Rapporto esplicativo

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 (capitolo 1), corrispondenza postale (capitolo 2), traffico delle telecomunicazioni (capitolo 3) e disposizioni finali (capitolo 4). 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 regolano, se del caso, la sorveglianza in tempo reale e quella retroattiva. Ne consegue che sono fissati 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 informazione e di sorveglianza nell'ambito della sorveglianza delle telecomunicazioni, favorendo in tal modo le procedure automatiche.

Un'ulteriore differenza rispetto all'OSCPT del 31 ottobre 2001 è 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. 61–66).

Inoltre, nell'ambito della revisione totale della LSCPT 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. 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 dall'articolo 4

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

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.

Tenuto conto di queste osservazioni 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 probabilmente il loro numero diminuirà perché il Consiglio federale si è servito della possibilità prevista nella legge di liberare i fornitori di servizi di telecomunicazione da determinati obblighi di sorveglianza se forniscono servizi di esigua importanza economica o nel settore dell'educazione È presumibile che il numero dei fornitori di servizi di telecomunicazione (FST) attivamente assoggettati all'obbligo di sorveglianza diminuirà da circa 600 a circa 20–30 FST. Malgrado la liberazione da determinati obblighi, la sorveglianza delle telecomunicazione continuerà a essere garantita. Le sorveglianze possono essere eseguite anche presso i FST con obblighi di sorveglianza ridotti, poiché questi fornitori continuano ad avere l'obbligo di tollerare la sorveglianza o collaborarvi. Il Servizio SCPT deve intraprendere quanto necessario per far sì che le sorveglianze continuino a poter essere eseguite (art. 17 lett. e LSCPT; cfr. il commento all'art. 51).

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 (art. 27 cpv. 3 LSCPT). Anche a questo riguardo il Consiglio federale ha precisato la disposizione nell'articolo 52. 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. 52) 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 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). La liberazione di molti fornitori dalla sorveglianza attiva non causa lacune nella sorveglianza perché sono il Servizio SCPT o i terzi incaricati a eseguire le sorveglianze ordinate presso questi fornitori. Inoltre, con la revisione totale è 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 (SECO), 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 (SIC) potrà procurarsi tutti i tipi di informazione tramite il Servizio SCPT (cfr. art. 15 LSCPT).

[2] RS **784.2**

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. La nuova ordinanza stabilisce il livello di qualità necessario e chi è tenuto ad assicurarlo (cfr. il commento all'art. 29). 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, il Servizio SCPT esegue inoltre i cosiddetti controlli di conformità (procedura di compliance). Si tratta della procedura tesa a verificare la disponibilità a 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 (cfr. il n. 2.7 del messaggio[3] e i commenti agli art. 31–34).

3 FF **2013** 2283 2344 segg.

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[4] (stato al 1° gennaio 2012).

Il *capoverso 2* precisa il campo d'applicazione personale dell'articolo 2 nLSCPT. Come nell'articolo 1 OSCPT previgente 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[5] l'elenco è stato inoltre integrato con il Servizio delle attività informative della Confederazione (*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 della presente ordinanza.

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[6] sulle poste (LPO)[7];

- *lettera i*: i FST secondo l'articolo 3 lettera b della legge sulle telecomunicazioni del 30 aprile 1997 (LTC)[8];

4 RS **780.11**
5 RS **780.11**
6 RS **783.0**
7 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT; commento all'art. 2 lett. a, FF **2013** 2283 2306.
8 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. b, 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)[9];

- *lettera k*: i gestori di reti di telecomunicazione interne[10];

- *lettera l*: le persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazione[11];

- *lettera m*: i rivenditori professionali di carte o altri mezzi analoghi che consentono di accedere a una rete pubblica di telecomunicazione[12].

Nella pratica, il Servizio SCPT stabilirà una lista per indicare quali servizi sono considerati servizi di comunicazione derivati ai sensi dell'articolo 1 capoverso 2 lettera j e aggiornerà regolarmente tale lista.

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[13].

Sezione 2: Ordine di sorveglianza

Art. 3 Trasmissione al Servizio SCPT

Il *capoverso 1* disciplina i mezzi di trasmissione approvati per l'inoltro al Servizio SCPT, da parte delle autorità disponenti, degli ordini di sorveglianza e delle loro proroghe e revoche come pure 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. 49). 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 15.11.2017 sul sistema di trattamento per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni [OST-SCPT]).

9 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. c, FF **2013** 2283 2307.
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 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, commento all'art. 2 lett. c, FF **2013** 2283 2308.
13 RS **780.11**

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. 49).

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. Se il Servizio SCPT o le autorità penali hanno comunque notato la svista prima di trasmettere il mandato al provider, è emessa una fattura soltanto per il mandato effettivo. 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 dal Dipartimento federale di giustizia e polizia nell'ordinanza del DFGP del 15 novembre 2017 sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT; cfr. anche il commento all'art. 68).

La *lettera b* permette una trasmissione alternativa dei summenzionati ordini dell'autorità disponente per posta o telefax al Servizio SCPT. A tal fine vanno utilizzati i moduli predisposti dal Servizio SCPT. Questa modalità di trasmissione va utilizzata soltanto se motivi tecnici impediscono la trasmissione conformemente alla lettera a. Le autorità di perseguimento penale devono fare tutto il possibile per effettuare la trasmissione 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

14 RS **780.11**

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 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. Anche il Servizio SCPT deve informare immediatamente le persone obbligate a collaborare, se per suoi problemi di esercizio non è in grado di eseguire le sue sorveglianze.

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[16] o 70*b* PPM[17] (*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

15 RS **780.11**
16 RS **312.0**
17 RS **322.1**

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)»[18].

Secondo gli articoli 15 lettere j e k (corrispondenza postale) e 49 capoverso 1 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 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 i documenti relativi alle misure speciali di protezione ordinate fanno anch'essi parte del fascicolo relativo alla sorveglianza).

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[19]. 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 misura di protezione.

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 selezione di informazioni (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[20]. 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 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[21] e disciplina l'obbligo del segreto.

18 FF **2013** 2283 2324; v. anche le spiegazioni del messaggio concernente la LSCPT relative agli art. 271 CPP e 70*b* PPM.
19 FF **2013** 2283 2296; n. 1.4.5.
20 FF **2006** 989 1152
21 RS **780.11**

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).

Art. 7 Selezione tecnica dei dati (cernita)

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

La selezione prevista (cernita) 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[22]. 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

22 FF **2013** 2283 2326

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 [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* disciplina 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 nel sistema di trattamento secondo l'OST–SCPT; 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'a*rticolo 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[23] sul personale federale.

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 23 e 26. 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* indica le persone obbligate a collaborare che devono sostenere il Servizio SCPT al di fuori degli orari d'ufficio ordinari. Sono tenuti a garantire un servizio di picchetto i FST e i fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari secondo l'articolo 51. Per motivi di proporzionalità sono sollevati da questi obblighi i FST con obblighi di sorveglianza ridotti (art. 50) e i fornitori di servizi di comunicazione derivati senza obblighi di sorveglianza supplementari (ossia coloro i quali non sono contemplati dall'art. 51). Pertanto le misure che devono attuare tali fornitori non possono essere eseguite durante il picchetto. Anche i FSP sono esentati dai servizi di picchetto.

Informazioni e sorveglianze particolari secondo l'articolo 25 sono le cosiddette misure speciali che possono essere eseguite dal Servizio SCPT o da terzi incaricati. Visto che la loro esecuzione richiede più tempo, sono nettamente più complesse e nella maggior parte dei casi devono collaborarvi più persone, il *capoverso 3* prevede che durante i picchetti non siano né accettati né trattati gli ordini di sorveglianze speciali e le richieste di informazioni speciali.

Sezione 4: Statistiche

Art. 12 Statistiche delle sorveglianza e delle informazioni

La LSCPT del 6 ottobre 2000 stabiliva che il Servizio SCPT tiene una statistica delle sorveglianze. Poiché, secondo le disposizioni transitorie (art. 74 cpv. 6 lett. a OSCPT), il Servizio SCPT può, durante il periodo transitorio, allestire le statistiche (art. 12) secondo il diritto anteriore, ci si basa ancora su queste disposizioni: l'articolo 11 capoverso 1 lettera f della LSCPT del 6 ottobre 2000 è la base legale per le statistiche sulla sorveglianza della corrispondenza postale e l'articolo 13 capoverso 1 lettera j della LSCPT del 6 ottobre 2000 per quelle sulla sorveglianza del traffico delle telecomunicazioni.

23 RS **172.220.111.3**

L'articolo 16 lettera k LSCPT del 18 marzo 2016 è stato introdotto il 10 marzo 2014 dal Consiglio degli Stati e prevede che il Servizio SCPT continui a tenere una statistica delle sorveglianze.

L'articolo 35 capoverso 3 LSCPT del 18 marzo 2016 (ricerca d'emergenza) e l'articolo 36 capoverso 2 LSCPT del 18 marzo 2016 LSCPT (ricerca di condannati) contengono ulteriori disposizioni relative alla statistica, mentre l'OSCPT del 31 ottobre 2001 non contiene alcuna disposizione in merito alla statistica. 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 anteriore. 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[24]). 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 anteriore 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.

24 RS **0.780.151.41**

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 CPP per i pubblici ministeri e dei nuovi articoli 70*bis* capoverso 2 e 70*ter* capoverso 4 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 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; questi punti sono sanciti dall'articolo 13.

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 consolidate. 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.

Per le misure di sorveglianza con apparecchi tecnici speciali e programmi informatici speciali non vi è alcun emolumento o indennità. Sono state esaminate le possibilità di comprovare le spese di tali misure di sorveglianza. Di regola, i programmi informatici speciali, dopo il loro acquisto, devono essere adeguati ai relativi impieghi speciali o occorrono sviluppi particolari. A seconda del modello

25 RS **322.2**

d'acquisto, ai costi di acquisto unici e ai costi d'esercizio ricorrenti si possono aggiungere diritti di licenza per ogni impiego. Insorgono inoltre costi per l'impiego del personale al fine di preparare il funzionamento di GovWare (polizia, informatici, traduttori ecc.). Poiché illustrare correttamente i costi a ogni impiego comporterebbe un onere molto elevato, si rinuncia a indicare i costi nella presente statistica.

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.

Il *capoverso 1* indica le sorveglianze che devono eseguire gli FSP; il *capoverso 2* indica soprattutto gli orari durante i quali questi ultimi devono essere raggiungibili.

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. 48).

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 in tempo reale occorre indicare, se disponibili, anche il luogo da cui è stato spedito l'invio postale (cfr. lett. b n. 4) e la firma del ricevente (cfr. lett. b n. 6). Il ricevente può essere il destinatario dell'invio postale ma anche un terzo autorizzato a ricevere la spedizione. 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).

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

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.

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

Il presente articolo disciplina le modalità della presentazione delle domande di informazioni alle tre categorie di persone obbligate a collaborare (FST, fornitori di servizi di comunicazione derivati e gestori di reti di telecomunicazione interne) da parte delle autorità legittimate conformemente all'articolo 15 LSCPT, come pure la ritrasmissione delle informazioni alle autorità. Il Servizio SCPT gestisce un sistema di trattamento che, tra le altre cose, trasmette le domande di informazioni e le risposte (componenti di sistema per le informazioni).

Il *capoverso 1* stabilisce che le autorità legittimate trasmettono le loro domande di informazioni e ricevono tramite il sistema di trattamento le informazioni dalle persone obbligate a collaborare. Tutte le altre vie di trasmissione delle domande di informazioni sono ammissibili soltanto se la procedura di richiamo mediante il sistema di trattamento non è disponibile per motivi tecnici, o in casi urgenti secondo il capoverso 3. Le domande di informazioni devono sempre essere presentate attraverso il Servizio SCPT. Non sono permesse domande dirette delle autorità legittimate alle persone obbligate a collaborare (cfr. art. 26 cpv. 2).

In alternativa, nei casi di problemi tecnici, il *capoverso 2* prevede la trasmissione delle domande di informazioni e delle risposte per posta o fax; le domande di informazioni sono trasmesse dalle autorità richiedenti al Servizio SCPT mentre le risposte seguono l'iter inverso dal Servizio SCPT alle autorità richiedenti.

Anche le informazioni fornite dalle persone obbligate a collaborare sono trasmesse mediante il sistema di trattamento (cfr. il commento all'art. 18). Sono previste eccezioni se il sistema non è disponibile per motivi tecnici e nei casi di cui all'articolo 18 capoversi 3 e 5 (cfr. il commento all'art. 18).

Nei casi urgenti le autorità legittimate possono presentare le domande di informazioni per telefono al Servizio SCPT con successivi inoltro elettronico di cui al capoverso 1 o trasmissione scritta secondo il capoverso 2 (*cpv. 3*). La presente normativa si ispira alle prescrizioni per gli ordini di sorveglianza urgenti di cui all'articolo 3 capoverso 1 lettera c.

Secondo il *capoverso 4,* 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

Questo articolo precisa gli obblighi degli FST e dei fornitori di servizi di comunicazione derivati. Occorre dapprima spiegare l'abituale svolgimento della fornitura di informazioni (p. es. ai fini di identificazione dei partecipanti): il fornitore cerca, nei dati relativi agli utenti e nei metadati conservati, o, se non sussiste alcun obbligo di sorveglianza, nei metadati disponibili, le indicazioni corrispondenti alla domanda d'informazioni nel periodo indicato. Fornisce i dati corrispondenti sugli utenti e gli utilizzatori finali nonché sui servizi di telecomunicazione e sui servizi di comunicazione derivati da essi impiegati secondo i dettami della domanda di informazioni.

In considerazione della liberazione di determinati FST dagli obblighi di sorveglianza e dell'obbligo di determinati fornitori di servizi di comunicazione derivati di fornire informazioni supplementari, sussistono le seguenti sottocategorie di persone obbligate a collaborare con diversi obblighi riguardo alle informazioni da fornire:

- FST, salvo quelli con obblighi di sorveglianza ridotti secondo l'articolo 51;
- FST con obbighi di sorveglianza ridotti secondo l'articolo 51;
- fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari secondo l'articolo 22.

Le due sottocategorie di FST hanno in linea di massima i medesimi obblighi di fornire informazioni. Le deroghe per i FST con obblighi di sorveglianza ridotti sussistono soltanto nella procedura seguita per fornire le informazioni (nessun obbligo di fornire le informazioni in modo automatizzato secondo il capoverso 2 e permesso di fornire informazioni senza usare il sistema di trattamento secondo il capoverso 3) nonché per i tipi di informazione speciali relativi agli indirizzi IP non assegnati in modo univoco (art. 37 e 38), che non devono fornire nella procedura standardizzata ma in modo non formale in base ai dati di cui dispongono. Tutte le tre summenzionate categorie di persone obbligate a collaborare devono garantire la disponibilità a fornire informazioni. Devono in particolare essere in grado di fornire le informazioni di cui agli articoli 35–37 e 40–48 nonché all'articolo 27 in combinato disposto con gli articoli 35, 40, 42 e 43 riguardanti i servizi da loro offerti (*cpv. 1*).

Le autorità legittimate di cui all'articolo 15 LSCPT presentano le domande di informazioni mediante il sistema di trattamento del Servizio SCPT (componenti di sistema per le informazioni). Il sistema di trattamento trasmette poi le domande di informazioni alle persone obbligate a collaborare, sempre che queste ultime forniscano le loro informazioni mediante il sistema di trattamento. Le persone obbligate a collaborare forniscono le informazioni desiderate mediante il sistema di trattamento che poi trasmette i risultati alle autorità richiedenti. Per quanto concerne

le persone obbligate a collaborare che non devono trasmettere le loro informazioni mediante il sistema di trattamento, il Servizio SCPT si occupa della trasmissione della domanda di informazioni alle persone obbligate a collaborare e riceve le informazioni fornite per poi trasmetterle alle autorità richiedenti mediante il sistema di trattamento.

I tipi di informazione secondo gli articoli 34–41 sono caratterizzati da un'elevata densità normativa. Essi corrispondono sostanzialmente alle precedenti informazioni semplici A0. Visto il numero molto elevato di informazioni semplici (202 052 informazioni nel 2016[30]), queste ultime sono fornite in linea di massima secondo una procedura automatizzata (24 ore / 365 giorni) mediante l'interfaccia elettronica del sistema di trattamento (*cpv. 2*). L'automatizzazione richiede regole precise, in particolare per quanto concerne i singoli parametri e tipi di dati. Il DFGP fissa queste regole nella nuova ordinanza OE–SCPT e nel suo allegato tecnico 1.

Secondo il *capoverso 3* i FST con obblighi di sorveglianza ridotti ai sensi dell'articolo 51, 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.

Vi sono tipi speciali di informazione per gli indirizzi IP non assegnati univocamente (art. 38 e 39) e altri tipi di informazione (art. 42–47) che possono anche essere forniti secondo una procedura manuale. Per questi, le persone obbligate a collaborare sono libere di scegliere se fornire le informazioni in modo manuale o automatizzato. Le persone obbligate a collaborare che devono fornire le loro informazioni mediante il sistema di trattamento (*cpv. 4*) devono tuttavia provvedere a trasmettere mediante il sistema di trattamento anche le informazioni fornite manualmente (*cpv. 2*).

Il *capoverso 4* disciplina gli obblighi di fornire i tipi di informazione secondo l'articolo 38 (IR_8_IP (NAT)) e l'articolo 39 (IR_9_NAT), che richiedono la conservazione dei metadati durante sei mesi. I FST con obblighi di sorveglianza ridotti (art. 51) sono esentati dall'obbligo di conservare i metadati. Non sono pertanto tenuti a fornire i tipi di informazione standardizzati secondo gli articoli 38 e 39. Non sono tuttavia esentati dal fornire informazioni senza requisiti formali in base ai metadati disponibili.

Il *capoverso 5* precisa quali categorie di persone obbligate a collaborare non sono obbligate a fornire le informazioni secondo i tipi d'informazioni definiti. Essi forniscono per scritto, per via postale o fax o con un mezzo di trasmissione sicuro autorizzato dal Servizio SCPT, le informazioni di cui dispongono. Si tratta dei fornitori di servizi di comunicazione derivati senza obblighi di informazione supplementari (quelli che non soddisfano le condizioni di cui all'art. 22) e dei gestori di reti di telecomunicazione interne (art. 1 cpv. 2 lett. k). Le due categorie precedentemente menzionate di persone obbligate a collaborare possono fornire volontariamente le loro informazioni secondo la procedura standardizzata attraverso il sistema di trattamento. Dall'obbligo precedentemente menzionato sono esentate anche le persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazioni (art. 1 cpv. 2 lett. l). In caso di ordine di sorveglianza devono però fornire le informazioni necessarie alla sorveglianza (art. 29 cpv. 1 lett. b LSCPT).

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

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. 6*). 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 25.

Art. 19 Identificazione degli utenti

In linea di massima è sufficiente se i FST che forniscono servizi di telecomunicazione identificano gli utenti con mezzi adeguati (*cpv. 1*).

Per quanto concerne i punti di accesso WLAN pubblici gestiti in maniera professionale, i FST devono tuttavia garantire con mezzi adeguati l'identificazione degli utilizzatori finali, vale a dire gli utilizzatori effettivi (*cpv. 2*). L'espressione «gestiti in maniera professionale» significa che un FST o un servizio di prestazioni IT specializzato nei punti di accesso WLAN pubblici si occupa dell'esercizio tecnico del punto d'accesso pubblico WLAN e di altri punti di accesso pubblici WLAN in altri luoghi. Se una persona fisica o giuridica nel suo accesso Internet gestisce un punto di accesso WLAN pubblico e lo mette a disposizione di terzi, i FST che offrono l'accesso Internet non devono garantire l'identificazione degli utilizzatori finali. In questo contesto è sufficiente l'identificazione degli utenti secondo il capoverso 1. La limitazione alla «gestione professionale» è effettuata per motivi di proporzionalità, per evitare che ad esempio le economie domestiche e le piccole imprese che lasciano «aperti» i loro WLAN siano tenuti a effettuare l'onerosa identificazione degli utilizzatori finali.

Per mezzi di identificazione adeguati, anche chiamati identificazione indiretta, si intendono le registrazioni implicite o semplificate mediante indicazioni affidabili (trusted). Esempi possibili:

- codice di accesso via SMS sul cellulare e memorizzazione del MSISDN;
- identificazione mediante carta di credito e memorizzazione dei dati dell'autorizzazione;
- identificazione mediante carta d'imbarco negli aeroporti e memorizzazione dei relativi dati;
- identificazione mediante la carta di un programma per frequent flyer che permette l'accesso alla lounge e memorizzazione dei dati dell'autorizzazione;
- identificazione mediante i dati del documento d'identità con una zona leggibile elettronicamente (MRZ) e memorizzazione di tali dati;
- identificazione mediante indicazioni affidabili dei partner di roaming e memorizzazione dei dati dell'autorizzazione;
- codice di accesso individuale in albergo associato alla registrazione dell'ospite;
- identificazione mediante carta SIM e memorizzazione dell'IMSI.

Art. 20 Registrazione dei dati degli utenti dei servizi di telefonia mobile

L'*articolo 20* corrisponde all'articolo 19*a* dell'OSCPT del 31 ottobre 2001[31] 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[32].

Il capoverso 1 prevede che, in occasione della prima attivazione dei mezzi di accesso ai servizi di telefonia mobile (p. es. GSM, GPRS, UMTS, LTE, VoLTE, VoWiFi), gli utenti debbano essere identificati sulla scorta di un passaporto o di una carta d'identità ai sensi degli articoli 71 e 71*a* dell'ordinanza del 24 ottobbre 2007 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 da parte del fornitore nel caso di strumenti di accesso già attivi al momento della sua consegna o di una embedded SIM (eSIM) inserita all'interno del dispositivo. Esempio: un tablet predisposto per la telefonia mobile con una carta SIM fissata all'interno del dispositivo viene venduto da un negozio di elettronica che non può eseguire l'attivazione di un servizio di telefonia mobile. Dapprima il cliente può utilizzare il tablet soltanto tramite WiFi. Soltanto se viene attivata da parte di un fornitore di servizi di telefonia mobile, la eSIM inserita nel tablet può essere utilizzata come «mezzo d'accesso» alla rete di telefonia mobile. Il mezzo di accesso è parte integrante del tablet ed è fornito, seppur non ancora in funzione, già al momento della vendita. Interessa le autorità di perseguimento penale soltanto dal momento in cui viene attivato. Inoltre, è importante anche l'identità di chi è tenuto a eseguire la registrazione. In questo esempio, il negozio di elettronica non esegue l'attivazione del mezzo di accesso alla telefonia mobile. Pertanto, la registrazione non è compito del negozio di elettronica, che non è considerato rivenditore di carte o mezzi analoghi, ma del fornitore di telefonia mobile in occasione dell'attivazione della eSIM.

In caso di contatti con nuovi utenti, si parte dal presupposto che i fornitori verifichino sempre i dati e i documenti perché hanno un interesse proprio a farlo. 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 a tutti i servizi di telefonia mobile indipendentemente dal metodo di pagamento (p. es. abbonamento, prepagato, gratis). Nella prassi i fornitori di servizi di telefonia mobile chiedono già da molto tempo un documento di identità al cliente che stipula un abbonamento.

I fornitori di servizi di telecomunicazione, i fornitori di servizi di comunicazione derivati con obblighi supplementari ai sensi dell'articolo 22 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 (art. 23 cpv. 1 nLSCPT); la verifica si fonda sulla copia del documento d'identità. Se il documento dispone di una zona leggibile elettronicamente (MRZ), si raccomanda di leggere i dati che vi figurano a macchina o con un dispositivo ottico e di registrarli come segue:

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

- nome(i) e cognome(i) rilevati dalla zona leggibile elettronicamente (MRZ) come pseudonimo o identità secondaria. Poiché questi consistono in un set di caratteri latini ridotti, possono essere utilizzati direttamente per la ricerca normale dei nomi (letterale) (cfr. art. 35).

Per le seguenti indicazioni sulla persona o sul documento devono essere registrati, se disponibili, i dati della zona leggibile elettronicamente, invece di procedere a un'immissione manuale:

- Paese o organizzazione (abbreviazione di tre lettere);
- numero di documento;
- cittadinanza (abbreviazione di tre lettere);
- data di nascita (YYMMDD);
- sesso ("M"=maschile / "F"=femminile / "<"=nessuna indicazione).

Osservazione: nella presente ordinanza, la formulazione «se disponibile» (if available), significa che i relativi dati devono essere forniti se sono disponibili sotto il profilo tecnico, ad esempio un determinato parametro in una notifica di segnalazione. Nel singolo caso ciò dipende da numerosi fattori, come la tecnologia, lo standard applicabile, il servizio di comunicazione e lo scenario concreto. I dettagli sono disciplinati nell'allegato 1 della OE–SCPT. Se i dati esistono sussiste quindi un obbligo dei fornitori di fornirli o di memorizzarli a fini di informazione e di sorveglianza retroattiva. Esempio: non vi è sempre un numero di cliente e il fornitore non ne deve generare uno. Per questo motivo, l'articolo 34 cpv. 1 lett. a recita «se disponibile». L'espressione «se disponibile» non deve essere confusa con l'espressione della LSCPT «i metadati delle telecomunicazioni della persona sorvegliata di cui dispongono» (p. es. art. 28 cpv. 2 OSCPT) che esprime un obbligo passivo di tollerare e non un obbligo attivo di memorizzare.

I dati di cui ai capoversi 2 e 3 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. Non è pertanto richiesta nemmeno una registrazione successiva dei dati dei clienti. Va rilevato che, se la relazione commerciale non è stata registrata correttamente e non è stato sottoscritto un abbonamento (Prepaid), il fornitore deve bloccare l'accesso ai servizi di telecomunicazione (art. 6*a* LTC[33]).

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

33 FF **2016** 1675 1703

19 dicembre 2003 sui servizi di certificazione nel campo della firma elettronica [Legge sulla firma elettronica, FiEle] e la futura legge sull'identità elettronica) (cfr. art. 23 cpv. 1 nLSCPT). Sarebbe possibile anche un'identificazione online che soddisfi gli standard di sicurezza e qualità della Circolare 2016/7 «Video identificazione e identificazione online» per il settore bancario. Nell'ambito dell'identificazione degli utenti mediante un'identità elettronica valida (eID) o simili, della summenzionata identificazione online e delle procedure equivalenti si può rinunciare alla comparizione personale dell'utente.

Non occorre per forza copiare e conservare il documento d'identità in forma cartacea. Tuttavia nel sistema del fornitore deve esserci una copia elettronica ben leggibile del documento d'identità (cpv. 1 e 2), non importa se fotografata o scannerizzata (cfr. art. 23 cpv. 1 nLSCPT). Per l'identificazione degli utenti mediante un'identità elettronica o simili, i dati devono essere registrati elettronicamente e non occorre presentare la copia del documento. I dati di cui al capoverso 2 e 3 non contenuti nell'identità elettronica (p. es. indirizzo) devono essere registrati in base alle indicazioni dell'utente.

Il *capoverso 2* precisa i dati che devono essere registrati nel caso di persone fisiche. I dati necessari (cognome(i), nome(i), data di nascita, tipo di documento d'identità e numero, indirizzo) sono già previsti nell'articolo 19*a* dell'OSCPT del 31 ottobre 2001[34] e corrispondono alla prassi anteriore. Devono d'ora innanzi essere indicati anche il Paese o l'organizzazione d'emissione, la cittadinanza (art. 21 cpv. 1 lett. d nLSCPT) e, se nota, anche la professione (art. 21 cpv. 1 lett. a nLSCPT). L'indicazione del Paese o dell'organizzazione che ha emesso il documento d'identità è necessaria per evitare alle autorità di perseguimento penale di dover eseguire eventuali verifiche.

Il *capoverso 3* elenca i dati che devono essere registrati per le persone giuridiche. I nuovi dati da registrare sono il nome, la sede e i dati di contatto della persona giuridica (*lett. a*), il numero d'identificazione dell'impresa secondo la legge del 18 giugno 2010[35] sul numero d'identificazione dell'impresa (*lett. b*), nonché, se disponibili, i cognomi e i nomi delle persone che si servono dei servizi dei fornitori, per esempio i collaboratori (*lett. c*).

Il *capoverso 4* 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, offerte gratuite). 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 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).

34 RS **780.11**
35 RS **431.03**
36 Cfr. Messaggio del 27 febbraio 2013 concernente la LSCPT, FF **2013** 2283 2308.
37 RS **784.101.1**

Art. 21 Termine di conservazione

L'*articolo 21* 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 primo periodo* 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 20 capoversi 1-3. Inoltre anche in questa disposizione vi è un rimando all'articolo 45 capoverso 3 LSCPT.

Il *capoverso 1 secondo periodo* disciplina, in modo analogo al primo periodo, la durata di conservazione dei dati di identificazione di cui all'articolo 19 capoverso 2 che i FST devono registrare per i punti di accesso WLAN pubblici gestiti a titolo professionale. Per semplificare l'amministrazione degli utenti nei punti di accesso WLAN pubblici gestiti a titolo professionale la durata della relazione con il cliente è considerata equivalente alla durata dell'autorizzazione di accesso al punto di accesso WLAN pubblico.

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 più breve di quello del capoverso 1. Le indicazioni in questione sono l'elenco degli identificatori dell'apparecchio effettivamente utilizzati (p. es. IMEI, indirizzo IP; cfr art. 36 cpv. 1 lett. d e art. 41 cpv. 1 lett. d) nonché i dati sulla concessione delle informazioni di cui agli articoli 38 e 39.

Per gli FST con obblighi di sorveglianza ridotti di cui all'articolo 51, l'obbligo di conservazione di cui al capoverso 2 sarebbe in contraddizione con la prevista liberazione dagli obblighi di sorveglianza secondo l'articolo 51. Tale liberazione è pertanto attuata in modo coerente anche nel presente contesto.

Con il *capoverso 3* si adempie la raccomandazione della Commissione degli affari giuridici del Consiglio nazionale del 19 settembre 2017 secondo cui, per motivi di certezza del diritto, occorre prevedere un obbligo di cancellare dopo 6 mesi i dati menzionati nel capoverso 2.

Art. 22 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 dei normali FST (non ridotti). Sono soltanto tenuti a tollerare la sorveglianza e a consegnare i dati a loro disposizione necessari per lo svolgimento della stessa. A tal fine, su richiesta devono consegnare i metadati di cui dispongono relativi al traffico delle telecomunicazioni della persona sorvegliata (art. 27 cpv. 2 LSCPT). 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.

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, secondo la *lettera a*, ha dovuto espletare 100 domande d'informazione negli ultimi 12 mesi (data di riferimento 30 giugno) o se, secondo la lettera b, ha raggiunto un fatturato annuo in Svizzera di 100 milioni di franchi per due esercizi consecutivi. La *lettera a* riprende il criterio del «gran numero di utenti» dell'articolo 22 capoverso 4 nLSCPT. Dal punto di vista della sorveglianza delle telecomunicazioni è difficile dare una definizione *assoluta* della nozione di «gran numero di utenti», tanto più se è necessario darne una definizione anticipata in relazione con l'offerta di diversi servizi tecnici. Per questo motivo alla lettera a si applica il criterio del numero di domande d'informazione, che ha dato buoni risultati nella pratica. La statistica della sorveglianza delle telecomunicazioni degli ultimi anni mostra che il numero di domande d'informazione riflette il concetto di gran numero di utenti in modo affidabile e adeguato al tipo di servizio. Nel contempo questo criterio tiene conto anche della proporzionalità, nella misura in cui comprende soltanto fornitori veramente rilevanti per la sorveglianza delle telecomunicazioni. Il secondo criterio (*lett. b*) 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 un obbligo di informazione per i fornitori che non raggiungono più oppure superano i valori soglia di cui al capoverso 1 lettere a o b ne informino il Servizio SCPT. A tal fine il Servizio SCPT mette a disposizione strumenti di comunicazione adeguati.

Il *capoverso 4* dà al Servizio SCPT i mezzi necessari soprattutto per accertare se i valori menzionati nel capoverso 1 non sono raggiunti o sono superati. Tuttavia al Servizio SCPT occorrono anche i dati per stabilire se un fornitore va considerato fornitore di servizi di comunicazione derivati o no. Può anche procurarsi i documenti necessari a tal fine presso altre autorità.

Secondo il *capoverso 5* 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 dalla presa di conoscenza della decisione del Servizio SCPT. Il Servizio SCPT sostiene i fornitori nell'adempimento dei loro obblighi prestando loro consulenza.

Art. 23 Ausiliari per la fornitura di informazioni o l'esecuzione di sorveglianze

L'*articolo 23* regola il ricorso ad ausiliari da parte dei fornitori. È essenziale che il ricorso ad ausiliari non provochi ritardi, non comprometta la qualità o produca lacune nella sorveglianza. Pertanto gli ausiliari sono assoggettati alle medesime regole dei fornitori. Inoltre il Servizio SCPT, in caso di necessità, ad esempio se vi è un problema di trasferimento, deve poter contattare direttamente il fornitore o gli ausiliari, a seconda del modo di procedere che ritiene più appropriato nel singolo caso.

Art. 24 Standardizzazione dei tipi di informazione e di sorveglianza

Il presente articolo riguarda la standardizzazione tecnica e amministrativa dei tipi di informazione e di sorveglianza definiti nell'ordinanza.

Per standardizzazione di un tipo di informazione o di sorveglianza da parte del DFGP (*cpv. 1*) si intende la regolamentazione dei suoi dettagli tecnici e amministrativi nell'ordinanza del DFGP OE-SCPT (sulla nozione di tipo di informazione vedi il commento all'art. 26; sulla nozione di tipo di sorveglianza, vedi il commento all'art. 28). Le condizioni per questa standardizzazione sono da un lato l'esistenza del relativo standard internazionale e dall'altro la fattibilità e la proporzionalità della sua attuazione nella pratica.

Se queste condizioni non dovessero essere ancora essere adempiute per determinati tipi all'entrata in vigore della presente ordinanza, il DFGP rinuncia in un primo momento alla 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.

Art. 25 Informazioni e sorveglianze particolari

Tutti i tipi comuni di informazione e di sorveglianza sono menzionati negli articoli 24 e 25 e rispettivamente nelle sezioni 1 (art. 27) e 4-6 (art. 35-48) e 8-11 (art. 54-68) del 3° capitolo.

Le informazioni e le sorveglianze non espressamente elencate nella presente ordinanza sono le cosiddette misure speciali, effettuate dal Servizio SCPT o dalle persone da esso incaricate. Ciò corrisponde alla prassi anteriore 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

38 RS **780.11**

interessati devono tollerare l'esecuzione di simili misure di sorveglianza mettendo a disposizione del Servizio le interfacce già esistenti.

I fornitori devono tollerare anche l'accesso agli impianti (art. 52), in particolare devono mettere a disposizione gratuitamente gli accessi esistenti alle reti di comunicazioni pubbliche.

Art. 26 Tipi di informazione in generale

Il *capoverso 1* offre una panoramica sommaria dei diversi tipi di informazione definiti nelle sezioni 1 e 4-6 del capitolo 3 (art. 27 e 34-47). Per tipo di informazione 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.

Nella nuova ordinanza i tipi di informazione 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 informazione.

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. 35 e 40) e «informazioni sui servizi» (art. 36 e 41). Tale suddivisione corrisponde all'incirca alle precedenti informazioni A0 e A1 ed è volta a limitare il numero di informazioni per ogni tipo di informazione, al fine di facilitare e velocizzare il trattamento automatizzato.

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 informazione (art. 36-38) volti ad identificare gli utenti in caso di reati commessi via Internet (art. 22 nLSCPT).

Per i tipi di informazione di cui agli articoli 35, 40, 42 e 43 è in ogni caso possibile una ricerca flessibile dei nomi definita nell'articolo 27.

Secondo il *capoverso 2* le informazioni che devono essere consegnate dai fornitori nell'ambito della presente ordinanza possono essere richieste dalle autorità soltanto nella procedura prevista dalla presente ordinanza, ciò significa che le autorità presentano le domande di informazioni mediante il sistema di trattamento del Servizio SCPT oppure, alle condizioni di cui all'articolo 17 capoversi 2 e 3, al servizio SCPT per posta o fax o telefono, ma non le presentano mai direttamente alle persona obbligate a collaborare.

Art. 27 Tipi di informazione con ricerca flessibile dei nomi

Il presente articolo riassume quattro tipi di informazione supplementari che si basano sui tipi di informazione di cui agli articoli 35 (IR_4_NA), 40 (IR_10_TEL), 42 (IR_13_EMAIL) e 43 (IR_15_COM) e si distinguono da questi ultimi soltanto per il tipo di ricerca dei nomi:

- IR_5_NA_FLEX;

- IR_11_TEL_FLEX;
- IR_14_EMAIL_FLEX;
- IR_16_COM_FLEX.

La ricerca dei nomi è il criterio della ricerca secondo il capoverso 2 lettera a dei summenzionati articoli. Si tratta di una ricerca dei nomi fonetica e tollerante agli errori (ossia flessibile). Poiché l'interfaccia ETSI non consente di trasmettere istruzioni quanto al tipo di ricerca per le domande di informazioni e le risposte, sono definiti questi quattro tipi supplementari di informazione.

Le domande di informazioni secondo i nomi saranno in futuro svolte in modo automatico dai FST e dai fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari. Queste ricerche erano finora svolte dai collaboratori dei fornitori mediante la loro intelligenza umana. Per ottenere in futuro risultati almeno equivalenti con la ricerca automatica dei nomi, oltre alla ricerca letterale deve essere possibile effettuare anche una ricerca fonetica e tollerante agli errori (tipi di base secondo gli art. 35, 40, 42 e 43). In tal modo si tiene conto delle necessità delle autorità di perseguimento penale.

La pratica ha rivelato che la registrazione dei dati personali è spesso errata a causa di:

1. parti di nomi mancanti o invertiti nella loro successione;
2. errori ortografici;
3. traslitterazioni diverse di nomi da alfabeti stranieri nei diversi set di caratteri latini. Ciò può già essere avvenuto nel documento di identità ma spesso accade in occasione della registrazione, quando i dati personali sono rilevati o memorizzati nella banca dati dei clienti, poiché i sistemi IT spesso non permettono di usare tutti i caratteri diacritici esistenti;
4. trascrizioni diverse (p. es. inglese, francese) di nomi da caratteri non latini in caratteri latini.

La ricerca flessibile dei nomi non consiste quindi in un confronto esatto della sequenza di segni ma da una parte in una ricerca secondo la concordanza fonetica e dall'altra in un confronto delle componenti dei nomi (name matching), per esempio per individuare concordanze di parti di nomi e gli errori nella loro successione. Gli attuali sistemi di gestione delle banche dati contengono già funzioni di ricerca specializzate nella ricerca flessibile dei nomi. Per ulteriori dettagli sulla ricerca flessibile si rimanda al commento all'articolo 13 capoverso 2 OE-SCPT.

Art. 28 Tipi di sorveglianza

Il presente *articolo* offre una breve panoramica sui diversi tipi di sorveglianza definiti nelle sezioni 8-11 del capitolo 3 (art. 54-68). 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 (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 da sorvegliare (target ID). 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_23_NA_CC_IRI per l'accesso a Internet e la seconda del tipo RT_25_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.

Sezione 2: Garanzia della qualità

Art. 29 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.

Il *capoverso 1* elenca tre requisiti della qualità dei dati trasmessi. Per la lettera b va osservato che soltanto il trasferimento dei dati della sorveglianza e delle informazioni deve avvenire senza perdita di dati e interruzioni. 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.

Il *capoverso 2* disciplina 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 fino al punto di transizione (art. 12 cpv. 3 LSCPT). Dettagli sul punto di transizione sono forniti nell'allegato 2 dell'OE-SCPT. Il Servizio SCPT sostiene la persona obbligata a collaborare 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. 3*). 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. Le persone obbligate a collaborare con obblighi di sorveglianza sono i FST, eccetto quelli con obblighi di sorveglianza ridotti secondo l'articolo 51 e i fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari secondo l'articolo 52.

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 DFGP per i singoli livelli di gravità e informa, per scritto e alle scadenze regolari stabilite dal DFGP, 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. 30 Collegamenti test

Per *collegamento test* s'intende la sorveglianza tecnica di un servizio di comunicazione (p. es. telefonia mobile, accesso mobile a internet, conto di posta elettronica) o di un servizio di comunicazione derivato (p. es. servizi di messaggistica istantanea, chat) 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 test l'obbiettivo della sorveglianza è chiamato *target del test*. I dati usati o raccolti nell'ambito di un collegamento test (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, delle autorità di perseguimento penale e del SIC, autorizzati a effettuare un collegamento test.

Poiché sono usati solo per collegamenti test, i dati relativi ai test non sottostanno al segreto delle telecomunicazioni. Per i collegamenti test non è pertanto necessaria l'autorizzazione dell'autorità di approvazione e non devono essere neppure soddisfatti i requisiti dell'articolo 269 capoverso 1 CPP o dell'articolo 70 cpv. 1 PPM. Poiché per i collegamenti test non vi è un'autorità investita del procedimento, il Servizio SCPT può prendere conoscenza del contenuto dei dati relativi ai propri test senza doverne richiedere l'autorizzazione (art. 18 cpv. 2 nLSCPT).

Per i collegamenti test, 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 collegamenti test e al nome delle persone autorizzate a elaborare i dati relativi al test. I collegamenti test sono tuttavia protocollati in modo simile alle sorveglianze normali.

Pertanto, anche nel caso di un collegamento test il Servizio SCPT protocolla il trattamento dei dati di tutti i collegamenti test. Il Servizio SCPT gestisce anche un dato numero di collegamenti test, che può mettere a disposizione delle autorità di perseguimento penale e del SIC per test o formazioni. Questi sono considerati collegamenti test gratuiti del Servizio SCPT. I collegamenti test gratuiti del Servizio SCPT messi a disposizione delle autorità non sono fonte di alcun costo per i servizi di telecomunicazione necessari a tal fine né per i servizi di comunicazione derivati, a condizione che siano rispettate le regole dell'utilizzazione adeguata. Utilizzazioni straordinariamente costose devono essere dapprima convenute separatamente con il Servizio SCPT. In caso di non rispetto il Servizio SCPT fa salve le pretese di regresso.

Al mandato di sorveglianza, il Servizio SCPT deve apporre un'annotazione che indichi che si tratta in realtà di un collegamento test. Se per creare dati relativi ai test ha bisogno delle persone obbligate a collaborare, il Servizio SCPT può incaricarle di tale compito e dopo averle sentite allestisce un piano di test (*cpv. 2*). Inoltre, la persona obbligata a collaborare deve mettere gratuitamente e permanentemente a disposizione del Servizio SCPT, su sua richiesta, i collegamenti test 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.

L'utilizzazione dei collegamenti test soggiace alla regola dell'utilizzazione adeguata. Utilizzazioni straordinariamente costose devono essere dapprima convenute separatamente tra il Servizio SCPT e le persone obbligate a collaborare.

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 test.

Secondo il *capoverso 4*, oltre ai collegamenti test messi a loro disposizione gratuitamente dal Servizio SCPT, le autorità di perseguimento penale e il SIC possono eseguire a proprie spese dei test ai fini della garanzia della qualità della trasmissione del traffico delle comunicazioni e a scopi di formazione. Quindi da una parte vi sono i collegamenti test gratuiti del Servizio SCPT (cpv. 3) e dall'altra i collegamenti test a pagamento delle autorità di perseguimento penale e del SIC (cpv. 4). Affinché possa chiedere un collegamento test, un'autorità di perseguimento penale o il SIC 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 autorizzarli a trasmettere al Servizio SCPT le richieste necessarie per i collegamenti test. A proprie spese significa che le autorità di perseguimento penale e il SIC devono versare al Servizio SCPT per lo svolgimento di collegamenti test gli emolumenti secondo la pertinente ordinanza, 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 e il SIC assumono i costi per i

servizi di telecomunicazioni o di comunicazione derivati e per gli apparecchi terminali necessari ai rispettivi collegamenti test. Essi possono trasferire i dati ottenuti con i collegamenti test al sistema di trattamento del Servizio SCPT oppure direttamente a sé stesse. All'accesso del Servizio SCPT ai dati dei collegamenti test delle autorità di perseguimento penale e del SIC si applica per analogia l'articolo 18 capoverso 2 nLSCPT.

I collegamenti test effettuati su richiesta delle autorità di perseguimento penale o del SIC (collegamenti test delle autorità) devono seguire una procedura formale simile a quella per le sorveglianze usuali. L'autorità in questione deve trasmettere la richiesta al Servizio SCPT indicando lo scopo di utilizzazione, il tipo di sorveglianza e la durata del collegamento test che 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 indicando che si tratta di collegamenti di test delle autorità per verificare tali collegamenti. Previo emolumento e su richiesta, le persone autorizzate presso le autorità possono prorogare i collegamenti test al massimo per ulteriori 12 mesi. Al più tardi tre mesi prima della fine di un collegamento test, il Servizio SCPT invia una pertinente comunicazione alla persona autorizzata presso l'autorità che ha chiesto il collegamento test in questione. Il collegamento test rimane attivo se i requisiti per la proroga sono soddisfatti. In caso contrario il Servizio SCPT mette fine al collegamento trasmettendo l'incarico alla persona obbligata a collaborare.

Sezione 3: Garanzia della disponibilità a informare e sorvegliare

Art. 31 Verifica della disponibilità a informare e sorvegliare

Per disponibilità a informare s'intende che le seguenti persone obbligate a collaborare siano in grado di fornire o far fornire da terzi le seguenti informazioni concernenti i servizi da esse offerti (cfr. art. 18):

- i FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari di cui all'articolo 22: le informazioni di cui agli articoli 35–37 e 40–48 nonché di cui all'articolo 27 in combinato disposto con gli articoli 35, 40, 42 e 43;
- i FST, salvo quelli con obblighi di sorveglianza ridotti secondo l'articolo 51, e i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari di cui all'articolo 52: le informazioni di cui agli articoli 38 e 39.

Per disponibilità a sorvegliare s'intende che le seguenti persone obbligate a collaborare siano in grado di eseguire o far eseguire da terzi le sorveglianze concernenti i servizi da esse offerti (cfr. art. 50):

- i FST, salvo quelli con obblighi di sorveglianza ridotti secondo l'articolo 51, e i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari di cui all'articolo 52: le sorveglianze di cui agli articoli 54–68.

Per dimostrare la disponibilità a informare o a sorvegliare i fornitori summenzionati dovranno provare di essere in grado di fornire le informazioni 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 un terzo, i fornitori possono incaricare quest'ultimo di fornire la prova della disponibilità a informare e sorvegliare. In ogni caso è il fornitore a essere responsabile della prova.

Nella verifica della disponibilità a informare e sorvegliare il Servizio SCPT svolge i compiti di cui al *capoverso 3.* I verbali (*lett. e*) possono fungere da mezzo di prova in caso di controversia ed essere di aiuto per la prossima verifica della disponibilità a informare e sorvegliare.

Giacché ogni fornitore offre altri servizi, secondo il *capoverso 4* il Servizio SCPT stabilisce individualmente, secondo le regole del Dipartimento, la conferma per ogni fornitore, con determinati criteri di validità per il trasferimento dei dati. Fanno tra l'altro parte di questi criteri di validità le indicazioni sui sistemi, sui servizi e sui tipi di sorveglianza testati, i verbali dei test con gli allegati e le interfacce. Sono testati sia i sistemi del Servizio SCPT (ADMF[39], LEMF[40]) come pure quelli dei fornitori (ADMF, MF[41]/DF[42], IIF[43]). Nell'ambito dei test dei servizi, come la telefonia, è testato anche il tipo di tecnologia, ad esempio il VoLTE. I test per i tipi di sorveglianza sono in linea di massima effettuati per le sorveglianza in tempo reale (come RT_24_TEL_IRI, RT_25_TEL_CC_IRI).

Art. 32 Durata di validità dell'attestato

A titolo preliminare occorre rilevare che le conferme concesse secondo la pratica anteriore del Servizio SCPT, i cosiddetti «Statement of Compliance» o «Confirmation of Compliance», non valgono come attestato della disponibilità a informare e a sorvegliare ai sensi dell'articolo 33 capoverso 6 LSCPT.

Non appena viene fornita la prova della disponibilità a informare e a sorvegliare, il Servizio SCPT rilascia alla persona obbligata a collaborare un attestato che, secondo il *capoverso 1* 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 sul trasferimento 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.

39 ADMinistration Function (vgl. ETSI TS 101 671)
40 Law Enforcement Monitoring Facility (vgl. ETSI TS 101 671)
41 Mediation Function (vgl. ETSI TS 101 671)
42 Distribution Function (vgl. ETSI TS 101 671)
43 Internal Interception Function (vgl. ETSI TS 101 671)

Art. 33 Procedura di collaudo

Questa disposizione conferisce al DFGP 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. 34 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 il fornitore non è in grado in più casi di garantire il trasferimento 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. 35 Tipo d'informazione IR_4_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. i*).

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 informazione 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_6_NA (*art. 36*).

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_4_NA (art. 35) e IR_10_TEL (art. 40). Il fornitore Y risponde al tipo d'informazione IR_4_NA (art. 35) con cinque risultati (considerati cinque pacchetti di dati, cfr. il commento all'art. 17 cpv. 4) e al tipo d'informazione IR_10_TEL (art. 40) 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 20.

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.

  Osservazione: nella presente ordinanza l'espressione «se del caso» (if applicable) significa che la normativa in questione riguarda soltanto tale caso di applicazione, ad esempio un numero SIM (ICCID) può essere consegnato soltanto se si tratta di un servizio di telefonia mobile. Può tuttavia succedere

che, in un caso speciale, il numero SIM non sia disponibile presso un servizio di telefonia mobile;

- 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 designazioni che usa abitualmente, 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 gratuiti o prepagati (prepaid), 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**. Per cercare una sequenza di segni (*lett. a, c, d ed e*) il fornitore deve compiere una cosiddetta ricerca letterale secondo l'articolo 13 capoverso 1 OE-SCPT. In via di principio si tratta di una ricerca esatta, tuttavia la sequenza di segni ricercata e le sequenze di segni con le quali è compiuto il confronto durante la ricerca sono normalizzate nel seguente modo: le lettere che non fanno parte dell'alfabeto latino di 26 lettere sono convertite, all'inizio della ricerca, in 1 o 2 lettere dell'alfabeto latino secondo un elenco di conversione. Una ricerca

esatta al 100 per cento nella pratica spesso non darebbe i risultati desiderati, poiché sono utilizzate lettere diverse che non possono rappresentare tutti i caratteri e i segni di interpunzione nei nomi sono spesso impiegati in modo scorretto o dimenticati.

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_7_IP (art. 37), IR_8_IP_NAT (art. 38) e IR_9_NAT (art. 39) (cfr. il commento agli art. 37, 38 e 39).

Art. 36 Tipo di informazione IR_6_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), nella misura in cui il fornitore ha obblighi di sorveglianza. I fornitori senza obblighi di sorveglianza forniscono i dati disponibili. Ciò significa che dalla risposta non deve trasparire quando, come e dove sono stati utilizzati gli apparecchi.

Il periodo di validità indicato nella risposta si riferisce ai tre parametri di cui alle lettere b (identificativo del servizio), c (IMSI e MSISDN) ed e (numero SIM) del capoverso 1. Come già fatto notare questo periodo di validità non fa riferimento agli identificativi degli apparecchi. Se uno dei tre parametri citati si è modificato nel periodo indicato nella domanda, la persona obbligata a collaborare deve consegnare un numero di pacchetti dati equivalente ai vari stati delle informazioni. Poiché il codice PUK è strettamente vincolato a una carta SIM, per il parametro di risposta di cui al capoverso 1 lettera f (codice PUK) non deve essere indicato alcun periodo di validità. La sua validità risulta direttamente dalla validità del numero SIM (*cpv. 1 lett. e*).

Art. 37 Tipo di informazione IR_7_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 statico e attribuito univocamente, giacché non è possibile evincere da quest'ultimo se è o è stato assegnato in modo statico o dinamico. Inoltre c'è anche l'assegnazione univoca dell'indirizzo IP (cfr. art. 38 e 39).

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 non si vede se l'indirizzo IP è stato assegnato univocamente, soltanto il risultato di questo tipo di informazione può fare chiarezza.

Nella domanda di informazioni è importante da una parte indicare un momento sufficientemente preciso, al secondo, visto che per gli indirizzi IP 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. Dall'altra, si dovrebbe tenere conto di un intervallo di tolleranza a causa della possibile inesattezza degli orologi di sistema. Nella domanda di informazioni si può pertanto indicare un intervallo di tempo invece di un momento preciso (*cpv. 2 lett. b*).

Se una domanda di informazioni del tipo IR_7_IP fornisce più risultati, ci sono due possibili cause che le autorità autorizzate devono poi chiarire con il fornitore:

1) L'intervallo di tempo nella domanda è troppo grande. Durante tale intervallo, l'indirizzo IP in questione è stato assegnato a più utenti.
2) L'indirizzo IP in questione non è stato assegnato univocamente.

Nel primo caso la domanda d'informazioni del tipo IR_7_IP va ripresentata con un intervallo di tempo minore.

Nel secondo caso va presentata una nuova domanda di informazioni del tipo IR_8_IP (NAT) per la quale vanno tuttavia indicati ulteriori criteri di ricerca (cfr. il commento all'art. 38).

Se una domanda d'informazioni del tipo IR_7_IP non dà alcun risultato, probabilmente è stato scelto un intervallo troppo breve o l'indicazione temporale era imprecisa, per esempio a causa di un calcolo errato dei fusi orari.

Art. 38 Tipo di informazione IR_8_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) un numero di utenti che può raggiungere le migliaia può 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 del collegamento (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 dei singoli collegamenti di destinazione. Sotto il profilo della protezione dei dati vanno implementate procedure per le quali la memorizzazione della destinazione del collegamento non è necessaria e può quindi essere omessa.

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* stabilisce le indicazioni da fornire in caso di identificazione dell'utente. In caso di mancata identificazione, non sono forniti risultati. Se l'identificazione ha avuto diversi risultati positivi, questi pacchetti di dati vanno consegnati se il numero di risultati positivi non eccede il valore massimo indicato. Altrimenti deve essere comunicato soltanto il numero di risultati positivi (art. 18 cpv. 6).

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 procedura NAT non deterministica, l'indirizzo IP pubblico e il numero di porta della destinazione del collegamento (p. es. Webserver) nonché il tipo di protocollo di trasporto, ad esempio TCP, UDP (*lett. c-e*);
- l'indicazione della data e dell'ora (*lett. f*). Nella domanda d'informazioni, invece di un momento preciso si può indicare un intervallo di tempo, in particolare per compensare possibili inesattezze degli orologi di sistema. L'indicazione deve essere sufficientemente precisa e l'intervallo di ricerca il più breve possibile per evitare falsi risultati positivi (cfr. commenti dell'art. 37).

Riassumendo, per la procedura sono previste le seguenti tappe:

- 1ª tappa (fa parte dei lavori preliminari e non è parte di questo tipo di informazione): IP history per l'account utente ricercato presso il gestore del servizio Internet (server) per determinare i dettagli di connessione del login in questione.

- 2ª tappa: domanda di informazioni al fornitore di accesso a Internet (indicando i dettagli di connessione di un login concreto determinato nella 1ª tappa) per identificare gli utenti.

- 3ª tappa (non fa parte di questo tipo di informazione): domanda di informazione al fornitore di accesso Internet (indicazione degli identificativi dell'utente e del servizio trovati nella 2ª tappa), per consultare i dati personali degli utenti.

Dettagli sulla 1ª tappa (fa parte dei lavori preliminari e non di questo tipo di informazione): chiedere la cosiddetta IP history per uno specifico account utente presso il fornitore del server, ossia presso la destinazione della connessione (esempio: 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), destinazione del collegamento (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. Il fornitore di accesso comunica quindi gli identificativi dell'utente e del servizio (p. es. MSISDN, IMSI) in quanto risultato di questo tipo di informazione.

Dettagli sulla 3ª tappa (non fa parte di questo tipo di informazione): l'autorità di perseguimento penale presenta alla fine un'ulteriore domanda di informazioni (IR_4_NA) per consultare i dati personali corrispondenti agli identificativi degli utenti e dei servizi (p. es. MSISDN, IMSI) trovati nella seconda tappa.

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, per questo tipo di informazione, in considerazione dell'assegnazione dinamica degli elementi di indirizzo occorre cercare nei metadati conservati a chi era attribuito l'elemento di indirizzo ricercato nel momento in questione. È possibile che questa ricerca debba essere effettuata in più tappe, seguendo la traccia nota fino all'origine e alla destinazione della connessione. Non si tratta però di una sorveglianza retroattiva perché la connessione cercata è già nota e se ne deve scoprire soltanto l'effettiva origine o destinazione. I dati sull'assegnazione di indirizzi IP dinamici e, se necessario per identificare l'utenza, sulla traduzione di indirizzi IP e numeri di porto devono essere memorizzati da parte del fornitore di accesso per sei mesi (art. 21 cpv. 2 secondo periodo nonché art. 22 cpv. 2 secondo periodo e cpv. 4 nLSCPT e art. 21 cpv. 2 OSCPT). I FST con obblighi di sorveglianza ridotti di cui all'articolo 51 sono esentati dall'obbligo di conservare i metadati (cfr. anche il commento all'art. 18 cpv. 4).

Art. 39 Tipo di informazione IR_9_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.

Indicazione: in seguito la traduzione NAT è chiamata *operazione NAT* Sono possibili due tipi di ricerca: «prima» e «dopo» l'operazione NAT, da intendersi in senso temporale e dal punto di vista delle persone obbligate a collaborare:

- Ricerca 1

  Sono noti i dati **dopo** l'operazione NAT e si cercano quelli **prima**; ad esempio: si conoscono l'indirizzo IP sorgente pubblico e il numero di porta risultanti dall'operazione NAT, si cerca l'indirizzo IP precedente alla stessa.
  Analogamente all'articolo 38 capoverso 2, la domanda di informazioni sulle operazioni NAT deve contenere le seguenti indicazioni (*cpv. 2*):

  - l'indirizzo IP sorgente e il numero di porta dopo l'operazione 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 dell'operazione NAT (*lett. f*);

- qualora fosse necessario per l'identificazione (dipende dal tipo di procedura NAT), la domanda di informazioni deve indicare l'indirizzo IP pubblico e il numero di porta (*lett. c e d*) della destinazione del collegamento.

- 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** l'operazione NAT (p. es. l'indirizzo IP sorgente pubblico).
  La domanda di informazioni sulle operazioni NAT deve contenere le seguenti indicazioni (*cpv. 2*):

  - l'indirizzo IP sorgente e il numero di porta sulle operazioni 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 dell'operazione NAT (*lett. f*);
  - qualora fosse necessario per l'identificazione (dipende dal tipo di procedura NAT), la domanda di informazioni deve indicare l'indirizzo IP pubblico e il numero di porta (*lett. c e d*) della destinazione del collegamento.

Esempio di ricerca 1: se il tipo d'informazione IR_8_IP (NAT) di cui all'articolo 38 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 un'operazione 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 dell'operazione 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. 40 Tipo di informazione IR_10_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 gli identificativi (*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_12_TEL (art. 41).

Questo tipo di informazione si applica sia agli abbonamenti che alle offerte prepagate e gratuite. Data l'analogia tra le disposizioni, si rimanda al commento all'articolo 35.

Analogamente all'articolo 35, 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. 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[44] 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 35 capoverso 2, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e come vanno usati (cfr. il commento all'art. 35 cpv. 2). Per una ricerca di sequenze di segni (*lett. a, c, d e f*) il fornitore deve

44 RS **784.101.112**

compiere una cosiddetta ricerca letterale secondo l'articolo 13 capoverso 1 OE-SCPT (cfr. commento all'art. 35 cpv. 2).

Si distingue tra i criteri delle lettere h, j e k e quello della lettera i. Le lettere h, j e k definiscono univocamente il tipo di servizi di telefonia e multimedia, ma, contrariamente alla lettera i, 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[45] 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. 41 Tipo di informazione IR_12_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 40.

Come nel caso dell'articolo 36 capoverso 1, 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*) si rimanda al commento all'articolo 36 capoverso 1 lettera d.

Il periodo di validità indicato nella risposta si riferisce ai tre parametri di cui alle lettere b (elemento di indirizzo), c (IMSI) ed e (numero SIM) del capoverso 1. Come già fatto notare questo periodo di validità non fa riferimento agli identificativi degli apparecchi. Se uno dei tre parametri menzionati si è modificato nel periodo indicato nella domanda, la persona obbligata a collaborare deve consegnare un numero di pacchetti dati equivalente ai vari stati delle informazioni. Poiché il codice PUK è strettamente vincolato a una carta SIM, per il parametro di risposta di cui al capoverso 1 lettera f (codice PUK) non deve essere indicato alcun periodo di validità. La sua validità risulta direttamente dalla validità del numero SIM (*cpv. 1 lett. e*).

Analogamente all'articolo 36 capoverso 2, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e come vanno usati (cfr. commento all'art. 36 cpv. 2).

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

45 RS **784.104**

Art. 42 Tipo di informazione IR_13_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 al commento all'articolo 40. 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.

Se pertinenti, secondo il *numero 5* vanno indicati tutti gli indirizzi di posta elettronica ai quali sono automaticamente trasmessi i messaggi destinati all'indirizzo di posta elettronica in questione, ad esempio nel caso di una mailing list. La mailing list è 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. In questo esempio, devono essere indicati gli indirizzi di posta elettronica dei membri della mailing list.

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 40, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e le relative modalità d'uso (cfr. il commento all'art. 40 cpv. 2). Per una ricerca di sequenze di segni (*lett. a, c, d e f*) il fornitore deve compiere una cosiddetta ricerca letterale secondo l'articolo 13 capoverso 1 OE-SCPT (cfr. commento all'art. 35 cpv. 2).

Art. 43 Tipo di informazione IR_15_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 40–42.

Anche in questo caso, il *capoverso 1* stabilisce quali informazioni devono essere fornite sugli utenti di altri servizi di telecomunicazione o di servizi di comunicazione derivati. L'identificativo di cui alla lettera c numero 5 può ad esempio essere un identificativo univoco specifico di un'applicazione o di un apparecchio utilizzato per le comunicazioni di una App. Un identificativo di questo genere garantisce che le comunicazioni di una determinata App siano inviate a un determinato apparecchio (p. es. Device Token des Apple Push Notification service, Registration Identifier des Google Cloud Messaging, Channel URI des Windows Push Notification Service). Questo parametro può essere utilizzato per fornire, nella risposta, un identificativo univoco specifico di un'applicazione o di un apparecchio.

Analogamente agli articoli 40–42, il *capoverso 2* stabilisce i criteri di ricerca per il tipo di informazione e come vanno usati (cfr. commento all'art. 40 cpv. 2). Per una ricerca di sequenze di segni (*lett. a, c, d e f*) il fornitore deve compiere una cosiddetta ricerca letterale secondo l'articolo 13 capoverso 1 OE-SCPT (cfr. commento all'art. 35 cpv. 2). Il parametro di cui alla lettera i può ad esempio essere utilizzato per una domanda d'informazioni mediante identificativo univoco specifico di un'applicazione o di un apparecchio.

Sezione 6: Altri tipi di informazione

Art. 44 Tipo di informazione IR_17_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. 45 Tipo di informazione IR_18_ID: copia del documento di identità

L'articolo 20 definisce quali dati identificativi dell'utente devono essere registrati, nel settore della telefonia mobile, 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.

Con questo tipo di informazione le autorità abilitate possono consultare la copia memorizzata di un documento d'identità di un determinato utente o servizio. L'autorità abilitata deve precisare nella domanda di informazioni il momento 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. Per i servizi di accesso alla rete la domanda può essere effettuata in base a un numero di apparecchio. Una relazione diretta tra l'identificativo dell'apparecchio e la copia del documento d'identità sussiste soltanto se l'apparecchio è stato ottenuto al momento della conclusione del contratto e della registrazione del documento d'identità. Inoltre, vi è sempre la possibilità di cedere l'apparecchio a terzi (p. es. vendita), il che non può essere monitorato dal fornitore.

Art. 46 Tipo di informazione IR_19_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. 47 Tipo di informazione IR_20_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

legittimata deve precisare nella domanda di informazioni il momento e l'identificativo univoco dell'utente o del servizio a cui si riferisce la richiesta (*cpv. 2*). Per i servizi di accesso alla rete la domanda può essere effettuata in base a un numero di apparecchio. Una relazione diretta tra l'identificativo dell'apparecchio e la copia del documento d'identità sussiste soltanto se l'apparecchio è stato ottenuto al momento della conclusione del contratto e della registrazione del documento d'identità. Inoltre, vi è sempre la possibilità di cedere l'apparecchio a terzi (p. es. vendita), il che non può essere monitorato dal fornitore.

Art. 48 Tipo di informazione IR_21_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). Devono conservare questi dati per sei mesi in modo retroattivo. Sarebbe tuttavia possibile che, ad esempio per una sorveglianza effettuata retroattivamente siano in un momento successivo chiesti dati sulla copertura d'antenna che risalgono a più di sei mesi prima. In questo caso le persone obbligate a collaborare dovrebbero fornire tali dati nella misura in cui sono ancora disponibili.

Questo tipo d'informazione corrisponde all'attuale informazione A3. Si tratta innanzitutto dei dati relativi all'ubicazione delle antenne di telefonia mobile e dei punti di accesso WLAN pubblici. La trasmissione di altri dati, come il tipo di tecnologia di telefonia mobile e le frequenze, non è attualmente prevista nello standard ETSI. Si prevede di aggiungere questo tipo di trasmissione in una futura revisione parziale della presente ordinanza, non appena ve ne saranno le condizioni nello standard ETSI. Lo standard proprietario per la trasmissione dei risultati di una ricerca d'emergenza EP_35_PAGING contiene queste informazioni.

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. La direzione di trasmissione è disponibile nello standard ETSI. Può però essere utilizzato in modo ragionevole soltanto se effettivamente esiste, pertanto il testo dell'ordinanza contiene l'espressione «se del caso». Per la ricerca d'emergenza è stato sviluppato un meccanismo particolare, che consente la trasmissione di attributi come «omnidirectional». Questo meccanismo non è tuttavia disponibile nel presente contesto.

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. In caso di domande per mezzo delle coordinate geografiche (*lett. a*), queste ultime vanno indicate con sufficiente precisione e riferite a un'unica ubicazione. Il fornitore deve fornire i dati tecnici per tutti gli elementi di rete che si trovano in un raggio di 50 m attorno all'ubicazione designata. Questo intervallo di tolleranza garantisce che l'elemento di rete ricercato possa essere trovato anche con un ricerca in coordinate geografiche molto precise. 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_32_PREP_COV (art. 64).

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

Art. 49 Ordine di sorveglianza del traffico delle telecomunicazioni

La disposizione corrisponde essenzialmente all'articolo 15 dell'OSCPT del 31 ottobre 2001[46] 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 della sorveglianza o identificativo da sorvegliare [target ID]) 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 e se una sorveglianza del SIC ha ricevuto l'autorizzazione e il nullaosta di cui agli articoli 29–31 LAIn (art. 16 lett. a n. 2 nLSCPT).

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.

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 la fattispecie penale è possibile ordinare una sorveglianza ai sensi degli articoli 269 (sorveglianze in tempo reale) oppure 273 CPP e 70*d* PPM (sorveglianza retroattiva).

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 identificativi 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.

46 RS **780.11**

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. Nel caso della lettera k, 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 di una persona tenuta al segreto d'ufficio o professionale ed eventualmente applicare la procedura di cui alla lettera l.

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

Art. 50 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 52. 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. 31–34). Le fasi test e le fasi pilota non sono considerate inizio dell'esercizio commerciale.

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'OE-SCPT.

Il *capoverso 4* disciplina il periodo di riferimento e gli elementi del traffico delle telecomunicazioni da sorvegliare. Il Servizio SCPT, nel caso della sorveglianza in tempo reale, invia alle persone obbligate a collaborare 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 sorvegliato (target ID, 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 procedura operativa ordinaria (routing, segnalazione). In linea di massima, le procedure operative ordinarie per l'utente (target) o il servizio sorvegliato (target) non sono diverse da quelle per un utente o servizio non 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 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.

Nello scenario B deve semplicemente fare in modo che siano sorvegliati i metadati e i contenuti che controlla nell'ambito della procedura operativa ordinaria 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 sorvegliato (target ID) sono associati altri identificativi, i fornitori devono garantire che anche questi siano sorvegliati nell'ambito del tipo di sorveglianza. I casi possibili di identificativi associati sono

definiti dal Servizio SCPT dopo aver sentito individualmente il fornitore (p. es. indirizzi e-mail alias di un fornitore di servizi di posta elettronica).

Art. 51 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 propri criptaggi, garantire l'accesso ai propri impianti e, su richiesta, trasmettere i metadati relativi alle telecomunicazioni della persona sorvegliata di cui dispongono (art. 26 cpv. 2 nLSCPT). Nella consultazione è stato proposto di sostituire, nelle ordinanze, la nozione «settore dell'istruzione» con quella di «settore dell'istruzione e della ricerca». È stato dato seguito a questa richiesta.

Il *capoverso 1* specifica le condizioni in base alle quali il Servizio SCPT può, su richiesta, prendere una decisione in cui dichiara che un FST ha obblighi di sorveglianza ridotti. Da quel momento il FST richiedente non ha alcun obbligo oltre ai summenzionati obblighi minimi in materia di sorveglianza. Il Servizio SCPT può dichiarare tale un FST che offre i propri servizi di telecomunicazione soltanto nel settore dell'istruzione e della ricerca (lett. a) o che non raggiunge entrambi i valori di cui alla lettera b. Se, dopo aver consultato la documentazione, il Servizio SCPT giunge alla conclusione che il FST adempie le condizioni di cui al capoverso 1, prende una decisione in tal senso e la comunica al FST interessato. La disponibilità a sorvegliare decade con l'emanazione della pertinente decisione. Il Servizio SCPT deve compiere i passi necessari per poter continuare a eseguire le sorveglianze (art. 17 lett. e e art. 26 cpv. 2 lett. b nLSCPT; cfr. anche il commento all'art. 53, accesso agli impianti).

Secondo la *lettera a*, il Servizio SCPT deve dichiarare che i FST che offrono i propri servizi esclusivamente nel settore dell'istruzione e della ricerca hanno obblighi di sorveglianza ridotti e sottostanno soltanto all'obbligo legale minimo per il fatto stesso che operano solo in tale settore. La prima condizione di cui alla *lettera b numero 1* per considerare che un FST ha obblighi di sorveglianza ridotti è che negli ultimi dodici mesi abbia ricevuto incarichi di sorveglianza concernenti meno di dieci diversi obiettivi. A tal fine è determinante la data del 30 giugno. La disposizione si riferisce al numero totale delle sorveglianze, in tempo reale e retroattive. Si utilizza un criterio consolidato, quello del numero degli incarichi di sorveglianza. L'articolo 26 capoverso 6 non prevede tuttavia espressamente un tale criterio. La formulazione aperta (termini «può» e «in particolare») danno al Consiglio federale la libertà di scegliere altri criteri oggettivi. La statistica della sorveglianza delle telecomunicazioni degli ultimi anni mostra che i fornitori rilevanti sotto il profilo della sorveglianza delle telecomunicazioni hanno dato luogo a un determinato numero di incarichi di sorveglianza. Quindi, è relativamente sicuro imporre soltanto obblighi di sorveglianza minimi ai FST meno rilevanti che non

raggiungono un determinato numero di incarichi di sorveglianza. In tal modo il principio di proporzionalità è meglio salvaguardato.

Inoltre, secondo la *lettera b numero 2*, il FST che non raggiunge un fatturato annuo di 100 milioni di franchi per due esercizi consecutivi può essere riconosciuto dal Servizio SCPT come FST con obblighi di sorveglianza ridotti. Questo criterio è ulteriormente limitato dal fatto che viene preso in considerazione soltanto il fatturato annuo realizzato con servizi di telecomunicazione o servizi di comunicazione derivati.

Si presume che con l'applicazione di queste soglie il numero di FST tenuti alla sorveglianza attiva si ridurrà da circa 600 a circa 20–30. L'esenzione da determinati obblighi di sorveglianza non dovrebbe comunque provocare 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. Non sono infatti esentati dall'obbligo di fornire, su richiesta, i metadati del traffico delle telecomunicazioni della persona sorvegliata di cui dispongono (art. 26 cpv. 6 nLSCPT). Il Servizio SCPT deve intraprendere quanto necessario affinché le sorveglianze possano continuare a essere effettuate (art. 17 lett. e LSCPT).

Per i gruppi d'imprese secondo il *capoverso 2* si rimanda all'articolo 22 capoverso 2. Questa disposizione disciplina il caso 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. 22).

Il *capoverso 3* impone un obbligo di comunicazione ai FST con obblighi di sorveglianza ridotti. Se non dovesse più fornire i propri servizi esclusivamente nel settore dell'istruzione e della ricerca (*lett. a*) o dovesse raggiungere il valore di cui al capoverso 1 lettera b numero 2 per il secondo esercizio consecutivo (*lett. b*), un FST deve comunicare tali fatti al Servizio SCPT entro tre mesi dalla conclusione dell'esercizio annuale, presentando i relativi giustificativi. Nella consultazione è stato criticato il fatto che gli obblighi dei FST con obblighi di sorveglianza ridotti non siano chiari. La presente ordinanza sceglie tuttavia di non disciplinare insieme la portata degli obblighi delle diverse categorie e sottocategorie di persone obbligate a collaborare ma di farlo nell'ambito della normativa materiale. La tabella alla fine del presente rapporto esplicativo dà una panoramica degli obblighi delle diverse persone obbligate a collaborare.

Il *capoverso 4* permette al Servizio SCPT di consultare altri dati per verificare il superamento o il mancato raggiungimento dei valori di cui al capoverso 4 e decidere riguardo al FST.

Analogamente a quanto previsto dall'articolo 22 capoverso 5, 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 decide che non è più considerato un FST con obblighi di sorveglianza ridotti (*cpv. 5*).

Art. 52 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 22, 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 da adempiere: aver svolto incarichi di sorveglianza di almeno dieci diversi obiettivi (target) negli ultimi 12 mesi. La lettera a riprende il criterio dell'articolo 27 capoverso 3 nLSCPT del «gran numero di utenti». Dal punto di vista della sorveglianza delle telecomunicazioni è difficile dare una definizione assoluta del concetto di gran numero di utenti, tanto più se occorre definirlo in relazione con l'offerta di diversi servizi tecnici. Per questo motivo nella lettera a viene utilizzato un criterio che ha dato buoni risultati nella pratica, il criterio del numero di incarichi di sorveglianza. La statistica della sorveglianza delle telecomunicazioni degli ultimi anni mostra che il numero di incarichi di sorveglianza riflette il concetto di gran numero di utenti in modo affidabile e adeguato al tipo di servizio offerto. Nel contempo questo criterio copre la proporzionalità, nella misura in cui riguarda soltanto fornitori veramente rilevanti per la sorveglianza delle telecomunicazioni. Dato che le due disposizioni disciplinano lo stesso oggetto si rimanda al commento all'articolo 22.

Gli obblighi da osservare sono quelli previsti per i FST, ossia in particolare gli obblighi previsti dall'articolo 26 capoversi 1-5 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. 53 Accesso agli impianti

Il Servizio SCPT svolge o fa svolgere a terzi (art. 26 cpv. 2 lett. b 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. 51) o non sono in grado di eseguire attivamente le persone obbligate a collaborare. Inoltre, il Servizio SCPT o i terzi da esso incaricati eseguono le sorveglianze non standardizzate (art. 32 cpv. 2 nLSCPT). 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, l'accesso fisico e l'accesso a distanza 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. Nella misura in cui ciò è necessario per la sorveglianza, le persone obbligate a collaborare allestiscono, d'intesa con il Servizio SCPT o i terzi incaricati, nuovi accessi alla rete a spese del Servizio SCPT.

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

Art. 54 Tipo di sorveglianza RT_22_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 55, il presente tipo di sorveglianza prevede soltanto la trasmissione dei metadati del traffico delle telecomunicazioni; è impiegato soltanto nel caso degli accessi a Internet da rete mobile (*cpv. 1*) 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 sorveglianza delle applicazioni sono infatti previsti appositi tipi 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.

Il *capoverso 2* definisce i metadati del traffico delle telecomunicazioni, inviato o ricevuto tramite il servizio di accesso alla rete sorvegliato, che vanno trasmessi in tempo reale. 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 ad esempio la modifica del servizio portante (*bearer modification*) o la *location update*.

Il *capoverso 3* specifica i dati da includere nell'indicazione dell'ubicazione di cui al capoverso 2 lettera h. La persona obbligata a collaborare può in questo caso scegliere tra tre alternative per la trasmissione delle indicazioni dell'ubicazione. Riguardo alle indicazioni dell'ubicazione fornite dalla rete deve apporre una pertinente annotazione, poiché tali ubicazioni sono verificate e quindi più affidabili di quelle che provengono da un apparecchiatura terminale o da un'applicazione.

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 univoca. 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 se ogni settore dispone di un proprio identificativo (p. es. Cell ID). Nel caso di una cella semplice, la direzione di trasmissione della cella indica l'angolo in gradi [°] tra il nord geografico e la trasmissione principale, invece per le celle complesse con molteplici direzioni di trasmissione e per le celle onnidirezionali (trasmissione equivalente in tutte le direzioni) questo campo resta vuoto. Se disponibile, deve essere indicato il tipo di tecnologia di telefonia mobile. Per il 2G e il 3G questa comunicazione non è possibile perché non è disponibile nello standard. È invece possibile per il 4G che dispone del parametro «Radio Access Technology (RAT)» che può contenere l'indicazione «4G» o «WiFi».

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. 55 Tipo di sorveglianza RT_23_NA_CC_IRI: sorveglianza in tempo reale dei contenuti e dei metadati per i servizi di accesso alla rete

Il tipo di sorveglianza definito nel presente articolo 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 54.

Come spiegato nel commento all'articolo 50 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 che sono tuttavia disponibili nell'ambito del tipo di sorveglianza RT_24_TEL_IRI (art. 56) o RT_25_TEL_CC_IRI (art. 57).

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. 56 Tipo di sorveglianza RT_24_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 57. Tuttavia, al contrario di quanto previsto dall'articolo 57, nell'ambito di un incarico di sorveglianza secondo l'articolo 56 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 possono trasferiti 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 (lett. e n. 9). Per le spiegazioni relative all'indicazione dell'ubicazione si veda il commento all'articolo 54 capoverso 3.

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. 57 Tipo di sorveglianza RT_25_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[47] 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 56.

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. 58 Tipo di sorveglianza RT_26_EMAIL_IRI: sorveglianza in tempo reale dei metadati per servizi di posta elettronica

Analogamente all'articolo 59 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[48]). Le nuove disposizioni eliminano questa restrizione. Tecnicamente la sorveglianza e il trasferimento 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. 74).

A differenza dell'articolo 59, nell'ambito di un incarico di sorveglianza secondo l'articolo 58 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.

47 RS **784.101.112**
48 Cfr. anche FF **1998** III 3319 3356 ad art. 13 cpv. 3

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. 42).

Art. 59 Tipo di sorveglianza RT_27_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. 58). Il fornitore deve sopprimere i propri criptaggi (art. 26 cpv. 2 lett. c nLSCPT).

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*. Osservazione: vi è sorveglianza retroattiva anche per la corrispondenza postale (cfr. art. 16 lett. c).

In virtù delle competenze che l'articolo 31 nLSCPT conferisce al Consiglio federale, nella sezione 10 del capitolo 3 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 nell'articolo 21 capoverso 2.

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[49], non devono essere conservati soltanto i metadati delle comunicazioni, dei login o degli accessi alla rete effettivamente riusciti, bensì anche quelli dei tentativi di comunicazione.

Nei servizi di telefonia o multimedia è considerato un tentativo di comunicazione la situazione in cui un collegamento è stato instaurato con successo, ma la comunicazione non è stabilita perché 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 la trasmissione 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.

I metadati dei tentativi di comunicazione devono essere tuttavia conservati dalle persone obbligate a collaborare soltanto conformemente all'articolo 50 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 dispone sotto il profilo tecnico.

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 (Target ID) i relativi metadati non si potrebbero trovare, poiché nei metadati conservati il numero sorvegliato (Target ID) 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).

Art. 60 Tipo di sorveglianza HD_28_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.

Le *lettere a–i* 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*), in

49 FF **2013** 2283 2336.

alternativa alla fine può essere indicata la durata della sessione; il tipo (p. es. xDSL, modem via cavo, WLAN, rete mobile) e il risultato (p. es. riuscito) dell'accesso alla rete (*lett. b*); l'identificativo utilizzato per l'autenticazione dell'utente nel punto d'accesso sorvegliato, ad esempio il nome utente (*lett. c*); gli indirizzi IP o i settori di indirizzi assegnati al target dal fornitore del servizio di accesso e al loro tipo (*lett. d*). Se disponibili vanno inoltre memorizzati e trasmessi l'identificativo univoco dell'apparecchio terminale mobile utilizzato del target (*lett. e*) e il volume di dati caricato e scaricato durante la sessione (*lett. g*).

Le indicazioni relative all'ubicazione (*lett. g e h*) corrispondono all'ubicazione dell'antenna della cella che serve il target di rete mobile per l'accesso a commutazione di pacchetto alla rete e all'ubicazione del punto d'accesso WLAN pubblico che serve il target mediante WLAN. Devono essere fornite le indicazioni relative all'ubicazione all'inizio e alla fine di ciascuna sessione di accesso alla rete del target che ha avuto luogo durante il periodo di sorveglianza, vale a dire se l'inizio o la fine della sessione o entrambe rientrano nel periodo di sorveglianza. Se disponibili vanno fornite anche le indicazioni relative all'ubicazione durante la sessione.

In caso di accesso alla rete mediante rete mobile devono inoltre essere trasmesse, oltre ai dati menzionati nelle lettere a–f, le indicazioni relative all'ubicazione (*lett. g*). La persona obbligata a collaborare, conformemente alla lettera g, può scegliere tra tre modi di trasmettere le indicazioni relative all'ubicazione.

In caso di accesso alla rete mediante WLAN pubblico (*lett. h)* devono inoltre essere trasmesse, oltre ai dati menzionati nelle lettere a–f, le seguenti informazioni:

- il BSSID (indirizzo MAC del punto di accesso);
- se disponibile il SSID (in forma leggibile per l'uomo);
- se disponibile, le informazioni sull'ubicazione sotto forma di coordinate geografiche e/o indirizzo postale del punto d'accesso WLAN utilizzato dal target;
- il nome utente, come noto alla persona obbligata a collaborare (verifica non necessaria);
- il tipo di autenticazione dell'utente (p. es. SMS, EAPSIM, Voucher);
- le informazioni supplementari disponibili sull'autenticazione dell'utente (numero di telefono, indirizzo MAC, se pertinente l'IMSI, l'identificativo dell'utente e la password impiegati per l'autenticazione); e
- l'indirizzo IP del punto di accesso WLAN.

In caso di accesso alla rete via rete mobile o WLAN pubblico devono inoltre essere trasmesse, se pertinenti, le informazioni disponibili sull'ubicazione relative alla navigazione marittima (nome e numero della nave) o alla navigazione aerea (codice della linea aerea, registrazione dell'aeromobile secondo il registro degli aeromobili, numero di volo della linea aerea).

In caso di accesso alla rete fissa (*lett. i*) devono essere trasmessi, oltre ai dati menzionati alle lettere a–f, anche gli elementi di indirizzo dell'accesso alla rete e se disponibile il suo accesso postale.

Art. 61 Tipo di sorveglianza HD_29_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 57. Nell'introduzione alla Sezione 10 si spiega cosa si debba intendere per *tentativo di comunicazione* (cfr. sopra).

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 57. 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.

Lo standard prevede due diverse strutture di dati per la consegna dei dati storici della telefonia e dei servizi multimediali. Tuttavia, in questa sede non si illustrano le singole particolarità.

Le indicazioni relative all'ubicazione corrispondono all'ubicazione dell'antenna della cella che serve il target di rete mobile, del punto di accesso WLAN pubblico che serve il target mediante WLAN o dell'accesso alla rete per i servizi multimedia. Devono essere comunicate le indicazioni relative all'ubicazione all'inizio e alla fine di ogni comunicazione o tentativo di comunicazione del target avvenuti durante il periodo di sorveglianza, vale a dire l'inizio o la fine della comunicazione o del tentativo di comunicazione o entrambi rientrano nel periodo di sorveglianza. Se disponibili devono essere comunicate anche le indicazioni relative all'ubicazione durante la comunicazione. Per quanto concerne i servizi multimedia la sessione è considerata una comunicazione. Se disponibili devono essere trasmesse informazioni supplementari sull'ubicazione relative alla navigazione marittima (nome e numero della nave) o alla navigazione aerea (codice della linea aerea, registrazione dell'aeromobile secondo il registro degli aeromobili, numero di volo della linea aerea).

Le *lettere a–i* elencano i dati che le persone obbligate a collaborare devono conservare e trasmettere. Si tratta dei seguenti dati:

a. il tipo della comunicazione (p. es. telefonia fissa a commutazione di circuito, telefonia mobile a commutazione di circuito, SMS, MMS, rete fissa multimedia, multimedia mobile), la data e l'ora di inizio della comunicazione ed eventualmente la sua fine (ciò non è p. es. necessario per SMS e MMS) oppure la sua durata. Per i tentativi di comunicazione devono essere indicati il tipo, la data e l'ora di inizio;

b. gli elementi di indirizzo (p. es. MSISDN, numero E.164, SIP URI, IMPU) di tutti i partecipanti alla comunicazione e i loro ruoli (p. es. chiamante, ricevente, autore della deviazione, destinatario della deviazione);

c. il motivo della fine della comunicazione o del tentativo di comunicazione (p. es. normale, occupato, nessuna risposta o in caso di SIP il corrispondente codice);

d. per la telefonia mobile (se disponibile per i servizi multimedia): l'IMEI dell'apparecchiatura terminale del target e l'IMSI del target;

e. se pertinente, il tipo di servizio portante (Bearer Service, p. es. lingua, dati, fax);

f. per SMS e MMS: le informazioni sull'evento (evento SMS o MMS), il tipo di SMS e lo stato (stato SMS o MMS);

g. per la telefonia mobile: le indicazioni relative all'ubicazione della cella utilizzata dal target all'inizio e alla fine della comunicazione o del tentativo di comunicazione:
   1. gli identificativi della cella e della zona, le coordinate geografiche e, se del caso, la direzione di trasmissione e l'indirizzo postale, o
   2. la posizione del target calcolata dalla rete (p. es. sotto forma di coordinate geografiche e relativo valore di incertezza oppure di poligonali con indicazione delle coordinate geografiche di ogni punto poligonometrico) nonché i relativi indirizzi postali, o
   3. altre indicazioni, conformi agli standard internazionali, sull'ubicazione del target o delle celle usate da quest'ultimo nonché i relativi indirizzi postali;

h. per i servizi multimedia:
   1. l'indirizzo IP del client, il suo tipo e numero di porto,
   2. l'identificativo di correlazione della comunicazione,
   3. i tipi di contenuto multimedia,
   4. le informazioni sui componenti multimedia (ora, nome, descrizione, iniziatore, identificativo del correlativo d'accesso), e
   5. se pertinenti, le informazioni sui servizi IMS (tipo di servizio IMS utilizzato, ruolo dell'elemento di rete da cui provengono i metadati); e

i. per i servizi multimedia: le informazioni sull'accesso alla rete del target:
   1. il tipo di accesso (p. es. 3GPP E-UTRAN TDD),
   2. la classe di accesso (p. es. 3GPP HSPA),
   3. l'indicazione se le informazioni sull'accesso alla rete provengono dalla rete (le indicazioni relative all'ubicazione che non sono qualificate come provenienti dalla rete e potrebbero provenire dall'apparecchiatura terminale o da un'applicazione sono meno affidabili perché potrebbero essere falsate), e
   4. le indicazioni relative all'ubicazione dell'accesso alla rete all'inizio e alla fine della sessione multimediale nonché, se disponibili, durante la sessione multimediale:
      - per l'accesso alla rete via rete di telefonia mobile; le indicazioni relative all'ubicazione della cella utilizzata dal target secondo la lettera g, o
      - per l'accesso alla rete via WLAN: le indicazioni disponibili relative all'ubicazione del punto di accesso WLAN (coordinate geografiche, indirizzo postale), o

- per l'accesso alla rete fissa: l'indirizzo postale disponibile dell'accesso utilizzato dal target.

Art. 62 Tipo di sorveglianza HD_30_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. 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_32_PAGING: determinazione dell'ultima attività dell'apparecchiatura terminale mobile della persona sorvegliata

Il tipo di sorveglianza HD_31_PAGING comprende la determinazione dell'ultima attività (servizi di accesso alla rete, di telefonia e multimedia) rilevata dal fornitore di telefonia mobile per l'apparecchiatura terminale mobile della persona sorvegliata. Sotto il profilo tecnico corrisponde al nuovo tipo di ricerca d'emergenza EP_35_PAGING basato sul precedente tipo di ricerca d'emergenza N1. La forma di sorveglianza finora riservata alla ricerca d'emergenza è pertanto ora messa a disposizione come misura di sorveglianza nella procedura penale secondo l'articolo 273 CPP o l'art. 70*d* PPM.

Art. 64 Tipo di sorveglianza AS_28_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* definisce le indicazioni che il FST deve fornire al Servizio SCPT conformemente alla domanda.

Art. 65 Tipo di sorveglianza AS_33_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 definisce le indicazioni che devono fornire al Servizio SCPT.

Art. 66 Tipo di sorveglianza AS_34: 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) e comprende la comunicazione PS.

Il presente articolo elenca le indicazioni che deve fornire il FST.

Come presupposto del tipo di sorveglianza AS_34: per la ricerca per zona di copertura dell'antenna non deve essere imperativamente necessario il tipo di sorveglianza AS_32_PREP_COV o il tipo di sorveglianza AS_33_PREP_REF.

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. Ad esempio, se 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 disponente 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). Il giudice dei provvedimenti coercitivi deve approvare ogni ordine. Nel presente ambito, a causa del gran numero di persone interessate dalla misura, deve valutare con particolare attenzione la proporzionalità. A tale proposito, in occasione dell'indagine (tenuto conto dei presupposti tecnici e delle finalità dell'indagine) si può privilegiare il modo di procedere che riduce al minimo necessario il numero dei sospettati.

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 disponente 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 da sorvegliare (target ID) 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 del 31 ottobre 2001 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* definisce il tipo di sorveglianza «paging», che permette di determinare l'ultima attività rilevata dalla persona obbligata a collaborare per l'apparecchiatura terminale mobile della persona dispersa. Deve essere trasmessa l'ultima ubicazione disponibile, indipendentemente dalla tecnologia e dal tipo di accesso alla rete utilizzati dall'apparecchiatura. 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 definisce 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 55 e 57, 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_36_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 di contenuti e metadati per i servizi di telefonia e di multimedia (art. 57) e per l'accesso alla rete una sorveglianza in tempo reale di contenuti e metadati per i servizi di accesso alla rete (art. 55). 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* definisce 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 54 e 56, 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.

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 da sorvegliare (target ID) 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 del 31 ottobre 2001, il presente articolo 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 i cosiddetti elementi di indirizzo esterni. Per semplificare nei commenti qui appresso si impiegano i termini «proprio» e «altrui» dal punto di vista del fornitore incaricato della sorveglianza. Gli elementi di indirizzo esterni riguardano la sorveglianza degli identificativi «altrui» che compaiono come partner nella comunicazione con servizi «propri». Vanno valutati soltanto gli elementi di indirizzo. Non deve in particolare essere eseguita alcuna ispezione dei dati di contenuto. Non appena il fornitore incaricato della sorveglianza ritiene che un cliente «proprio» comunichi con l'elemento di indirizzo sorvegliato «altrui» mediante un'applicazione «propria», tale comunicazione va sorvegliata, vale a dire che conformemente al tipo della sorveglianza vanno trasferiti i relativi metadati e se del caso i dati di contenuto. Da anni è prassi corrente la sorveglianza degli elementi di indirizzo esterni nella telefonia, nel cui ambito viene sorvegliato un numero telefonico «altrui».

Gli elementi di indirizzo esterni sono standardizzati soltanto per quanto concerne le applicazioni (servizi di telefonia e multimedia, servizi di posta elettronica) ma non per l'accesso alla rete. Inoltre, in riferimento agli identificativi da sorvegliare (target ID) vi sono alcune limitazioni (p. es. per i servizi di telefonia mobile non è possibile nessun IMSI e nessun IMEI). A causa delle diverse specificità tecniche a seconda del fornitore e del servizio di telecomunicazione da sorvegliare si raccomanda all'autorità disponente di chiedere la consulenza del Servizio SCPT per accertare la fattibilità di una sorveglianza prima di darne l'ordine.

Contrariamente alla prassi vigente, nell'ordine e nel mandato di sorveglianza non occorre aggiungere una relativa annotazione.

È pure nuova la standardizzazione degli elementi di indirizzo esterni per i servizi di posta elettronica: la sorveglianza di un indirizzo di posta elettronica «altrui» presso un fornitore di servizi di posta elettronica, in altri termini la sorveglianza dei

messaggi di posta elettronica in entrata per un cliente «proprio» da un servizio di posta elettronica «altrui» sorvegliato e, inversamente, la sorveglianza dei messaggi di posta elettronica del cliente «proprio» in uscita per un indirizzo «altrui» sorvegliato. Come precedentemente rilevato, vanno valutati soltanto gli elementi di indirizzo dell'indirizzo SMTP. Per motivi tecnici, nell'ambito degli elementi di indirizzo esterni della posta elettronica possono essere sorvegliate soltanto operazioni del server di posta elettronica come l'invio e il ricevimento di messaggi, ma non l'accesso alla casella di posta elettronica «altrui».

Va precisato che gli elementi di indirizzo esterni non sono un tipo di esplorazione di segnali via cavo. Per quanto concerne la nozione di «elementi di indirizzo esterni» si rimanda anche ai commenti che figurano nel messaggio concernente la LSCPT del 27 febbraio 2013[50] riguardo all'articolo 31 LSCPT.

Capitolo 4: Disposizioni finali

Art. 70 Prescrizioni organizzative, amministrative e tecniche

La disposizione corrisponde, all'articolo 33 dell'OSCPT del 31 ottobre 2001[51] ad eccezione delle modifiche necessarie.

Insieme all'articolo 31 capoverso 3 nLSCPT[52], l'articolo 70 costituisce la base legale per l'ordinanza del DFGP del 15 novembre 2017 sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT). Per contro, l'ordinanza del DFGP del 15 novembre 2017 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[53]; cfr. www.li.admin.ch)

Altre norme di delega al DFGP sono contenute negli articoli 33 (procedura di collaudo) 49 capoverso 2 (indicazioni tecniche nell'ordine di sorveglianza) e 29 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.

50 FF **2013** 2283 2346.
51 RS **780.11**
52 FF **2013** 2283, 2347.
53 RS **780.11**

Art. 71 Esecuzione

Il *capoverso 1* corrisponde sostanzialmente all'articolo 33 capoverso 2 dell'OSCPT del 31 ottobre 2001[54]. 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.

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 di un altro atto normativo

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

Art. 73 Modifica di altri atti normativi

Nel contempo sono in parte modificate altre due ordinanze:

- l'ordinanza del 17 novembre 1999[55] sull'organizzazione del Dipartimento federale di giustizia e polizia (Org-DFGP), il cui articolo 25 viene modificato;

- l'ordinanza del 9 marzo 2007[56] sui servizi di telecomunicazione (OST), il cui articolo 80 è oggetto di una modifica formale.

Art. 74 Disposizioni transitorie

L'articolo 45 nLSCPT prevede disposizioni transitorie. In parte è necessario precisarle e adottare ulteriori disposizioni transitorie. Ciò permette di rinunciare a un'entrata in vigore scaglionata delle ordinanze d'esecuzione relative alla nLSCPT oggetto di revisione totale.

Le disposizioni transitorie dell'articolo 74 sono in ordine cronologico. Il momento determinante per i capoversi da uno a sei è l'entrata in vigore della presente ordinanza, per i capoversi sette e otto l'entrata in funzione del nuovo sistema di trattamento, vale a dire delle nuove componenti del sistema acquisite nel quadro del programma STT.

Secondo l'articolo 45 capoverso 1 nLSCPT, alle sorveglianze in corso sono in particolare applicabili il nuovo diritto di consultare gli atti e di essere informati (art. 10 nLSCPT), il nuovo diritto di vigilanza (art. 41 nLSCPT), la nuova tutela giurisdizionale (art. 42 nLSCPT) e le norme concernenti la qualità dei dati trasmessi (art. 18 e 29 nLSCPT).

Fa parte del processo transitorio il fatto che le autorità disponenti e le autorità legittimate possono ordinare i tipi di informazione e di sorveglianza anteriori solo

54 RS **780.11**
55 RS **172.213.1**
56 RS **784.101.1**

fintanto che i loro incarichi possono essere assegnati dal Servizio SCPT alle persone obbligate a collaborare prima dell'entrata in vigore della presente ordinanza. Dall'entrata in vigore della presente ordinanza, per ordini di sorveglianza e domande di informazioni nuovi delle autorità saranno impiegati soltanto i nuovi tipi di informazione e di sorveglianza.

Poiché, nel momento dell'entrata in vigore della presente ordinanza saranno ancora attive numerose sorveglianze in tempo reale, ordinate prima dell'entrata in vigore conformemente al diritto anteriore, il *capoverso 1* prevede una disposizione transitoria per questi casi. Secondo l'articolo 45 capoverso 1 nLSCPT, le sorveglianze in corso nel momento dell'entrata in vigore della legge continuano secondo il nuovo diritto. Tuttavia, ciò non deve complicare eccessivamente l'esecuzione delle sorveglianze in corso[57]. Pertanto occorre partire dal presupposto che il legislatore non voleva applicare i nuovi tipi di sorveglianza alle sorveglianze in corso, perché ciò le complicherebbe eccessivamente. Il capoverso 1 prevede che tali sorveglianze continuino immutate. In caso contrario esse dovrebbero essere cancellate e riattivata; ciò ne complicherebbe fortemente l'esecuzione per i seguenti motivi: per le autorità, per il Servizio SCPT e le persone obbligate a collaborare ne deriverebbero un onere amministrativo e tecnico sproporzionatamente elevato e forti costi. Per le sorveglianze in corso il passaggio ai nuovi tipi di sorveglianza dovrebbe essere ordinato dalle autorità e approvato dal giudice dei provvedimenti coercitivi. In seguito il Servizio SCPT e le persone obbligate a collaborare dovrebbero riattivare queste misure di sorveglianza ed eliminare le misure anteriori. Inoltre, le sorveglianze in corso verrebbero divise in due parti (vecchia, nuova), il che aumenterebbe il rischio di perdite di dati.

Il suddetto disciplinamento si applica per analogia anche alle sorveglianze e alle informazioni retroattive secondo il diritto anteriore il cui trattamento è ancora in corso nel momento dell'entrata in vigore della presente ordinanza. Sono infatti eseguite secondo il diritto anteriore.

Le proroghe e la cancellazione delle summenzionate sorveglianze in corso avvengono ugualmente con i tipi di sorveglianza anteriori. Con la nozione di proroghe si intendono le proroghe periodiche di sorveglianze in tempo reale secondo l'articolo 274 CPP e l'articolo 70*e* PPM. Questo processo amministrativo si svolgerà ancora tra l'autorità disponente, l'autorità di approvazione e il Servizio SCPT. Anche in questo contesto durante il periodo transitorio si applicano i tipi di sorveglianza anteriori. Anche questo processo viene così semplificato poiché una sorveglianza ordinata secondo il diritto anteriore già prima dell'entrata in vigore della presente ordinanza può essere prorogata senza dover essere modificata. La persona obbligate a collaborare presso la quale è in corso una sorveglianza in tempo reale continua a non essere informata della proroga.

Per motivi tecnici l'applicazione dei tipi di sorveglianza anteriori alla cancellazione (disattivazione) delle sorveglianze è possibile soltanto fintanto che le vecchie componenti del sistema per la gestione degli incarichi (AMIS) del Servizio SCPT sono ancora in esercizio. Nell'ambito del programma STT sarà sostituita da una nuova componente di sistema che funzionerà soltanto con i nuovi tipi di

57 cfr. FF **2013** 2364 ad Art. 45 cpv. 1 LSCPT

sorveglianza. Tenuto conto della durata media di una sorveglianza in tempo reale, nel momento della sostituzione di AMIS con la nuova componente di sistema la maggior parte delle sorveglianze ordinate secondo il diritto anteriore saranno regolarmente concluse. Il *capoverso 2* prevede che con l'entrata in vigore della presente ordinanza i collegamenti test secondo la prassi anteriore (cfr. il commento all'art. 30) saranno stati eliminati dal Servizio SCPT, perché corrispondono a tipi di sorveglianze anteriori che non devono più essere controllati.

Il *capoverso 3* prevede una disposizione transitoria per i FST che desiderano presentare una domanda per essere considerati FST con obblighi di sorveglianza ridotti secondo l'articolo 51. Se l'approvazione della domanda è probabile, sono considerati FST con obblighi di sorveglianza ridotti dalla presentazione della domanda e lo rimangono fino alla decisione del Servizio SCPT. La disposizione è stata adottata per tutelare i FST da inutili investimenti per l'adeguamento dei loro sistemi e per garantire la disponibilità a sorvegliare nel periodo tra l'entrata in vigore della presente ordinanza e la decisione del Servizio SCPT. Dall'entrata in vigore dell'ordinanza i FST hanno tre mesi per presentare la domanda presso il Servizio SCPT. Il Servizio SCPT esamina i dati della domanda e i giustificativi presentati e stabilisce, con decisione o decisione incidentale ai sensi degli articoli 5, 45 e 46 della legge federale del 20 dicembre 1968[58] sulla procedura amministrativa (PA), se riconoscerli come FST con obblighi di sorveglianza ridotti o come FST con obblighi pieni. L'ultimo periodo del capoverso 3 esclude l'applicazione del termine transitorio di cui all'articolo 51 capoverso 5 agli FST di un determinato gruppo di FST che non sono più considerati FST con obblighi di sorveglianza ridotti. I FST assoggettati all'obbligo di notificazione secondo il diritto anteriore, vale a dire gli FST che avevano obblighi di sorveglianza secondo la vecchia LSCPT, potrebbero essere tentati di presentare una domanda per approfittare dei termini transitori dell'articolo 51 capoverso 5. Per evitare questo rischio, l'ultimo periodo del capoverso 3 esclude l'applicazione dell'articolo 51 capoverso 5 agli FST finora assoggettati all'obbligo di notificazione. Il Servizio SCPT li considera come FST con obblighi pieni e determina unicamente il termine per memorizzare i dati necessari alla sorveglianza e quelli per la disponibilità a sorvegliare.

Con la normativa di cui al *capoverso 4* è stata accolta la richiesta dei fornitori di un termine transitorio per permettere ai punti di vendita di servizi di telefonia mobile di dotarsi degli equipaggiamenti tecnici necessari per registrare le copie dei documenti d'identità, per adeguare i sistemi per registrare i dati degli utenti e per garantire con mezzi adeguati l'identificazione degli utenti e, nel caso dei punti di accesso WLAN gestiti in maniera professionale, degli utenti finali .

Il *capoverso 5* prevede che i fornitori che hanno l'obbligo di conservare i metadati (cfr. art. 21 cpv. 2 lett. b) dispongono di un termine di sei mesi al massimo dopo l'entrata in vigore della presente ordinanza per adeguare di conseguenza i loro sistemi al fine di poter fornire le informazioni secondo gli articoli 38 (identificazione dell'utenza in caso di indirizzi IP non assegnati univocamente [NAT]) e 39 (informazioni su procedure di traduzione NAT) (cfr. anche il commento all'art. 18 cpv. 4).

58 RS **172.021**

Il *capoverso 6* prevede un termine transitorio di 24 mesi dall'entrata in vigore della presente ordinanza entro il quale i FST devono essere in grado, nell'ambito della sorveglianza retroattiva, di fornire i metadati sui tentativi di comunicazione (*lett. a*). Questo termine permette ai FST di adeguare di conseguenza i loro sistemi. I fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari secondo l'articolo 52 non sono menzionati perché non dispongono ancora di tali sistemi. Ad essi si applica il termine di 12 mesi dalla decisione del Servizio SCPT secondo l'articolo 52 capoverso 2 in combinato disposto con l'articolo 22 capoverso 5. Il medesimo termine transitorio di 24 mesi è concesso ai FST per adeguare gli attuali sistemi di sorveglianza della posta elettronica conformemente alle prescrizioni della presente ordinanza e della OE–SCPT (*lett. b*). Le prescrizioni nell'ambito della sorveglianza della posta elettronica, proprie della Svizzera e ormai obsolete, non sono infatti più contemplate dalla OE-SCPT. Il sistema di trattamento del Servizio SCPT supporta i sistemi operativi prima dell'entrata in vigore della presente ordinanza per un determinato periodo transitorio.

Il *capoverso 7 lettera a* dà al Servizio SCPT la possibilità di tenere la statistica secondo il diritto previgente fino a quando, dopo la prima fase del programma di sviluppo ed esercizio del sistema di trattamento per la sorveglianza del traffico delle telecomunicazioni e dei sistemi d'informazione di polizia[59], i componenti del sistema sono messi in esercizio. I sistemi anteriori, innanzitutto il CCIS, il cui contratto di manutenzione non può più essere adeguato, non permettono di elaborare le statistiche richieste dal nuovo diritto.

Inoltre, la *lettera b* prevede che, fino alla messa in esercizio del nuovo sistema di trattamento del programma STT, ii nuovi tipi d'informazione (art. 27 e 35–48) e di sorveglianza (art. 54–68) sono trattati ancora con il sistema esistente, con i formati anteriori e i relativi moduli. Le domande di informazioni, gli incarichi alle persone obbligate a collaborare e le loro risposte sono trasmessi per posta o fax con un sistema di trasmissione sicuro autorizzato dal Servizio SCPT (cfr. il commento all'art. 3 cpv. 1 lett. a). Per le domande di informazioni e le sorveglianze posteriori all'entrata in vigore della presente ordinanza valgono i nuovi tipi di informazione e sorveglianza. Le sorveglianze ordinate prima dell'entrata in vigore della presente ordinanza rimangono nel sistema esistente con i tipi di sorveglianza e i formati anteriori. Il nuovo diritto è tuttavia applicabile a queste sorveglianze (art. 45 cpv. 1 LSCPT), ad esempio alla vigilanza del Servizio SCPT (art. 41 segg. LSCPT) e alla qualità dei dati trasmessi (art. 28 LSCPT).

La *lettera c* va letta in relazione al capoverso 8. Poiché, nel momento dell'entrata in vigore della presente ordinanza, il nuovo sistema di trattamento non è ancora in esercizio, non possono inizialmente essere presentate domande di informazioni con ricerca flessibile dei nomi secondo l'articolo 27. Dalla messa in esercizio del nuovo sistema di trattamento, i FST e i fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari hanno 12 mesi per adeguare i loro sistemi per la ricerca flessibile dei nomi (cpv. 8). Se, dopo la messa in esercizio del nuovo sistema, un'autorità legittimata secondo l'articolo 15 LSCPT presenta una domanda

59 FF **2015** 2543

di informazione con ricerca flessibile dei nomi, possono logicamente rispondere a quest'ultima soltanto i fornitori che hanno già adeguato i loro sistemi.

Il *capoverso 8* definisce il termine di 12 mesi dalla messa in esercizio del nuovo sistema di trattamento entro il quale i FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari secondo l'articolo 22 devono adeguare i loro sistemi in modo tale da essere in grado di fornire in modo automatico le informazioni secondo gli articoli 34–36 e 39–41 mediante l'interfaccia di consultazione del nuovo sistema di trattamento. Il medesimo termine vale per l'adeguamento dei loro sistemi al fine di poter eseguire le domande di informazioni con ricerca flessibile dei nomi (cfr. cpv. 7 lett. c). Anche se non devono fornire alcuna informazione in modo automatizzato mediante l'interfaccia di consultazione del nuovo sistema di trattamento, i FST con obblighi di sorveglianza ridotti (art. 51) possono implementarla volontariamente.

Art. 75 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 (aggiornato il 23.08.2018)

		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[60] (o settore educazione[61]) Art. 26 cpv. 6 nLSCPT	21/22	11 cpv. 2 18 cpv. 1 e 3 19, 20 21 31 (compliance)	A	26 cpv. 2 e 6	11 cpv. 2 51	B
	STANDARD	21/22	11 cpv. 2, 18 cpv. 1 e 2, 19, 20 21 31 (compliance) 74 (disp. trans.)	C	26 cpv. 1-5	11 cpv. 2 50 31 (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[62] (obblighi supplementari) Art. 27 nLSCPT	22 cpv. 4	11 cpv. 2 18 cpv. 1 e 2 22 31 (compliance) 74 (disp. trans.)	G	27 cpv. 3 26 cpv. 1-5	11 cpv. 2 31 (compliance) 50 52	H

[60] Downgrade
[61] Nelle ordinanze, le espressioni «settore dell'educazione» e «settore dell'istruzione» sono sostituite dall'espressione «settore dell'istruzione e della ricerca» in considerazione di una proposta fatta in sede di consultazione.
[62] Upgrade

A. Obblighi dei FST con obblighi di sorveglianza ridotti (art. 51 OSCPT) in caso di domande di informazioni

Presupposto: il FST offre servizi di scarsa importanza economica o nel settore dell'istruzione e della ricerca (criteri di cui all'art. 51 cpv. 1 e 2 OSCPT).

- In linea di massima gli stessi obblighi dei FST di dimensioni standard (nessun downgrade per informazioni), ciò significa che devono garantire la disponibilità a informare (art. 31 e 32 OSCPT)
- Vi sono le seguenti eccezioni:
  - possono fornire informazioni anche per scritto senza usare il sistema di trattamento (art. 18 cpv. 3 OSCPT), vale a dire che:
    - non devono collegarsi all'interfaccia di consultazione del sistema di trattamento del Servizio SCPT, e
    - non devono fornire in modo automatizzato le informazioni di cui agli articoli 35-37 e 40-42 OSCPT nonché all'articolo 27 in combinato disposto con gli articoli 35, 40 e 42 OSCPT;
  - non devono fornire le informazioni di cui agli articoli 38 e 39 OSCPT con una procedura standardizzata ma soltanto in base ai metadati di cui dispongono;
  - sono esonerati dai servizi di picchetto secondo l'articolo 11 capoverso 2 OSCPT.

B. Obblighi dei FST con obblighi di sorveglianza ridotti (art. 51 OSCPT) 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 e della ricerca (criteri di cui all'art. 51 cpv. 1 e 2 OSCPT).

- Esonero dagli obblighi ai sensi dell'articolo 26 capoversi 1 e 3–5 LSCPT, in particolare non devono garantire la disponibilità a sorvegliare
- Esonero dal servizio di picchetto ai sensi dell'articolo 11 capoverso 2 OSCPT
- Soltanto i seguenti obblighi ai sensi dell'articolo 26 capoverso 2 LSCPT:
  - fornire le informazioni necessarie all'attuazione della sorveglianza,
  - tollerare le sorveglianze,
  - sopprimere i loro criptaggi,
  - su richiesta, fornire i metadati del traffico delle telecomunicazioni della persona sorvegliata di cui dispongono.

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)
- Devono garantire la disponibilità a informare (art. 31 e 32 OSCPT)
- Fornire le informazioni di tutti i tipi mediante l'interfaccia di consultazione del sistema di trattamento del Servizio SCPT
- Fornire le informazioni di cui agli articoli 38 e 39 OSCPT
- Fornire le informazioni di cui agli articoli 35-37 e 40-42 OSCPT nonché all'articolo 27 in combinato disposto con gli articoli 35, 40 e 42 OSCPT
- Obblighi di conservazione dei dati di cui all'articolo 21 capoverso 2 e 22 capoverso 2 OSCPT nonché all'articolo 21 OSCPT
- Servizio di picchetto di cui all'articolo 11 capoverso 2 OSCPT

Autorizzazione:

- sono autorizzati a fornire manualmente le informazioni di cui agli articoli 38, 39, 43–48 OSCPT nonché di cui all'articolo 27 in combinato disposto con l'articolo 43 OSCPT

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

- Obblighi di cui all'articolo 26 LSCPT:
  - fornire il contenuto del traffico delle telecomunicazioni della persona sorvegliata,
  - fornire i metadati delle telecomunicazioni della persona sorvegliata,
  - fornire le informazioni necessarie all'attuazione della sorveglianza,
  - tollerare la sorveglianza,
  - sopprimere i loro criptaggi,
  - conservare i metadati del traffico delle telecomunicazioni per 6 mesi.
- Devono garantire la disponibilità a sorvegliare (art. 31 e 32 OSCPT)
- Servizio di picchetto di cui all'articolo 11 capoverso 2 OSCPT
- Obblighi di sorveglianza di cui all'articolo 50 OSCPT

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

- Devono fornire al Servizio SCPT le indicazioni di cui dispongono per identificare gli autori di reati commessi via Internet (art. 22 cpv. 3 LSCPT)
- Sono esonerati dal servizio di picchetto di cui all'articolo 11 capoverso 2 OSCPT
- Non sono vincolati ai tipi standardizzati di informazioni, ma forniscono senza requisiti formali i dati di cui dispongono (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

- Obblighi secondo l'articolo 27 LSCPT:
  - tollerare la sorveglianza, (dare accesso ai loro impianti e fornire le informazioni necessarie alla sorveglianza),
  - su richiesta fornire i metadati del traffico delle telecomunicazioni della persona sorvegliata di cui dispongono.
- Sono esonerati dal servizio di picchetto di cui all'articolo 11 capoverso 2 OSCPT

G. Obblighi dei fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari (art. 22 OSCPT) in caso di domande di informazioni

Presupposto: il fornitore offre servizi di grande importanza economica o servizi a un gran numero di utenti (criteri di cui all'art. 22 cpv. 1 e 2 OSCPT)

- Equiparati ai FST di dimensioni standard per quanto concerne le informazioni
- Fornire informazioni sui servizi di comunicazione derivati (art. 21 LSCPT per analogia)
- Fornire informazioni per identificare gli autori di reati commessi via Internet (art. 22 LSCPT)
- Garantire la disponibilità a informare (art. 31 e 32 OSCPT)
- Fornire le informazioni di tutti i tipi mediante l'interfaccia di consultazione del sistema di trattamento del Servizio SCPT
- Fornire, anche manualmente, le informazioni di cui agli articoli 38 e 39 OSCPT nella misura in cui hanno obblighi di informazione supplementari (conservazione dei metadati)
- Fornire in modo automatizzato le informazioni di cui agli articoli 35–37 e 40–42 OSCPT nonché di cui all'articolo 27 in combinato disposto con gli articoli 35, 40 e 42 OSCPT
- Obblighi di conservazione dei dati di cui all'articolo 21 capoverso 2 e 22 capoverso 2 LSCPT nonché all'articolo 21 OSCPT
- Esonerati dal servizio di picchetto secondo l'articolo 11 capoverso 2 OSCPT
-

Autorizzazione:

- sono autorizzati a fornire in modo manuale le informazioni di cui agli articoli 43–48 OSCPT nonché di cui all'articolo 27 in combinato disposto con l'articolo 43 OSCPT

H. Obblighi dei fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari (art. 52 OSCPT) in caso di ordine di sorveglianza, ricerca d'emergenza e ricerca di condannati

Presupposto: il fornitore offre servizi di grande importanza economica o servizi a un gran numero di utenti (criteri di cui all'art. 52 cpv. 1 e 2 OSCPT)

- Equiparati ai FST di dimensioni standard per quanto concerne le sorveglianze, le ricerche d'emergenza e le ricerche di condannati (art. 27 cpv. 3 LSCPT)
- Obblighi di cui all'articolo 26 capoversi 1–5 LSCPT:
  - fornire il contenuto del traffico delle telecomunicazioni della persona sorvegliata,
  - fornire i metadati delle telecomunicazioni della persona sorvegliata,
  - fornire le informazioni necessarie all'attuazione della sorveglianza,
  - tollerare la sorveglianza,
  - sopprimere i loro criptaggi,
  - conservare i metadati del traffico delle telecomunicazioni per 6 mesi
- Devono garantire la disponibilità a sorvegliare (art. 31 e 32 OSCPT)
- Servizio di picchetto di cui all'articolo 11 capoverso 2 OSCPT
- Obblighi di sorveglianza di cui all'articolo 50 OSCPT