Rapporto esplicativo

concernente l'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT, RS 780.117)

1. Situazione iniziale

Affinché sia possibile procedere in modo efficace alla trasmissione dei diversi tipi di informazione e all'esecuzione dei diversi tipi di sorveglianza che, nell'ambito della revisione totale della legge federale del 18 marzo 2016[1] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) e della relativa ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT[2]), sono stati adeguati per stare al passo con l'evoluzione tecnologica degli ultimi anni, i fornitori di servizi di telecomunicazione (FST) e i fornitori di servizi postali (FSP) nonché i fornitori di servizi di comunicazione derivati con obblighi di informazione e di sorveglianza supplementari devono attuare le misure necessarie a tal scopo. Quali siano concretamente le misure necessarie e come queste debbano essere attuate è attualmente disciplinato nelle seguenti direttive del Servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT): Direttive organizzative e amministrative per i fornitori di servizi postali (versione 1.5), *Organisational and Administrative Requirements* (OAR; versione 2.15) e *Technical Requirements for Telecommunication Surveillance* (TR TS; versione 3.2).

In futuro, invece, ogni dettaglio di natura organizzativa, amministrativa e tecnica volto a garantire la trasmissione e l'esecuzione regolare e a costi contenuti dei diversi tipi di informazione e di sorveglianza standardizzati sarà disciplinato in un'ordinanza del Dipartimento federale di giustizia e polizia (DFGP). In questo modo si intende tener conto da una parte del principio di determinatezza e disciplinare dall'altra la materia a un livello normativo superiore.

Conformemente alla legge sulle pubblicazioni ufficiali (LPubb[3]), l'ordinanza del Dipartimento è pubblicata nelle tre lingue ufficiali: tedesco, francese e italiano. I suoi allegati, invece, per via del loro carattere speciale, non figurano nella Raccolta ufficiale (art. 5 LPubb). Alla stregua delle direttive sopra menzionate, i dettagli tecnici rilevanti per i fornitori sono quindi disponibili soltanto in lingua inglese. Questo non solo perché gli standard dell'ETSI (*European Telecommunications Standards Institute*) sono già redatti in lingua inglese, ma anche perché l'inglese rappresenta la lingua franca nell'ambito delle tecnologie delle telecomunicazioni (art. 14 cpv. 2 LPubb in combinato disposto con l'art. 33 cpv. 1 dell'ordinanza sulle pubblicazioni ufficiali [OPubb[4]]).

1 RS **780.1**
2 RS **780.11**
3 RS **170.512**
4 RS **170.512.1**

2. Commento ai singoli articoli

Ingresso

Il diritto vigente conferisce al Servizio SCPT la competenza di disciplinare i dettagli organizzativi, amministrativi e tecnici per l'esecuzione delle sorveglianze, ragion per cui esso ha redatto le *OAR* e le *TR TS*. Nell'ambito della revisione totale della LSCPT si è deciso, però, che in futuro tali dettagli saranno disciplinati dal DFGP a livello di ordinanza e non più all'interno di direttive del Servizio SCPT: prevista fino a questo momento a livello di ordinanza (cfr. art. 17 cpv. 1 OSCPT del 31 ottobre 2001), infatti, con la revisione totale della LSCPT la norma di delega nell'ambito del traffico delle telecomunicazioni si colloca ora a livello di legge. In futuro, l'articolo 31 capoverso 3 LSCPT costituirà la base legale per le disposizioni tecniche e amministrative necessarie affinché la trasmissione delle informazioni e l'esecuzione delle sorveglianze nell'ambito del traffico delle telecomunicazioni siano conformi agli standard in uso. Per tutte le altre norme organizzative, amministrative e tecniche nell'ambito del traffico delle telecomunicazioni nonché nell'ambito della corrispondenza postale, la nuova base legale è rappresentata dall'articolo 68 OSCPT.

Sezione 1: Disposizioni generali

Art. 1 Campo d'applicazione

Destinatari della presente ordinanza sono il Servizio SCPT e le persone obbligate a collaborare secondo l'articolo 2 LSCPT, comprese quelle di cui alle lettere e ed f LSCPT, ossia, rispettivamente, le persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazione e i rivenditori professionali di carte o di altri mezzi analoghi che consentono di accedere a una rete pubblica di telecomunicazione.

Art. 2 Obbligo d'informare sul quadro legale

La sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni deve avvenire in modo confidenziale, in particolare affinché l'attività di perseguimento penale possa concludersi con successo. I dati della corrispondenza postale e del traffico delle telecomunicazioni sono soggetti al segreto postale e delle telecomunicazioni. Le persone obbligate a collaborare sono pertanto tenute a informare i loro collaboratori responsabili delle sorveglianze sulla confidenzialità delle misure e sul segreto postale e delle telecomunicazioni cui queste sottostanno (*lett. a e b*). I collaboratori devono essere informati altresì sulle conseguenze penali secondo l'articolo 321ter del Codice penale[5] e l'articolo 39 LSCPT in caso di violazione degli obblighi, così da scongiurare comportamenti scorretti (*lett. c*).

Art. 3 Sicurezza della comunicazione

Dal momento che nell'ambito della corrispondenza postale e del traffico delle telecomunicazioni vengono trattati dati degni di particolare protezione, il canale e la forma delle comunicazioni che hanno luogo tra le persone obbligate a collaborare e il

5 RS **311.0**

Servizio SCPT sono fissati nell'ordinanza: soltanto le persone in precedenza designate possono inviare e ricevere comunicazioni confidenziali (*lett. a*) e i messaggi di posta elettronica devono essere sempre cifrati e firmati (*lett. b*). Grazie alla cifratura, i messaggi non possono essere letti da terzi non autorizzati lungo il percorso dal mittente al destinatario e, grazie alla firma, il destinatario può assicurarsi che essi provengano effettivamente dal mittente indicato.

Art. 4 Forma di trasmissione dei mandati

L'articolo 4 disciplina la forma di trasmissione dei mandati. ll Servizio SCPT trasmette i mandati alle persone obbligate a collaborare per via elettronica (*cpv. 1*). In casi urgenti è prevista tuttavia la possibilità di conferire un mandato di sorveglianza o di richiedere un'informazione anche per telefono; il giorno lavorativo seguente il Servizio SCPT deve tuttavia trasmettere il mandato per via elettronica (*cpv. 2*).

Art. 5 Centro di contatto

All'inizio dell'esercizio commerciale, ogni FSP (art. 2 lett. a LSCPT), ogni FST (art. 2 lett. b LSCPT) e ogni fornitore di servizi di comunicazione derivati (art. 2 lett. c LSCPT) comunica al Servizio SCPT un centro di contatto responsabile per le sorveglianze e le informazioni. Su richiesta del Servizio SCPT, si può imporre anche ai gestori di reti di telecomunicazione interne (art. 2 lett. d LSCPT), alle persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazione (art. 2 lett. e LSCPT) nonché ai rivenditori professionali di carte o di altri mezzi analoghi che consentono di accedere a una rete pubblica di telecomunicazione (art. 2 lett. f LSCPT) di designare un simile centro di contatto. Il centro di contatto deve poter essere raggiungibile telefonicamente per il Servizio SCPT (*cpv. 1*).

I fornitori devono comunicare, per via elettronica, i dati di contatto (nome, cognome, funzione), il numero di telefono diretto e l'indirizzo di posta elettronica dell'interlocutore, nonché le chiavi crittografiche, necessarie per la cifratura dei messaggi di posta elettronica inviati dal Servizio SCPT alle persone obbligate a collaborare e per la verifica della firma dei messaggi di posta elettronica da queste ultime inviati al Servizio SCPT. Qualunque cambiamento riguardante tali dati deve essere segnalato immediatamente al Servizio SCPT.

Le persone obbligate a collaborare devono altresì indicare un indirizzo postale in Svizzera al quale è possibile consegnare validamente in particolare comunicazioni, citazioni, mandati di sorveglianza e decisioni di altra natura (*cpv. 3*).

Art. 6 Termini per il trattamento

Il *capoverso 1* disciplina i termini per il trattamento degli ordini, delle domande e dei mandati. Il Servizio SCPT e le persone obbligate a collaborare devono trattarli quanto prima, ma al più tardi entro la scadenza dei termini previsti nella presente ordinanza.

Se il Servizio SCPT o un terzo incaricato assume un mandato di sorveglianza per un fornitore, i termini per il trattamento previsti per le persone obbligate a collaborare non valgono (p. es. negli art. 16–18). Infatti, per il Servizio SCPT e per i terzi incaricati l'esecuzione della sorveglianza comporta un onere supplementare. Si deve ad esempio analizzare il sistema esterno a disposizione e decidere se la sorveglianza deve essere attivata via accesso a distanza o sul posto, eventualmente occorre del

tempo anche per recarsi sul posto e si deve trovare una soluzione per poter infine attivare la sorveglianza (*cpv. 2*).

Art. 7 Garanzia della qualità del trasferimento dei dati

Per garantire lo svolgimento regolare delle sorveglianze nell'ambito del traffico delle telecomunicazioni nonché la qualità necessaria in materia di trasferimento dei dati, il Servizio SCPT, i FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione e di sorveglianza supplementari eseguono controlli in linea di massima automatizzati. Se necessario, per controllare la qualità possono tuttavia essere eseguiti anche test specifici. Dopo aver sentito i fornitori, il Servizio SCPT elabora un piano di test (*cpv. 1*). Il fornitore mette i dati relativi ai test a disposizione del Servizio SCPT secondo le regole dell'Allegato 1 (*cpv. 3 lett. a*). I fornitori concedono altresì al Servizio SCPT l'accesso sul posto o a distanza per permettere il collegamento delle apparecchiature di test o la gestione di informazioni e collegamenti di test (*cpv. 3 lett. b*) e, se necessario, forniscono sostegno sul posto al Servizio SCPT (*cpv. 4*).

Al fine di garantire anche la qualità del trasferimento di singoli dati, dopo aver consultato i fornitori il Servizio SCPT fissa all'interno delle sue istruzioni i dettagli relativi alla garanzia della qualità in materia di trasferimento di singoli dati (*cpv. 2*).

Art. 8 Guasti ai sistemi dei fornitori

Affinché l'attività di perseguimento penale possa effettivamente trarre beneficio dalle sorveglianze disposte nell'ambito del traffico delle comunicazioni, è fondamentale che i FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione e di sorveglianza supplementari comunichino immediatamente al Servizio SCPT ogni guasto ai loro sistemi. Dal momento che comunicazioni di questo genere sono considerate urgenti, i fornitori possono effettuarle anche per telefono. Tuttavia, entro i cinque giorni lavorativi seguenti, essi devono trasmettere una comunicazione scritta che riporti, oltre alle misure adottate, il periodo di tempo nel quale si è verificato il guasto nonché le cause e le conseguenze dello stesso.

Spetta ai fornitori riparare i guasti che si verificano all'interno dei loro sistemi per poter tornare a eseguire sorveglianze nell'ambito delle telecomunicazioni e a trasmettere le informazioni loro richieste. Per ragioni di trasparenza, i fornitori sono altresì tenuti ad aggiornare con regolarità il Servizio SCPT sullo stato del guasto. Va tuttavia osservato che l'obbligo previsto per i fornitori di riparare i guasti all'interno dei loro sistemi e di tenerne al corrente il Servizio SCPT non li esonera dall'obbligo di eseguire sorveglianze e trasmettere informazioni (*cpv. 2 e 3*).

Art. 9 Guasti alla rete di trasferimento

Si veda anche il commento all'articolo 8.

I FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione e di sorveglianza supplementari sono responsabili per la riparazione dei guasti nei rispettivi sistemi, così come il Servizio SCPT lo è per i guasti che si verificano all'interno del sistema di trattamento. Qualora interessino però la rete di trasferimento e rientrino quindi nella sfera di competenza comune, i guasti devono essere riparati congiuntamente dalle parti coinvolte conformemente ai processi per il trattamento

degli errori stabiliti insieme al Servizio SCPT. Le parti coinvolte si tengono inoltre reciprocamente al corrente sulle singole misure adottate o da adottare.

Sezione 2: Sorveglianza della corrispondenza postale

Art. 10 Sorveglianza in tempo reale

La presente disposizione disciplina le misure da adottare per l'esecuzione di una sorveglianza in tempo reale.

Il *capoverso 1* definisce il termine «intercettazione degli invii postali» di cui all'articolo 16 lettera a OSCPT, con il quale si intendono l'identificazione e lo smistamento, la tenuta a disposizione per il ritiro da parte dell'autorità che dispone la sorveglianza nonché, eventualmente, la ripresa a carico a e la consegna degli invii postali a controllo avvenuto.

Secondo *il capoverso 2* la trasmissione dei dati secondo l'articolo 16 lettera b OSCPT consiste nella comunicazione dei dati disponibili, senza interrompere la consegna dei pertinenti invii postali. Il riferimento è, nello specifico, all'identità del mittente e del destinatario nonché alla natura degli invii e allo stadio in cui si trovano. Questi metadati devono quindi essere forniti soltanto se effettivamente disponibili e non devono essere necessariamente conservati. I dati che, al contrario, devono essere comunicati obbligatoriamente e con continuità, ossia almeno una volta al giorno, all'autorità designata dal Servizio SCPT al momento dell'ordine sono quelli che permettono di identificare gli utenti, come i dati relativi al traffico e alla fatturazione.

Il *capoverso 3* stabilisce che i FSP devono allestire una sorveglianza in tempo reale entro un giorno lavorativo. Questo significa che la risposta deve essere trasmessa al Servizio SCPT al più tardi entro le ore 17.00 del giorno lavorativo seguente alla ricezione del mandato.

Esempio 1: un ordine di sorveglianza è trasmesso al Servizio SCPT alle ore 08.00, che lo inoltra al fornitore alla fine dell'ora a sua disposizione per il trattamento. Il mandato giunge quindi al fornitore alle ore 09.01. In questo caso, il fornitore ha tempo fino alle ore 17.00 del giorno lavorativo seguente per allestire la sorveglianza.

Esempio 2: un ordine di sorveglianza è trasmesso al Servizio SCPT alle ore 16.01 del giovedì, che lo inoltra al fornitore alla fine dell'ora a sua disposizione per il trattamento. Il mandato giunge quindi al fornitore alle ore 17.02. In questo caso, il fornitore ha tempo fino alle ore 17.00 del venerdì per allestire la sorveglianza.

Art. 11 Sorveglianza retroattiva

Secondo l'articolo 11 i FSP hanno a disposizione tre giorni lavorativi a partire dalla ricezione del mandato per eseguire una sorveglianza retroattiva della corrispondenza postale.

Sezione 3: Informazioni sul traffico delle telecomunicazioni

Art. 12 Domanda di informazioni

Per le domande di informazioni, è fondamentale lo stato delle informazioni nel momento o nel periodo di tempo indicato nella domanda. Qualora questo non dovesse essere specificato, la domanda di informazioni si riferisce al momento in cui viene presentata. Se le informazioni si sono modificate nel periodo indicato nella domanda, a dipendenza dello stato delle informazioni la persona obbligata a collaborare deve fornire le diverse informazioni indicando nel pacchetto di dati i pertinenti periodi di validità. Se la struttura dei dati predefinita non lo permette devono essere forniti di conseguenza diversi pacchetti di dati.

Art. 13 Ricerca letterale e ricerca flessibile dei nomi

Il *capoverso 1* prescrive come va eseguita la ricerca letterale. Si tratta di una ricerca precisa che tiene però conto soltanto delle 26 lettere maiuscole dell'alfabeto latino (A-Z) e dei numeri (0-9). Nella pratica, sovente una ricerca basata su un'immissione esatta al 100 per cento del termine ricercato non darebbe i risultati voluti perché i sistemi delle persone obbligate a collaborare e il sistema di trattamento del Servizio SCPT usano set di caratteri diversi. Inoltre, le persone obbligate a collaborare non possono sempre immettere correttamente tutti i caratteri dei dati personali che registrano. Anche i segni di interpunzione (p. es. virgola, punto, trattino, apostrofo, spazio, virgolette, barra trasversale) nei nomi sono spesso digitati in modo scorretto. Le stringhe ricercate e i relativi dati nella banca dei dati dei clienti (indice della ricerca) devono essere normalizzati per la ricerca secondo le regole del capoverso 2. Il principio di base consiste nel rimuovere dapprima tutti i segni che non sono né lettere né numeri e poi, prima di eseguire la ricerca, nel convertire tutte le lettere rimanenti che non fanno parte dell'alfabeto latino di 26 lettere in una o due lettere di quest'ultimo (A-Z) in base a una lista di conversione. I segni diacritici (piccoli segni come riga, punto, caron, arco, tondo posti al di sopra, al di sotto o nella lettera) sono per lo più ignorati. Esempi di segni diacritici sono dieresi, accento, breve, cediglia, accento grafico, accento tonico, tondo, caron (hacek), punto tra due lettere, ogonek, macron, barra traversa, punto sopra/sotto, barra attraverso la lettera. La pronuncia non è considerata per la conversione salvo nel caso delle dieresi e la «ß» (S dura). Questa lista di trasposizione si trova nell'Istruzione del DFGP del 1° gennaio 2012 sulla determinazione e ortografia dei nomi di cittadini stranieri - Allegato 2: Lista per la trasposizione di caratteri speciali. Si basa sulle raccomandazioni dell'Organizzazione internazionale dell'aviazione civile (International Civil Aviation Organisation, ICAO) riguardo ai documenti di viaggio leggibili automaticamente.

Nel *capoverso 2* sono stabiliti i requisiti della cosiddetta ricerca flessibile. Si tratta di una combinazione di ricerca fonetica e di ricerca tollerante agli errori. La ricerca fonetica consiste nel trasformare con un algoritmo fonetico la stringa ricercata e i relativi dati nella banca dei dati di clienti (indice della ricerca) in una stringa fonetica per poi procedere al confronto. In primo piano non vi è la concordanza fonetica esatta con la lingua di origine del nome ma la concordanza approssimativa con il suono in inglese e se possibile nelle tre lingue ufficiali (tedesco, francese e italiano). La funzione di ricerca fonetica per l'inglese è già contenuta nei sistemi di gestione delle banche dati ordinarie.

La ricerca tollerante agli errori comprende gli errori di battitura e gli errori di ortografia, ad esempio le lettere invertite, l'omissione o l'aggiunta di lettere e segni e le inversioni nella successione delle componenti dei nomi o la loro omissione, perché possono essere stati omessi già durante la loro registrazione o essere stati registrati in modo incompleto, un esempio è l'inversione di nomi e cognomi.

I risultati della ricerca flessibile sono tutti i nomi che foneticamente corrispondono o assomigliano a una parte almeno del nome cercato. Le funzioni di ricerca dei sistemi di gestione delle banche dati idonee alla ricerca dei nomi devono per quanto possibile essere utilizzate. A causa della sua tolleranza agli errori, la ricerca flessibile fornisce un numero maggiore di risultati della ricerca letterale di cui al capoverso 1, tuttavia soltanto la persona autorizzata ad effettuare la ricerca può sapere quali risultati sono rilevanti. A tal fine deve poter vagliare tutti i risultati.

Art. 14 Termini per il trattamento delle domande di informazioni

Il Servizio SCPT inoltra le domande di informazioni alle persone obbligate a collaborare secondo l'articolo 2 lettere b–d LSCPT entro un'ora dalla loro ricezione (*cpv. 1*).

Dal momento che il processo di risposta per i tipi di informazione previsti dall'OSCPT è ormai automatizzato, i tempi di reazione si riducono notevolmente. I FST, ad eccezione di quelli con obblighi di sorveglianza ridotti, e i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari devono quindi rispondere quanto prima alle domande di informazioni del tipo IR_4_NA (art. 35), IR_5_NA_FLEX (art. 27 e 35), IR_6_NA (art. 36), IR_7_IP (art. 37), IR_10_TEL (art. 40), IR_11_TEL_FLEX (art. 27 e 40), IR_12_TEL (art. 41), IR_13_EMAIL (art. 42) e IR_14_EMAIL_FLEX (art. 27 e 42), ma al più tardi entro un'ora dalla ricezione[6]. Per rispondere a tutti gli altri tipi di domande di informazioni, invece, il tempo a disposizione è di un giorno lavorativo (*cpv. 2*).

Dal canto loro, i FST con obblighi di sorveglianza ridotti, i fornitori di servizi di comunicazione derivati, ad eccezione di quelli con obblighi di informazione supplementari, e i gestori di reti di telecomunicazione interne hanno a disposizione due giorni lavorativi per rispondere a tutte le domande di informazioni (*cpv. 3*).

Questo significa che la risposta deve essere trasmessa al Servizio SCPT al più tardi entro le ore 17.00 del giorno lavorativo seguente (cfr. esempio all'art. 10).

Sezione 4: Sorveglianza del traffico delle telecomunicazioni

Art. 15 Esecuzione

L'autorità che dispone la sorveglianza trasmette al Servizio SCPT un ordine di sorveglianza da sottoporre all'esame dell'autorità d'approvazione. Qualora quest'ultima reputi che l'ordine rispetta tutti i requisiti formali, il Servizio SCPT trasmette un mandato di sorveglianza al FST o al fornitore di servizi di comunicazione derivati con obblighi di sorveglianza supplementari. Occorre segnalare che l'obbligo di eseguire sorveglianze in tempo reale, sorveglianze retroattive, ricerche d'emergenza e ricerche di condannati o di farle eseguire da terzi non si applica ai FST

[6] Aggiornato il 20.09.2019.

con obblighi di sorveglianza ridotti (cfr. commenti agli art. 49 cpv. 1 e 50 OSCPT), i quali devono però adempiere gli obblighi secondo l'articolo 26 capoverso 2 LSCPT e fornire i metadati relativi al traffico delle telecomunicazioni della persona sorvegliata (art. 26 cpv. 6 LSCPT); in questi casi non si applicano i tipi di sorveglianza standardizzati ai sensi del capitolo 3 sezione 10 OSCPT.

L'esecuzione di una sorveglianza in tempo reale si articola in tre fasi: fase di attivazione, fase di sorveglianza (detta anche «fase attiva») e fase di disattivazione. La fase di attivazione corrisponde alla trasmissione del mandato di sorveglianza per attivazione e all'allestimento della sorveglianza in tempo reale (inizio della sorveglianza), la fase di sorveglianza al trasferimento in tempo reale dei dati relativi al traffico delle telecomunicazioni oggetto della sorveglianza e la fase di disattivazione alla trasmissione del mandato di disattivazione della sorveglianza e allo smantellamento della sorveglianza in tempo reale (fine della sorveglianza).

Per attivare una sorveglianza in tempo reale, quindi, il Servizio SCPT trasmette il mandato al fornitore incaricato della sua esecuzione. Il fornitore conferma al Servizio SCPT la ricezione del mandato e allestisce, o fa allestire da terzi, la sorveglianza in tempo reale. Dopodiché, comunica al Servizio SCPT che è possibile procedere all'esecuzione della sorveglianza in tempo reale e indica il momento preciso (data e ora) dell'attivazione.

La sorveglianza in tempo reale è quindi attiva, il che significa che i dati relativi al traffico delle telecomunicazioni oggetto della sorveglianza sono trasmessi al sistema di trattamento del Servizio SCPT nel quale sono messi a disposizione delle autorità interessate. La sorveglianza rimane attiva fintantoché il Servizio SCPT non trasmette al fornitore, mediante il sistema di trattamento, un mandato di disattivazione.

Il fornitore conferma al Servizio SCPT la ricezione del mandato di disattivazione, la sua esecuzione e, infine, indicando il momento preciso (data e ora) della disattivazione, lo smantellamento della sorveglianza in tempo reale. La sorveglianza può così considerarsi conclusa (*cpv. 1 e 2*).

L'esecuzione di una sorveglianza retroattiva si articola, invece, in due fasi: fase di assegnazione e fase di esecuzione. La fase di assegnazione corrisponde alla trasmissione del mandato di sorveglianza, mediante il sistema di trattamento, dal Servizio SCPT al fornitore incaricato della sua esecuzione e alla conferma da parte di quest'ultimo della ricezione del mandato. Durante la fase di esecuzione, invece, il fornitore esegue, o fa eseguire da terzi, la sorveglianza retroattiva. Ricerca a tale scopo i metadati conservati rilevanti ai fini del mandato e li trasmette al sistema di trattamento. Conferma infine l'esecuzione della sorveglianza retroattiva e indica il momento preciso (data e ora) della trasmissione dei metadati (*cpv. 3*).

La varietà di servizi da sorvegliare, di informazioni da mettere a disposizione e di sorveglianze in tempo reale, ha automaticamente per conseguenza che sono possibili diverse combinazioni. Il Servizio SCPT allestirà a tal fine un compendio che pubblicherà sul suo sito Internet.

Art. 16 Termini per il trattamento di sorveglianze in tempo reale

Si vedano anche i commenti all'articolo 15.

La riduzione dei tempi di esecuzione delle sorveglianze riguarda in linea di massima tutti i tipi di sorveglianze e non solo quelle in tempo reale. Si rinuncia inoltre a

distinguere diversi gradi di priorità, di modo che a uno stesso tipo di sorveglianza corrispondano sempre gli stessi tempi di esecuzione.

I termini di trattamento variano, invece, a seconda del momento in cui viene conferito il mandato di sorveglianza in tempo reale. Si distingue tra mandati conferiti durante gli orari d'ufficio ordinari ai sensi dell'articolo 10 OSCPT e mandati conferiti al di fuori di tali orari.

Mentre il Servizio SCPT deve trasmettere l'ordine per l'esecuzione di una sorveglianza in tempo reale sempre entro un'ora dalla ricezione (*cpv. 1*), a prescindere dal momento in cui ha ricevuto l'ordine, il fornitore è tenuto a eseguirlo a sua volta entro un'ora dalla sua ricezione soltanto nel caso in cui venga conferito durante gli orari d'ufficio ordinari (*cpv. 2*). Per definire il momento del conferimento del mandato è determinante il momento della ricezione da parte del fornitore. Durante la consultazione sono state espresse preoccupazioni isolate che il termine di un'ora sia troppo breve. In considerazione della sua esperienza e del numero dei pareri ricevuti in proposito, il Servizio SCPT parte tuttavia dal presupposto che il termine di un'ora sia in linea di massima realistico. Il superamento dell'ora non ha immediatamente per conseguenza, in casi eccezionali motivati, una procedura di vigilanza.

Il *capoverso 3* disciplina i casi in cui una sorveglianza in tempo reale deve essere eseguita a partire da un determinato momento. In questi casi, la data e l'ora esatta sono indicati nel mandato stesso. Tali mandati sono eseguiti esclusivamente durante gli orari d'ufficio ordinari.

Se una sorveglianza in tempo reale è assegnata dal Servizio SCPT al di fuori degli orari d'ufficio ordinari, il fornitore ha due ore di tempo dalla ricezione del mandato per procedere alla sua esecuzione (*cpv. 4*). Anche riguardo a questo capoverso è stato proposto di estendere il termine. Di nuovo, il Servizio SCPT parte dal presupposto che il termine di due ore sia in linea di massima adeguato. Il superamento delle due ore non ha immediatamente per conseguenza, in casi eccezionali motivati, una procedura di vigilanza.

I tempi di esecuzione si applicano tanto all'attivazione di un mandato di sorveglianza quanto alla sua disattivazione. A tale proposito, il *capoverso 5* precisa però che il Servizio SCPT può trasmettere un mandato di disattivazione soltanto durante gli orari d'ufficio ordinari. Il fornitore ha poi a disposizione un giorno lavorativo per procedere alla disattivazione.

Se un ordine di disattivazione è trasmesso al Servizio SCPT alle ore 16.00 del venerdì e questo lo inoltra al fornitore alla fine dell'ora a sua disposizione per il trattamento, il mandato giunge al fornitore alle ore 17.01. In questo caso, il fornitore ha tempo fino alle ore 17.00 del lunedì seguente per procedere alla disattivazione.

Quando si calcola il tempo totale necessario per il trattamento di un ordine, bisogna tener conto tanto dei tempi di esecuzione previsti per il Servizio SCPT quanto di quelli previsti per i fornitori. È possibile che un ordine di sorveglianza in tempo reale trasmesso al Servizio SCPT durante gli orari d'ufficio ordinari possa essere trattato dal fornitore soltanto al di fuori di questi. Per esempio, se un ordine di sorveglianza in tempo reale viene trasmesso al Servizio SCPT alle ore 16.00, quest'ultimo avrà tempo fino alle ore 17.00 per trattarlo e per conferire il mandato al fornitore, che lo riceverà quindi alle ore 17.01. In questo caso, il tempo a disposizione del fornitore per l'esecuzione del mandato si colloca al di fuori degli orari d'ufficio ordinari ed è quindi dovuto l'importo forfettario supplementare per prestazioni fornite al di fuori degli

orari d'ufficio ordinari (art. 6 dell'ordinanza sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni; OEm-SCPT).

Art. 17 Termini per il trattamento di sorveglianze retroattive

Si vedano anche i commenti agli articoli 15 e 16.

Di norma, secondo il *capoverso 2*, i mandati di sorveglianza retroattiva sono conferiti durante gli orari d'ufficio ordinari. Tuttavia, in casi urgenti, come ad esempio in caso di minaccia di attentato alla bomba o di rapimento, possono essere conferiti anche al di fuori di questi.

Per l'esecuzione di una sorveglianza retroattiva il fornitore ha a disposizione tre giorni lavorativi dalla ricezione del mandato. Qualora si tratti di un caso urgente o il mandato sia conferito al di fuori degli orari d'ufficio ordinari, il tempo a sua disposizione si riduce a sei ore. Va tuttavia segnalato che, a seconda del sistema del fornitore, per il trattamento e la messa a disposizione dei metadati delle 24 ore immediatamente precedenti può essere necessario più di un giorno. Nel caso di una sorveglianza retroattiva urgente, quindi, i metadati più recenti potrebbero non essere ancora disponibili. Il fornitore è tenuto allora a contattare il Servizio SCPT e a trasmetterli quanto prima (*cpv. 3*).

Per la determinazione dei tempi di esecuzione fa stato il momento in cui il fornitore riceve il mandato. Il Servizio SCPT deve trasmetterlo entro un'ora dalla ricezione dell'ordine dell'autorità che dispone la sorveglianza.

Dal momento che nel caso di una procedura accelerata non è possibile esigere la stessa qualità dei dati trasmessi in condizioni normali, una sorveglianza retroattiva urgente può presentare spesso un livello di qualità inferiore. Inoltre, a causa del ritardo, per motivi tecnici, dei fornitori nel trattamento e nella messa a disposizione dei metadati relativi al traffico delle telecomunicazioni, quelli relativi alle 24 ore immediatamente precedenti al conferimento del mandato potrebbero essere incompleti.

Art. 18 Termini per il trattamento di ricerche d'emergenza e ricerche di condannati

Si vedano anche i commenti agli articoli 15–17.

L'esecuzione delle ricerche d'emergenza e delle ricerche di condannati deve avvenire quanto prima. Nel primo caso, infatti, è presumibile che la vita o l'integrità fisica della persona scomparsa sia in pericolo; nel secondo, possono esserlo sia la persona ricercata sia terzi.

Secondo il *capoverso 1*, anche nel caso di ricerche d'emergenza e di ricerche di condannati il Servizio SCPT deve trasmettere il mandato al fornitore quanto prima, ma al più tardi entro un'ora dalla ricezione dell'ordine. L'esperienza ha mostrato che il più delle volte è possibile trasmettere questi mandati nel giro di pochi minuti.

Data l'urgenza delle misure in questione, anche i tempi di esecuzione previsti per i fornitori sono molto ridotti. I fornitori devono infatti eseguire il mandato di sorveglianza quanto prima, ma al più tardi, di regola, entro una (EP_30_PAGING, EP_31_RT_CC+IRI e EP_32_RT_IRI) o quattro (EP_33_HD) ore dalla ricezione del mandato (*cpv. 2 e 3*).

Poiché la procedura accelerata non può rispettare i medesimi requisiti di qualità dei dati e dei pacchetti di dati trasmessi, nella maggior parte delle sorveglianze retroattive urgenti per le ricerche d'emergenza e le ricerche di condannati del tipo EP_34_HD vi è una perdita di qualità. È pure possibile che i metadati trasmessi relativi alle 24 ore immediatamente precedenti siano incompleti a causa del ritardo del fornitore, dovuto a motivi tecnici, nel trattamento e nella messa a disposizione dei metadati del traffico delle telecomunicazioni passato (*cpv. 3*).

Art. 19 Annullamento di mandati di sorveglianza

Si confrontino anche i commenti agli articoli 15–18.

Annullare un mandato di sorveglianza in tempo reale è possibile fintantoché il fornitore non ne ha confermato l'attivazione con una ricevuta (*cpv. 1*). Se la sorveglianza è già stata confermata, invece, il Servizio SCPT non può più procedere all'annullamento e può soltanto conferire un mandato di disattivazione (*cpv. 4*). Lo stesso vale per i casi in cui venga meno una delle condizioni per un ordine di sorveglianza già trasmesso.

Il *capoverso 2* dispone che una sorveglianza retroattiva può essere annullata soltanto se il fornitore non ha ancora trasmesso i dati.

Il *capoverso 3* descrive le singole fasi della procedura di annullamento: il Servizio SCPT contatta il fornitore e lo incarica per scritto, o in casi eccezionali per telefono con successivo incarico scritto, di annullare la sorveglianza (*lett. a*); il fornitore conferma la ricezione del mandato di annullamento (*lett. b*), lo esegue (*lett. c*) e conferma infine l'annullamento al Servizio SCPT (*lett. d*).

In linea con la prassi vigente, un annullamento secondo i capoversi 1 e 2 non comporta né la riscossione di emolumenti né il versamento di indennità (art. 4 OEm-SCPT), e questo a discapito del Servizio SCPT e delle persone obbligate a collaborare, che, nel momento in cui dovesse sopraggiungere un mandato di annullamento, potrebbero trovarsi a dover interrompere l'esecuzione di una sorveglianza già avviata. Poiché il Servizio SCPT e in parte le persone obbligate a collaborare già oggi non riscuotono alcun emolumento né indennità in caso di annullamento è stato deciso di mantenere questa prassi.

Sezione 5: Disponibilità a informare e sorvegliare

Art. 20 Collegamento dei sistemi del fornitore con il sistema di trattamento del Servizio SCPT

Nell'ambito della sorveglianza del traffico delle telecomunicazioni, il Servizio SCPT rappresenta il punto di snodo tra i FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione e di sorveglianza supplementari da una parte e le autorità di perseguimento penale dall'altra. Queste ultime possono consultare le informazioni e i dati delle sorveglianze trasmessi dai fornitori accedendo al sistema di trattamento del Servizio SCPT mediante procedura di richiamo (online). I fornitori, dal canto loro, trasmettono i dati mediante i loro sistemi che sono collegati al sistema di trattamento del Servizio SCPT.

Per istituire la sua disponibilità a informare e sorvegliare, il fornitore comunica al Servizio SCPT i servizi offerti. Devono inoltre comunicargli come intendono attuare per i singoli servizi i tipi d'informazione e di sorveglianza standardizzati (*cpv. 1*). Dopo aver sentito il fornitore, il Servizio SCPT stabilisce i dettagli relativi allo svolgimento del mandato e alla rete di trasferimento nonché gli identificativi, come tipo e formato, per ogni informazione e sorveglianza (*cpv. 2*). Il fornitore procede poi all'implementazione della rete nel rispetto delle istruzioni specifiche ricevute dal Servizio SCPT e di quelle contenute nell'allegato 2 (*cpv. 3*).

Art. 21 Obbligo d'informazione reciproca

Affinché il perseguimento penale possa effettivamente trarre beneficio dalle sorveglianze disposte nell'ambito del traffico delle comunicazioni, è fondamentale che i FST e i fornitori di servizi di comunicazione derivati con obblighi di informazione e di sorveglianza supplementari dispongano in ogni momento dei mezzi tecnici necessari a fornire le informazioni richieste e a eseguire i mandati di sorveglianza loro conferiti. È per questo motivo che il *capoverso 1* introduce l'obbligo per i fornitori menzionati di comunicare al Servizio SCPT, al più tardi cinque giorni lavorativi prima, ogni cambiamento che può influire sul trasferimento dei dati o sulla disponibilità a informare e sorvegliare. Il *capoverso 2* introduce questo obbligo anche per il Servizio SCPT, che è quindi tenuto a comunicare ogni cambiamento ai fornitori alle stesse condizioni previste per questi ultimi. Secondo il *capoverso 3*, infine, il Servizio SCPT e i fornitori si informano reciprocamente anche sui possibili effetti e sul grado di priorità dei cambiamenti previsti.

Art. 22 Verifica della disponibilità a informare e sorvegliare

Si vedano anche i commenti agli articoli 20 e 21.

Per ogni nuovo servizio di telecomunicazione o di comunicazione derivato soggetto all'obbligo di informazione e sorveglianza, il Servizio SCPT verifica che il fornitore sia in grado di eseguire un'eventuale sorveglianza e di fornire le informazioni necessarie. Ai fini della verifica della disponibilità a informare e sorvegliare, il Servizio SCPT comunica ai fornitori i test da eseguire, le condizioni da creare a tale scopo e, dopo averli consultati, il periodo di esecuzione (*cpv. 1*). Una condizione potrebbe essere, per esempio, l'esistenza di un collegamento a determinati sistemi o reti di trasferimento (*delivery network*). Il fornitore esegue i test in prima persona o li fa eseguire da terzi. Il Servizio SCPT sorveglia i test e controlla i risultati (cfr. commento all'art. 16).

È possibile che l'introduzione di un nuovo servizio renda necessario un adeguamento della rete di trasferimento (*delivery network*) e dei parametri tecnici. Il Servizio SCPT stabilisce i parametri tecnici dopo aver consultato i fornitori, che in seguito adeguano la rete di trasferimento. Successivamente, il Servizio SCPT verifica, in collaborazione con i fornitori, che la rete di trasferimento funzioni correttamente (*cpv. 2*).

La verifica della disponibilità a informare e sorvegliare deve essere eseguita anche nel caso in cui un servizio di telecomunicazione o di comunicazione derivato sia in funzione già da diverso tempo. Ripetendo regolarmente questo genere di verifica è possibile garantire in ogni momento la disponibilità a informare e sorvegliare dei fornitori (*cpv. 3*). Anche piccoli cambiamenti riguardanti i sistemi dei fornitori o il sistema di trattamento del Servizio SCPT possono ripercuotersi sulla disponibilità a

informare e sorvegliare, ragion per cui una nuova verifica potrebbe rendersi necessaria anche in questi casi. Spetta al Servizio SCPT, sulla base delle informazioni dei fornitori o di nuovi dati, decidere il momento e le modalità per l'esecuzione di un'eventuale nuova verifica della disponibilità a informare e sorvegliare. La nuova verifica è retta dalle stesse prescrizioni alla base della verifica secondo i capoversi 1 e 2.

Art. 23 Test per la verifica della disponibilità a informare

Si vedano anche i commenti agli articoli 20–22.

L'articolo 23 illustra come preparare ed eseguire i test per la verifica della disponibilità a informare di cui all'articolo 22. L'allestimento dei dati di test incombe rispettivamente ai FST e ai fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari. Conformemente alle istruzioni del Servizio SCPT, i fornitori mettono a disposizione, all'interno dei loro sistemi, i dati di test necessari per rispondere alle domande di informazioni di test (*cpv. 1*), il Servizio SCPT invia loro il questionario secondo l'articolo 31 capoverso 2 lettera b OSCPT e le domande di informazioni di test (*cpv. 2*). Il questionario elaborato dal Servizio SCPT serve per ottenere dal fornitore la conferma che adempie le prescrizioni riguardo alle informazioni standardizzate che non possono essere comprovate da test. Il fornitore risponde al questionario e fornisce le informazioni sul test (*cpv. 3*).

Art. 24 Test per la verifica della disponibilità a sorvegliare

Si vedano anche i commenti agli articoli 20–23.

L'articolo 24 illustra come preparare ed eseguire i test per la verifica della disponibilità a sorvegliare di cui all'articolo 22. L'allestimento dei servizi di telecomunicazione e dei servizi di comunicazione derivati necessari per il test incombe rispettivamente ai FST e ai fornitori di servizi di comunicazione derivati con obblighi di sorveglianza supplementari. I fornitori comunicano al Servizio SCPT gli identificativi (p. es. numero di telefono) di questo servizio (*cpv. 1*). Il Servizio SCPT invia loro il questionario e i mandati di sorveglianza per i collegamenti di test (*cpv. 2*). Il questionario elaborato dal Servizio SCPT serve per ottenere dal fornitore la conferma che adempie le prescrizioni riguardo alle informazioni standardizzate che non possono essere comprovate da test. I fornitori preparano i relativi collegamenti di test nei loro sistemi ed eseguono i test in maniera autonoma attenendosi all'elenco dei casi di test (*cpv. 3*) e infine inviano l'elenco completato (p. es. data, ora, durata delle comunicazioni e identificativi dei partecipanti alla comunicazione), insieme al questionario compilato, al Servizio SCPT (*cpv. 4*).

Art. 25 Analisi e conferma della disponibilità a informare e sorvegliare

Una volta eseguiti i vari test, il Servizio SCPT analizza i questionari e l'elenco dei casi di test nonché le informazioni di test e i dati di test delle sorveglianze (*cpv. 1*). Se necessario, chiede ai fornitori di ripetere alcuni test o di eseguirne di nuovi (*cpv. 2*). Se non è possibile concludere con successo i test, il Servizio SCPT può decidere di annullarli e avviare una nuova procedura di verifica (*cpv. 3*). Se i test hanno successo il Servizio SCPT conferma per scritto la disponibilità a informare e sorvegliare dei fornitori (*cpv. 4*).

Sezione 6: Prescrizioni tecniche

Art. 26

Per maggiori dettagli sulle prescrizioni tecniche in materia di esecuzione della sorveglianza delle telecomunicazioni e di trasmissione delle informazioni si rimanda agli allegati 1 e 2 della presente ordinanza.

Sezione 7: Disposizioni finali

Art. 27 Disposizione transitoria

Poiché il nuovo sistema di trattamento non è ancora in esercizio al momento dell'entrata in vigore dell'OSCPT e quindi non può ancora rispondere automaticamente, ai fornitori di servizi di telecomunicazione e ai fornitori di servizi di comunicazione derivati è concesso un termine più lungo per trattare i tipi di informazione IR_6_NA e IR_12_TEL.

Art. 28 Entrata in vigore

La presente ordinanza entra in vigore unitamente alla legge federale del 18 marzo 2016[7] concernente la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni e alle sue ordinanze esecutive.

7 RS **780.1**

Termini per il trattamento: visione d'insieme[8]				
Mandato	**Tipo di mandato**	**Servizio SCPT**	**Fornitori di servizi di telecomunicazione** **Fornitori di servizi di comunicazione derivati**	**Altre persone obbligate a collaborare**
Sorveglianza in tempo reale **Corrispondenza postale** Durante gli orari d'ufficio	PO_1_RT_INTERCEPTION PO_2_RT_DELIVERY	≤ 1 ora	≤ 1 giorno lavorativo	
Sorveglianza retroattiva **Corrispondenza postale** Durante gli orari d'ufficio	PO_3_HD	≤ 1 ora	≤ 3 giorni lavorativi	
Informazioni	IR_4_NA IR_5_NA_FLEX IR_6_NA IR_7_IP IR_10_TEL IR_11_TEL_FLEX IR_12_TEL IR_13_EMAIL IR_14_EMAIL_FLEX	≤ 1 ora	≤ 1 ora	≤ 2 giorni lavorativi
	IR_8_IP (NAT) IR_9_NAT IR_15_COM IR_16_COM_FLEX IR_17_PAY IR_18_ID IR_19_BILL IR_20_CONTRACT IR_21_TECH	≤ 1 ora	≤ 1 giorno lavorativo	≤ 2 giorni lavorativi
Sorveglianza in tempo reale Durante gli orari d'ufficio	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 ora	≤ 1 ora	
Sorveglianza in tempo reale con indicazione della data Durante gli orari d'ufficio	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 ora	Da allestire al momento indicato nel mandato	
Sorveglianza in tempo reale Durante il picchetto	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 ora	≤ 2 ore	

8 Aggiornato il 1°.02.2018.

Mandato	**Tipo di mandato**	**Servizio SCPT**	**Fornitori di servizi di telecomunicazione** **Fornitori di servizi di comunicazione derivati**	**Altre persone obbligate a collaborare**
Sorveglianza retroattiva Durante gli orari d'ufficio	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV AS_33_PREP_REF AS_34	≤ 1 ora	≤ 3 giorni lavorativi	
Sorveglianza retroattiva In casi urgenti (durante gli orari d'ufficio o il picchetto)	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV* AS_33_PREP_REF AS_34	≤ 1 ora	≤ 6 ore	
Ricerca d'emergenza Durante gli orari d'ufficio e il picchetto	EP_35_PAGING EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 ora	≤ 1 ora	
	EP_38_HD	≤ 1 ora	≤ 4 ore	
Ricerche di condannati **Sorveglianza in tempo reale** Durante gli orari d'ufficio e il picchetto	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 ora	≤ 1 ora	
Ricerche di condannati **Sorveglianza retroattiva** Durante gli orari d'ufficio e il picchetto	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV* AS_33_PREP_REF AS_34	≤ 1 ora	≤ 4 ore	
Disattivazione Solo durante gli orari d'ufficio	PO_1_RT_INTERCEPTION RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_25_TEL_IRI_CC RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 ora	≤ 1 giorno lavorativo	

* AS_32_PREP_COV (art. 64 OSCPT) non è possibile durante il picchetto (art. 11 cpv. 1 let. d OSCPT).