 2 lett. c nLSCPT	STANDARD	22 cpv. 3	11 cpv. 2 18 cpv. 4	E	27 cpv. 1 e 2	11 cpv. 2	F
	GRANDI[55] (obblighi supplementari) Art. 27 nLSCPT	22 cpv. 4	18 cpv. 1 e 2 21 29 (compliance) 73 (disp. trans.)	G	27 cpv. 3 26 cpv. 1-5	11 cpv. 2 29 (compliance) 48 50	H

[54] Downgrade
[55] Upgrade

A. Obblighi dei FST con obblighi di sorveglianza ridotti (piccole dimensioni) in caso di domande di informazioni

Presupposto: il FST offre servizi di scarsa importanza economica o nel settore dell'istruzione.

- Stessi obblighi dei FST di dimensioni standard (nessun downgrade per informazioni)
- Esonero dal servizio di picchetto ai sensi dell'art. 11 cpv. 2 OSCPT
- Esonero ai sensi dell'art. 18 cpv. 3 OSCPT per quanto riguarda l'automatizzazione delle risposte alle domande di informazioni di cui agli art. 33–46 OSCPT (possono rispondere anche per scritto)

B. Obblighi dei FST con obblighi di sorveglianza ridotti (piccole dimensioni) in caso di ordine di sorveglianza, ricerca d'emergenza e ricerca di condannati

Presupposto: il FST offre servizi di scarsa importanza economica o nel settore dell'istruzione.

- Esonero dagli obblighi ai sensi dell'art. 26 cpv. 1 e 3–5 LSCPT
- Esonero dal servizio di picchetto ai sensi dell'art. 11 cpv. 2 OSCPT
- Soltanto i seguenti obblighi (ai sensi dell'art. 26 cpv. 2 LSCPT):
  - fornire le informazioni necessarie all'attuazione della sorveglianza,
  - tollerare le sorveglianze,
  - sopprimere i loro criptaggi.

C. Obblighi dei FST (dimensioni standard) in caso di domande di informazioni

- Fornire informazioni sui servizi di telecomunicazione (art. 21 LSCPT)
- Fornire informazioni per identificare gli autori di reati commessi via Internet (art. 22 LSCPT)
- Essere in grado di fornire le informazioni di cui agli articoli 33-46 OSCPT (art. 18 cpv. 1 OSCPT)
- Se tecnicamente possibile, forniscono le informazioni di cui agli articoli 33–40 in modo automatizzato tramite l'interfaccia di consultazione del sistema di trattamento; alle domande di informazioni di cui agli articoli 41–46 possono anche rispondere manualmente (art. 18 cpv. 2 OSCPT).
- Obblighi di conservazione dei dati ai sensi degli art. 21 e 22 LSCPT e dell'art. 20 OSCPT
- Art. 11 cpv. 2 OSCPT

D. Obblighi dei FST (dimensioni standard) in caso di ordine di sorveglianza, ricerca d'emergenza e ricerca di condannati

- Art. 26 LSCPT (obblighi dei fornitori di servizi di telecomunicazione)

1 Su richiesta, i fornitori di servizi di telecomunicazione trasmettono al Servizio o, nei casi di cui all'articolo 17 lettera c, all'autorità che ha disposto la sorveglianza o all'autorità da essa designata:
   a. il contenuto del traffico delle telecomunicazioni della persona sorvegliata;
   b. i metadati delle telecomunicazioni della persona sorvegliata.

2 Sono inoltre tenuti a:
   a. fornire le informazioni necessarie all'attuazione della sorveglianza;
   b. tollerare le sorveglianze attuate dal Servizio o dalle persone da esso incaricate; a tal fine, devono permettere senza indugio l'accesso ai loro impianti;
   c. sopprimere i loro criptaggi.

3 I fornitori di servizi di telecomunicazione che partecipano all'esercizio del servizio di telecomunicazione da sorvegliare trasmettono i dati di cui dispongono al Servizio o al fornitore incaricato della sorveglianza.

4 L'ordine di sorveglianza può prevedere che la sorveglianza sia attuata in tempo reale o che siano trasmessi i metadati delle telecomunicazioni passate conservati (sorveglianza retroattiva).

5 I fornitori di servizi di telecomunicazione conservano per sei mesi i metadati delle telecomunicazioni.

- Obblighi durante il servizio di picchetto (art. 11 cpv. 2 OSCPT)
- Art. 48 OSCPT

E. Obblighi dei fornitori di servizi di comunicazione derivati (dimensioni standard) in caso di domande di informazioni

- I fornitori di servizi di comunicazione derivati trasmettono al Servizio SCPT le indicazioni di cui dispongono (art. 22 cpv. 3 nLSCPT)
- Art. 11 cpv. 2 OSCPT
- Art. 18 cpv. 4 OSCPT

F. Obblighi dei fornitori di servizi di comunicazione derivati (dimensioni standard) in caso di ordine di sorveglianza, ricerca d'emergenza e ricerca di condannati

- Obbligo di tollerare le sorveglianze (art. 27 cpv. 1 LSCPT)
- Art. 27 cpv. 2 LSCPT
- Art. 11 cpv. 2 OSCPT

G. Obblighi dei fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari (grandi dimensioni) in caso di domande di informazioni

Presupposto: il fornitore offre servizi di grande importanza economica o servizi a un gran numero di utenti

- Equiparati ai FST di dimensioni standard
- Fornire informazioni per identificare gli autori di reati commessi via Internet (art. 22 LSCPT)
- Essere in grado di fornire le informazioni di cui agli articoli 31–44 OSCPT (art. 18 cpv. 1 in combinato disposto con art. 21 cpv. 4 OSCPT)
- Se tecnicamente possibile, forniscono le informazioni di cui agli articoli 33–40 in modo automatizzato tramite l'interfaccia di consultazione del sistema di trattamento; alle domande di informazioni di cui agli articoli 41–46 possono anche rispondere manualmente (art. 18 cpv. 2 OSCPT).
- Obblighi di conservazione dei dati ai sensi degli art. 22 LSCPT e 20 OSCPT
- Art. 11 cpv. 2 OSCPT

H. Obblighi dei fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari (grandi dimensioni) in caso di ordine di sorveglianza

Presupposto: il fornitore offre servizi di grande importanza economica o servizi a un gran numero di utenti

- Equiparati ai FST di dimensioni standard (art. 27 cpv. 3 nLSCPT)
- Obblighi durante il servizio di picchetto (art. 11 cpv. 2 OSCPT)
- Soddisfano gli obblighi ai sensi dell'art. 26 cpv. 1–5 LSCPT
- Art. 48 OSCPT