Rapporto esplicativo

concernente l'ordinanza sul sistema di trattamento per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OST-SCPT; RS 780.12)

1. Situazione iniziale

Il servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT) del Dipartimento federale di giustizia e polizia (DFGP) ha il compito di garantire la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, monitorare l'evoluzione tecnologica in questo settore e adeguare di conseguenza le basi legali. Per adempiere i suoi compiti, il Servizio SCPT gestisce un sistema per il trattamento (sistema di trattamento) delle informazioni e delle sorveglianze nell'ambito del traffico delle telecomunicazioni, per la gestione delle pratiche e dei mandati nonché per la conservazione a lungo termine dei dati e per la verbalizzazione. Le nuove basi legali risultanti dalla revisione della legge federale del 18 marzo 2016[1] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) rendono necessarie funzioni supplementari (p. es. conservazione a lungo termine dei dati, infrastrutture per la formazione). Il nuovo sistema di trattamento automatizza inoltre un alto numero di procedure e garantisce così un'elevata continuità operativa in materia di trattamento delle informazioni e dei dati delle sorveglianze.

Ai fini della leggibilità dell'ordinanza del 15 novembre 2017[2] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT) e per soddisfare il principio di trasparenza, le basi legali per il sistema di trattamento sono fissate, oltre che nella LSCPT, in una nuova ordinanza.

2. Commento ai singoli articoli

Ingresso

L'OST-SCPT si fonda sugli articoli 10 capoverso 4, 11 capoverso 6 e 12 capoverso 2 LSCPT e precisa gli articoli 6–14 LSCPT, che contengono disposizioni riguardanti il sistema informatico di competenza del Servizio SCPT e sono illustrati nel relativo messaggio[3].

Sezione 1: Disposizioni generali

Art. 1 Oggetto

L'ordinanza disciplina il funzionamento e l'utilizzo del sistema di trattamento del Servizio SCPT per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

---

1 RS **780.1**

2 RS **780.11**

3 FF **2013** 2283 2310–2319

Per quanto riguarda l'ambito del traffico delle telecomunicazioni, lo scopo del sistema di trattamento viene definito già all'articolo 7 LSCPT.

Art. 2 Rete di trasferimento dei dati

Secondo il *capoverso 1,* i fornitori di servizi di telecomunicazione (FST), ad eccezione di quelli con obblighi di sorveglianza ridotti ai sensi dell'articolo 51 capoverso 1 OSCPT, e i fornitori di servizi di comunicazione derivati con obblighi di informazione supplementari ai sensi dell'articolo 22 capoverso 1 OSCPT o con obblighi di sorveglianza supplementari ai sensi dell'articolo 52 capoverso 1 OSCPT, si avvalgono di una rete (fibra ottica, VPN) che trasferisce le informazioni e i dati delle sorveglianze direttamente all'interfaccia del Servizio SCPT; dettagli tecnici come le interfacce (cfr. art. 12 cpv. 3 LSCPT) sono disicplinati nell'allegato 2 dell'ordinanza del DFGP del 15 novembre 2017[4] sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT). I fornitori menzionati sono responsabili della gestione della rete di trasferimento dei dati e si fanno carico, conformemente all'articolo 38 capoverso 1 LSCPT, delle spese risultanti dalla trasmissione dei dati all'interfaccia del Servizio SCPT. Del resto, la trasmissione dei dati è parte integrante della disponibilità a sorvegliare e, in quanto debito portabile, deve essere assunta dalle persone obbligate a collaborare. Analogamente, secondo l'articolo 53 capoverso 2 OSCPT, le persone obbligate a collaborare mettono gratuitamente a disposizione gli accessi esistenti alle reti pubbliche di telecomunicazione o ne creano nuovi d'intesa con il Servizio SCPT o terzi da esso incaricati, se necessario per la sorveglianza.

Secondo il *capoverso 2,* la rete sicura può essere utilizzata sia per le domande di informazioni e gli ordini di sorveglianza sia per lo scambio di informazioni tra le persone obbligate a collaborare e il Servizio SCPT in caso di incertezze, dubbi o problemi relativi alle domande di informazioni o agli ordini di sorveglianza.

Il *capoverso 3* conferisce al DFGP il compito di emanare disposizioni che regolino dettagli tecnici e amministrativi come la struttura, il funzionamento e la gestione della rete di trasferimento dei dati.

Sezione 2: Dati e trattamento dei dati

Art. 3 Dati

Il contenuto del sistema di trattamento è definito all'articolo 8 LSCPT. Tuttavia, mentre l'articolo 8 LSCPT elenca in particolare i dati che possono essere acquisiti nel caso di una sorveglianza nell'ambito del traffico delle telecomunicazioni, il *capoverso 1* del presente articolo riporta, in maniera generale, tutti i dati contenuti nel sistema di trattamento e descrive il modo in cui vengono acquisiti, a prescindere dal fatto che vengano conservati a lungo termine o meno. Di questi dati fanno parte dati personali e semplici dati tecnici, ma anche dati aggiunti dalle autorità medesime sia per semplificare la rappresentazione tramite programmi speciali sia sotto forma di caratteristiche di trattamento, come l'inserimento manuale di commenti o informazioni inerenti agli elementi d'indirizzo.

4 RS **780.117**

Le informazioni e i dati delle sorveglianze menzionati alla *lettera a*, di cui fanno parte anche le indicazioni sui servizi di telecomunicazione (art. 8 lett. c LSCPT), corrispondono ai dati non trattati che le persone obbligate a collaborare trasmettono al sistema di trattamento nei formati indicati nell'OE-SCPT. Una volta trasmessi, questi dati vengono trattati per poter essere analizzati più facilmente dalle autorità competenti; sono uniformati (p. es. formati orari uniformi), resi leggibili, udibili e visibili (p. es. rappresentazione cartografica, associazione dei numeri a nomi leggibili) nonché ripuliti, per quanto possibile, da eventuali duplicati ed errori (*lett. b*). Tali dati possono essere trattati mediante procedura di richiamo (accesso online).

La *lettera c* prescrive che il sistema di trattamento contiene anche le domande di informazioni e gli ordini di sorveglianza delle autorità disponenti. Alcune parti di tali domande e ordini sono necessarie anche per lo svolgimento e il controllo delle pratiche (lett. e). Tuttavia, poiché non tutti i dati delle domande di informazioni sono indicati nell'articolo 5, per chiarezza tali domande e ordini sono indicati separatamente nella lettera c.

Le autorità che analizzano i dati hanno bisogno di poter applicare ad alcuni dati caratteristiche come evidenziature, sottolineature, trascrizioni, ecc. (*lett. d*).

I dati di cui alla *lettera e*, ad esempio dati sulla gestione dei mandati, decisioni, approvazioni, dati rilevanti per la sicurezza nonché dati relativi ai controlli (p. es. controllo della qualità, dati relativi ai test) e alle statistiche del Servizio SCPT, sono necessari al Servizio SCPT per l'adempimento dei suoi compiti. Il Servizio SCPT tratta inoltre dati contabili per adempiere gli obblighi di fatturazione risultanti dall'articolo 38 LSCPT e poter quindi riscuotere gli emolumenti e versare le indennità di cui all'ordinanza del 15 novembre 2017[5] sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OEm-SCPT). Per quanto riguarda il controllo della qualità, si rimanda all'articolo 18 LSCPT, all'articolo 29 OSCPT, all'articolo 7 OE-SCPT e al relativo allegato nonché ai commenti contenuti nei rispettivi rapporti esplicativi e nel messaggio del 27 febbraio 2013[6] concernente la LSCPT (pag. 2326 seg.). Negli articoli 23 e 24 OE-SCPT sono disciplinati anche i test per verificare la disponibilità a informare e sorvegliare; anche i dati relativi a questi test sono contenuti nel sistema di trattamento. Le statistiche del Servizio SCPT sulle misure di sorveglianza, invece, sono disciplinate dagli articoli 16 lettera k, 35 capoverso 3 e 36 capoverso 2 LSCPT nonché dall'articolo 12 OSCPT. Occorre tuttavia segnalare che, secondo la prassi consolidata, il Servizio SCPT elabora anche una statistica sulle informazioni. Tale prassi continuerà anche con il nuovo diritto. Al Servizio SCPT spetta inoltre la pubblicazione delle statistiche dei pubblici ministeri e dei giudici istruttori militari (cfr. art. 269*bis* cpv. 2 e 269*ter* cpv 4 del Codice di procedura penale [CPP[7]], art. 70*bis* cpv 2 e 70*ter* cpv 4 della Procedura penale militare del 23 marzo 1979[8] [PPM] e art. 13 OSCPT). Dal momento che gli articoli della LSCPT qui menzionati sono stati aggiunti soltanto in fase di dibattito parlamentare e che non sono quindi ancora commentati nel relativo messaggio, per maggiori spiegazioni si rimanda al commento all'articolo 29 del rapporto esplicativo concernente l'OSCPT.

---

5 RS **780.115.1**

6 FF **2013** 2283 segg.

7 RS **312.0**

8 RS **322.1**

Secondo la *lettera f* è consentito utilizzare dati supplementari (p. es. informazioni cartografiche o dati estrapolati da banche dati utilizzate per la portabilità dei numeri) per semplificare la rappresentazione, intesa in senso lato (p. es. rappresentazione sulle carte, decodifica, confronto con altri dati), delle informazioni e dei dati delle sorveglianze.

Il sistema di trattamento contiene inoltre chiavi crittografiche (*lett. g*) che permettono di decifrare, con la chiave privata, i messaggi crittografati con la chiave pubblica del destinatario, di crittografare i messaggi con la chiave pubblica del destinatario e di firmarli con la chiave privata nonché di verificare l'autenticità dei messaggi ricevuti con la chiave pubblica del mittente (firma).

Anche se non esplicitamente menzionato nel presente articolo, il sistema di trattamento tratta anche dati ausiliari quali quelli risultanti dalle operazioni di verbalizzazione o dalla cernita. Il contenuto del sistema di trattamento è illustrato nell'articolo 8 LSCPT.

Il sistema permette al servizio SCPT di trattare i dati di cui necessita per l'adempimento dei suoi compiti. Il *capoverso 2* illustra la struttura del sistema di trattamento. Si tratta di un sistema in cui il trattamento dei dati avviene a livello centralizzato e che permette quindi, tanto in caso di un procedimento penale quanto in caso di ricerche d'emergenza o di condannati, di trattare trasversalmente i diversi dati (p. es. informazioni, dati storici, commenti, traduzioni, ecc.). Inoltre, essendo il sistema di trattamento un'unità logica, non è possibile eliminare sottosistemi dedicati.

Secondo la *lettera a* il sistema di trattamento ingloba i compiti dell'attuale *Call Center Information System* (CCIS) e i compiti supplementari previsti nella LSCPT, il che comporta, in particolare, il trattamento di semplici informazioni riguardanti gli elementi d'indirizzo nonché di informazioni tecniche e amministrative inerenti a contratti e infrastrutture di rete.

Secondo la *lettera b,* nel sistema sono trattati i dati delle sorveglianze in tempo reale. Le persone obbligate a collaborare sono pertanto tenute a trasferire il contenuto e i metadati in tempo reale, ossia non appena vengono generati. Grazie alle funzioni per il trattamento previste nonché ai decoder e alle funzioni di analisi di cui dispone il sistema, le autorità che analizzano i dati possono visualizzare i dati ricevuti in modo chiaro.

Secondo la *lettera c* il sistema di trattamento è in grado di trattare anche dati storici. A tale scopo, le persone obbligate a collaborare trasferiscono i metadati relativi a comunicazioni non più vecchie di sei mesi. Anche in questo caso, grazie alle funzioni per il trattamento previste nonché ai decoder e alle funzioni di analisi di cui dispone il sistema, le autorità che analizzano i dati possono visualizzare i dati ricevuti in modo chiaro.

Secondo la *lettera d* il sistema di trattmento permette al Servizio SCPT di svolgere e controllare le pratiche. Il sistema documenta l'attività del Servizio SCPT e gestisce documenti e fascicoli, permettendo a quest'ultimo di trattare tali dati, inclusi i dati per il controllo della qualità, la statistica e la contabilità. Il sistema di trattamento va concepito in modo tale da assistere il Servizio SCPT nello svolgimento dei suoi compiti relativi al controllo della qualità dei dati trasmessi dai fornitori e alla statistica. I dati da trattare a tale scopo sono elencati all'articolo 6.

Art. 4 Origine dei dati

L'*articolo 4* stabilisce chi può generare i dati e da dove provengono.

I dati possono provenire dalle autorità di perseguimento penale, che, mediante procedura di richiamo (accesso online), possono aggiungere per esempio commenti o documenti (*cpv. 1 lett. a*).

Possono inoltre provenire dalle persone obbligate a collaborare, che trasmettono i dati al Servizio SCPT attraverso la rete di trasferimento dei dati o un altro canale da esso autorizzato (*lett. b*).

Anche il Servizio SCPT genera dati, ad esempio registri, note dei collaboratori o verbalizzazioni (*lett. c*).

I dati devono però poter essere importati anche da banche dati (*lett. d*), indipendentemente dal fatto che esse siano accessibili pubblicamente o meno; tra queste, ad esempio, la banca dati per la portabilità dei numeri «Telecom Data Service» (TelDas) o la banca dati per interrogazioni in materia di intervalli di indirizzi IP «Reti IP Europee» (RIPE).

È prevista inoltre la possibilità di utilizzare geoinformazioni e materiale cartografico per semplificare la rappresentazione delle coordinate (*lett. e*), il che permette di localizzare più facilmente le persone in caso di ricerche d'emergenza. È altresì possibile creare profili di movimento e localizzazione e completarli, per esempio, con il materiale cartografico di swisstopo (geologia, edifici, impianti, ecc.). È necessario che il materiale e le informazioni siano consultati in modo tale che i fornitori e gli *hosting provider* non vengano a conoscenza degli accertamenti in corso, dato che potrebbero essere ospitati su server di fornitori stranieri all'estero.

Il *capoverso 2* dispone che le autorità che analizzano i dati (art. 4 cpv. 1 lett. a) possono integrare i dati delle sorveglianze soltanto con le caratteristiche di trattamento secondo l'articolo 3 capoverso 1 lettera d e con le chiavi crittografiche secondo la lettera g, fondamentali per poter rappresentare e trattare i dati crittografati delle sorveglianze (cfr. art. 7 LSCPT, in particolare lett. a, b e d). L'importazione di altri dati relativi alle indagini è espressamente esclusa.

Art. 5 Funzioni per il trattamento delle informazioni e dei dati delle sorveglianze

Gli articoli 5 e 6 disciplinano importanti aspetti per il trattamento dei dati nel sistema di trattamento. Dal momento che al suo interno sono trattati anche dati personali degni di particolare protezione, è necessaria una base legale formale. Questa risulta essenzialmente dagli articoli contenuti nella seconda sezione della LSCPT. I dati personali degni di particolare protezione sono trattati prevalentemente nell'ambito delle sorveglianze, mentre nell'ambito delle domande di informazioni il trattamento di tali dati non è previsto. Secondo la definizione completa di cui all'articolo 3 della legge federale del 19 giugno 1992[9] sulla protezione dei dati (LPD), con «dati personali degni di particolare protezione» si intendono i dati relativi alle opinioni o attività religiose, filosofiche, politiche o sindacali, alla salute, alla sfera intima o all'appartenenza a una razza, alle misure d'assistenza sociale, ai procedimenti o alle sanzioni amministrative e penali.

9 RS **235.1**

L'articolo 5 precisa nell'ordinanza le funzioni per il trattamento delle informazioni e delle sorveglianze conformemente all'articolo 7 lettera d LSCPT, secondo cui il sistema di trattamento deve disporre di funzioni per il trattamento dei dati in esso contenuti. A tale proposito, il messaggio concernente la LSCPT osserva che l'analisi da parte delle autorità di perseguimento penale dei dati raccolti mediante le sorveglianze ha luogo nei pertinenti sistemi d'informazione della rete dei sistemi d'informazione di polizia dell'Ufficio federale di polizia (cfr. FF **2013** 2283, pag. 2313).

In fase di revisione delle ordinanze si è posto il problema della distinzione tra le funzioni per il trattamento secondo l'articolo 7 lettera d LSCPT e il trattamento dei dati secondo la legge federale del 13 giugno 2008[10] sui sistemi d'informazione di polizia della Confederazione (LSIP); lo stesso dicasi per il trattamento dei dati per il sistema d'informazione del Servizio delle attività informative della Confederazione (SIC). Concretamente ci si è chiesti se nell'ambito delle funzioni del sistema di trattamento sia possibile utilizzare le funzioni di analisi, in particolare quelle che rappresentano un valore aggiunto per le indagini, fermo restando, ovviamente, che non verrebbe importato nessun dato personale non pubblico da fonti esterne alla sorveglianza. Nonostante la LSCPT non presenti espressamente una base legale per queste funzioni, è infatti auspicabile che il sistema di trattamento possa continuare a disporne o che esse possano essere implementate al suo interno. Questo non solo nell'ottica di un adeguamento progressivo della situazione giuridica, ma anche perché tali funzioni fanno parte delle funzioni standard del sistema di sorveglianza delle telecomunicazioni del Servizio SCPT e perché, allo stesso tempo, i sistemi di fedpol e del SIC non dispongono di funzioni analoghe. Del resto, se all'interno dei sistemi previsti dalla LSIP e dalla legge federale sulle attività informative (LAIn) si dovessero implementare le stesse funzioni già presenti nel sistema di trattamento, si andrebbe incontro a spese elevate. Nell'ambito della prevista revisione della LSIP sono auspicabili una più netta distinzione tra i diversi sistemi e la creazione di basi legali più chiare, senza ostacolare il rapido sviluppo e le innovazioni nel campo delle tecnologie dell'informazione e delle comunicazione (TIC), ma anche evitando di restare irrimediabilmente indietro in questo campo.

L'articolo 5 elenca esaustivamente nel dettaglio le funzioni del sistema di trattamento, comprese quelle che rappresentano un valore aggiunto per le indagini. Tutti i dati trasmessi nel sistema di trattamento dalle persone obbligate a collaborare possono così essere trattati dalle autorità che dispongono dei relativi diritti di accesso. L'articolo 9 capoversi 1 e 2 LSCPT designa in linea di massima chi ha diritto di accesso e può quindi trattare i dati. Inoltre, la matrice nell'allegato alla OST-SCPT concretizza gli accessi, nella lettera f per le informazioni e nella lettera g per le sorveglianze. Per il responsabile della sorveglianza (n. 2.4 della matrice) questi accessi sono quindi limitati ai dati dei casi di sorveglianza attribuitigli. Inoltre le lettere ae della matrice illustrano concretamente la distruzione dei dati nel sistema di trattamento. I dati trasmessi possono essere completati con dati supplementari (cfr. art. 4). Tuttavia, a meno che non siano indispensabili per la rappresentazione dei dati già ottenuti (p. es. chiavi crittografiche), non è consentito utilizzare all'interno del sistema di trattamento dati personali degni di particolare protezione provenienti da fonti esterne alla sorveglianza, e quindi neanche i dati delle sorveglianze eseguite con dispositivi come gli IMSI-catcher e i GovWare secondo gli articoli 269*bis*–269*quater* CPP o gli articoli

10 RS **361**

70^{bis}–70^{quater} PPM. Il sistema di trattamento può inoltre inviare e ricevere dati relativi a corrispondenze come e-mail, fax, SMS e telefonate.

Secondo la *lettera a* è possibile ascoltare in diretta sorveglianze in tempo reale, ad esempio telefonate con o senza immagini o tramite VoIP. È inoltre possibile riprodurre in differita conversazioni pre-registrate.

Secondo la *lettera b* i dati acquisiti possono essere visualizzati e stampati. Ciò concerne soprattutto l'analisi dei verbali o le indicazioni sullo stato (p. es. se un telefono è acceso o spento). I dati, gli SMS, le e-mail, le informazioni http e le conversazioni sono trattati in modo tale che possano essere visualizzati nel modo più chiaro possibile e, di conseguenza, facilmente analizzati dalle autorità di perseguimento penale. Nel caso dei dati trasmessi dalle persone obbligate a collaborare, e in particolare nel caso delle sorveglianze dei collegamenti Internet, dove si ha a che fare con grandi sequenze di numeri e lettere, vengono impiegati strumenti diversi affinché, ad esempio, le immagini scaricate nel corso della sessione Internet siano riconoscibili come tali. Ad essere stampate sono per lo più le informazioni relative ai casi, ad esempio per il pubblico ministero.

Secondo la *lettera c* i dati relativi ai telefoni cellulari possono essere localizzati grazie alle coordinate ottenute nel corso della misura. Per agevolarne il trattamento, questi dati possono essere rappresentati su una carta geografica insieme ad altri dati, di modo che, per esempio nel caso di una ricerca d'emergenza, la persona scomparsa possa essere trovata più velocemente.

Attraverso la decodifica secondo la *lettera d* è possibile convertire i dati in altri formati; i dati ricevuti o inviati sono spesso convertiti in formati speciali che permettono di comprimerli in fase di trasmissione. Una volta trasmessi, i dati devono però essere riconvertiti nel formato originale. I dati, tuttavia, non vengono soltanto decodificati. In alcuni casi, infatti, per evitare letture indesiderate, i dati vengono crittografati ed è quindi successivamente necessaria una chiave specifica per poterli rendere nuovamente leggibili.

Secondo la *lettera e* è possibile raggruppare i dati in modo da averne una visione d'insieme più chiara e poterli paragonare in modo più efficace.

Secondo la *lettera f* è possibile effettuare una ricerca, per esempio di un particolare elemento di testo, o una cernita, per esempio secondo un particolare tipo di comunicazione (e-mail, SMS, conversazione, parole chiave, intervalli di tempo, aree geografiche, ecc.). L'importante è non confondere questo tipo di cernita con la cernita automatica eseguita dal Servizio SCPT secondo gli articoli 7 OSCPT e 17 lettera g LSCPT: mentre nel caso della cernita automatica i dati scartati non vengono salvati nel sistema di trattamento, in questo caso è possibile annullare la cernita in modo da visualizzare nuovamente tutti i dati.

Grazie alla funzione di cui alla *lettera g* il collaboratore di un'autorità autorizzata può associare una registrazione vocale a una determinata persona. Il sistema è in grado di riconoscere questa voce in base a una registrazione vocale e di associarla a una determinata persona, il che permette in un procedimento penale, ad esempio, di poter stabilire più facilmente con chi si svolge una conversazione. La registrazione vocale è tuttavia possibile soltanto per i casi di sorveglianza di un'autorità autorizzata e non può essere utilizzata per l'intero sistema. Nell'ambito del trattamento di dati delle sorveglianze (*lett. g*) nella matrice allegata alla OST-SCPT ciò viene eseguito per le autorità autorizzate (n. 2) con i doppi asterischi.

Secondo la *lettera h* è possibile trascrivere file audio e video. Ciò significa che il testo o le immagini vengono trascritte in un verbale e, se necessario, successivamente tradotte in una lingua nazionale. Nella sorveglianza delle telecomunicazioni è prioritaria la trascrizione di ciò che viene detto.

La *lettera i* prevede la possibilità di commentare i diversi elementi, annotando ad esempio impressioni, informazioni o denominazioni dei casi.

Secondo la *lettera j* il sistema può segnalare, ad esempio via telefono o SMS, un particolare evento in corso.

La *lettera k* permette di trasmettere informazioni in modo sicuro, in particolare alle persone autorizzate delle autorità di perseguimento penale mediante un'interfaccia della rete dei sistemi d'informazione di polizia dell'Ufficio federale di polizia (art. 14 cpv. 1 LSCPT) e del sistema d'informazione del SIC (art. 14*a* LSCPT) o mediante procedura di richiamo (accesso online). In tal modo gli inquirenti possono scaricare i dati di cui hanno bisogno.

Secondo la *lettera l* le informazioni e i dati delle sorveglianze possono anche essere distrutti. Tuttavia, quest'ultima funzione si applica esclusivamente nel caso della selezione dei dati su ordine del giudice competente di cui all'articolo 16 lettera e LSCPT o per altri tipi di distruzione previsti dalle legge (p. es. art. 276 e 277 CPP).

Il *capoverso 2* precisa che queste funzioni si applicano soltanto ai dati a cui la persona che le esegue ha accesso. Nel caso di una ricerca o a di una cernita di dati appaiono pertanto soltanto i dati a cui la persona in questione è autorizzata ad accedere.

Art. 6 Trattamento dei dati per lo svolgimento e il controllo delle pratiche

Dal momento che il perseguimento penale non rientra nella sua sfera di competenza, l'attività del Servizio SCPT in questo settore è subordinata agli ordini ricevuti, e in particolare a quelli delle autorità competenti in materia. Il Servizio SCPT gestisce il sistema di trattamento (art. 6 LSCPT), ma non è il detentore dei dati (art. 13 LSCPT). Detentrici e responsabili dei dati sono invece le autorità che dispongono le sorveglianze. Il Servizio SCPT si limita a richiedere tali dati e a renderli accessibili online nel rispetto dei diritti di accesso. Il Servizio SCPT è però detentore e responsabile dei dati che esso genera per lo svolgimento e il controllo delle pratiche (art. 3 cpv. 2 lett. d) nonché dei dati risultanti dalla verbalizzazione.

Il presente articolo contiene un elenco dei dati trattati dal Servizio SCPT nell'ambito dell'esecuzione e del controllo degli ordini di sorveglianza del traffico delle telecomunicazioni.

Sulla base dei dati di contatto di cui alla *lettera a*, il Servizio SCPT assegna alle persone designate dall'autorità competente, di norma l'autorità inquirente, i diritti di accesso al sistema di trattamento, le contatta in caso di dubbi e trasmette la fattura alle autorità che hanno disposto la sorveglianza. I dati di contatto possono essere registrati anche precedentemente alla trasmissione del primo ordine, di modo che in occasione dell'ordine di sorveglianza risultino già presenti nel sistema di trattamento. Inoltre ciò permette di informare le autorità su eventuali novità.

I dati di cui alla *lettera b* sono utilizzati dalle persone obbligate a collaborare e dal Servizio SCPT per verificare che un'applicazione o un accesso alla rete siano effettivamente connessi alla persona da sorvegliare. Grazie all'indicazione della

professione, il Servizio SCPT può verificare che siano state adottate le misure di cui all'articolo 271 capoverso 1 CPP (art. 5 OSCPT).

Inoltre, avvalendosi dei dati di cui alla *lettera c*, il Servizio SCPT verifica formalmente che le sorveglianze siano disposte per perseguire i reati di cui agli articoli 269 e 273 CPP (sorveglianze retroattive) ed elabora una statistica annua relativa ai mandati di sorveglianza e alle informazioni nell'ambito della corrispondenza postale e del traffico delle telecomunicazioni.

I tipi d'informazione e di sorveglianza ordinati di cui alla *lettera d* sono assegnati alle persone obbligate a collaborare, fatturati e analizzati a fini statistici.

Secondo la *lettera e* nel sistema si possono trattare le comunicazioni scritte e orali nonché le telefonate registrate per fini probatori secondo l'articolo 8 OSCPT, effettuate nell'ambito dello svolgimento e del controllo delle pratiche. Di tali comunicazioni fanno ad esempio parte anche le comunicazioni sonore trasmesse via e-mail.

Secondo la *lettera f* nel sistema di trattamento vengono conservate anche le decisioni delle autorità. Si tratta, da un lato, di decisioni dei pubblici ministeri e dei giudici dei provvedimenti coercitivi (ordini, approvazioni, proroghe) conservate per fini probatori e, dall'altro, di decisioni del Servizio SCPT (p. es. secondo l'art. 40 cpv. 1 LSCPT) e delle autorità giudiziarie in merito a ricorsi. Ciò permette la conservazione centralizzata di tutti i dati relativi a un fascicolo. I dati generati in fase di elaborazione delle decisioni del Servizio SCPT sono trattati nel sistema GEVER e solo la decisione stessa è conservata, laddove necessario, nel sistema di trattamento nel relativo fascicolo.

La *lettera g* rimanda agli articoli 15 lettere h–k e 49 capoverso 1 lettere h–l OSCPT, dove sono elencati i dati che devono figurare negli ordini di sorveglianza. Per ulteriori spiegazioni si veda il commento alle pertinenti disposizioni nel rapporto esplicativo concernente l'OSCPT.

Secondo la *lettera h* nel sistema di trattamento possono essere inseriti anche i numeri di riferimento assegnati dai pubblici ministeri e le denominazioni delle informazioni e delle sorveglianze nonché i numeri di riferimento univoci assegnati dal Servizio SCPT a ogni fascicolo.

Secondo la *lettera i* il Servizio SCPT tratta anche i dati di contatto delle persone obbligate a collaborare. Questi dati sono utilizzati, da un lato, per trasmettere l'ordine d'informazione e di sorveglianza alle persone obbligate a collaborare o ai loro collaboratori e, dall'altro, per verificare e confermare la loro disponibilità a informare e sorvegliare.

A tal fine, secondo la *lettera j*, il Servizio SCPT tratta anche altri dati sulle persone obbligate a collaborare, come certificati, identificativi (p. es. numero d'identificazione delle imprese e dei fornitori secondo l'art. 38 lett. a dell'ordinanza del 17 ottobre 2007[11] sul registro di commercio; ORC), numeri di telefono, indirizzi IP, stato della disponibilità a informare e sorvegliare, informazioni relative alla ridotta importanza economica secondo l'articolo 51 capoverso 1 OSCPT o ancora alle sanzioni amministrative o penali di cui alle sezioni 10 e 11 LSCPT. Tali dati sono necessari al Servizio SCPT anche per trasmettere i dati comunicati dalle persone obbligate a collaborare, per verificare la disponibilità a informare e sorvegliare e per

11 RS **221.411**

l'assegnazione nelle categorie delle persone obbligate a collaborare o dei servizi da esse forniti (art. 1 cpv. 2 lett. i–m OSCPT). ~~Il Servizio SCPT tratta tuttavia anche informazioni necessarie ad assegnare le persone obbligate a collaborare nelle pertinenti categorie (cfr. art. 1 cpv. 2 lett. i–m OSCPT), come i servizi da esse forniti.~~ Tralaltro sono anche necessari i dati richiesti dagli articoli 22 capoverso 1, 51 capoverso 1 e 52 capoverso 1 OSCPT sul settore di attività e sul fatturato annuo per determinare quali fornitori hanno obblighi ridotti (art. 51 OSCPT) o obblighi supplementari (art. 22 e 52 OSCPT).

Gli elementi d'indirizzo, indicati nella maggior parte degli ordini e definiti all'articolo 3 della legge del 30 aprile 1997[12] sul traffico delle telecomunicazioni (LTC) come parametri di comunicazione ed elementi di numerazione quali indicativi, numeri di chiamata e numeri brevi, servono per instaurare una comunicazione e possono essere attribuiti in modo univoco a una persona specifica. Secondo la *lettera k* nel sistema di trattamento possono essere trattati anche questi dati. Lo stesso dicasi per gli identificativi che, a differenza degli elementi d'indirizzo, non possono essere attribuiti in modo univoco a una persona specifica.

Secondo la *lettera l* nel sistema di trattamento sono conservate inoltre le informazioni di natura tecnica, tra cui quelle per casi speciali, necessarie allo svolgimento e al controllo degli ordini di sorveglianza nell'ambito del traffico delle telecomunicazioni. È il caso, ad esempio, delle chiavi crittografiche per la trasmissione sicura dei dati, dei numeri di porta o dei dati per la rete di trasferimento dei dati (art. 2), come indirizzi IP e password.

Secondo la *lettera m* nel sistema di trattamento sono trattati anche i dati per la riscossione degli emolumenti dalle autorità di perseguimento penale e il versamento delle indennità alle persone obbligate a collaborare. Di tali dati fanno parte, ad esempio, lo stato della fatturazione e l'emolumento per prestazioni non elencate, fissato per ciascun caso specifico e in funzione del tempo impiegato (cfr. art. 13 OEm-SCPT).

Art. 7 Diritti di accesso al sistema di trattamento

Mentre all'articolo 9 LSCPT i diritti di accesso delle diverse persone al sistema di trattamento sono definiti in maniera generale, l'OST-SCPT disciplina, rispettivamente all'articolo 7 e all'articolo 8, i diritti di accesso fondamentali e i diritti di accesso supplementari ai dati di singole sorveglianze.

Il sistema di trattamento, oltre a dover rispondere alle esigenze di numerose persone e autorità, deve essere dotato di molteplici interfacce nonché permettere agli aventi diritto o ai membri delle autorità (cfr. art. 1 cpv. 2 lett. a–f OSCPT) o alle categorie professionali menzionate di accedere a diverse funzioni.

Secondo il *capoverso 1* i diritti di accesso fondamentali al sistema di trattamento sono garantiti previa compilazione dell'apposito modulo messo a disposizione dal Servizio SCPT. In futuro questo modulo potrà essere compilato elettronicamente, ad esempio mediante il sistema online o il tool ZP. L'accesso permette, tra le altre cose, la trasmissione di domande di informazioni e di ordini di sorveglianza. Le modalità di comunicazione di eventuali cambiamenti al Servizio SCPT sono disciplinate dall'articolo 3 OSCPT. I diritti di accesso possono essere concessi soltanto a persone

12 RS **784.10**

fisiche. Queste persone, a cui viene assegnato un conto utente, sono responsabili per gli accessi eseguiti e devono essere in grado di spiegare le ragioni per cui l'accesso ai dati del sistema di trattamento sia necessario all'adempimento dei loro compiti.

Secondo la *lettera a* hanno diritto di accedere ai dati i collaboratori delle autorità che, rispettivamente secondo l'articolo 9 e l'articolo 15 LSCPT, possono disporre sorveglianze e richiedere informazioni nell'ambito di un procedimento penale, di una ricerca d'emergenza o di una ricerca di condannati. Si tratta per lo più delle autorità di perseguimento penale, come fedpol, ma anche delle autorità che trattano cause penali amministrative nonché delle autorità cantonali di esecuzione, che, qualora una pertinente base legale cantonale lo preveda, possono a loro volta disporre una sorveglianza nell'ambito di una ricerca di condannati. A queste si aggiungono anche le autorità di perseguimento penale dei singoli Cantoni, che dispongono di un accesso sicuro alle misure di sorveglianza del sistema di trattamento per le loro attività inquirenti e giudiziarie, nonché, in veste di autorità che analizzano i dati, le organizzazioni di polizia, che accedono ai dati del sistema di trattamento attraverso una rete autorizzata a tale scopo. L'accesso è altresì garantito al Ministero pubblico della Confederazione, in quanto autorità di perseguimento penale federale che ordina la sorveglianza, e al Tribunale penale federale. Infine, con la revisione totale della legge federale del 25 settembre 2015[13] sulle attività informative (LAIn), anche il SIC ottiene la possibilità, oltre che di trasmettere domande di informazioni (art. 25 cpv. 2 LAIn), di disporre sorveglianze (art. 26 cpv. 1 lett. a LAIn).

Secondo la *lettera b* hanno diritto di accesso anche i collaboratori dei FST e dei fornitori di servizi di comunicazione derivati, che possono in questo modo rispondere alle domande trasmesse loro, sempre attraverso il sistema di trattamento, dalle autorità che dispongono le sorveglianze e da quelle che analizzano i dati. Le persone obbligate a tollerare la sorveglianza, dal canto loro, sono le sole che non necessitano generalmente di un accesso al sistema di trattamento, dal momento che, in questi casi, è il Servizio SCPT a eseguire i vari compiti.

Per assolvere i loro obblighi in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni nonché per garantire la manutenzione dei sistemi, secondo la *lettera c* hanno diritto di accedere al sistema di trattamento anche i collaboratori del Servizio SCPT.

Infine, secondo la *lettera d*, hanno diritto di accesso i terzi cui il Servizio SCPT ha delegato compiti di manutenzione, gestione e programmazione.

Secondo il *capoverso 2,* determinati collaboratori di un'autorità (cosiddetti «OrgAdmin») possono assegnare diritti d'accesso ad altre persone. Questi accessi possono essere concessi a tutti i collaboratori dell'autorità in questione. È il Servizio SCPT che, su ordine della persona competente, ad esempio un comandante di polizia, conferisce il diritto di assegnare accessi a terzi. A tal fine gli OrgAdmin ricevono accessi speciali (token che generano numeri) da assegnare in misura limitata. In questo modo viene ad esempio concesso l'accesso a traduttori, rappresentanti legali e difensori, al fine di garantire i diritti previsti dalla legge. Il diritto di consultare gli atti è concesso dai detentori e responsabili della collezione di dati, ossia, secondo l'articolo 13 LSCPT, dalle autorità che hanno accesso al sistema di trattamento conformemente all'articolo 9 LSCPT. Gli accessi non avvengono quindi dal computer personale del rappresentante legale, bensì mediante procedura di richiamo (accesso

13 Legge federale sulle attività informative (**LAIn**, RS **121**)

online) in locali stabiliti dall'autorità investita del caso o mediante altri mezzi da essa messi a disposizione, ad esempio un supporto di dati. Soprattutto nel caso di procedimenti in cui occorre proteggere i testimoni, è ipotizzabile che le autorità siano autorizzate a riprodurre soltanto alcuni passaggi di un messaggio o che debbano oscurare parte dei verbali. Ai privati oggetto della misura di sorveglianza o da questa interessati e che possono far valere i loro diritti di parte è concesso l'accesso ai dati alla stregua di quanto avviene per i rappresentanti legali. Il Servizio SCPT non è in contatto diretto con le persone interessate dalla misura o i loro rappresentanti legali. Qualora un token venga assegnato a terzi, la persona competente secondo il capoverso 1 lettera a (il collaboratore dell'autorità) resta responsabile, ad esempio anche per la perdita del token. Deve inoltre documentare in modo dettagliato l'utilizzo del token affinché per il Servizio SCPT sia chiaro chi ha avuto accesso a quali dati e quando. Il Servizio SCPT si adopera affinché, in caso di cambiamento di sistema, l'attribuzione dei token per il sistema di trattamento possa essere verbalizzata direttamente nel sistema medesimo.

Secondo il *capoverso 3* il Servizio SCPT ha l'obbligo di verificare periodicamente se sussistono le condizioni per i diritti di accesso. In questo modo si intende evitare che, a causa di cambiamenti non segnalati, ad esempio un collaboratore che lascia o cambia la sua funzione, restino attivi accessi ormai non più necessari.

Secondo il *capoverso 4* i diritti di accesso al sistema di trattamento sono disciplinati nell'allegato, dal quale emerge con chiarezza quali funzioni possono essere assegnate a quali gruppi di persone. Maggiori dettagli sono contenuti nel regolamento per il trattamento dei dati redatto dal Servizio SCPT.

Art. 8 Diritti di accesso ai dati di singole sorveglianze

Il collaboratore di un'autorità cui è stato concesso l'accesso al sistema di trattamento può avviare l'applicazione per trattare i dati delle sorveglianze. In questa fase, però, non è ancora in grado di visualizzare i dati. Secondo il *capoverso 1*, infatti, a tal fine è necessario che egli disponga dei diritti di accesso ai dati di singole sorveglianze. Per ottenere tali diritti esistono due possibilità: o il Servizio SCPT concede l'accesso alle persone elencate nell'ordine di sorveglianza[14] o un collaboratore autorizzato secondo il capoverso 3 concede l'accesso a un collaboratore che ne ha bisogno per l'adempimento dei suoi compiti.

Secondo il *capoverso 2,* le persone di cui agli articoli 279 CPP, 70*j* PPM, 33 LAIn nonché 35 e 36 LSCPT, e in particolare gli imputati e le persone un tempo scomparse oggetto di una sorveglianza, possono trasmettere una domanda all'autorità competente, al fine di esercitare il loro diritto di consultare gli atti o di accedere ai dati (cfr. art. 10 cpv. 4 LSCPT). Anche le persone interessate secondo la legge federale del 19 giugno 1992[15] sulla protezione dei dati (LPD) possono esercitare il diritto di consultare gli atti o di accedere ai dati secondo l'articolo 10 capoversi 1–3 LSCPT.

A seconda delle disposizioni applicabili (p. es. art. 279 cpv. 2 CPP, art. 70*j* cpv. 2 PPM, art. 63 cpv. 2, 4 e 5 LAIn), tali diritti possono essere prorogati o limitati. Nell'ambito di un procedimento penale, con «autorità competente» si intende l'autorità investita del procedimento fino al momento della sua conclusione. Dopodiché il diritto di accesso è retto dalla LPD o dalle rispettive leggi cantonali (cfr.

14 Cfr. art. 3 OSCPT.
15 RS **235.1**

art. 10 cpv. 1 lett. b LSCPT), così come avviene nel caso di sorveglianze ordinate nell'ambito di una ricerca d'emergenza o di una ricerca di condannati. Il SIC registra i dati risultanti dalle misure soggette ad autorizzazione, quali la sorveglianza della corrispondenza posta e del traffico delle telecomunicazioni, per ogni singolo caso e separatamente dai sistemi d'informazione secondo l'articolo 47 LAIn (art. 58 cpv. 1 LAIn), li seleziona e in seguito registra, per l'ulteriore analisi, nel relativo sistema d'informazione soltanto i dati di cui ha bisogno per adempiere il suo compito. Nel caso di una misura di sorveglianza disposta dal SIC, il diritto di accesso è retto dall'articolo 63 LAIn, secondo cui il SIC esamina dapprima una domanda di informazioni, ma differisce l'informazione qualora sussista un interesse a preservare il segreto o qualora si tratti di una persona non registrata. Dopo aver ricevuto comunicazione del differimento, la persona interessata può rivolgersi all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), che applica per analogia la procedura dell'informazione indiretta. Il Servizio SCPT non prende in carico simili domande, dal momento che non è responsabile per la loro valutazione. Qualora la domanda venga approvata dall'autorità competente, alle persone interessate viene concesso di accedere ai dati di cui hanno bisogno per l'esercizio dei loro diritti, e questo mediante procedura di richiamo (accesso online temporaneo, p. es. mediante token) in locali stabiliti dall'autorità o mediante altri mezzi da essa messi a disposizione, come un supporto di dati. Mediante procedura di richiamo le persone interessate hanno la possibilità di utilizzare singole funzioni di visualizzazione e analisi del sistema di trattamento (p. es. stampa e trasmissione sicura alle persone autorizzate), ma soltanto nella misura in cui ne abbiano bisogno per l'esercizio dei loro diritti. Ove necessario, è però possibile fare richiesta di un supporto di dati supplementare secondo l'articolo 9 OEm-SCPT. Spetta in particolar modo all'autorità competente decidere se le persone interessate possano procedere autonomamente all'accesso o se debbano essere assistite da un agente di polizia formato a tal scopo.

Secondo il *capoverso 3*, oltre al Servizio SCPT, anche singoli collaboratori delle autorità possono assegnare internamente gli accessi ai dati delle sorveglianze. Una pratica del tutto sensata, per esempio, nel caso in cui, dopo l'ordine di una sorveglianza, un OrgAdmin intenda concedere o revocare l'accesso ai dati di una particolare sorveglianza ad altri inquirenti qualificati della sua unità organizzativa, a persone autorizzate o ai loro rappresentanti legali secondo il capoverso 2. Dal momento che alcuni cambiamenti devono poter essere registrati in tempi molto rapidi, è sicuramente vantaggioso potersene occupare direttamente sul posto. Il Servizio SCPT, dal canto suo, concede l'accesso ai dati delle sorveglianze soltanto su ordine dell'autorità che dispone la sorveglianza.

Secondo il *capoverso 4* il Servizio SCPT ha il compito di redigere un pertinente regolamento per il trattamento dei dati del servizio medesimo (cfr. art. 7 cpv. 4) anche per questo tipo di accessi.

Art. 9 Interfacce

Il sistema di trattamento dispone di diverse interfacce, la cui base legale sono gli articoli 14 e 14*a* (disposizione di coordinamento con LAIn) LSCPT.

Secondo la *lettera a* esiste un'interfaccia con i sistemi delle persone obbligate a collaborare affinché si possano trasmettere i mandati e ricevere i dati e le conferme (cfr. art. 9 cpv. 2 lett. c OSCPT). Dei mandati fanno parte sorveglianze e domande di

informazioni semplici, ma anche di natura tecnico-amministrativa. Le relative istruzioni tecniche figurano nell'allegato 1 dell'OE-SCPT.

Secondo la *lettera b* è possibile trasmettere una copia dei dati ai sistemi d'informazione di polizia dell'Ufficio federale di polizia e al sistema d'informazione del SIC. Il sistema di trattamento permette di accedere online ai dati nonché di copiarli e scaricarli per mezzo di un'interfaccia con i sistemi d'informazione di polizia, nello specifico con la banca dati della Polizia giudiziaria federale (JANUS)[16]. Nel momento in cui la LSCPT entrerà in vigore, in virtù dell'articolo 14*a* LSCPT sarà introdotta un'interfaccia supplementare con il sistema d'informazione del SIC, ragion per cui il sistema di trattamento permetterà di accedere online ai dati nonché di copiarli e scaricarli anche per mezzo di un'interfaccia con questo sistema. La trasmissione di una copia dei dati ai sistemi dei Cantoni deve in linea di massima avvenire attraverso uno dei due sistemi.

Secondo la *lettera c* le interfacce possono servire anche per accedere a banche dati per l'accertamento di elementi d'indirizzo, con i quali si intendono parametri di comunicazione ed elementi di numerazione quali indicativi, numeri di chiamata e numeri brevi, ma anche informazioni geografiche e materiale cartografico. Si tratta di dati meramente tecnici, e quindi non personali, che possono provenire, ad esempio, da TelDas, RIPE o swisstopo.

Sezione 3: Protezione e sicurezza dei dati

Art. 10 Misure per la sicurezza dei dati

Dal momento che il sistema di trattamento contiene dati personali degni di particolare protezione, è necessario adottare tutte le misure tecniche e organizzative necessarie a proteggere i dati. La norma di delega dell'articolo 12 capoverso 2 LSCPT è attuata in particolare con la presente disposizione e con gli altri articoli che compongono la terza sezione dell'ordinanza.

Secondo il *capoverso 1 lettera a* è garantita la protezione dagli accessi e dalle modifiche. Per poter procedere all'autenticazione, le persone devono essere quindi registrate nel sistema di trattamento, in modo da scongiurare ogni accesso non autorizzato e, con questo, il furto o l'utilizzo illegale dei dati. Inoltre, le persone autorizzate dispongono soltanto dei diritti d'accesso di cui hanno bisogno per l'adempimento dei loro compiti (p. es. diritti di lettura e scrittura). In particolare, le persone autorizzate non possono cancellare definitivamente alcun dato. I pertinenti diritti sono elencati nell'allegato. Tutti i dati presenti nel sistema di trattamento sono tramessi in maniera sicura e il più delle volte criptati. Non sono per esempio criptati i dati trasmessi direttamente al sistema di trattamento attraverso una rete di fibra ottica.

Secondo la *lettera b* la protezione dei dati è garantita anche grazie al controllo effettuato nella fase di trasporto, durante la quale, ricorrendo a una trasmissione sicura, si fa in modo che i dati non vengano letti, copiati, modificati o cancellati in modo non autorizzato.

Secondo la *lettera c* è garantito anche il controllo degli accessi e delle modifiche. A tal fine, si procede alla verbalizzazione di tutte le modifiche, in particolare di quelle

16 Cfr. art. 14 LSCPT.

effettuate sulla base dell'articolo 5, ma anche degli accessi in modalità lettura e delle ricerche ad esempio mediante file log. Il Servizio SCPT analizza i dati e gli accessi, in modo periodico e a campione, per individuare eventuali irregolarità. Per una simile analisi può anche consultare le autorità di perseguimento penale.

Secondo il *capoverso 2* il Servizio SCPT deve stabilire le misure da adottare sulla base di un'analisi dei rischi. Il tipo di controllo varia a seconda delle categorie di utenti e può interessare, per esempio, l'accesso al sistema, gli utenti, l'accesso ai dati o il trasporto. L'analisi dei rischi è condotta conformemente allo stato tecnologico fissato in modo uniforme negli standard internazionali quali l'ETSI (*European Telecommunications Standards Institute*). Si tratta di standard collaudati, noti sia alle persone obbligate a collaborare sia alle autorità di perseguimento penale, che non solo concorrono a migliorare la qualità della trasmissione dei dati, ma anche a semplificare procedure tecniche complesse.

Con il *capoverso 3* il Servizio SCPT è incaricato di emanare istruzioni per l'esecuzione di misure tecniche e organizzative in materia di sicurezza dei dati destinate ai diversi utenti del sistema (Servizio SCPT, ma anche autorità di perseguimento penale e persone obbligate a collaborare). Si tratta di istruzioni necessarie affinché i dati, segnatamente quelli personali degni di particolare protezione, siano trattati correttamente all'interno del sistema di trattamento e di conseguenza siano debitamente protetti, per esempio dai furti. Le istruzioni contengono, tra le altre cose, indicazioni in merito alle possibili modalità di trattamento dei dati nonché alle procedure previste in caso di perdita di un token o se un utente intende disconnettersi.

Secondo il *capoverso 4* tutti i trattamenti di dati nel sistema, tutti gli accessi in modalità lettura, tutte le ricerche e tutti gli interventi di manutenzione sono verbalizzati (chi ha fatto cosa, quando e dove?). Il Servizio SCPT conserva i verbali per tutta la durata di conservazione delle informazioni e dei dati delle sorveglianze. Secondo l'articolo 10 capoverso 2 dell'ordinanza del 14 giugno 1993[17] relativa alla legge federale sulla protezione dei dati (OLPD), i verbali sono conservati per un anno. Dato che la OST-SCPT è una lex specialis, la maggiore durata di conservazione ivi prevista prevale sulla disposizione della OLPD.

Art. 11 Misure per la sicurezza del sistema

In caso di guasti o di rischio di guasti nel funzionamento regolare del sistema di trattamento, per esempio nel caso in cui il sistema risulti sovraccarico a causa di una misura di sorveglianza o nel caso di un crash del sistema, è necessario agire velocemente al fine di scongiurare l'eventualità che il sistema non sia più disponibile e che vada così persa una grande quantità di dati. Non appena rilevato il guasto, il Servizio SCPT contatta, a sua discrezione, l'autorità che ha disposto la sorveglianza (p. es. un pubblico ministero) o l'autorità che analizza i dati (p. es. polizia) e discute con essa le misure da adottare; dopodiché decide come procedere. Qualora sia necessario agire immediatamente, il Servizio SCPT può prendere una decisione anche senza contattare le autorità.

[17] RS **235.11**

Art. 12 Anonimizzazione

I dati possono essere utilizzati anche per fini statistici (art. 12 OSCPT). Tuttavia, al fine di proteggere i dati personali, tali dati devono essere anonimizzati prima di poter essere pubblicati. I dati che vengono trasmessi all'Archivio federale svizzero (AFS) non vengono anonimizzati.

Sezione 4: Accesso ai dati delle sorveglianze mediante procedura di richiamo, distruzione e archiviazione dei dati

Art. 13 Accesso ai dati delle sorveglianze mediante procedura di richiamo

L'articolo 11 LSCPT si pronuncia in maniera generale sui termini di conservazione dei dati del sistema di trattamento.

Il *capoverso 1* dispone invece che i dati delle sorveglianze, di cui fanno parte anche i dati relativi allo svolgimento e al controllo delle pratiche, restano a disposizione delle autorità fino a un momento specifico. Tale momento interviene al passaggio in giudicato della decisione sul procedimento penale (*lett. a*), sei mesi dopo la conclusione di un'operazione del SIC (*lett. b*) e sei mesi dopo la conclusione di una ricerca d'emergenza (*lett. c*) o di una ricerca di condannati (*lett. d*). Nell'ambito di una procedura di assistenza giudiziaria internazionale (*lett. e)*, invece, i dati delle sorveglianze restano a disposizione al massimo fino all'invio dei supporti di dati o dei documenti all'autorità affinché li trasmetta a un'autorità estera (cfr. art. 9 cpv. 4 LSCPT). Se vengono allestiti supporti di dati prima della fine di una sorveglianza, i dati della sorveglianza rimangono disponibili con tutte le caratteristiche di trattamento fino a quando l'ultimo supporto di dati o l'ultimo documento è stato inviato all'autorità per trasmissione all'autorità straniera. Le lettere d ed e si applicano anche nel caso di un'estradizione e non si limitano soltanto ai casi inerenti all'assistenza giudiziaria accessoria (piccola). Finora il Servizio SCPT era tenuto a distruggere i dati delle sorveglianze al più tardi tre mesi dopo il termine della misura di sorveglianza (art. 10 cpv. 1 OSCPT in vigore)[18]. La pratica ha tuttavia mostrato che la polizia, in particolare, ha bisogno di ben più di tre mesi per analizzare i dati. Inoltre, si è reso talvolta necessario trattare alcuni dati nel corso dell'iter giurisdizionale, per esempio dinanzi a un'istanza di secondo grado o al Tribunale federale. Affinché questo sia possibile, i dati secondo la *lettera a* e le diverse funzioni per il trattamento dovrebbero rimanere a disposizione, mediamente, per circa cinque anni, ossia fino al passaggio in giudicato della decisione. L'autorità può tuttavia disporre che i dati non debbano essere necessariamente messi a disposizione con tutte le funzioni per il trattamento; in tal caso, conformemente al capoverso 2, i dati sono conservati a lungo termine nel sistema di trattamento con funzioni di trattamento ridotte. Questa è la procedura che sarà presumibilmente applicata nella maggior parte dei casi, dal momento che, dodici mesi dopo la revoca della sorveglianza (cosiddetto «termine di conservazione»), secondo l'articolo 11 OEm-SCPT è riscosso un emolumento per ogni proroga dell'accesso di tre mesi. Di norma, le autorità accedono ai dati delle sorveglianze (cfr. art. 9 cpv. 4 LSCPT), direttamente mediante procedura di richiamo (accesso online) o tramite le interfacce con i sistemi d'informazione di polizia dell'Ufficio federale di polizia e con il sistema d'informazione del SIC (art. 9 lett. b).

---

18 Ordinanza del 31 ottobre 2001 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

Secondo il *capoverso 2*, dopo il momento di cui al capoverso 1, come il passaggio in giudicato della decisione, i dati sono conservati a lungo termine nel sistema di trattamento con funzioni per il trattamento ridotte. Tuttavia, qualora non abbia più bisogno dei dati e di tutte le funzioni per il trattamento, l'autorità può comunicarlo al Servizio SCPT anche prima di questo momento, di modo che i dati possano essere conservati di conseguenza (secondo periodo). In questo caso non si applicano gli emolumenti previsti per la conservazione e tutte le funzioni per il trattamento (art. 11 OEm-SCPT). I dati conservati sono ad esempio necessari per concedere alle parti in un procedimento penale di esaminare gli atti secondo l'articolo 101 CPP. Un'autorità potrebbe tuttavia aver nuovamente bisogno dei dati dopo il passaggio in giudicato della decisione, per esempio in caso di riapertura (art. 323 CPP) e di revisione (art. 410 CPP) di un procedimento o qualora i dati siano necessari nell'ambito di un altro procedimento. A seconda del tipo e del volume dei dati, il sistema di trattamento prevede a tale scopo soluzioni tecniche di volta in volta differenti. In questi casi i dati possono essere trattati con funzioni ridotte (lettura, ricerca, cernita, scaricamento selettivo, ecc.). Allo stato attuale del progetto Programma STT[19], non è ancora chiaro se soltanto un numero limitato di utenti potrà disporre di funzioni per il trattamento ridotte. Se così fosse, i dati conservati a lungo termine saranno trasmessi al sistema investigativo delle autorità che non hanno accesso a tali dati nel sistema del Servizio SCPT. Non è previsto un nuovo accesso online con funzioni per il trattamento. I corrispondenti accessi sono concretizzati dalla matrice nella lettera z. I diversi termini di conservazione sono retti dall'articolo 11 LSCPT. 30 anni dopo la conclusione di una sorveglianza, il Servizio SCPT deve informarsi presso l'autorità che si occupa del procedimento o, se nessuna autorità se ne occupa più, presso l'ultima che se ne è occupata, per chiarire come procedere con i dati ancora presenti nel sistema (art. 11 cpv. 5 ultimo periodo LSCPT).

Secondo il *capoverso 3*, in caso di modifiche tecniche sostanziali al sistema di trattamento, i dati e tutte le funzioni per il trattamento restano a disposizione delle autorità per un periodo successivo compreso tra i sei e i dodici mesi. Una limitazione temporale delle possibilità di trattamento può rivelarsi ad esempio necessaria nel caso di un cambiamento di sistema o fornitore. Modifiche tecniche sostanziali possono inoltre verificarsi anche quando la struttura dei dati viene modificata in modo significativo, come avviene in seguito a un importante aggiornamento (release): per mantenere le funzioni per il trattamento, in questi casi potrebbe altrimenti essere necessario utilizzare contemporaneamente, per oltre un anno, sia i vecchi che i nuovi componenti, il che comporterebbe costi non indifferenti. È per questo motivo che i dati, insieme a tutte le funzioni per il trattamento, non devono poter essere trattati con i vecchi componenti per un periodo superiore a dodici mesi. La durata esatta (tra sei e dodici mesi) è stabilita, d'intesa con le autorità, dal Servizio SCPT, che decide anche se i dati dovranno poi essere migrati o conservati con funzioni per il trattamento ridotte secondo l'articolo 11 LSCPT.

Art. 14 Distruzione

Secondo il *capoverso 1* l'ultima autorità investita del procedimento può comunicare al Servizio SCPT se intende far distruggere i dati prima della scadenza del termine di conservazione secondo l'articolo 11 LSCPT o se questi, per esempio a fini di archiviazione (cfr. art. 15), debbano essere prima messi a disposizione di un'autorità

19 FF **2014** 5719

da essa designata. In quest'ultimo caso troverebbe applicazione l'articolo 9 capoverso 4 LSCPT e, laddove possibile, i dati verrebbero quindi crittografati e trasmessi via posta per mezzo di supporti di dati o documenti. Tra i dati da distruggere all'interno del sistema di trattamento rientrano anche quelli relativi allo svolgimento e al controllo delle pratiche. È possibile che, scaduto il termine di conservazione, l'ultima autorità investita del procedimento si dimentichi di contattare il Servizio SCPT; spetta allora a quest'ultimo mettersi in contatto con l'autorità e chiedere informazioni sul modo di procedere. Così facendo, il Servizio SCPT adempie anche all'obbligo di cui all'articolo 11 capoverso 5 ultimo periodo LSCPT, secondo cui, trent'anni dopo la fine della sorveglianza, è tenuto a informarsi presso l'autorità investita del procedimento.

Affinché si possa procedere alla distruzione dei dati nel sistema di trattamento anche qualora non sia più possibile risalire all'autorità competente o qualora questa non fornisca istruzioni in merito, il *capoverso 2* dispone che il Servizio SCPT può salvare i dati su un supporto di dati, che è consegnato, nel caso di procedimenti cantonali, alla massima autorità giudiziaria del Cantone in questione e, nel caso di procedimenti delle autorità federali, al Tribunale penale federale. Tale operazione è verbalizzata. Dopo aver ricevuto conferma della leggibilità del supporto, il Servizio SCPT distrugge i dati.

Il *capoverso 3* stabilisce che le informazioni sono conservate per dodici mesi con tutte le funzioni di trattamento. In seguito, prima di essere eliminate, le informazioni che possono essere attribuite a una misura di sorveglianza grazie a un numero di riferimento o al nome del caso sono conservate in modo centralizzato con funzioni di trattamento ridotte per la durata di conservazione prevista per i pertinenti dati di sorveglianza. Il termine di conservazione è quindi retto dall'articolo 11 LSCPT, che rimanda all'articolo 103 CPP. Con «informazioni» si intende qualunque indizio che rappresenti un punto di partenza per le indagini delle autorità di perseguimento penale. Queste ultime possono inserire tali informazioni anche in altri documenti e aggiungerle così al fascicolo penale. La matrice concretizza i corrispondenti accessi nella lettera z.

Art. 15 Archiviazione

Dal momento che, di norma[20], il detentore dei dati è l'autorità che dispone la sorveglianza e non il Servizio SCPT, la loro archiviazione è retta dalle diverse basi legali applicabili ai detentori.

Il *capoverso 1* stabilisce la procedura da seguire nel caso di dati della Confederazione. In questi casi, conformemente alla legge federale del 26 giugno 1998[21] sull'archiviazione (LAr), il Servizio SCPT è tenuto a offrire i dati all'AFS, che, d'intesa con esso, decide se sono degni di archiviazione o meno. Il Servizio SCPT prepara i dati degni di archiviazione conformemente all'articolo 5 capoverso 1 dell'ordinanza dell'8 settembre 1999[22] relativa alla legge federale sull'archiviazione (OLAr) in combinato disposto con l'articolo 5 capoverso 1 e l'articolo 8 delle istruzioni del 28 settembre 1999[23] sull'obbligo generale di offerta e di versamento dei

20 Cfr. commento all'art. 6 OST-SCPT.

21 RS **152.1**

22 RS **152.11**

23 https://www.bar.admin.ch/bar/it/home/archiviazione/versamento-di-documenti.html

documenti all'Archivio federale svizzero. I dati non reputati degni di archiviazione sono distrutti nel rispetto dei termini di cui all'articolo 11 LSCPT.

Il *capoverso 2* rimanda all'articolo 4 capoverso 2 LAr e stabilisce la procedura da seguire in presenza di dati dei Cantoni. In questi casi si applica il diritto cantonale. Il detentore dei dati, per esempio l'autorità penale cantonale, offre i dati all'autorità cantonale competente affinché proceda alla loro archiviazione.

Sezione 5: Disposizioni finali

Art. 16 Disposizioni transitorie

Secondo il *capoverso 1* il Servizio SCPT può procedere alle verbalizzazioni secondo il diritto previgente fino alla messa in funzione dei nuovi componenti del sistema secondo la prima fase del programma STT[24]. I vecchi sistemi, in particolare il CCIS, il cui contratto di manutenzione non può più essere modificato, non permettono le verbalizzazioni auspicate.

Dal momento che la conservazione a lungo termine non è stata ancora pianificata e che non è chiaro se sarà già operativa al momento dell'entrata in vigore della LSCPT e delle ordinanze di esecuzione, il *capoverso 2* dispone che, come avviene secondo la prassi vigente, i dati vengono messi a disposizione dell'autorità che dispone la sorveglianza o di un'autorità da essa designata su un supporto di dati (cfr. art. 19 cpv. 4 OEm-SCPT). In alternativa, qualora il sistema di trattamento lo permetta già da un punto di vista tecnico, le autorità potranno scegliere di scaricare i dati nel loro sistema.

Art. 17 Entrata in vigore

La presente ordinanza entra in vigore contemporaneamente alla LSCPT totalmente riveduta e alle altre ordinanze di esecuzione.

[24] FF **2014** 5719