Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia (DFGP)

Berna, 15 novembre 2023

Revisione parziale di ordinanze esecutive della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)

Rapporto esplicativo

ISC-EJPD-D-D4B13401/90

Indice

1 Situazione iniziale

Attualmente le ordinanze esecutive della legge federale del 18 marzo 2016[1] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) vanno riviste alla luce di quanto segue:

- in occasione della modifica del 22 marzo 2019 della legge del 30 aprile 1997[2] sulle telecomunicazioni (LTC) è stato aggiunto un secondo capoverso all'articolo 2 della LSCPT che autorizza il Consiglio federale a precisare le categorie di persone obbligate a collaborare (POC), segnatamente quelle di cui all'articolo 2 capoverso 1 lettere b, c ed e LSCPT (RU *2020* 6159, in particolare 6180);
- la tecnologia 5G comporta alcuni adeguamenti dell'ordinanza del 15 novembre 2017[3] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT), sono altresì necessarie determinate misure per migliorare e garantire in generale la trasmissione di dati. Infine vanno adeguate alcune disposizioni dell'ordinanza del 15 novembre 2017[4] sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OEm-SCPT), dell'ordinanza del DFGP del 15 novembre 2017[5] sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT) e dell'ordinanza del 15 novembre 2017[6] sul sistema di trattamento per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OST-SCPT).

Per non rinviare gli adeguamenti imposti dalla tecnologia 5G, la revisione sarà attuata in due tappe. Il presente pacchetto di modifiche non comprende la definizione delle varie categorie di POC e dei loro obblighi che sarà invece materia del secondo pacchetto. La prevista revisione totale della OEm-SCPT che introduce gli importi forfettari (cfr. art. 38*a* LSCPT, in vigore dal 1° gennaio 2022) sarà oggetto di un progetto separato, ossia l'ordinanza sul finanziamento della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OF-SCPT).

Il presente progetto tiene conto dei progressi tecnologici come la tecnologia 5G e l'IP Multimedia Subsystem (IMS) (cfr. n. 3.1).

2 Procedura preliminare e procedura di consultazione

Dal 16 febbraio al 23 maggio 2022 si è svolta la procedura di consultazione nell'ambito della quale il DFGP (Servizio SCPT) ha ricevuto 70 pareri.

1 RS **780.1**
2 RS **784.10**
3 RS **780.11**
4 RS **780.115.1**
5 RS **780.117**
6 RS **780.12**

In sede di consultazione sono emerse due posizioni contrastanti: da un lato i Cantoni e le autorità di perseguimento penale che sostanzialmente sostengono il progetto e dall'altro le organizzazioni della telecomunicazione e le POC che invece lo criticano aspramente o in certi casi lo respingono sostenendo che le modifiche non riguardano solamente disposizioni concernenti la tecnologia 5G ma anche altre che ampliano la sorveglianza in generale. In particolare criticano l'ulteriore automatizzazione, la virtual private network (VPN, rete privata virtuale), la rimozione dei criptaggi applicati dai fornitori, la memorizzazione delle porte, degli indirizzi IP e di altri dati (considerata una forma di conservazione preventiva dei dati)[7], la localizzazione (LALS), la marca temporale, i termini di attuazione ridotti e i termini transitori troppo brevi. L'adeguamento agli sviluppi tecnologici cela, secondo loro, una massiccia estensione delle sorveglianze. In sintesi, queste estensioni degli obblighi di cooperare da un lato imporrebbero alle imprese oneri nuovi e sproporzionati e dall'altro limiterebbero la privacy e la protezione dei dati degli utenti.

Nel riformulare il progetto si è tenuto conto dei punti seguenti emersi in sede di consultazione:

- alcune disposizioni sono state adeguate o completamente stralciate affinché l'onere a carico delle POC risultante dalle modifiche delle ordinanze (in particolare l'adeguamento dei sistemi) sia proporzionato ai vantaggi per le autorità di perseguimento penale (proporzionalità delle modifiche);
- diversi partecipanti hanno criticato la memorizzazione dei numeri di porta e degli indirizzi IP di destinazione sostenendo in particolare che la memorizzazione di questi dati equivale a un'estensione della sorveglianza, che non vi è una base legale al riguardo e che tale memorizzazione è inoltre problematica alla luce delle vigenti disposizioni in materia di protezione dei dati. Il nuovo obbligo di trasmettere gli elementi d'indirizzo di destinazione (destination NAT) è rimandato alla seconda revisione in modo da introdurre contemporaneamente le categorie di POC e i relativi obblighi. Qui si tratta di un'informazione e non di una sorveglianza. Se necessario ai fini dell'identificazione, le informazioni di cui all'articolo 22 LSCPT possono fondarsi anche sui metadati, i quali non vengono diffusi. Inoltre si suggerisce ai fornitori di scegliere una procedura che non necessiti degli indirizzi IP e delle porte di destinazione per identificare gli utenti così da non doverli neppure memorizzare. La LSCPT (in particolare gli art. 21 e 22) costituisce una base legale sufficiente. Anche se si trattasse di una sorveglianza, l'articolo 269 del Codice di procedura penale (CPP)[8] non prevede alcuna limitazione pertinente;
- il capoverso dell'articolo 50 che prevedeva l'obbligo per i fornitori di servizi di comunicazione derivati (FSCD) con obblighi di sorveglianza supplementari di sopprimere i criptaggi è stato stralciato. I fornitori di servizi di telecomunicazione (FST) continuano ad essere tenuti a sopprimere i loro criptaggi come previsto all'articolo 26 capoverso 2 lettera c LSCPT;
- i termini transitori per l'adeguamento dei sistemi delle POC sono stati prolungati (24 mesi dall'entrata in vigore della OSCPT);

7 Concerne le modifiche agli art. 21, 38, 42*a*, 43, 43*a*, 60, 62 e 63 OSCPT.
8 RS **312.0**

- gli emolumenti dei nuovi tipi di sorveglianza della determinazione della posizione sono stati leggermente ridotti. Inoltre anche l'emolumento complessivo per il tipo di informazione che implica l'impiego di un IMSI catcher (p. es. nelle ricerche d'emergenza) è stato abbassato (cfr. n. 3.2).

Nel riformulare il progetto si è potuto tener conto solo parzialmente dei punti seguenti emersi in sede di consultazione:

- le POC e alcuni partiti hanno criticato il fatto che, oltre agli adeguamenti alla tecnologia 5G, siano state apportate modifiche che ampliano massicciamente la sorveglianza e conseguentemente gli obblighi a carico delle POC. Sono stati particolarmente criticati i dati necessari all'identificazione degli utenti, la fornitura in forma automatizzata di determinate informazioni, la determinazione della posizione e i termini di trattamento ridotti (su questi punti in particolare si rimanda ai commenti riportati di seguito). A questa critica generale va replicato che gli adeguamenti alla tecnologia 5G offriranno nuove possibilità di sorveglianza (p. es. la localizzazione). Anche gli standard ETSI sono già stati modificati conseguentemente. Le numerose modifiche nelle ordinanze, e in particolare nella OSCPT, hanno lo scopo di adeguare questi atti normativi allo sviluppo tecnologico in modo da garantire una sorveglianza impeccabile. Anche le possibilità di localizzazione, ottimizzate grazie alla tecnologia 5G, migliorano la qualità dei dati della sorveglianza. Alcuni adeguamenti perfezionano l'identificazione degli utenti e non costituiscono obblighi supplementari. Tuttavia si è tenuto parzialmente conto di queste critiche: da un lato, varie disposizioni del progetto precisano che i nuovi tipi di informazione e sorveglianza non riguardano i FSCD con obblighi supplementari, pertanto questi fornitori non hanno alcun obbligo corrispondente. Dall'altro, alcune modifiche degli obblighi a carico delle POC, ossia i tipi di informazione concernenti l'identificazione dell'utente di cui ai nuovi articoli 42*a* e 43*a* OSCPT, sono rimandati alla seconda revisione. In questo modo è possibile introdurre i nuovi obblighi insieme a una descrizione più dettagliata delle categorie di POC interessate;
- le POC hanno chiesto che la fornitura in forma automatizzata delle informazioni sia introdotta come opzione e non come obbligo. La richiesta è stata soddisfatta nella misura in cui l'obbligo di fornire in forma automatizzata le informazioni è imposto esclusivamente alle POC che già oggi lo fanno e che quindi hanno già effettuato gli investimenti necessari al riguardo. Adesso il tipo di informazione IR_13_EMAIL (informazioni su utenti di servizi di posta elettronica) va trasmesso manualmente poiché, con i nuovi requisiti, sarebbe troppo complicato per le POC trasmetterlo in forma automatizzata. Il nuovo tipo di informazione IR_52_ASSOC_TEMP (informazioni immediate su identificativi attribuiti per breve tempo) va invece fornito in forma automatizzata poiché i dati devono essere immediatamente disponibili, il che non sarebbe possibile fornendoli manualmente;
- il disciplinamento riguardante la determinazione della posizione concerne solamente la tecnologia 5G e il termine per l'implementazione è stato portato da 12 o 18 mesi a 24.

Nel riformulare il progetto non si è potuto tener conto dei punti seguenti emersi in sede di consultazione:

- alcuni Cantoni come anche la CCPCS chiedono che le formulazioni nelle ordinanze siano neutre dal punto di vista tecnologico. A loro parere i dettagli tecnici andrebbero spostati in allegati o in istruzioni di modo da poterli rapidamente adeguare. Formulare solamente singole disposizioni in modo neutro dal punto di vista tecnologico compromette l'impianto globale della OSCPT rendendola meno comprensibile. Pertanto questa richiesta può essere soddisfatta soltanto nel quadro di una revisione totale della OSCPT. Poiché in questo modo si ritarderebbero eccessivamente gli adeguamenti alla tecnologia 5G, la richiesta sarà esaminata in occasione della prossima revisione;
- le POC hanno criticato la riduzione dei termini di trattamento della risposta nel caso di determinati tipi di informazione. Nella pratica le autorità legittimate ritengono che un giorno lavorativo per il trattamento della risposta sia un intervallo troppo lungo se la richiesta è presentata nel fine settimana o in un giorno festivo. Il termine di un giorno lavorativo può far sì che le informazioni arrivino troppo tardi, il che può avere gravi conseguenze in alcuni casi urgenti, come le minacce anonime di attentati dinamitardi. La corrispondente riduzione del termine nella OE-SCPT è quindi adeguata anche perché si applica solamente alle domande di informazioni giunte al di fuori degli orari d'ufficio ordinari e nei giorni festivi;
- molti fornitori, ma anche altre organizzazioni, hanno chiesto di aumentare l'indennità per le POC, mentre quattro Cantoni ne chiedono la riduzione. Le POC ritengono in particolare troppo basse le indennità di tre franchi per tutte le informazioni semplici. Nella sentenza del 27 luglio 2021 (2C-650/2020), il Tribunale federale ha tuttavia considerato equa ai sensi dell'articolo 38 capoverso 2 LSCPT un'indennità di tre franchi per la risposta a una domanda di informazione IR-7 IP (art. 37 OSCPT). Questa richiesta non viene trattata nel presente progetto, poiché anche gli emolumenti e le indennità per i nuovi tipi di informazione e sorveglianza sono disciplinati nella OF-SCPT che introduce gli importi forfettari.

3 Punti essenziali del progetto

3.1 Adeguamenti della OSCPT

La OSCPT è adeguata ai progressi tecnologici come la tecnologia 5G e l'IMS e introduce tre nuovi tipi di informazione e quattro nuovi tipi di sorveglianza:

- il tipo di informazione IR_51_ASSOC_PERM, informazioni su identificativi attribuiti a lungo termine (art. 48*a* OSCPT);
- il tipo di informazione IR_52_ASSOC_TEMP, informazioni immediate su identificativi attribuiti per breve tempo (art. 48*b* OSCPT);
- il tipo di informazione IR_53_TEL_ADJ_NET, determinazione delle reti adiacenti di servizi di telefonia e multimedia (art. 48*c* OSCPT);

- il tipo di sorveglianza (sorveglianza in tempo reale) RT_54_POS_ONCE, determinazione unica e immediata della posizione mediante la rete (art. 56*a* OSCPT);
- il tipo di sorveglianza (sorveglianza in tempo reale) RT_55_POS_PERIOD, determinazione ricorrente e periodica della posizione mediante la rete (art. 56*b* OSCPT);
- il tipo di sorveglianza (ricerca d'emergenza) EP_56_POS_ONCE, determinazione unica e immediata della posizione mediante la rete (art. 67 lett. b OSCPT); e
- il tipo di sorveglianza (ricerca d'emergenza) EP_57_POS_PERIOD, determinazione ricorrente e periodica della posizione mediante la rete (art. 67 lett. c OSCPT).

Viene introdotto il tipo di informazione IR_51_ASSOC_PERM per acquisire gli identificativi attribuiti a lungo termine a un determinato identificativo nell'IMS. Con il nuovo tipo di informazione IR_52_ASSOC_Temp si può consultare, quasi in tempo reale e in modo automatizzato, l'identificativo permanente di un identificativo temporaneo della tecnologia 5G ricorrendo a un apparecchio tecnico speciale di sorveglianza del traffico delle telecomunicazioni (art. 269bis CPP; i cosiddetti IMSI catcher). Il nuovo tipo di informazione IR_53_TEL_ADJ_NET permette di risolvere problemi specifici, legati all'identificazione degli autori di reati, che si verificano quando il numero di telefono del chiamante o del mittente del messaggio è falsificato (spoofing) o sconosciuto. Questo può essere utile, ad esempio, per rintracciare la telefonata o il messaggio anonimi in caso di minacce di attentati dinamitardi. Per sfruttare le nuove possibilità tecniche offerte dal «Lawful Access to Location Services» (LALS) al fine di determinare la posizione nella telefonia mobile sono introdotti quattro nuovi tipi di sorveglianza che permettono la determinazione unica o periodica della posizione mediante la rete come sorveglianza in tempo reale (art. 56*a* e 56*b*) o come ricerca d'emergenza (art. 67 lett. b e c).

Il nuovo articolo 4*a* OSCPT fissa la regola del «dies a quo» per il calcolo, finora controverso nella pratica, del termine di sei mesi applicato alle sorveglianze retroattive.

Per migliorarne la leggibilità, l'attuale articolo 18 OSCPT è ora suddiviso in quattro articoli (art. 18, 18*a*, 18*b* e 18*c*) che specificano meglio gli obblighi per la fornitura di informazioni. Viene precisato che le POC di cui al capoverso 1 devono fornire in forma automatizzata le informazioni indicate mentre per le altre informazioni possono scegliere una trasmissione manuale o, d'accordo con il Servizio SCPT, in forma automatizzata.

L'articolo 20 OSCPT (registrazione dei dati degli utenti dei servizi di telefonia mobile) è ora completato e le disposizioni concernenti le persone fisiche e giuridiche suddivise nei successivi articoli intercalari. L'articolo 20*c* OSCPT disciplina la consegna di mezzi di accesso e l'attivazione di servizi per le autorità di polizia federali e cantonali nonché per il Servizio delle attività informative della Confederazione (SIC), a condizione che i dati siano accessibili solamente a una cerchia ristretta di persone. Il vigente articolo 20 prevede la verifica dell'identità di tutti gli utenti quindi anche dei membri delle autorità di polizia e dei collaboratori del SIC. Nella pratica questo disciplinamento si è dimostrato negli ultimi anni particolarmente problematico per queste autorità.

Per garantire un'introduzione ineccepibile dei nuovi tipi di informazione e di sorveglianza presso le POC e il Servizio SCPT, l'articolo 74*a* OSCPT prevede dettagliate disposizioni transitorie per le singole modifiche.

3.2 Adeguamenti della OEm-SCPT

In seguito all'introduzione nella OSCPT dei nuovi tipi di informazione e dei tipi di sorveglianza, è stato necessario adeguare anche l'allegato della OEm-SCPT. Gli emolumenti e le indennità degli altri tipi di informazione e di sorveglianza restano invariati. Poiché si prevede che la OF-SCPT e la presente revisione entrino in vigore contemporaneamente il 1° gennaio 2024, si rinuncia a modificare la OEm-SCPT. Le modifiche necessarie sono riprese nell'avamprogetto della OF-SCPT.

3.3 Adeguamenti della OE-SCPT

La revisione della OE-SCPT modifica leggermente i termini per il trattamento delle domande di informazioni (art. 14 OE-SCPT) al fine di tenere conto della richiesta urgente di termini più corti espressa dalle autorità di perseguimento penale. Inoltre, il campo di applicazione della OE-SCPT comprende ora anche le autorità di cui all'articolo 1 capoverso 2 lettere a-f OSCPT. In questo modo il nuovo articolo 3 OE-SCPT, che disciplina la sicurezza della comunicazione, ora vale anche per le autorità.

3.4 Adeguamenti della OST-SCPT

Il presente progetto permette di rivedere alcune disposizioni della OST-SCPT. Oltre agli accessi alla segnalazione dello stato di esercizio delle componenti relative alla sorveglianza del sistema di trattamento (la cosiddetta «dashboard PTSS»), adesso sono disciplinati anche gli accessi del Servizio SCPT ai dati del sistema di trattamento (art. 8 cpv. 3-6) e la durata di conservazione dei verbali della distruzione dei dati (art. 10 cpv. 4).

4 Commento ai singoli articoli

4.1 Ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT)

Osservazione preliminare

Nel testo dell'ordinanza sono utilizzate le espressioni «se del caso», «se disponibili», «se noti» e «se possibile»; esse sottintendono che il relativo disciplinamento va considerato nel rispettivo contesto. Dette espressioni riguardano parametri o funzioni opzionali, nonché tecnologie, standard o versioni di standard i cui dettagli non possono

essere approfonditi nella OSCPT. Su richiesta del Servizio SCPT, i fornitori devono motivare dettagliatamente perché, nell'ambito dei loro obblighi di collaborazione, determinati parametri, dati e funzioni non sono disponibili o non possono essere forniti.

Sostituzione di espressioni

Ai sensi del *capoverso 1,* l'espressione «punto di accesso WLAN» è sostituita con l'espressione più generale «accesso WLAN» poiché quest'ultima comprende sia i punti di accesso che gli hotspot. Questo adeguamento è opportuno poiché la prassi ha evidenziato che l'identificazione di un determinato accesso WLAN spesso non è possibile al livello del punto di accesso (access point), bensì soltanto al livello dell'hotspot.

Il *capoverso 2* stabilisce che la revisione permette di introdurre nella OSCPT l'abbreviazione *FSCD* (fornitori di servizi di comunicazione derivati; art. 2 lett. c LSCPT), già usata nella prassi insieme all'abbreviazione *FST (*fornitori di servizi di telecomunicazione; art. 2 lett. b LSCPT; cfr. anche la modifica dell'art. 1 cpv. 2 lett. j).

Il *capoverso 3* riguarda l'espressione «identificativo sorvegliato (Target ID)» che può essere abbreviata in «target ID».

Art. 1 cpv. 1 e 2 lett. j

Il *capoverso 1* subisce una lieve modifica redazionale.

Il *capoverso 2 lettera j* introduce l'abbreviazione *FSCD* (cfr. l'abbreviazione *FST* già usata nella lett. i). Il passaggio «fornitori di servizi che si fondano su servizi di telecomunicazione e permettono una comunicazione unilaterale o multilaterale», ripreso dal testo di legge (art. 2 lett. c LSCPT), è stralciato per evitare un'inutile ripetizione. Per i FSCD con obblighi di informazione supplementari (art. 22) e per quelli con obblighi di sorveglianza supplementari (art. 52) si utilizza l'espressione generica *FSCD con obblighi supplementari*. Sotto il profilo materiale la disposizione non cambia.

Art. 3 **Richieste al Servizio SCPT**

La frase introduttiva è adeguata in modo da disciplinare anche le trasmissioni delle autorità di approvazione. La presente disposizione contempla anche la possibilità di rilevare, mediante procedura di richiamo, le autorizzazioni alla sorveglianza nonché eventuali condizioni poste dall'autorità di approvazione. L'approvazione fa parte dello svolgimento e del controllo delle pratiche di cui all'articolo 6 lettera f OST-SCPT in combinato disposto con l'articolo 7 lettera e LSCPT.

Seconda la *lettera a* in futuro sarà il DFGP e non più il Servizio SCPT a definire il mezzo di trasmissione sicuro nell'articolo 3 OE-SCPT (ordinanza dipartimentale). Poiché il telefax è tecnologicamente superato e non soddisfa più gli attuali standard di sicurezza, la *lettera b* non lo riporta più. La *lettera c* non contiene modifiche materiali.

Poiché oggi di norma l'accesso è online, il vigente *capoverso 2* non è più attuale ed è stralciato.

Art. 4a **Inizio e fine della sorveglianza retroattiva**

Il nuovo articolo 4*a* si applica sia alla corrispondenza postale che al traffico delle telecomunicazioni; per questo motivo l'articolo è collocato nella sezione 2 «ordine di sorveglianza».

La durata massima di una sorveglianza retroattiva è definita nella legge. L'autorità che dispone la sorveglianza può anche ordinare una durata più breve. I metadati possono essere richiesti con effetto retroattivo fino a sei mesi, indipendentemente dalla durata della sorveglianza (art. 273 cpv. 3 CPP). A tale scopo i fornitori interessati devono conservare per sei mesi i metadati della corrispondenza postale e del traffico delle telecomunicazioni (art. 19 cpv. 4 e 26 cpv. 5 LSCPT) nonché i metadati ai fini dell'identificazione (art. 21 cpv. 5 OSCPT in combinato disposto con gli art. 21 cpv. 2 e 22 cpv. 2 LSCPT). Finora nessuna ordinanza stabiliva dettagliatamente come intendere nella prassi il termine di sei mesi per il calcolo dell'inizio e della fine di una sorveglianza retroattiva, il che in varie occasioni ha dato adito a discussioni.

Il nuovo *capoverso 1* fissa la regola del «dies a quo» per il calcolo del termine di sei mesi nelle sorveglianze retroattive. Il giorno determinante per il calcolo è quello nel quale si riceve l'ordine del Servizio SCPT e non la data dell'ordine o della trasmissione[9] da parte dell'autorità che dispone la sorveglianza.

Si preferisce fare riferimento al giorno della ricezione invece che a quello della trasmissione dell'ordine per i seguenti motivi: nella consueta trasmissione mediante la componente di gestione dei mandati WMC[10], non fa differenza se il calcolo del termine si basa sul giorno di trasmissione o di ricezione, poiché tra il momento in cui l'autorità trasmette l'ordine e quello in cui il Servizio SCPT lo riceve passano solamente pochi secondi. Solo se l'ordine è trasmesso per posta, ossia solo in casi eccezionali e qualora un mezzo sicuro di trasmissione autorizzato dal DFGP non sia a disposizione per motivi tecnici (art. 3 OSCPT), vi è una differenza temporale di uno o addirittura più giorni (cfr. sotto es. 4). L'autorità che dispone la sorveglianza può evitare questo ritardo impartendo l'ordine al Servizio SCPT per telefono secondo l'articolo 3 lettera c. Se l'ordine è impartito per telefono, fa stato il momento della telefonata e non quello della ricezione dell'ordine trasmesso successivamente per iscritto (cfr. sotto es. 3).

Un intervallo di uno o più giorni tra la trasmissione dell'ordine da parte dell'autorità e l'assegnazione, da parte del Servizio SCPT, del mandato al fornitore sarebbe problematico poiché, ai sensi dell'articolo 21 capoverso 7, i fornitori sono tenuti anche a distruggere i dati storici una volta scaduto il termine di conservazione di sei mesi. Come illustrato all'esempio 4, vi è dunque il rischio che i dati più vecchi richiesti dalle autorità che dispongono la sorveglianza siano già stati distrutti dal fornitore quando quest'ultimo riceve il mandato di sorveglianza. Il Servizio SCPT garantisce che dal momento in cui riceve l'ordine di sorveglianza a quando trasmette i relativi mandati

9 Per trasmissione s'intende uno dei mezzi di trasmissione previsti dall'articolo 3 OSCPT (SYLVAIN Métille, in KUHN/ JEANNERET, Commentaire romand du Code de procédure pénale suisse, Helbling Lichtenhahn, 2ª ed. 2019, Basilea, ad art. 274, pag. 1794, n. marg. 12).

10 Warrant Management Component (WMC): una componente del sistema di trattamento del Servizio SCPT (cfr. il programma STT), operativa dal 18 mar. 2019.

al fornitore trascorra al massimo un'ora. Poiché il momento della ricezione dell'ordine è determinante per calcolare quando far iniziare al più presto la sorveglianza retroattiva, non vi è dunque alcun conflitto per il fornitore tra la conservazione e la cancellazione dei metadati.

Va osservato che nel momento in cui l'autorità che dispone la sorveglianza trasmette l'ordine al Servizio SCPT inizia a decorrere anche il termine di 24 ore per la presentazione dei documenti al giudice dei provvedimenti coercitivi previsto dall'articolo 274 capoverso 1 CPP[11].

Di norma l'ordine viene caricato nella componente WMC del sistema di trattamento del Servizio SCPT in modo tale che il Servizio SCPT lo riceva il giorno stesso in cui l'autorità che dispone la sorveglianza lo trasmette (cfr. sotto es. 2).

La sorveglianza retroattiva inizia pertanto al più presto sei mesi prima del giorno in cui il Servizio SCPT riceve l'ordine. Va ricordato che l'articolo 273 capoverso 3 CPP prevede un termine espresso in mesi e non in giorni o ore.

Il calcolo del termine di sei mesi si fonda sulla dottrina[12] e sulla giurisprudenza[13]: il termine fissato in mesi scade il giorno che, nel calendario, corrisponde al giorno in cui l'evento è attivato; se il mese in questione non ha tale numero, il giorno coincide con l'ultimo giorno di tale mese[14]. Per la sorveglianza retroattiva questo significa che un termine fissato in mesi decorre il giorno il cui numero corrisponde alla data della ricezione dell'ordine da parte del Servizio SCPT. Il giorno dell'inizio della sorveglianza retroattiva ha di norma lo stesso numero del giorno (GG) della data (GG.MM.AAAA) della ricezione dell'ordine da parte del Servizio SCPT.

Il *secondo periodo* disciplina il caso particolare in cui il giorno corrispondente manca nel mese di inizio della sorveglianza retroattiva, ossia se questo mese ha meno giorni di quello dell'ordine. Se ad esempio il Servizio SCPT riceve l'ordine il 31 del mese, il giorno di inizio della sorveglianza retroattiva è il giorno 31 di sei mesi prima. Se però il 31 non esiste in tale mese, si prende l'ultimo giorno del mese (p. es. il 31 aprile non esiste, quindi si prende il 30 aprile, cfr. sotto esempi 2 e 3).

Secondo il *capoverso 2* la sorveglianza retroattiva finisce al più tardi il giorno della ricezione dell'ordine da parte del Servizio SCPT, ossia alle 23.59 e 59 secondi[15] ora svizzera di tale giorno (cfr. sotto es. 1-4). Di norma, le sorveglianze retroattive sono effettuate solamente in uno dei giorni successivi (periodo di trattamento nei casi normali: 3 giorni lavorativi). Se invece la sorveglianza retroattiva è eseguita lo stesso giorno – ossia prima delle 23.59 e 59 secondi – l'autorità legittimata riceve soltanto i

11 MARC JEAN-Richard-DIT-BRESSEL, in Basler Kommentar, NIGGLI, HEER, WIPRÄCHTIGER, Helbling Lichtenhahn, 2ª ed. 2014, Basilea ad art. 274, pag. 2168, n. marg. 4 in fine; SYLVAIN MÉTILLE, op.cit., ad art. 274, pag. 1796, n. marg. 23 («Le délai [de vingt-quatre heures] se compte à la minute près, dès la transmission de l'ordre de surveillance au Service SCPT»).

12 In particolare DANIEL STOLL, in KUHN/ JEANNERET, Commentaire romand du Code de procédure pénale suisse, Helbling Lichtenhahn, 2ª ed. 2019, Basilea, ad art. 90, pag. 430 e 431, n. marg. 12.

13 In particolare DTF 144 IV 161 (sentenza 6B_80/2018 del 25 aprile 2018).

14 Cfr. anche p. es. art. 22 cpv. 2 dell'ordinanza del 30 ago. 1995 sulla tassa d'esenzione dall'obbligo militare (OTEO; RS **661.1**)

15 Per le sorveglianze retroattive, l'ora è indicata con i secondi arrotondati.

metadati (dati storici, HD) disponibili presso il fornitore fino al momento dell'esecuzione della sorveglianza. Gli altri dati storici, ossia quelli rilevati tra il momento dell'esecuzione della sorveglianza e la fine di tale giorno, non sono trasmessi successivamente. Ciò è rilevante soprattutto se una sorveglianza retroattiva è stata dichiarata urgente (cfr. sotto es. 5). Il fornitore non è tenuto neppure a trasmettere successivamente i dati storici rilevanti di cui dispone solo in un secondo momento a causa di ritardi usuali (p. es. dati del roaming). Se tali dati sono importanti per l'autorità che dispone la sorveglianza, questa dovrebbe prendere in considerazione un'altra sorveglianza retroattiva in un momento successivo (cfr. sotto es. 5). Pretendere la trasmissione successiva di dati storici di cui il fornitore non dispone, per ragioni obiettive, al momento della prima trasmissione di dati comporterebbe per quest'ultimo oneri sproporzionati. L'autorità che dispone la sorveglianza può gestire il momento dell'esecuzione della sorveglianza retroattiva in base ai dati storici che ritiene importanti (i più vecchi o i più recenti). Se sono importanti i dati storici più vecchi, l'ordine per la sorveglianza retroattiva va impartito il prima possibile. Per ricevere i dati storici completi più recenti, l'autorità che dispone la sorveglianza ha due possibilità: un normale ordine di sorveglianza dei dati storici con esecuzione in uno dei giorni successivi, se questi dati non sono necessari nell'immediato, oppure un ordine di sorveglianza in tempo reale «solo metadati (IRI only)» se i metadati più recenti sono necessari nell'immediato e se l'obiettivo è aggirare l'inevitabile ritardo legato ai dati storici. Tuttavia, i dati storici e i metadati in tempo reale non si equivalgono per volume e dettagli: di regola gli IRI sono più ampi e dettagliati.

I fornitori tenuti a conservare i metadati devono garantire un tempo sufficientemente lungo di conservazione tenendo conto sia della suddetta regola per il calcolo dell'inizio più tempestivo possibile di una sorveglianza retroattiva sia dei termini di trattamento di cui agli articoli 17 e 18 OE-SCPT. Nei casi normali, il fornitore esegue la sorveglianza retroattiva entro tre giorni lavorativi dalla ricezione del mandato, mentre nei casi urgenti, la esegue entro sei ore (art. 17 cpv. 3 OE-SCPT).

Di seguito sono riportati alcuni esempi per il calcolo del termine di sei mesi. I valori standard dell'ora (svizzera) dell'inizio e della fine della sorveglianza sono rispettivamente le ore 00.00 e 0 secondi[16] e le ore 23.59 e 59 secondi (negli esempi i secondi non sono indicati) a meno che la sorveglianza non sia eseguita lo stesso giorno dell'ordine; in tal caso l'ora della fine della sorveglianza corrisponde esattamente a quella dell'inizio più 59 secondi. Il fornitore deve trasmettere i dati storici disponibili al momento dell'esecuzione.

Esempio 1: a causa di ritardi interni presso l'autorità che ha disposto la sorveglianza, l'ordine, datato martedì 8 novembre 2022, è spedito mediante messaggio elettronico criptato solamente giovedì **10 novembre 2022** alle 09.00 e il Servizio SCPT lo riceve alla stessa ora.
→ **GG** inizio **= 10**, MM: 11 - 6 = 5 → **MM = 05**, **AAAA = 2022**
Inizio non prima del 10 maggio 2022, ore 00.00;
fine non oltre il 10 novembre 2022, ore 23.59.

Osservazione: questo esempio illustra il problema della trasmissione ritardata dell'ordine. Se l'ordine fosse stato trasmesso immediatamente, l'autorità che ha disposto la

16 Per la sorveglianza retroattiva, l'ora è indicata con i secondi arrotondati.

sorveglianza avrebbe potuto ricevere i dati storici dall'8 maggio 2022, ossia due giorni prima, ma la sorveglianza sarebbe terminata due giorni prima, ossia l'8 novembre 2022.

Esempio 2: ordine caricato in WMC mercoledì **31 agosto 2022** alle 18.00
→ **GG** inizio **= 31**, MM: 8 - 6 = 2 → **MM = 02**, **AAAA = 2022**
Poiché il 31 febbraio 2022 non esiste, si prende l'ultimo giorno di febbraio 2022.
Inizio non prima del 28 febbraio 2022, ore 00.00;
fine non oltre il 31 agosto 2022, ore 23.59.

Esempio 3: ordine orale per telefono al Servizio SCPT la domenica **31 dicembre 2023** alle 16.50.
→ **GG** inizio **= 31**, MM: 12 - 6 = 6 → **MM** = **06**, **AAAA = 2023**
Poiché il 31 giugno 2023 non esiste, si prende l'ultimo giorno di giugno 2023.
Inizio non prima del 30 giugno 2023, ore 00.00;
fine non oltre il 31 dicembre 2023 ore 23.59.

Esempio 4: ordine datato mercoledì 13 aprile 2022, inviato per posta giovedì 14 aprile 2022 (timbro postale), nessun avviso telefonico. Ricevuto dal Servizio SCPT martedì **19 aprile 2022** (dopo Pasqua) alle ore 9.00. Mandato di sorveglianza inoltrato al fornitore il 19 aprile 2022 alle 9.50.
→ **GG** inizio **= 19**, MM: 4 - 6 = -2 + 12 → **MM** = **10** dell'anno precedente, AAAA: 2022 - 1 → **AAAA = 2021**
Inizio non prima del 19 ottobre 2021, ore 00.00;
fine non oltre il 19 aprile 2022, ore 23.59.

Osservazione: in caso di ordine per telefono, il giorno determinante è quello della chiamata e non quello della ricezione della conferma scritta (cfr. es. 3). In questo esempio, se ci fosse stato un avviso telefonico il 14 aprile 2022 (5 giorni prima), la sorveglianza retroattiva sarebbe potuta cominciare già il 14 ottobre 2021, ma sarebbe quindi finita il 14 aprile 2022.

Esempio 5: ordine di sorveglianza retroattiva **urgente**, caricato in WMC venerdì **26 agosto 2022** alle **16.00** dall'autorità che ha disposto la sorveglianza, mandato trasmesso alla POC dal Servizio SCPT alle 16.30.
→ **GG** inizio **= 26**, MM: 8 - 6 = 2 → **MM = 02**, **AAAA = 2022**
Inizio non prima del 26 febbraio 2022, ore 00.00;
fine non oltre il 26 agosto 2022.

Poiché la sorveglianza retroattiva finisce il giorno in cui è stata disposta, l'ora determinante per la fine risulta dal momento dell'esecuzione da parte della POC (ha al massimo 6 ore di tempo dopo la ricezione del mandato, ossia, nell'esempio, non più tardi delle 22.30). Per motivi tecnici, i dati storici più recenti presso la POC non sono ancora pronti per essere trasmessi. L'autorità che ha disposto la sorveglianza deve effettuare una ponderazione tra la velocità della trasmissione e la disponibilità dei metadati. I metadati retroattivi possono essere disponibili presso la POC soltanto con alcune ore di ritardo. Si dovrebbe prendere in considerazione una sorveglianza retroattiva con inizio in un momento successivo (il che comporterebbe però la perdita dei metadati più vecchi) o, in caso di sorveglianze urgenti, una sorveglianza in tempo reale «solamente di metadati» (cfr. più sopra).

Art. 11 Prestazioni al di fuori degli orari d'ufficio ordinari e nei giorni festivi

Questa disposizione, interamente rivista a seguito delle numerose modifiche, disciplina le prestazioni delle POC elencate e del Servizio SCPT al di fuori degli orari d'ufficio ordinari, ossia dal lunedì al venerdì tra le 17.01 e le 07.59, nonché durante il fine settimana e nei giorni festivi (cfr. art. 10). Durante questi periodi, il Servizio SCPT e le POC elencate mettono a disposizione un servizio di picchetto. I termini di trattamento per le prestazioni del Servizio SCPT e delle POC sia durante il servizio di picchetto sia negli orari d'ufficio ordinari sono disciplinati nella OE-SCPT. La POC può fornire, su base volontaria durante il servizio di picchetto, prestazioni concernenti informazioni standardizzate (art. 26 cpv. 1) e sorveglianze standardizzate (art. 28) che esulano dai suoi obblighi di picchetto; tali prestazioni non sono soggette ai termini di trattamento.

Il capoverso 1 è adeguato e strutturato in modo diverso. Sotto il profilo materiale non vi sono modifiche sostanziali per il Servizio SCPT, le autorità e le POC. In particolare per le POC la soluzione di eventuali problemi è già prevista nel vigente articolo 11 (cpv. 1 lett. e in combinato disposto con il cpv. 2) come pure la reperibilità 24 ore su 24, 7 giorni su 7 («in ogni momento», fine cpv. 2). I FST con obblighi integrali (ossia non esentati ai sensi dell'art. 51) e i FSCD con obblighi di sorveglianza supplementari (art. 52) devono assicurare un servizio di picchetto per tutte le prestazioni di cui al capoverso 1 lettere a–e, a condizione che siano tenuti a fornire dette prestazioni ai sensi degli articoli 18 e 50. Questa restrizione è dovuta al fatto che i FSCD con obblighi di sorveglianza supplementari (art. 52) non devono fornire i nuovi tipi di informazioni di cui agli articoli 48*a*–48*c* né eseguire i nuovi tipi di sorveglianza di cui agli articoli 56*a* e 56*b* o i nuovi tipi di ricerca d'emergenza di cui all'articolo 67 capoverso 1 lettere b e c oppure i nuovi tipi di ricerca di condannati di cui all'articolo 68 capoverso 1 lettere b e c. In questo capoverso non sono citati i FST con obblighi di sorveglianza ridotti (art. 51), i FSCD senza obblighi supplementari (vale a dire quelli che non soddisfano i criteri di cui all'art. 22 e 52), i FSCD con obblighi d'informazione supplementari (art. 22) e le POC di cui all'articolo 1 capoverso 2 lettere k, l e m, poiché non devono prestare servizio di picchetto.

Le lettere a–e enumerano in modo esaustivo le prestazioni da fornire durante il servizio di picchetto. Va notato che, durante il picchetto, il Servizio SCPT fornisce solamente una consulenza limitata. La *lettera a* disciplina la trasmissione di determinate informazioni. Va precisato che le informazioni di cui agli articoli 44-48 non vanno necessariamente trasmesse durante il servizio di picchetto. La *lettera b* disciplina i tipi di sorveglianza in tempo reale da attivare durante il picchetto, mentre la *lettera c* stabilisce i tipi di sorveglianza retroattiva, dichiarati urgenti, da effettuare durante il picchetto. La *lettera d* elenca i tipi di ricerche d'emergenza e di condannati da effettuare durante il picchetto. La lettera d^{bis}[17], in vigore dal 1° giugno 2022, diventa la nuova *lettera e*.

[17] Ordinanza del 4 mag. 2022 sulle misure di polizia per la lotta al terrorismo (OMPT; RU **2022** 301)

Il *capoverso 2* sancisce la prassi attuale secondo cui le autorità devono annunciare per telefono al servizio di picchetto del Servizio SCPT tutti i mandati di cui al capoverso 1. Fanno eccezione solamente le informazioni fornite in forma automatizzata. Solo in questo modo è possibile garantire che i collaboratori del Servizio SCPT siano avvertiti per tempo dei mandati, possano trattarli entro i termini previsti e informare a loro volta del mandato la POC in questione.

Il *capoverso 3* non subisce modifiche materiali rispetto a quello vigente. Si procede soltanto a una modifica redazionale al fine di riprendere il tenore del capoverso 1 («al di fuori degli orari d'ufficio ordinari e nei giorni festivi»). Il capoverso 3 stabilisce che le informazioni e le sorveglianze particolari (cfr. art. 25) sono escluse dalle prestazioni fornite durante il servizio di picchetto. Si tratta di informazioni e di sorveglianze che non corrispondono ad alcun tipo di informazione o di sorveglianza dell'ordinanza (le cosiddette informazioni o sorveglianze non standardizzate) e che competono al Servizio SCPT o a persone incaricate da quest'ultimo. La fornitura di queste informazioni o l'esecuzione di queste sorveglianze è molto più complessa rispetto ai tipi standardizzati; non sono pianificabili e l'onere sotto il profilo del personale è difficilmente stimabile. Mettere a disposizione il personale necessario per il servizio di picchetto presso il Servizio SCPT o presso terzi da esso incaricati implicherebbe costi eccessivi.

Il *capoverso 4* prevede ora che le POC esentate dall'obbligo di garantire un servizio di picchetto secondo il capoverso 1 ma raggiungibili, per altre ragioni, al di fuori degli orari d'ufficio ordinari e nei giorni festivi comunichino al Servizio SCPT i pertinenti numeri e le persone di contatto. La disposizione non impone alle POC nuovi obblighi al riguardo, in particolare non intende obbligarle a costituire un servizio di picchetto appositamente per il Servizio SCPT. Se invece la POC dispone già di un simile servizio, i relativi dati di contatto, se disponibili, vanno comunicati al Servizio SCPT; anche se non si tratta dei dati di contatto di specialisti del settore della sorveglianza (i cosiddetti «LI Officer»), questi contatti potranno aiutare il Servizio SCPT nei casi di particolare urgenza al di fuori degli orari d'ufficio ordinari e nei giorni festivi. I «casi di particolare urgenza» sono ad esempio le minacce dinamitarde, i rapimenti o altri casi nei quali è in gioco la vita o l'integrità fisica delle persone. In casi simili il Servizio SCPT o le autorità di polizia tentano di raggiungere qualsiasi persona presso la POC. L'indicazione di un numero o di una persona di contatto facilita dunque i compiti del Servizio SCPT, delle autorità di perseguimento penale e delle POC.

Art. 18 Obblighi per la trasmissione di informazioni da parte di FST e di FSCD con obblighi supplementari

Il vigente articolo 18, interamente rivisto a seguito delle numerose modifiche, è ora suddiviso in quattro articoli (art. 18, 18*a*, 18*b* e 18*c*) per migliorarne la leggibilità. I quattro articoli illustrano in dettaglio gli obblighi relativi alla fornitura di informazioni.

L'*articolo 18 capoverso 1* sancisce il principio secondo cui i FST con obblighi integrali e i FSCD con obblighi supplementari (art. 22 o 52) devono fornire le informazioni servendosi della IRC[18] del sistema di trattamento del Servizio SCPT.

I vigenti capoversi 1 e 4 prevedono che le POC debbano fornire le informazioni riguardanti i servizi da loro offerti. Il passaggio «riguardanti i servizi da loro offerti» è ridondante quindi non è ripreso nella presente versione. L'obbligo di fornire informazioni continua comunque a riguardare soltanto i servizi offerti dalle POC.

Il *primo periodo del capoverso 2* disciplina i tipi di informazioni che i FST con obblighi integrali devono fornire in forma automatizzata. L'obbligo della forma automatizzata riguarda informazioni frequenti, urgenti o semplici. Il *secondo periodo* precisa che i FST menzionati possono scegliere se fornire le altre informazioni standardizzate (gli altri tipi di informazioni previsti dalla OSCPT) manualmente o, d'accordo con il Servizio SCPT, in forma automatizzata.

La possibilità di scegliere se fornire le informazioni in forma automatizzata o meno è prevista anche per altre POC (cfr. cpv. 3 e 4) e va vista nell'ottica della libertà economica delle POC in oggetto, poiché la trasmissione automatizzata delle informazioni implica spese d'investimento, ma, d'altro canto, permette di risparmiare costi operativi rispetto alla fornitura manuale. Il Servizio SCPT decide, d'accordo con la POC, se il tipo di informazione richiesto possa essere trasmesso in forma automatizzata nella IRC. Questa possibilità di scelta fa sì che alcune POC forniscano determinati tipi di informazioni manualmente, mentre altre in forma automatizzata. Per poter fornire le informazioni richieste in forma automatizzata, le modifiche ai corrispondenti tipi di informazioni comportano per le POC in oggetto anche una serie di corrispondenti adeguamenti a livello di sistemi per la gestione dei clienti e di altri sistemi. Tali modifiche devono quindi tener conto anche degli aspetti di proporzionalità, ad esempio se la frequenza di utilizzo dei corrispondenti tipi di informazioni continua a giustificare un'automazione. Per questa ragione la nuova disposizione non contempla più il tipo di informazione di cui all'articolo 42 (IR_13_EMAIL), utilizzato meno frequentemente, tra le informazioni da trasmettere tassativamente in forma automatizzata (cfr. l'attuale cpv. 2), bensì tra le «altre informazioni» per le quali la POC con obblighi integrali può scegliere la trasmissione manuale o, d'accordo con il Servizio SCPT, quella automatizzata.

Dei tre nuovi tipi di informazioni, solamente il tipo di cui all'articolo 48*b* (IR_52_ASSOC_TEMP) deve essere fornito dai FST interessati in forma automatizzata e non manuale perché i dati in oggetto devono essere immediatamente disponibili. Per gli altri due nuovi tipi di informazioni di cui all'articolo 48*a* (IR_51_ASSOC_PERM) e 48*c* (IR_53_TEL_ADJ_NET), i FST interessati possono scegliere tra una fornitura manuale o, d'accordo con il Servizio SCPT, una trasmissione automatizzata.

La fornitura manuale e quella automatizzata tramite la IRC hanno le caratteristiche seguenti: la forma automatizzata non prevede l'intervento umano né del Servizio SCPT né della POC; l'autorità legittimata inserisce la domanda di informazioni nella

[18] IRC: Information request component; la componente per la fornitura di informazioni del sistema di trattamento del Servizio SCPT (cfr. il programma STT); in esercizio dal 18 marzo 2019.

IRC e riceve entro un'ora la risposta dai sistemi della POC. Nel caso della fornitura manuale tramite la IRC, l'autorità legittimata inserisce la domanda di informazioni nella IRC e la POC è avvertita che ha ricevuto una domanda di informazioni. I collaboratori della POC si collegano alla IRC e compilano a mano la relativa maschera di risposta. L'autorità legittimata riceve la risposta sempre nella IRC.

La terza possibilità è fornire manualmente l'informazione fuori dal sistema di trattamento (cpv. 3 lett. a). In questo caso l'autorità legittimata inserisce la domanda di informazioni nella IRC, ma è il Servizio SCPT che la trasmette alla POC, al di fuori della IRC, utilizzando un mezzo di trasmissione scritto autorizzato dal DFGP. La POC può fornire l'informazione senza particolari requisiti formali e trasmette la risposta, utilizzando un mezzo di trasmissione scritto autorizzato dal DFGP, al Servizio SCPT che a sua volta la inoltra, in modo sicuro, all'autorità legittimata.

Il *capoverso 3* disciplina la fornitura delle informazioni da parte dei FST con obblighi di sorveglianza ridotti (art. 51) esentati dal fornire le informazioni di cui all'articolo 48*b* per ragioni di proporzionalità. Data la criticità temporale del processo, fornire le informazioni di cui all'articolo 48*b* comporta per il FST una preparazione attiva paragonabile a quella prevista per l'esecuzione delle sorveglianze in tempo reale e quindi agli obblighi di sorveglianza di cui all'articolo 26 LSCPT. Per questo tipo di informazione da fornire praticamente subito, il FST interessato deve in particolare investire in una nuova interfaccia di consultazione e nel sistema per la trasmissione automatizzata delle informazioni. La nuova disposizione impone questi oneri aggiuntivi solamente ai grandi FST. A differenza delle altre informazioni, per il tipo di informazione di cui all'articolo 48*b* è difficile che il FST riesca a fornire manualmente informazioni o a trasmettere i dati di cui dispone senza una preparazione attiva.

Per la fornitura delle altre informazioni standardizzate (art. 26 cpv. 1), ai FST con obblighi di sorveglianza ridotti si applica il requisito minimo di cui alla *lettera a* ossia la trasmissione manuale per scritto al di fuori del sistema di trattamento, ma, se preferiscono, possono anche fornire le informazioni manualmente tramite la IRC (*lett. b*, cfr. il commento al cpv. 2). Un FST con obblighi di sorveglianza ridotti può chiedere di fornire determinate informazioni in forma automatizzata (*lett. c)*. Il Servizio SCPT decide, previo accordo con il FST, se ciò è fattibile nella IRC.

Il *capoverso 4 primo periodo* disciplina i tipi di informazioni che i FSCD con obblighi supplementari (art. 22 o 52) devono fornire in forma automatizzata. Il *secondo periodo* prevede che i FSCD menzionati siano esonerati dalla fornitura dei tipi di informazioni di cui ai nuovi articoli 48*a*-48*c*. Nel quadro della seconda revisione, quando sarà adottata una descrizione più dettagliata delle categorie dei FST e dei FSCD, verrà stabilito se in futuro anche questi ultimi dovranno eventualmente fornire dette informazioni. La presente revisione dunque si astiene dall'imporre ai FSCD nuovi obblighi collegati ai nuovi tipi di informazione. Il *terzo periodo* contiene la stessa disposizione, di cui al secondo periodo del capoverso 2 (cfr. i commenti corrispondenti), sulla possibilità di scegliere tra la fornitura in forma automatizzata o manuale delle informazioni tramite la IRC.

Art. 18a Obblighi per la trasmissione di informazioni da parte dei FSCD senza obblighi supplementari e dei gestori di reti di telecomunicazione interne

L'articolo 18*a*, inserito al fine di migliorare la leggibilità, disciplina gli obblighi per la trasmissione di informazioni da parte dei FSCD senza obblighi supplementari, ossia i FSCD che non hanno né obblighi d'informazione supplementari (art. 22) né obblighi di sorveglianza supplementari (art. 52), e dei gestori di reti di telecomunicazione interne.

Il *capoverso 1* stabilisce che, nel fornire le informazioni, essi non sono tenuti a rispettare i tipi previsti dall'ordinanza. Poiché non devono garantire la disponibilità a fornire informazioni, devono fornire soltanto i dati a loro disposizione.

Il *capoverso 2* disciplina la trasmissione dei dati. I FSCD senza obblighi supplementari e i gestori di reti di telecomunicazione interne sono tenuti a soddisfare almeno il requisito minimo ossia a trasmettere i dati disponibili, per scritto, al di fuori del sistema di trattamento e tramite un mezzo di trasmissione sicuro autorizzato dal DFGP.

Tuttavia, secondo il *capoverso 3,* hanno anche la possibilità di trasmettere i dati di cui dispongono, tramite l'interfaccia di consultazione (IRC) del sistema di trattamento del Servizio SCPT manualmente o, d'accordo con il Servizio SCPT, in forma automatizzata.

Art. 18b Ricorso a terzi per fornire informazioni

Il nuovo articolo 18*b*, inserito al fine di migliore la leggibilità, riprende il disciplinamento del diritto vigente (art. 18 cpv. 1 secondo periodo e cpv. 4 secondo periodo) secondo cui le POC possono ricorrere a terzi per fornire le informazioni.

Art. 18c Comunicazione del numero di pacchetti di dati al momento di fornire informazioni

Anche questo articolo è stato inserito per motivi di leggibilità e contiene il disciplinamento del vigente articolo 18 capoverso 6.

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

A seguito delle numerose modifiche, l'articolo è stato interamente rivisto. In caso di servizi di telefonia mobile, i requisiti per l'identificazione sono più severi rispetto ad altri servizi quali ad esempio WLAN (cfr. art. 19). La disposizione, come anche gli articoli 20*a* e 20*b*, si fonda sulle norme di delega al Consiglio federale di cui agli articoli 21 capoverso 1 lettera d, 22 capoverso 2 e 23 capoverso 1 LSCPT. Le differenti disposizioni relative alle persone fisiche (art. 20*a*) e a quelle giuridiche (art. 20*b*) sono completate e strutturate in modo più chiaro.

Il *capoverso 1* fissa il principio secondo cui alla consegna dei mezzi di accesso ai servizi di telefonia mobile (p. es. GSM, GPRS, UMTS, LTE, VoLTE, VoWiFi, 5G) o, se l'utente può utilizzare il servizio soltanto dopo averlo attivato, alla prima attivazione, i FST o i rivenditori (cpv. 2) devono verificare, nel caso di persone fisiche,

l'identità dell'utente (art. 20*a*) e, nel caso di persone giuridiche, i dati forniti da quest'ultime (art. 20*b*).

Per attivazione o sblocco s'intende il momento a partire dal quale l'utente può utilizzare il servizio. Nel caso di mezzi di accesso immediatamente utilizzabili, si tratta ad esempio del momento della loro consegna. Nel caso di una SIM integrata nel dispositivo (embedded SIM; eSIM), di regola il fornitore attiva il relativo profilo mentre, per un determinato servizio, ne sblocca l'accesso. Se ad esempio un negozio di elettronica vende a un cliente un tablet predisposto per la telefonia mobile con una eSIM, il cliente non può usarlo per l'accesso mobile a Internet fintanto che la eSIM non è attivata o sbloccata. Soltanto nel momento in cui la fa attivare da un fornitore di servizi di telefonia mobile, il cliente può utilizzare il mezzo di accesso alla telefonia mobile. Il mezzo di accesso è integrato nel tablet ed è «consegnato» al cliente già al momento dell'acquisto, ma, dato che al momento dell'acquisto il mezzo di accesso non funziona ancora, alle autorità di perseguimento penale interessa il momento a partire dal quale è attivato e quindi può essere utilizzato nella rete di telefonia mobile. È inoltre importante determinare chi deve procedere all'identificazione dell'utente e alla registrazione dei dati relativi alla persona. Poiché, nel suddetto esempio, il negozio di elettronica non procede all'attivazione del mezzo di accesso alla telefonia mobile, non deve neppure registrare i dati e quindi non è considerato un rivenditore professionale di carte e altri mezzi analoghi (art. 2 lett. f LSCPT). L'attivazione e la registrazione sono compiti del fornitore di telefonia mobile quando, in qualità di FST, trasferisce il profilo sulla eSIM (carta SIM virtuale come mezzo di accesso alla telefonia mobile) e lo attiva su quest'ultima.

Il *capoverso 2* chiarisce che la verifica dell'identità dell'utente (art. 20*a*) e dei dati forniti dalla persona giuridica (art. 20*b*) incombe ai rivenditori professionali (art. 2 lett. f LSCPT), se sono loro a consegnare i mezzi di accesso o ad attivare per la prima volta il servizio. Ad esempio, quando il mezzo di accesso viene consegnato in un negozio, è il rivenditore professionale a procedere all'identificazione dell'utente, a fare una copia del mezzo di identificazione (p. es. il documento d'identità) e successivamente a trasmettere al FST i dati richiesti relativi alla persona insieme alla copia elettronica del mezzo di identificazione conformemente all'articolo 20*a* capoverso 4.

Il *capoverso 3* prevede che i FST verifichino in modo adeguato che i rivenditori professionali identifichino e registrino correttamente gli utenti e che trasmettano loro i dati e la copia del documento. In ultima analisi, i FST devono essere in grado di poter fornire le informazioni richieste e non possono far valere eventuali omissioni commesse dal rivenditore professionale.

Si può presupporre che, nel caso di nuovi contatti con la clientela nel corso della loro relazione commerciale, i FST verifichino e aggiornino i dati dei clienti, in quanto hanno interesse a farlo. Se ad esempio un cliente cambia indirizzo e ne informa il FST, quest'ultimo registra il cambiamento d'indirizzo nella propria banca dati. Nel caso di una domanda di informazioni, oltre ai dati prescritti del cliente, vanno trasmessi anche tutti gli altri dati di contatto disponibili (p. es. nuovi indirizzi) e il loro periodo di validità. Non sussiste tuttavia alcun obbligo di verifica e aggiornamento costante dei dati. In particolare non è neppure richiesto l'aggiornamento dei dati della persona nel frattempo cambiati dalla registrazione iniziale. Se viene a conoscenza di una modifica

dei dati del cliente, il FST deve semplicemente comunicarlo nel quadro di un'eventuale domanda di informazioni.

Art. 20a Prova dell'identità di persone fisiche utenti di servizi di telefonia mobile

Il *capoverso 1* enumera in modo esaustivo i mezzi d'identificazione ammessi per provare la propria identità. Altri mezzi come la licenza di condurre non sono accettati. Nel caso del passaporto (*lett. a*) e della carta d'identità (*lett. b*), può trattarsi di un documento sia svizzero che straniero. Per i servizi di telefonia mobile, la verifica dell'identità del cliente mediante uno dei mezzi di identificazione menzionati è obbligatoria. Ciò corrisponde al disciplinamento precedente applicato ai servizi di telefonia prepagati (prepaid) che, con la revisione totale della OSCPT, è stato esteso a tutti i servizi di telefonia mobile, a prescindere dal metodo di pagamento (p. es. abbonamento, prepagato, gratuito)[19]. Nella pratica, i fornitori di servizi di telefonia mobile chiedono da tempo la presentazione di un documento d'identità per concludere un contratto. Il fornitore o il rivenditore professionale non deve verificare in modo dettagliato l'autenticità del documento d'identità. Di fatto non è neppure in grado di farlo poiché non ha a disposizione gli stessi mezzi di verifica di un'autorità di polizia. Il fornitore o il rivenditore professionale è soltanto tenuto ad accettare documenti d'identità la cui autenticità risulta plausibile. Se accetta un documento d'identità palesemente riconoscibile come falsificato o chiaramente non corrispondente alla persona che lo presenta, in determinate circostanze il fornitore o il rivenditore può essere condannato a una pena amministrativa (cfr. art. 39 LSCPT).

Le *lettere a-c* corrispondono ai documenti d'identità ammessi dal vigente articolo 20 capoverso 1. Se un cliente intende farsi identificare presso un operatore di servizi di telefonia mobile mediante uno di questi documenti, di regola si presenta di persona ed esibisce il documento. Poiché la procedura di verifica dell'identità non è disciplinata, è possibile anche un'identificazione per video o online[20]. In tal caso occorre rispettare gli standard di sicurezza e qualità riportati dalla circolare della FINMA 2016/7 «Video identificazione e identificazione online»[21] per l'identificazione online nel settore bancario.

Il documento d'identità (lett. a-c) deve essere valido al momento del rilevamento che corrisponde alla data e all'ora in cui il cliente presenta il suo documento al fornitore o al rivenditore professionale. L'identificazione sicura può essere garantita soltanto con un documento valido. La prassi ha evidenziato che in passato vi sono state registrazioni non valide con documenti d'identità scaduti.

I dati di cui al *capoverso 2* corrispondono a quelli del vigente articolo 20 capoverso 2 e si fondano sull'articolo 21 capoverso 1 LSCPT. Il FST o il rivenditore professionale

19 La sentenza della Corte EDU del 30 gen. 2020 (Az. 50001/12) nella causa Breyer contro la Germania ha stabilito che l'obbligo d'identificazione per l'acquisto di una carta SIM prepagata non viola la sfera privata tutelata dall'art. 8 CEDU.

20 Cfr. anche art. 6 cpv. 4 lett. b dell'ordinanza del DFGP sul riciclaggio di denaro **(**ORD-DFGP; RS **955.022)** e art. 5 cpv. 1 lett. e dell'ordinanza della CFCG sul riciclaggio di denaro (ORD-CFCG; RS **955.021**)

21 finma.ch =>Documentazione => Circolari

è responsabile del rilevamento corretto dei dati sulla persona in base al mezzo d'identificazione presentato. Nel caso di documenti fisici, per il controllo serve una copia del mezzo d'identificazione presentato. Se il mezzo d'identificazione (p. es. documento d'identità) dispone di una zona a lettura ottica (machine readable zone; MRZ), si raccomanda di leggere elettronicamente i dati e registrarli come segue:

- cognome (-i) e nome (-i) della MRZ come alias o identità secondaria. Poiché questi nomi sono disponibili in una ridotta sequenza di caratteri latini (traslitterazione), possono essere direttamente usati per la ricerca normale (ossia letterale) dei nomi (cfr. art. 35).

Per i seguenti dati relativi alla persona o al documento andrebbero rilevati i dati MRZ, se disponibili, al posto di una registrazione manuale:

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

L'indirizzo (*lett. b*) e la professione (*lett. c*), che non figurano nel documento, vanno rilevati secondo le indicazioni del cliente verificandone la plausibilità (nessuna indicazione inventata o palesemente errata). L'indirizzo da rilevare, completo di via e numero civico, è quello del domicilio, della seconda casa, del luogo di soggiorno settimanale o di quello abituale presso cui l'utente è contattato.

Il *capoverso 3* corrisponde al vigente articolo 20 capoverso 4. Se il cliente non ha un abbonamento (prepaid o gratuito), il FST e il rivenditore professionale sono tenuti a registrare ulteriori dati. Non sono contemplate le semplici carte telefoniche prepagate che permettono di telefonare ma non sono carte SIM o simili. Questi dati supplementari vanno rilevati affinché si possa risalire a chi abbia eventualmente effettuato registrazioni non valide (cfr. la corrispondente disposizione penale dell'art. 39 cpv. 1 lett. c LSCPT). Va rilevato che il FST deve bloccare l'accesso ai servizi di telecomunicazione se nella relazione commerciale con il cliente senza abbonamento (prepaid o gratuito) sono stati registrati dati non validi (art. 6*a* LTC). Ai sensi della *lettera a* si deve indicare il momento, ossia la data e l'ora, del rilevamento. Il nome e l'indirizzo di cui alla *lettera b* vanno riportati integralmente e dipendono da chi effettua il rilevamento (p. es. un negozio di un rivenditore, un call center del FST che procede all'attivazione o un ufficio postale che procede alla verifica dell'identità). Nel caso di video identificazione o identificazione online, vanno registrati integralmente il nome e l'indirizzo del servizio responsabile della registrazione. Secondo la *lettera c* devono essere rilevati integralmente anche i cognomi e i nomi della persona che effettua il rilevamento o della persona responsabile della video identificazione o dell'identificazione online. Per «persona che effettua il rilevamento» s'intende la persona che rileva effettivamente i dati di cui al capoverso 3 o, se il rilevamento è automatico, la persona che è responsabile del rilevamento dei dati (cfr. anche la corrispondente disposizione penale dell'art. 39 cpv. 1 lett. c LSCPT).

Secondo il *primo periodo* del *capoverso 4,* il FST o il rivenditore professionale deve allestire, come avviene già ora, una copia del documento d'identità presentato in originale. La misura continua a essere necessaria perché in passato si sono verificati molti

rilevamenti non validi dei dati personali. La copia del documento d'identità è attualmente il mezzo più adatto per evitare rilevamenti non validi. Si deve effettuare una copia elettronica ben leggibile del documento (p. es. fotografia, scansione). Le copie cartacee non soddisfano più i nuovi requisiti. La durata di conservazione per i FST è disciplinata all'articolo 21 capoverso 4. Il *secondo periodo* introduce un termine entro cui i rivenditori professionali devono trasmettere al FST i dati rilevati di cui ai capoversi 2 e 3 e la copia del documento. Il termine è fissato a tre giorni per il seguente motivo: se i numeri di telefono vengono acquisiti e utilizzati poco dopo aver lasciato il negozio, possono diventare rilevanti ai fini delle indagini lo stesso giorno. È pertanto importante che i dati e la copia del documento d'identità siano a disposizione delle autorità di perseguimento penale il prima possibile nella IRC. Il termine di tre giorni è accettabile anche per i rivenditori professionali più piccoli. Il capoverso intende delimitare le responsabilità in modo più chiaro (cfr. anche la corrispondente disposizione penale dell'art. 39 cpv. 1 lett. c LSCPT).

Art. 20b Prova dell'identità di persone giuridiche utenti di servizi di telefonia mobile

Il *capoverso 1* disciplina i dati da rilevare concernenti le persone giuridiche. Tali dati corrispondono a quelli del vigente dell'articolo 20 capoverso 3 e di norma sono rilevati in base all'estratto del registro di commercio o del registro IDI dell'Ufficio federale di statistica. Ora può essere rilevato anche il Legal Entity Identifier (LEI) internazionale secondo il sistema globale d'identificazione dei partecipanti ai mercati finanziari (*lett. b*). Per le persone giuridiche deve essere in linea di massima rilevato l'IDI o il LEI. L'utente citato alla *lettera c* che utilizzerà i servizi del fornitore potrebbe essere ad esempio un collaboratore che riceve la carta SIM dal suo datore di lavoro.

Il *capoverso 2* corrisponde all'articolo 20*a* capoverso 4 secondo periodo.

Il *capoverso 3* rimanda all'articolo 20*a* capoverso 3 («clienti senza abbonamento»).

Art. 20c Consegna di mezzi di accesso e attivazione di servizi per il SIC e le autorità di polizia

Per adempiere i propri compiti legali, le autorità di polizia e il SIC devono talvolta poter utilizzare mezzi di accesso per accedere a servizi di telecomunicazione (p. es. carte SIM prepagate). In questi casi, tali autorità e il loro personale non devono figurare né negli elenchi pubblici di cui all'articolo 12*d* LTC né nei dati elenco di cui all'articolo 21 LTC e neppure nella IRC. Necessitano di questi mezzi di accesso anzitutto per tutelare il loro personale, i loro contatti e le loro fonti nonché i loro metodi e le loro capacità tecniche (p. es. per comunicare durante l'osservazione di persone con accesso a mezzi tecnici avanzati, negli ambienti della criminalità organizzata e dello spionaggio).

Hanno bisogno di particolari misure di protezione i collaboratori delle autorità di polizia e del SIC che adempiono i loro compiti legali utilizzando la loro vera identità ossia senza avvalersi di un'identità fittizia. I collaboratori che ricorrono a un'identità fittizia (inquirenti in incognito ai sensi dell'art. 285*a* CPP e persone con un'identità

fittizia ai sensi degli art. 17 e 18 della legge federale del 25 settembre 2015 sulle attività informative [LAIn]) possono ottenere mezzi di accesso a servizi di telecomunicazione seguendo la procedura ordinaria ossia senza rendere nota la propria vera identità e godendo così di una protezione sufficiente. Anzi, l'acquisizione di simili mezzi per via ordinaria può addirittura consolidare la copertura.

Va detto che, ai sensi dell'articolo 12*d* LTC, la pubblicazione dei dati della clientela in elenchi pubblici non è obbligatoria; a tale riguardo i clienti sono liberi di scegliere. Tuttavia presso i FST e i rivenditori professionali un numero elevato e incontrollabile di persone ha accesso ai sistemi e quindi ai dati memorizzati per scopi di comunicazione commerciale.

In base alla presente disposizione, i FST sanno che alcune autorità legittimate sono utenti di determinati servizi e mezzi di accesso protetti, ma nel contempo sono anche tenuti a tutelare il più possibile questi dati e a renderli noti, su richiesta tramite il Servizio SCPT, solamente alle autorità legittimate. In questo modo i FST adempiono i loro obblighi, di cui agli articoli 21 e seguenti LSCPT, concernenti l'identificazione degli utenti e la fornitura di informazioni alle autorità legittimate, ma impediscono che potenziali criminali vengano a conoscenza di questi dati proteggendo così le attività operative delle autorità di polizia e del SIC.

Per le ragioni e le circostanze di cui sopra, il *capoverso 1* prevede ora che un FST e l'autorità in questione concludano un contratto con l'intermediazione del Servizio SCPT. In questo caso non si tratta di un contratto di abbonamento in senso stretto, ma di un'altra forma di contratto, tra un FST e un'autorità, che regola le modalità per la consegna di mezzi di accesso e l'attivazione di servizi. Per garantire uno standard di sicurezza uniforme e il più elevato possibile, i FST fissano i metodi di sicurezza d'intesa con il Servizio SCPT al fine di evitare che i dati siano diffusi al di fuori della ristretta cerchia delle persone selezionate degne di fiducia. È fondamentale ridurre al minimo la cerchia delle persone aventi accesso all'informazione del vero titolare. Verosimilmente la procedura è simile a quella del blocco dei dati delle persone politicamente esposte già oggi applicata dai FST.

Il *capoverso 2* disciplina il processo di consegna dei mezzi di accesso e di attivazione dei servizi per le autorità di polizia e per il SIC conformemente alla presente disposizione. L'autorità (l'autorità di polizia o il SIC) sceglie tra le proprie fila un responsabile autorizzato a suo nome a ottenere i mezzi di accesso o a farsi attivare i servizi presso il FST; questo collaboratore conosce anche chi, tra i suoi colleghi, è utente del FST. Da parte sua il FST documenta internamente i mezzi di accesso consegnati e i servizi attivati per le autorità. In questo modo è in grado di adempiere l'obbligo di fornire, su richiesta del Servizio SCPT, informazioni sugli utenti e potrebbe scagionarsi in caso di denuncia presso il Servizio SCPT ai sensi dell'articolo 39 capoverso 1 lettera c LSCPT.

Il *capoverso 3* stabilisce che le autorità legittimate possono utilizzare i mezzi di accesso e i servizi di cui al presente articolo solamente nel quadro delle pertinenti disposizioni legali (p. es. ai sensi dell'art. 298*a* CPP [indagine in incognito] o ai sensi degli art. 7 e 35 LAIn). Le autorità di polizia e il SIC continuano a poter ottenere i mezzi di accesso e a utilizzare determinati servizi conformemente ai requisiti generali di cui agli articoli 20*a* e 20*b*.

Art. 21 Termini di conservazione

L'articolo è stato ampiamente riveduto al fine di strutturare meglio, completare e precisare il disciplinamento dei termini di conservazione delle singole categorie di dati. La disposizione elenca quali POC devono conservare determinati dati e per quanto tempo. I termini di conservazione principali non sono modificati: come in precedenza, i dati sull'utente (*subscriber data*) devono essere conservati per l'intera durata della relazione commerciale e per sei mesi dopo il suo termine (cpv. 1 e 4). I dati identificativi degli utenti di accessi WLAN pubblici gestiti professionalmente vanno conservati per il periodo di validità dell'autorizzazione di accesso e per i sei mesi dopo la sua scadenza (cpv. 2), mentre i dati relativi all'uso (*usage data*) per sei mesi (cpv. 3) dal momento in cui sono generati. L'espressione generale *indicazioni ai fini dell'identificazione* è ora precisata nei singoli capoversi (cpv. 1, 3 e 5).

Il *capoverso 1* corrisponde al vigente capoverso 1 primo periodo. L'obbligo di conservare i dati (*lett. a*) vale per tutte le POC con obblighi d'informazione attivi (tutti i FST e i FSCD con obblighi supplementari ai sensi dell'art. 22 o 52). Ora è stato aggiunto l'obbligo di conservare le indicazioni su identificativi attribuiti a lungo termine per ottenere il tipo di informazione di cui all'articolo 48*a (lett. b);* quest'obbligo vale solamente per i FST in quanto i FSCD menzionati sono esentati dal fornire questo tipo di informazione (cfr. art. 18 cpv. 4).

Il *capoverso 2* si applica solamente ai FST; si tratta infatti di un accesso alla rete e corrisponde alla disposizione vigente con un adattamento redazionale («accesso al WLAN» anziché «punto di accesso WLAN»; cfr. i commenti sulla sostituzione di espressioni, cpv. 1). Inoltre si precisa che la disposizione riguarda solamente gli accessi ai WLAN pubblici gestiti professionalmente (cfr. anche i commenti introduttivi al presente articolo).

Anche il *capoverso 3* si applica solamente ai FST poiché anche in questo caso si tratta di un accesso alla rete; la disposizione disciplina la conservazione dei dati sull'attribuzione univoca di indirizzi IP (art. 37). Nel diritto vigente i dati sull'assegnazione e la traduzione degli indirizzi IP e dei numeri di porta (art. 37, 38 e 39) figurano insieme al capoverso 2 lettera b. Tuttavia, in base alla proporzionalità, si deve distinguere, in caso di un'attribuzione dinamica di indirizzi IP, tra assegnazione univoca di indirizzi IP (art. 37) da un lato e assegnazione non univoca e traduzione (NAT) di indirizzi IP e numeri di porta dall'altro (art. 38 e 39; cfr. il nuovo cpv. 5 lett. b). Per quanto riguarda gli indirizzi IP assegnati univocamente, ci sono quelli assegnati in modo permanente (indirizzi IP statici) e quelli in modo dinamico (indirizzi IP dinamici). Come per tutti i dati sull'utente, i dati sull'assegnazione di indirizzi IP statici vanno conservati per l'intera durata della relazione commerciale più ulteriori sei mesi (cpv. 1), mentre per gli indirizzi IP dinamici i dati sull'assegnazione vanno conservati solamente per sei mesi poiché si tratta di dati relativi all'uso. Per gli indirizzi IP statici, è l'assegnazione a fare la differenza indipendentemente dal loro uso (per la durata dell'uso, l'indirizzo IP è assegnato in modo permanente a prescindere dal fatto che il relativo accesso Internet sia effettivamente usato oppure no). Nel caso degli indirizzi IP dinamici, l'indirizzo è assegnato solamente quando l'accesso a Internet è davvero utilizzato e quindi è legato all'uso. Lo stesso indirizzo IP può essere assegnato a utenti diversi in momenti diversi, ma mai contemporaneamente a più utenti (infatti è assegnato «univocamente»).

Il *capoverso 4* disciplina espressamente il termine di conservazione dei dati relativi agli utenti e della copia del documento d'identità nel settore della telefonia mobile. L'obbligo di conservare questi dati vale solamente per i FST che offrono servizi di telefonia mobile (fornitori di servizi di telefonia mobile). Questi dati comprendono le informazioni sulla persona rilevate al momento della registrazione e, nel caso di persone fisiche, anche la copia elettronica del documento d'identità presentato. Nel diritto vigente ciò è disciplinato solo a livello implicito nel capoverso 1.

I dati di cui al *capoverso 5* corrispondono ai dati ai fini dell'identificazione secondo l'articolo 22 capoverso 2 secondo periodo LSCPT; di fatto si tratta di metadati. L'obbligo di conservarli è paragonabile alla conservazione dei metadati per la sorveglianza retroattiva. A causa delle grandi quantità di dati e dell'onere richiesto, soltanto i FST più grandi sono tenuti, per ragioni di proporzionalità, a conservare questi dati.

Questo capoverso si fonda sul vigente capoverso 2. La *lettera a* resta invariata (solo i rimandi alle disposizioni corrispondenti sono adeguati). La *lettera b* corrisponde alla vigente lettera b, la nuova formulazione, tuttavia, non comprende più le indicazioni di cui all'articolo 37 (indirizzi IP assegnati univocamente) in quanto adesso sono disciplinate al capoverso 3. Adesso la *lettera c* disciplina il termine di conservazione dei metadati per la determinazione delle reti immediatamente adiacenti, in questo modo possono essere fornite le informazioni di cui all'articolo 48*c* (cfr. il relativo commento). Lo stralcio della nozione di *trasmettere* («devono conservare per sei mesi» anziché «devono conservare e trasmettere per sei mesi») chiarisce che questi dati, utili all'identificazione, vanno conservati, ma non devono essere trasmessi con le informazioni se non rientrano esplicitamente nei dati da consegnare per il tipo di informazione. In questo caso i metadati, che non vanno consegnati, sono utilizzati dalle POC solamente per valutare ed identificare gli utenti. Vanno trasmesse solamente le indicazioni sull'identificazione dell'utenza (art. 38) o sul contesto di traduzione NAT (art. 39) contenute nella domanda di informazioni. I restanti metadati possono essere trasmessi dalle POC soltanto nell'ambito di sorveglianze (in tempo reale o retroattive), in quanto i metadati di cui alla lettera b non sono parte dei tipi di sorveglianza standardizzati.

I dati di cui al *capoverso 6* sono dello stesso tipo dei dati menzionati al capoverso 5 lettere a e b, pertanto si applica lo stesso termine di conservazione. Per una migliore leggibilità, questo capoverso disciplina espressamente il termine di conservazione applicato ai FSCD con obblighi di sorveglianza supplementari (art. 52) poiché questi ultimi non sottostanno al capoverso 5 lettera c. I commenti relativi al capoverso 5 lettere a e b valgono per analogia.

Il *capoverso 7* corrisponde al vigente capoverso 3 con il necessario adeguamento del rimando, disciplina la distruzione dei metadati descritti in dettaglio nel capoverso 5 e riguarda tutti i fornitori (cpv. 5 e 6) che conservano i metadati in oggetto.

Occorre osservare che non devono essere conservate indicazioni sugli identificativi attribuiti per un breve periodo di cui al nuovo articolo 48*b*. A causa del processo molto dinamico di queste attribuzioni, è possibile chiedere questo tipo di informazione praticamente solo in tempo reale (cfr. il commento all'art. 48*b*).

Art. 26 Tipi di informazioni

Il *capoverso 1* di questo articolo riassuntivo è rielaborato sotto il profilo formale. Per migliorare la leggibilità, l'enumerazione in cifre è sostituita da un'enumerazione un po' più ampia in lettere.

Nella *lettera d* il termine specifico «copia del documento d'identità» è sostituito da quello più generale «prova dell'identità», poiché adesso possono essere usate anche identità elettroniche. La *lettera h* menziona i due nuovi tipi di informazione di cui agli articoli 48*a* (IR_51_ASSOC_PERM: informazioni su identificativi attribuiti a lungo termine) e 48*b* (IR_52_ASSOC_TEMP: informazioni immediate su identificativi attribuiti per breve tempo) mentre la *lettera i* riporta il nuovo tipo di informazione di cui all'articolo 48*c* (IR_53_TEL_ADJ_NET: determinazione delle reti adiacenti di servizi di telefonia e multimedia).

Il *capoverso 2* contiene una modifica redazionale. Nel capoverso è opportuno usare l'espressione «persone obbligate a collaborare» al posto dell'espressione specifica «fornitori». Devono infatti fornire informazioni anche i gestori di reti di telecomunicazione interne (art. 2 lett. d LSCPT) e le persone che mettono a disposizione di terzi il loro accesso a una rete pubblica di telecomunicazione (art. 2 lett. e LSCPT). Questi non sono fornitori e vengono quindi contemplati dal termine generale POC. Il disciplinamento si applica anche se, in virtù dei suoi obblighi ridotti, la POC in questione deve fornire le informazioni senza requisiti formali e non in forma standardizzata.

Art. 28 Tipi di sorveglianza

Questo articolo riassuntivo è completato con quattro nuovi tipi di sorveglianza sulla determinazione della posizione (due per la sorveglianza in tempo reale e due per la ricerca d'emergenza) inoltre adegua le denominazioni di alcuni tipi di sorveglianza già vigenti. Per migliorarne la leggibilità, la disposizione ha una nuova struttura: si passa da una struttura in capoversi 1–5 a una in lettere a–e a loro volta suddivise in numeri.

La *lettera a numeri 1-3* resta fondamentalmente invariata. Il *numero 4* è nuovo e rimanda ai due nuovi tipi di sorveglianza in tempo reale relativi alla determinazione della posizione (LALS, cfr. art. 56*a* e 56*b*). La vigente lettera d diventa il *numero 5*.

La *lettera b numero 3* riporta ora *la determinazione della localizzazione al momento dell'ultima attività* (cfr. anche il commento all'art. 63).

Nella *lettera c numero 1* la denominazione della ricerca d'emergenza è stata modificata come segue: la determinazione della localizzazione al momento dell'ultima attività (cfr. art. 67 cpv. 1 lett. a). Il *numero 2* è nuovo e rimanda ai due nuovi tipi di ricerca d'emergenza relativi alla determinazione della posizione (LALS, cfr. art. 67 cpv. 1 lett. b e c). I *numeri 3, 4* e *5* restano invariati e corrispondono alle vigenti lettere b-d del capoverso 3. Sono adeguati soltanto i rimandi tra parentesi alle pertinenti disposizioni.

La *lettera d numero 1* riporta ora *la determinazione della localizzazione al momento dell'ultima attività* (cfr. anche il commento all'art. 63). Il *numero 2* è nuovo e rimanda ai due nuovi tipi di ricerca d'emergenza relativi alla determinazione della posizione mediante la rete (LALS, cfr. art. 68 cpv. 1 lett. b e c). I *numeri 3, 4 e 5* restano invariati

e corrispondono alle vigenti lettere b-d del capoverso 4. Sono adeguati soltanto i rimandi tra parentesi alle pertinenti disposizioni. Nel *numero 6* viene aggiunto il rimando alla già vigente ricerca per zona di copertura dell'antenna nell'ambito della ricerca di condannati (art. 68 cpv. 1 lett. g, finora lett. d).

La *lettera e* è stata leggermente accorciata e corrisponde contenutisticamente al vigente capoverso 5 entrato in vigore il 1° giugno 2022 con l'ordinanza del 4 maggio 2022[22] sulle misure di polizia per la lotta al terrorismo (OMPT).

Art. 30 cpv. 3

Il *capoverso 3* è completato con un secondo periodo secondo cui le POC permettono al Servizio SCPT di effettuare i collegamenti test necessari. Questa integrazione è necessaria poiché vi sono casi in cui le POC non sono in grado di mettere a disposizione i collegamenti test come disciplinato nel primo periodo. In questi casi detti collegamenti sono eseguiti dal Servizio SCPT o da persone da esso incaricate. Ciò si verifica soprattutto nel caso delle POC che non hanno obblighi attivi di sorveglianza (ossia non sono tenute a garantire alcuna disponibilità a sorvegliare). I collegamenti test possono essere effettuati anche per sorveglianze particolari (art. 25), i cosiddetti casi speciali. Oltre a tollerare la sorveglianza attuata dal Servizio SCPT o dalle persone da esso incaricate (art. 26 cpv. 2 lett. b LSCPT), alle POC incombe l'obbligo accessorio necessario (cfr. messaggio del 27 febbraio 2013 concernente la LSCPT, ad art. 26 cpv. 2, FF 2013 2283, in particolare 2337) di permettere al Servizio SCPT l'esecuzione di collegamenti test in relazione all'ordine di sorveglianza, al fine di verificare ad esempio il corretto funzionamento di quest'ultima. Per effettuare i collegamenti test, le POC devono garantire senza indugio al Servizio SCPT o alle persone da esso incaricate l'accesso ai propri impianti (cfr. art. 53 cpv. 1).

Art. 35 cpv. 1 lett. b, c e d, frase introduttiva e n. 2, 9–13, cpv. 2, frase introduttiva e lett. g, i, j e k, nonché cpv. 3

Al *capoverso 1 lettera b* le indicazioni da trasmettere sono suddivise in modo schematico in tre numeri e al *numero 1* sono adeguati i rimandi. Adesso gli articoli 20-20*b* disciplinano rispettivamente la verifica dei dati relativi agli utenti di servizi di telefonia mobile, la prova dell'identità di persone fisiche e la prova dell'identità di persone giuridiche. Al *numero 2* sono aggiunte le nozioni di «altri indirizzi» e il periodo di validità degli «altri indirizzi e dati di contatto». I fornitori spesso non memorizzano solo l'indirizzo al momento della registrazione ma anche il nuovo indirizzo in caso di trasloco e gli altri indirizzi degli utenti come un indirizzo diverso per la consegna o la fatturazione. Come «altri dati di contatto» la POC può ad esempio fornire altri numeri di telefono o indirizzi e-mail dell'utente di cui è a conoscenza. Per periodo di validità s'intende l'intervallo di tempo (data di inizio ed eventualmente di fine) in cui gli «altri indirizzi e dati di contatto» sono o erano registrati presso la POC. La POC rende noti i dati e i periodi di validità di cui dispone. Non è tenuta a rilevare correttamente e tenere aggiornati gli altri indirizzi e dati di contatto dei suoi utenti.

22 RU **2022** 301

La *lettera c* subisce per analogia le stesse modifiche della lettera b ma al numero 1 i rimandi non sono adeguati in quanto cambiano solo per i servizi di telefonia mobile. La lettera c è applicabile a tutti i servizi di accesso alla rete che non sono servizi di telefonia mobile. Va inoltre osservato che, come finora, vanno trasmessi i dati identificativi rilevati con mezzi adeguati ai sensi dell'articolo 19. La prassi ha evidenziato che, viste le molteplici possibilità d'identificazione e di rilevamento dei dati, non si può stabilire una struttura fissa dei dati. Le indicazioni possono quindi essere trasmesse senza una struttura, ma devono essere designate in modo adeguato affinché le autorità legittimate capiscano meglio il loro significato (p. es. MSISDN, numero della carta di credito, numero del documento d'identità, numero ID, boarding pass, MRZ, nome utente IPASS).

La versione italiana della frase introduttiva della *lettera d* subisce una modifica per adeguarla alla frase introduttiva dell'articolo 42 capoverso 1 lettera c.

Il *numero 2* subisce due modifiche. Anzitutto il termine vigente «identificativo univoco del servizio» è sostituito da «identificativo univoco principale del servizio» poiché vi sono abbonamenti a servizi di telefonia mobile con più numeri o carte SIM che possono essere usati contemporaneamente con diversi dispositivi (cosiddette offerte multiSIM o multidevice). Ne risulta una gerarchia all'interno dell'abbonamento: un numero principale (master) e altri numeri secondari (slave). Questa gerarchia può essere modificata dall'utente stesso, vale a dire che quest'ultimo può decidere quale carta SIM o quale dispositivo sta usando il numero principale o i numeri secondari. Ne consegue che a un IMSI possono ad esempio essere attribuiti più MSISDN. Nel caso semplice a un IMSI è attribuito soltanto un MSISDN. I numeri secondari possono essere anche numeri tecnici che in genere l'utente non conosce. Le offerte multiSIM o multidevice si ripercuotono sulle informazioni da fornire, sulle sorveglianze, sulle ricerche d'emergenza e sulle ricerche di condannati.

In secondo luogo l'*identificativo DLS* degli accessi Internet a banda larga nella rete fissa, finora citato a titolo esemplificativo, è ora sostituito da un nuovo identificativo del sistema 5G, il *Generic Public Subscription Identifier* (GPSI) poiché quest'ultimo sta diventando sempre più importante. Di conseguenza negli esempi della presente ordinanza *l'identificativo DSL* è sostituito ovunque con il *GPSI* al fine di avere esempi il più possibile verosimili e attuali. Questo però non significa che *l'identificativo DSL* non debba essere più trasmesso (questo vale anche per tutti gli altri esempi nei quali c'è stata una sostituzione). I *GPSI* sono identificativi pubblici usati sia all'interno che al di fuori del sistema 3GPP. Il *GPSI* può essere o un MSISDN (p. es. +41791234567) o un identificativo esterno sotto forma di <username>@<domain_name> (p. es. mario.rossi@mnc999.mcc228.csp.ch). Il GPSI è usato in particolare per l'indirizzo di un servizio 3GPP in reti al di fuori del sistema 3GPP, ad esempio se, per accedere alla rete l'utente usa un accesso non 3GPP (WLAN) e non la rete di telefonia mobile. L'aggiunta 3GPP indica che si tratta di un sistema o di un servizio di telefonia mobile standardizzato secondo il 3GPP (*sistema 3GPP* o servizio *3GPP*).

Un altro identificativo non menzionato negli esempi, ma che va eventualmente fornito è l'OTO-ID, che designa in modo univoco un collegamento domestico in fibra ottica (fiber to the home).

Il *numero 9* resta invariato. L'espressione «numero SIM» è semplicemente sostituita dall'acronimo tecnico universale ICCID (definito nell'allegato) poiché la funzione della carta SIM tradizionale può essere assunta anche da altri tipi di hardware (p. es. embedded SIM, eSIM) e non è sempre del tutto chiaro cosa s'intenda per numero SIM. L'acronimo ICCID è invece chiaro per tutte le forme di SIM.

Il *numero 10*, oltre all'*IMSI*, adesso menziona anche il *SUPI* ossia l'identificativo equivalente nel sistema 5G. Nel sistema 5G a ogni utente è assegnato un Subscription Permanent Identifier (SUPI). Il *SUPI* è univoco su scala mondiale ed è impostato nella banca dati degli utenti della rete domestica (UDM/UDR). Il *SUPI* è usato soltanto all'interno del sistema 3GPP. Come *SUPI* può ad esempio essere usato l'*IMSI*. Il dispositivo può comunicare il proprio *SUPI* alla rete in forma criptata (p. es. in occasione dell'annuncio alla rete) il che si ripercuote sull'impiego di apparecchi tecnici speciali di sorveglianza ai sensi dell'articolo 269bis CPP (cfr. art. 48*b*). Per permettere il roaming, il *SUPI* contiene l'indirizzo della rete domestica (p. es. Mobile Country Code *MCC* e Mobile Network Code *MNC*). Il sistema 5G memorizza nella banca dati degli utenti la relazione tra *GPSI* e relativo *SUPI*, ma tale relazione non deve essere necessariamente 1:1 (è possibile conoscere i *GPSI* e i *SUPI* corrispondenti ottenendo i tipi di informazioni di cui agli art. 36 o 41).

Nel *numero 11* viene corretto un errore. A causa di una svista nella traduzione dello standard ETSI redatto in inglese, nella versione in vigore è stata usata erroneamente l'espressione «tipo di servizio». In realtà si tratta del «tipo di relazione commerciale» (ingl. «subscription type»). Sotto il profilo del contenuto non cambia niente.

Il *numero 12* è precisato. Come illustrato al numero 2, ci possono essere anche altri elementi d'indirizzo (p. es. numeri di telefono «MSISDN») e identificativi del servizio (p. es. numero SIM «ICCID») che caratterizzano il servizio di accesso alla rete (p. es. abbonamento di telefonia mobile) oggetto della domanda. Detti elementi d'indirizzo e identificativi del servizio vanno riportati in questo campo sotto forma di elenco o di settore (range da – a). Questa categoria comprende anche elementi d'indirizzo e identificativi aggiunti dopo la registrazione, purché facciano parte dei dati sull'utente (*subscriber data*). Gli elementi d'indirizzo e gli identificativi attribuiti in base all'uso (*usage data*) non sono richiesti ai sensi della presente disposizione ma presentando la domanda per il tipo di informazione di cui all'articolo 36. Adesso occorre indicare il periodo di validità dell'elemento d'indirizzo o dell'identificativo.

Per facilitare alle autorità richiedenti la valutazione delle risposte ricevute e per precisare il servizio di cui si tratta, il *numero 13* prevede un campo per la trasmissione della designazione del servizio di accesso alla rete oggetto della domanda (p. es. nome del prodotto, dell'offerta, dell'abbonamento o della tariffa). Può ad esempio essere indicata la designazione dell'abbonamento venduto. Visti i molteplici servizi disponibili sul mercato, sono state le autorità di perseguimento penale a chiedere di aggiungere questo elemento.

I due periodi della frase introduttiva del *capoverso 2* sono stati ripresi dal vigente capoverso 2. La *lettera g* precisa che la domanda può ora essere presentata anche in base al LEI oltre che all'IDI (cfr. il commento all'art. 20*b* cpv. 1 lett. b). La *lettera i* aggiunge il criterio dell'identificativo dell'utente (p. es. numero cliente). Questo criterio

è utile per consultare tutti i servizi di un determinato utente oppure per consultare l'identificativo alternativo dell'utente di cui all'articolo 36 capoverso 1 lettera b numero 3 (p. es. nel caso di un accesso WLAN pubblico gestito professionalmente). Inoltre, per un identificativo del servizio, viene fatto un altro esempio (GPSI) al posto dell'identificativo DSL (cfr. il commento al cpv. 1 lett. d n. 2). La *lettera j* introduce il nuovo identificativo SUPI del sistema 5G (cfr. il commento al cpv. 1 lett. d n. 10). Nella *lettera k* il termine *numero di carta SIM* è sostituito dall'acronimo tecnico universale *ICCID* (cfr. il commento al cpv. 1 lett. d n. 9).

Il *primo periodo* del *capoverso 3* corrisponde fondamentalmente al terzo periodo del vigente capoverso 2. Si procede soltanto a una correzione: il criterio di cui alla lettera e (numero del documento d'identità) non è più previsto dalla nuova disposizione. Poiché questo criterio è univoco, non è necessario aggiungere un secondo criterio di ricerca nella domanda. Il *secondo periodo* corrisponde al quarto periodo del vigente capoverso 2.

Art. 36 Tipo di informazione IR_6_NA: informazioni su servizi di accesso alla rete

A seguito delle numerose modifiche, l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità.

Il *capoverso 1* ha una nuova struttura: la *lettera a* resta invariata mentre la *lettera b* specifica, ai numeri 1-6, le indicazioni da fornire per ciascun servizio. Al servizio oggetto della domanda possono essere infatti collegati anche altri servizi. Il secondo periodo della frase introduttiva del vigente capoverso 1 è stralciato poiché la comunicazione del periodo di validità di determinate indicazioni è ora disciplinata caso per caso.

Sotto il profilo del contenuto il *numero 1* corrisponde alla vigente lettera b. Il *numero 2* elenca i possibili altri identificativi del servizio tra cui anche il MSISDN. Questo tipo di informazione è utile per qualsiasi servizio di accesso alla rete e non solo per la telefonia mobile. Adesso, per ogni identificativo del servizio di cui al numero 2 si deve trasmettere il relativo periodo di validità affinché le autorità di perseguimento penale possano riconoscerne la rilevanza cronologica. Il *numero 3* è nuovo e serve per identificare l'utente nel caso di un accesso WLAN pubblico gestito professionalmente. Con l'identificativo così ottenuto, l'autorità legittimata può compilare in un secondo tempo una domanda di informazione IR_4_NA (art. 35) e ricevere quindi i dati identificativi ai sensi dell'articolo 19 capoverso 2. Il *numero 4*, che corrisponde sostanzialmente alla vigente lettera d, disciplina le indicazioni da trasmettere concernenti i dispositivi usati negli ultimi sei mesi in relazione a ciascun servizio del fornitore. Tra gli identificativi elencati adesso compare anche il «Permanent Equipment Identifier» (PEI) della tecnologia 5G. Il PEI serve all'identificazione univoca, su scala mondiale, dei dispositivi nelle reti di telefonia mobile 5G ed è costituito da un IMEI o da un IMEISV. Il *numero* 5 riunisce le vigenti lettere e (l'ICCID anziché il numero SIM, cfr. commento al cpv. 1 lett. d n. 9) e f (PUK), inoltre aggiunge il periodo di validità e altri identificativi come l'IMSI e il MSISDN per fornire alle autorità legittimate una migliore panoramica cronologica, per ogni accesso alla rete, delle carte SIM e di mezzi di accesso analoghi. Sono introdotti entrambi gli identificativi delle

reti di telefonia mobile 5G: SUPI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10) e GPSI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2). È stato aggiunto il *numero 6* concernente le informazioni in caso di un'offerta multidevice. Poiché l'attribuzione del dispositivo principale («primary») e dei dispositivi secondari («secondary») può essere modificata in ogni momento dall'utente, le informazioni sull'offerta multidevice sono dinamiche e vanno pertanto chieste mediante il tipo di informazione IR_6_NA basato sui dati relativi all'uso.

Il *capoverso 2* precisa, come in precedenza, che vanno fornite solamente le indicazioni valide durante il periodo a cui si riferisce la richiesta. Poiché questo tipo di informazione si basa su dati relativi all'uso, le POC con obbligo d'informazione devono conservare i dati elencati soltanto per sei mesi. Se la domanda d'informazione riguarda un periodo trascorso da più di sei, le POC devono fornire soltanto i dati ancora a loro disposizione.

Alla *lettera a,* l'identificativo DSL è sostituito da GPSI negli esempi (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2) e viene aggiunta la possibilità di formulare una domanda con un identificativo che permette di identificare l'utente in caso di un accesso WLAN pubblico gestito professionalmente. Alle *lettere b* e *c*, che restano in linea di principio uguali, vengono semplicemente aggiunti i nuovi identificativi del sistema 5G: SUPI e PEI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10 e art. 36 cpv. 1 lett. b n. 4). La *lettera d* resta invariata. La *lettera e* è nuova e permette di standardizzare la domanda del codice PUK e quindi di redigerla in modo più efficiente. Finora, a tal fine, erano necessarie due domande d'informazione: IR_4_NA e IR_6_NA. Ora è necessaria solamente una domanda IR_6_NA per richiedere il codice PUK di una determinata ICCID.

Art. 37 cpv. 1, frase introduttiva e lett. b

Il *capoverso 1* subisce una leggera modifica redazionale e nella versione tedesca è adeguato in modo da rispettare la parità di genere nella lingua.

Negli esempi della *lettera b* l'identificativo DSL è sostituito dall'identificativo GPSI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2). L'alternativa, introdotta con la presente revisione, «o un identificativo che permette di richiedere i dati identificativi ai sensi dell'articolo 19 capoverso 2» serve a identificare un utente in caso di accesso WLAN pubblico gestito professionalmente. Con l'identificativo così ottenuto, l'autorità legittimata può successivamente compilare una domanda di informazione IR_4_NA (art. 35) e ricevere quindi i dati identificativi ai sensi dell'articolo 19 capoverso 2.

Art. 38 cpv. 1, frase introduttiva e lett. b, nonché cpv. 2, frase introduttiva e lett. f

La frase introduttiva del *capoverso 1* è più breve, ma il suo contenuto non cambia. La formulazione «ai fini dell'identificazione» corrisponde alla versione francese. Negli esempi della *lettera b* l'identificativo DSL è sostituito dall'identificativo GPSI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2). L'alternativa, introdotta con la presente revisione, «o un identificativo che permette di richiedere i dati identifica-

tivi ai sensi dell'articolo 19 capoverso 2» serve a identificare un utente in caso di accesso WLAN pubblico gestito professionalmente (cfr. il commento all'art. 37 cpv. 1 lett. b).

La frase introduttiva del *capoverso 2* è precisata in modo tale che la domanda si riferisca all'intero «contesto di traduzione» anziché alla singola «procedura di traduzione» poiché le singole traduzioni NAT sono uguali per l'intero contesto di traduzione. L'aggiunta «ai fini dell'identificazione» in questa frase può essere cancellata in quanto compare già al capoverso 1.

Le modifiche della *lettera f* ridefiniscono il momento (adesso: momento determinante). Secondo la sentenza del Tribunale amministrativo federale A-6807/2019 (n. 4.5.1 pag. 24), il FST deve memorizzare i metadati sull'assegnazione e la traduzione degli indirizzi IP e dei numeri di porta (cfr. art. 21 cpv. 5 lett. b OSCPT) in modo tale da permettere di identificare l'utente in ogni momento richiesto dall'autorità richiedente e di fornire le indicazioni di cui all'articolo 38 capoverso 1 OSCPT, se l'autorità richiedente gli comunica le indicazioni di cui all'articolo 38 capoverso 2 OSCPT per il momento in questione. La presente modifica chiarisce che l'autorità richiedente può chiedere informazioni su un momento qualsiasi all'inizio, durante e alla fine di un determinato contesto di traduzione NAT. Il momento determinante indicato nella richiesta, non deve quindi necessariamente trovarsi vicino all'inizio del contesto di traduzione NAT (osservato) oggetto della domanda.

Questo tipo di informazione standardizzato permette solo risposte univoche, ossia va trovato un unico identificativo. Se le POC trovano più risultati corrispondenti, questi non vanno trasmessi come risultato di questo tipo di informazione. La limitazione è importante poiché questo tipo di informazione non prevede la possibilità di valutare la pertinenza dei singoli risultati.

Art. 39 Tipo di informazione IR_9_NAT: informazioni su contesti di traduzione NAT

L'articolo è stato oggetto di diverse modifiche di lieve entità anche per migliorarne la leggibilità e la comprensibilità. Rispetto all'articolo 38, riguardante le informazioni usuali sull'identificazione dell'utente in relazione con la NAT, l'articolo 39 focalizza gli aspetti tipici della NAT. Questo tipo di informazione serve agli specialisti per procedere al tracciamento (il cosiddetto *backtracking*) dei collegamenti oltre i confini NAT. Per indicazioni più precise su questa procedura si rimanda alla pagina 41 del rapporto esplicativo del 15 novembre 2017 concernente la revisione totale della OSCPT.

Come all'articolo 38, nella frase introduttiva del *capoverso 1* viene precisato che la domanda di informazioni si riferisce all'intero «contesto di traduzione» anziché alla singola «procedura di traduzione» poiché le singole traduzioni NAT sono uguali per l'intero contesto di traduzione. Il contenuto materiale delle *lettere a* e *b* non cambia.

Come al capoverso 1, anche al *capoverso 2* l'espressione «procedura di traduzione» è sostituita con «contesto di traduzione», poiché, anche qui, le singole traduzioni NAT sono uguali per l'intero contesto di traduzione. Inoltre la disposizione precisa che nella

richiesta vanno inserite soltanto le indicazioni note sul contesto di traduzione. L'autorità richiedente deve tuttavia mettere in conto che se le indicazioni sono poco dettagliate il fornitore potrebbe non riuscire a trovare il contesto di traduzione corretto.

Il contenuto materiale delle *lettere a-d* non cambia. Alla *lettera* e è aggiunta la precisazione «se necessario per l'identificazione», poiché, per ragioni di protezione dei dati, si intende limitare la memorizzazione di questo tipo di protocollo al minimo indispensabile. Alla *lettera f* viene precisato il momento determinante, analogamente all'articolo 38 capoverso 2 lettera f (cfr. il commento a tale lettera).

Art. 40 cpv. 1 lett. b, c e d, frase introduttiva e n. 2, 6, 7 e 10–13, cpv. 2, frase introduttiva e lett. g, j e k, nonché cpv. 3

Nel *capoverso 1 lettere b* e *c* è inserito il periodo di validità per gli altri indirizzi e dati di contatto (cfr. il commento alla modifica analoga dell'art. 35 cpv. 1 lett. b e c).

La *lettera d* (la frase introduttiva della lettera d subisce una leggera modifica redazionale) *numero 2* precisa che va trasmesso l'identificativo univoco principale del servizio, ad esempio il numero di telefono principale. Questa precisazione è necessaria poiché vi sono servizi di telefonia mobile con carte SIM supplementaru (p. es. multidevice, multiSIM) che hanno più di un identificativo (p. es. MSISDN). Gli altri identificativi sono contemplati al numero 7.

Secondo la *lettera d numero 6* ora può essere comunicato il periodo di validità degli stati del servizio, analogamente a quanto previsto per il tipo di informazione IR_4_NA (art. 35 cpv. 1 lett. d n. 6 vigente). Poiché lo standard ETSI prevede differenti formati di dati per i servizi di accesso alla rete (NA) e per i servizi multimedia (TEL), è stato anzitutto necessario presentare una richiesta di modifica (change request) all'ETSI affinché il parametro del periodo di validità, già esistente per i servizi di accesso alla rete (NA), fosse definito anche per i servizi multimedia (TEL). Ora che l'ETSI ha adeguato lo standard, la presente modifica può essere introdotta.

Al *numero 7* è inserita l'aggiunta «associati» per precisare che si tratta anche degli elementi d'indirizzo (p. es. numero di telefono) e degli identificativi (p. es. il numero SIM «ICCID») associati (associated) al servizio oggetto della domanda, ad esempio in caso di servizi di telefonia mobile con carte SIM supplementari. Ne fanno parte anche gli elementi d'indirizzo e gli identificativi, aggiunti solo dopo la registrazione, se sono dati sull'utente (subscriber data). Gli elementi d'indirizzo e gli identificativi assegnati in base all'utilizzo (usage data) non sono richiesti nella presente domanda di informazioni ma con quella di cui all'articolo 41. Va ora indicato il periodo di validità dei rispettivi elementi d'indirizzo e identificativi.

Al *numero 10* è inserito il nuovo identificativo SUPI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10). Inoltre si parla ora degli IMSI o dei SUPI associati per sottolineare il fatto che si può trattare di più IMSI o SUPI (p. es. servizi di telefonia mobile con carte SIM supplementari).

Al *numero 11* il termine *numero di carta SIM* è sostituito dal termine tecnico universale *ICCID* (cfr. il commento all'art. 35 cpv. 1 lett. d n. 9). Inoltre è aggiunta l'espressione «associati» per esprimere che si può trattare di più ICCID (p. es. servizi di telefonia mobile con carte SIM supplementari).

Il *numero 12* finora non poteva contemplare, in analogia all'articolo 35 capoverso 1 numero 11, il «tipo di relazione commerciale» (ingl. «subscription type») poiché all'epoca della stesura della OSCPT del 17 novembre 2017 il corrispondente standard ETSI non conteneva ancora il parametro necessario. Nel frattempo lo standard è stato adeguato e ora è possibile trasmettere il «tipo di relazione commerciale».

Al *numero 13* è inserito un campo per la trasmissione della «designazione del servizio». (cfr. il commento all'art. 35 cpv. 1 lett. d n. 13).

Il *capoverso 2 lettera g* precisa che la domanda può essere compilata anche basandosi sul LEI (cfr. il commento all'art. 20*b* cpv. 1 lett. b).

Nella *lettera j* è inserito il nuovo identificativo SUPI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10).

Nella *lettera k* il termine *numero di carta SIM* è sostituito dal termine tecnico universale *ICCID* (cfr. il commento all'art. 35 cpv. 1 lett. d n. 9).

Il *capoverso 3* corrisponde al terzo e al quarto periodo del vigente capoverso 2 spostati nel presente capoverso per motivi redazionali.

Art. 41 Tipo di informazione IR_12_TEL: informazioni su servizi di telefonia e multimedia

A seguito delle numerose modifiche l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Il secondo periodo della frase introduttiva del vigente capoverso 1 è stralciato poiché la comunicazione del periodo di validità di determinate indicazioni è ora disciplinata caso per caso.

Il *capoverso 1* è ora strutturato in due lettere. La *lettera a* resta invariata, mentre la *lettera b* è ora *suddivisa in* quattro numeri che illustrano le indicazioni da trasmettere per singolo servizio. Oltre al servizio oggetto della domanda ce ne possono essere altri ad esso associati. Nella frase introduttiva viene aggiunto «associati» per indicare che si tratta dei servizi associati (associated) al servizio oggetto della domanda con i loro elementi d'indirizzo e identificativi come nel caso, ad esempio, di servizi di telefonia mobile con carte SIM supplementari (p. es. multidevice, multiSIM), poiché questi hanno più di un identificativo (p. es. MSISDN). Il *numero 1* corrisponde in linea di massima alla vigente lettera b ma ora distingue tra elementi d'indirizzo privati e pubblici introducendo inoltre l'indicazione del loro periodo di validità (da – a). Il *numero 2* corrisponde, in linea di principio, alla vigente lettera d e disciplina le indicazioni da fornire sui dispositivi usati negli ultimi sei mesi in relazione a ciascuno dei servizi presso il fornitore. Come esempio sono indicati l'IMEI e il PEI (cfr. art. 36 cpv. 1 lett. b n. 4). L'indirizzo MEC, meno frequente, non viene più indicato come esempio, ma fa sempre parte degli identificativi del dispositivo. Il *numero 3* riunisce le vigenti lettere c (IMSI), e (ICCID) ed f (PUK) integrandovi altri identificativi come il SUPI, il MSISDN, il GPSI e l'eUICC-ID nonché il periodo di validità per permettere alle autorità legittimate di avere una visione cronologica migliore sui mezzi di accesso (SIM) e gli identificativi associati a ciascun servizio. Sono introdotti entrambi gli identificativi delle reti di telefonia mobile 5G: SUPI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10) e GPSI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2). Al posto di «numero della carta SIM» è utilizzato l'acronimo ICCID (cfr. il commento all'art. 35

cpv. 1 lett. d n. 9). Il *numero 4* è nuovo e serve per indicare, in caso di un'offerta multidevice, se si tratta del dispositivo principale o di un dispositivo secondario.

Nel *capoverso 2 lettera a* gli esempi sono ridotti: il numero di telefono è cancellato e *TEL URI* è sostituito da *GPSI* (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2); l'obiettivo della modifica è riportare soltanto pochi esempi attuali. Ciò non significa tuttavia che il numero di telefono e il *TEL URI* non possano essere più utilizzati come criteri nella domanda. Nelle *lettere b e c* sono inseriti i nuovi identificativi del sistema 5G SUPI e PEI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10 e all'art. 36 cpv. 1 lett. b n. 4). Le *lettere d* ed *e* restano invariate. Alla *lettera f* è aggiunto il criterio del numero della carta SIM (ICCID; cfr. il commento alla modifica analoga di cui all'art. 36 cpv. 2 lett. e).

Art. 42 cpv. 1 lett. c, frase introduttiva (concerne soltanto i testi tedesco e francese) e n. 6, e d, cpv. 2, frase introduttiva e lett. g e j, nonché cpv. 3

Come per gli altri tipi di informazione su servizi di comunicazione (art. 35, 40 e 43) anche qui, e più precisamente al *capoverso 1 lettera c* (il testo tedesco e francese subiscono, rispettivamente alla frase introduttiva e alla lettera c, una leggera modifica redazionale) *numero 6,* è aggiunto un campo per la trasmissione della designazione del servizio (cfr. il commento all'art. 35 cpv. 1 lett. d n. 13). La *lettera d* prevede ora il nuovo identificativo GPSI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2).

Nel *capoverso 2 lettera g* si precisa che la richiesta può essere compilata basandosi anche sul LEI oltre che sull'IDI (cfr. il commento 20*b* cpv. 1 lett. b). La *lettera j* prevede ora l'identificativo connesso al servizio oggetto della domanda. Si tratta ad esempio di un elemento d'indirizzo di ripristino quale l'indirizzo di posta elettronica o il numero di telefono.

Il *capoverso 3* corrisponde al terzo periodo del vigente capoverso 2.

Art. 43 cpv. 1 lett. c, frase introduttiva (concerne soltanto i testi tedesco e francese) e n. 6, cpv. 2, frase introduttiva, lett. g, i e j, nonché cpv. 3

Nel *capoverso 1* sono cancellati i servizi cloud, poiché tale termine non è abbastanza preciso. Infatti qualsiasi servizio può essere offerto come servizio cloud, anche servizi che non sono né servizi di telecomunicazione né servizi di comunicazione derivati (p. es. calcoli per computer, servizi di traduzione). Per lo stesso motivo sono cancellati anche i servizi proxy.

Come per gli altri tipi di informazione su servizi di comunicazione (art. 35, 40 e 42), anche qui, e più precisamente al *capoverso 1 lettera c* (il testo tedesco e francese subiscono una lieve modifica redazione) *numero 6*, è aggiunto un campo per la trasmissione della designazione del servizio (cfr. il commento all'art. 35 cpv. 1 lett. d n. 13).

Il *capoverso 2 lettera g* prevede ora che la domanda possa essere compilata anche in base al LEI (cfr. il commento all'art. 20*b* cpv. 1 lett. b).

La *lettera i* precisa che si tratta di un elemento d'indirizzo o di un identificativo del servizio oggetto della domanda (servizio di telecomunicazione o servizio di comunicazione derivato). La domanda di informazioni può ad esempio riguardare un determinato identificativo univoco, specifico di un'applicazione, che va indicato qui. Tale identificativo è utilizzato per le notifiche dell'applicazione in questione e permette di garantire che la notifica del servizio in questione possa essere inviata a una determinata applicazione su un determinato dispositivo (p. es. device token dell'Apple push notification service, registration identifier del Google cloud messaging, channel URI del Windows push notification service).

La nuova *lettera j* menziona l'identificativo connesso al servizio oggetto della domanda. Si tratta ad esempio di un elemento d'indirizzo di ripristino quale l'indirizzo di posta elettronica o il numero di telefono.

Il *capoverso 3* corrisponde al terzo e al quarto periodo del vigente capoverso 2.

Art. 44 cpv. 1, frase introduttiva e lett. c ed f (concerne soltanto il testo tedesco) nonché cpv. 3, frase introduttiva e lett. c, d (concerne soltanto il testo tedesco) ed f

La frase introduttiva del *capoverso 1*, nel testo italiano, subisce una correzione di carattere redazionale. Nella versione tedesca il *capoverso 1 lettere c* ed *f* come anche il *capoverso 3 lettere c* e *d* sono adeguate sotto il profilo redazionale.

La frase introduttiva del *capoverso 3* subisce, nella versione italiana, una modifica redazionale; inoltre è aggiunta la *lettera f* che permette di inoltrare la domanda di informazioni a partire dal codice per la ricarica del credito o per il pagamento del servizio usato di norma per i servizi prepagati (prepaid). Si tratta di un codice acquistabile ad esempio all'edicola o alla cassa del supermercato in forma di «carta gratta» o scontrino. Inserendo il codice si può versare il relativo importo su un conto prepagato. Finora lo standard ETSI non prevedeva un campo di dati per poter usare questo codice come criterio per una domanda di informazioni. Poiché questa possibilità di informazione sussisteva già secondo la vecchia OSCPT del 31 ottobre 2001, il Servizio SCPT ha presentato una pertinente richiesta di modifica all'ETSI che nel frattempo l'ha accolta e inserita nello standard. Pertanto le richieste pertinenti possono essere ora presentate secondo la procedura standard.

Art. 45 **Tipo di informazione IR_18_ID: prova dell'identità**

L'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Il *capoverso 1* è adeguato alla terminologia dell'articolo 20*a* («documento» invece di «documento d'identità»).

Nel *capoverso* 2 è inserito il nuovo identificativo SUPI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10). Per il resto, il capoverso resta invariato. L'abbreviazione *ICCID* è spiegata nell'allegato. Una domanda di informazioni in base al numero del dispositivo (limitata dalla locuzione avverbiale «se del caso») è possibile solamente se il fornitore ha consegnato il dispositivo e ne ha registrato il numero, cosa che di solito non avviene con i servizi di telefonia mobile.

Art. 46 cpv. 1

La modifica concerne soltanto la versione tedesca, adeguata sotto il profilo redazionale in modo da rispettare la parità di genere nella lingua.

Art. 47 cpv. 1 e 2

La modifica del *capoverso 1* concerne soltanto la versione tedesca, adeguata sotto il profilo redazionale in modo da rispettare la parità di genere nella lingua.

Nel *capoverso* 2 è inserito il nuovo identificativo SUPI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10). Per il resto, il capoverso resta invariato. L'abbreviazione *ICCID* è spiegata nell'allegato. La domanda di informazioni in base al numero del dispositivo (limitata dalla locuzione avverbiale «se del caso») è possibile solamente se il fornitore ha consegnato il dispositivo e ne ha registrato il numero, cosa che di solito non avviene con i servizi di telefonia mobile.

Art. 48 Tipo di informazione IR_21_TECH: dati tecnici

A seguito delle numerose modifiche l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Il *capoverso 1* stabilisce che questa domanda di informazioni si riferisce agli elementi di rete presenti «nella localizzazione oggetto della domanda». Inoltre precisa che sono interessati solamente gli accessi WLAN pubblici «gestiti professionalmente». La nozione «punto di accesso WLAN» è sostituita dalla nozione più generale «accesso WLAN» (cfr. il commento alla *sostituzione di espressioni,* cpv. 1 all'inizio dell'ordinanza).

Nel *capoverso 2 lettera a* l'enumerazione a titolo esemplificativo dei singoli identificativi è sostituita dall'espressione generale identificativi della cella o della zona. Il nuovo iperonimo «identificativo della cella o della zona» comprende gli esempi del testo vigente CGI (2G e 3G), ECGI (4G) e NCGI[23] (5G). I tre esempi per un'*area identity* (SAI[24], RAI[25] e TAI[26]) sono ora sostituiti dall'iperonimo «identificativo della zona». Queste modifiche redazionali concretamente non cambiano niente: i CGI, gli ECGI, i SAI, i RAI e i TAI dovranno essere sempre trasmessi se tecnicamente disponibili.

La prassi ha evidenziato che l'identificazione di un determinato accesso WLAN spesso non è possibile al livello del punto di accesso (access point), ma soltanto al livello dell'hotspot. Per questo motivo la disposizione introduce ora un'altra

23 **NCGI** (New Radio Cell Global Identity): identificativo statico di una cella nelle reti di telefonia mobile di quinta generazione (5G), secondo 3GPP TS 23.003, Clause 19.6A. Il NCGI è costituito da una catena che riprende l'identificativo PLMN (MCC + MNC) nonché la NR Cell Identity (NCI) ed è univoco su scala mondiale.

24 **SAI** (Service Area Identity): identificativo statico della zona di copertura di un servizio (service area), usato nelle reti di telefonia mobile per il mobility management (cfr. 3GPP TS 23.003, clause 12.5).

25 **RAI** (Routing Area Identity): identificativo statico per una zona di routing (routing area), usato nelle reti di telefonia mobile nell'ambito della trasmissione di pacchetti di dati per il mobility management (cfr. 3GPP TS 23.003, clause 4.2).

26 **TAI** (Tracking Area Identity): identificativo statico per una zona di tracciamento (tracking area), usato nelle reti di telefonia mobile della quarta generazione per il mobility management (cfr. 3GPP TS 23.003, clause 19.4.2.3).

designazione idonea in alternativa agli identificativi degli elementi di rete (p. es. nome dell'hotspot, in alternativa al BSSID), anche se non si tratta di un identificativo univoco (cfr. anche gli art. 48 cpv. 3 lett. b, 54 cpv. 3 lett. a, 56 cpv. 2 lett. e n. 9, 60 lett. h, 61 lett. i n. 4, 64 cpv. 2 e 65 cpv. 3). Poiché il fornitore dell'hotspot può sceglierne liberamente il nome, quest'ultimo non è univoco e spesso non è esplicativo dato che non se ne può dedurre il fornitore. I fornitori di hotspot pubblici devono pertanto mettere a disposizione delle autorità una possibilità adeguata d'identificazione dei loro hotspot, per esempio mediante un sito web generico (URL) cui si può accedere se si è collegati con l'hotspot e su cui si ricevono indicazioni sul fornitore dell'hotspot. Se il nome dell'hotspot non è abbastanza chiaro, cioè non designa in modo inequivocabile l'hotspot in loco, possono essere usate designazioni sufficientemente precise, come ad esempio una breve descrizione della localizzazione. Questa modifica non significa che il BSSID[27] non debba essere fornito: se noto, questo identificativo deve essere trasmesso. Le *lettere b, c* e *d* restano praticamente invariate.

La *lettera* e è nuova poiché nelle reti di telefonia mobile 5G le indicazioni sulla localizzazione degli elementi di rete (p. es. celle di telefonia mobile) possono essere provviste di marche temporali.

Nel *capoverso 3 lettera a*, in riferimento alla localizzazione, si aggiunge l'espressione «oggetto della domanda» per precisare che la richiesta può basarsi sulle coordinate geografiche di una localizzazione e quindi riferirsi a tutti gli elementi di rete della POC che si trovano nella localizzazione indicata dalle coordinate. Secondo la *lettera b,* sono possibili anche domande riguardanti un determinato elemento di rete in questa localizzazione; tali domande possono contenere, invece di un identificativo standardizzato, un'altra designazione idonea (p. es. nome dell'hotspot). Infine, come nel capoverso 2 lettera a, è utilizzato l'iperonimo «identificativo della cella o della zona» (cfr. sopra).

Art. 48a Tipo di informazione IR_51_ASSOC_PERM: informazioni su identificativi attribuiti a lungo termine

Per la fornitura di servizi di telefonia dell'IMS possono essere usati, in sostituzione degli identificativi permanenti del servizio o del dispositivo, anche identificativi attribuiti a lungo termine. È pertanto introdotto questo nuovo tipo di informazione che permette di richiedere gli identificativi attribuiti a lungo termine (IMPI privato per l'IMPU pubblico e viceversa). Poiché si tratta di indicazioni ai fini dell'identificazione ai sensi dell'articolo 22 LSCPT, i FST e i FSCD con obblighi supplementari secondo l'articolo 22 o 52 devono conservare e trasmettere questi dati per l'intera durata della relazione commerciale e per sei mesi dopo il suo termine (art. 21 cpv. 1).

[27] **BSSID** *(*Basic Service Set Identifier): identificativo univoco (indirizzo MAC) dell'accesso WLAN.

Art. 48b Tipo di informazione IR_52_ASSOC_TEMP: informazioni immediate su identificativi attribuiti per breve tempo

Secondo il *capoverso 1*, per la fornitura di servizi di telefonia mobile 5G possono essere usati, in alternativa agli identificativi permanenti del servizio o del dispositivo, anche identificativi attribuiti per breve tempo (temporanei). Questo nuovo tipo di informazione è introdotto per ottenere, praticamente in tempo reale, gli identificativi permanenti attribuiti a un identificativo temporaneo. Ciò significa che la risposta va di regola fornita in frazioni di secondo. Non è necessario conservare questi dati.

Il *capoverso 2* disciplina le indicazioni che deve contenere la domanda. Poiché gli identificativi temporanei possono essere attribuiti in maniera univoca soltanto in una determinata zona della telefonia mobile, tale zona deve essere precisata. I dettagli tecnici sono definiti nell'allegato 1 della OE-SCPT.

L'esempio riportato di seguito è un caso di applicazione importante per la tecnologia 5G. Nell'ambito dell'impiego di apparecchi tecnici speciali di cui all'articolo 269bis CPP, un'autorità legittimata rileva un identificativo temporaneo (p. es. 5G-GUTI o SUCI) mediante i suoi apparecchi radiotecnici (p. es. false base station); dopodiché compila una domanda in base a questo nuovo tipo di informazione in modo da ricevere subito il relativo identificativo permanente (p. es. SUPI).

Il tempo di risposta del nuovo tipo di informazione deve essere molto breve (praticamente in tempo reale), poiché gli identificativi temporanei cambiano spesso. Questa informazione deve pertanto essere consultata e fornita in forma automatizzata mediante una nuova interfaccia di consultazione. Con una domanda di informazioni si possono ottenere nel contempo più identificativi (cpv. 2). Poiché si tratta di una consultazione praticamente in tempo reale, non può essere indicato un momento determinante. Vale pertanto il momento della domanda cui va aggiunto un breve intervallo tecnico di tolleranza. Non è possibile procedere a consultazioni retroattive né effettuarne nel futuro.

Art. 48c Tipo di informazione IR_53_TEL_ADJ_NET: determinazione delle reti adiacenti di servizi di telefonia e multimedia

Questo tipo di informazione è introdotto per risolvere problemi specifici legati all'identificazione degli autori di reati collegabili ad esempio a numeri di telefono falsificati (spoofing) o sconosciuti utilizzati dal chiamante o dal mittente della comunicazione. Ciò può essere utile, nel caso ad esempio di una minaccia dinamitarda anonima, per potere seguire la traccia della chiamata o del messaggio anonimi.

I metadati storici delle connessioni e dei tentativi di connessione, conservati ai fini di permettere la sorveglianza retroattiva, contengono gli elementi d'indirizzo dei partecipanti alla comunicazione (chi con chi). Tuttavia, se il numero di provenienza o l'indirizzo del mittente sono falsificati o sconosciuti, le autorità legittimate hanno bisogno di un mezzo per rintracciare la chiamata o la comunicazione.

Il *capoverso 1* prescrive le indicazioni da trasmettere. Il fornitore deve trasmettere la designazione della rete di partenza immediatamente adiacente alla sua («da») e quella della rete di destinazione immediatamente adiacente alla sua («a») lungo il percorso della comunicazione, a condizione che tali reti fossero coinvolte nella comunicazione

o nel tentativo di comunicazione oggetto della domanda. Non deve trasmettere indicazioni su eventuali altre reti, a monte o a valle, di una connessione. Un esempio: una chiamata è stata effettuata dalla rete del fornitore A alla rete del fornitore C passando per la rete del fornitore B; se il fornitore B riceve la domanda di informazioni sulla chiamata, deve indicare i fornitori A («da») e C («a») come reti adiacenti. Se il destinatario della domanda è il fornitore A, quest'ultimo indicherà solamente il fornitore B («a»; non esiste una rete «da»). Se il destinatario della domanda è il fornitore C, quest'ultimo indicherà solamente il fornitore B («da», non esiste una rete «a»). È sufficiente che il fornitore trasmetta le designazioni che utilizza solitamente a livello interno, ad esempio un «Inter Operator Identifier» che designa un determinato fornitore o l'indirizzo IP della rete adiacente.

Il *capoverso 2* disciplina i criteri da indicare nella domanda affinché la comunicazione o il tentativo di comunicazione in questione possa essere determinato in modo univoco.

Questo tipo di informazione introduce un obbligo di conservare i relativi metadati per sei mesi (cfr. anche art. 21 cpv. 5 lett. c e art. 61 lett. j) per i FST con obblighi integrali e i FSCD con obblighi di sorveglianza supplementari (art. 52). Poiché ogni fornitore può controllare solamente le proprie interfacce di rete, per ottenere indicazioni affidabili è richiesta soltanto l'indicazione delle reti immediatamente adiacenti coinvolte nella comunicazione o nel tentativo di comunicazione. In questo modo, l'autorità legittimata può chiedere informazioni ai singoli fornitori al fine di ricostruire o seguire la comunicazione in questione.

Questo nuovo tipo di informazione istituisce una procedura standardizzata per ricostruire o seguire comunicazioni o tentativi di comunicazione. I tempi di trattamento sono disciplinati nell'articolo 14 OE-SCPT.

Art. 50 cpv. 1 e 5-9

Analogamente all'articolo 18 (obblighi per la trasmissione di informazioni), il *capoverso 1* è ampliato al fine di precisare gli obblighi legati all'esecuzione dei nuovi tipi di sorveglianza di cui agli articoli 56*a*, 56*b*, 67 lettere b e c nonché 68 capoverso 1 lettere b e c. Il *secondo periodo* esenta il FSCD con obblighi di sorveglianza supplementari (art. 52) dall'eseguire questi tipi di sorveglianza. Se in futuro queste sorveglianze dovranno essere effettuate anche dai FSCD sarà deciso nell'ambito della seconda revisione, quando si procederà a una descrizione più dettagliata delle categorie di FST e di FSCD. Pertanto il presente progetto non impone ai FSCD nuovi obblighi in relazione a questi nuovi tipi di sorveglianza.

Secondo il nuovo *capoverso 5*, la POC deve assistere il Servizio SCPT solo se quest'ultimo glielo chiede (anziché in caso di necessità).

Il *capoverso 6* disciplina la gestione degli identificativi associati dall'inizio della sorveglianza, della ricerca d'emergenza o della determinazione della posizione, mentre il capoverso 9 disciplina la modifica e l'aggiunta di identificativi durante una sorveglianza in tempo reale o una determinazione periodica della posizione. Nel caso di servizi di telefonia mobile con carte SIM supplementari (p. es. multidevice o multiSIM per altri dispositivi come smartphone, tablet, smartwatch) vanno sempre sorvegliati tutti i dispositivi, i numeri o le SIM associati all'identificativo target (p. es.

nel caso di un numero principale, tutti i numeri accessori). Questa regola si applica a tutti i tipi di sorveglianza (in tempo reale, retroattiva, determinazione della posizione, ricerca d'emergenza, ricerca di condannati). Se ad esempio viene sorvegliato il MSISDN o l'IMSI di un abbonamento, devono essere sorvegliati tutti i numeri principali e secondari di questo abbonamento compresi i relativi dispositivi come ad esempio smartwatch che utilizzano le SIM e i numeri di telefono associati. Fanno eccezione gli identificativi target secondari con cui non si può comunicare (p. es. numeri tecnici) e altri numeri del dispositivo se lo stesso identificativo target è un numero del dispositivo (ossia se il numero del dispositivo x è sorvegliato, gli altri numeri del dispositivo, collegabili indirettamente ad esso tramite l'abbonamento utilizzato, non devono essere sorvegliati). Non sono riscossi emolumenti o versate indennità per i dispositivi, i numeri o le SIM supplementari. Se necessario, il fornitore può richiedere al Servizio SCPT altri numeri di identificazione amministrativi della sorveglianza (LIID: Lawful Interception Identifier). Se l'autorità che ordina la misura di sorveglianza non auspica la sorveglianza di tutti i dispositivi, i numeri e le SIM associati all'identificativo target principale sorvegliato, deve esplicitamente indicarlo nel suo ordine.

Il *capoverso 7* amplia gli obblighi in caso di sorveglianza in tempo reale di servizi di telefonia mobile estendendoli alla sorveglianza delle banche dati tecniche degli utenti (p. es. HLR[28], HSS[29] e UDM[30]) ai fini del rilevamento e della trasmissione di importanti metadati del target. Le banche dati contengono in particolare informazioni sulla rete che fornisce il servizio, sulla modifica degli identificativi del servizio e del dispositivo attribuiti, sugli eventi relativi alla localizzazione sul cambio dell'elemento di rete che fornisce il servizio nonché sugli eventi di identificazione e di autenticazione.

Il *capoverso 8* prevede che nell'IMS sia eventualmente attivata la determinazione, da parte della rete (network provided), dei dati di localizzazione dell'identificativo durante la sorveglianza in tempo reale.

Il *capoverso 9* prevede che la POC sorvegli anche le modifiche e l'aggiunta di dispositivi multidevice, numeri e SIM associati al servizio già sottoposto a sorveglianza. La POC deve adeguare autonomamente la sorveglianza ai cambiamenti ed eventualmente estenderla ai nuovi identificativi target. Per questo onere supplementare le POC non hanno diritto ad alcuna indennità. Nemmeno il Servizio SCPT può chiedere un emolumento supplementare in questi casi. Se necessario, il fornitore può chiedere un ulteriore LIID per impostare le altre sorveglianze necessarie (cfr. il commento al cpv. 6).

28 **HLR** (Home Location Register): nelle reti di telefonia mobile di seconda e terza generazione, banca dati di un fornitore di servizi di telefonia mobile in cui sono registrate le caratteristiche funzionali dei suoi utenti (p. es. IMSI, MSISDN, configurazione, profili del servizio) e la loro attuale rete che fornisce il servizio.

29 **HSS** (Home Subscriber Server): nelle reti di telefonia mobile di quarta generazione, funzioni analoghe a HLR.

30 **UDM** (Unified Data Management): nelle reti di telefonia mobile di quinta generazione, funzioni analoghe a HLR e HSS.

Art. 53 Accesso agli impianti

Il *capoverso 1* precisa che anche presso le POC che devono solamente tollerare la sorveglianza è consentito eseguire i collegamenti test necessari. Detti collegamenti sono disciplinati all'articolo 30. Un collegamento test è necessario in particolare quando occorre predisporre una sorveglianza che è stata ordinata o controllare la qualità di una sorveglianza in corso, anche se quest'ultima è attuata, sotto il profilo tecnico, dal Servizio SCPT.

Il *capoverso 2* è identico al vigente capoverso 2 tranne che per un adeguamento redazionale nel secondo periodo («d'accordo» anziché «d'intesa»).

Art. 54 Tipo di sorveglianza RT_22_NA_IRI: sorveglianza in tempo reale dei metadati per i servizi di accesso alla rete

A seguito delle numerose modifiche l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. La tecnologia 5G permette registrazioni multiple nella rete (multiple registrations) o connessioni multiple (multiple attachments) nella stessa rete o in altre reti che forniscono il servizio, il che consente di cambiare l'obiettivo della sorveglianza (target) tra le diverse reti e tecnologie[31].

Il *capoverso 1* resta invariato.

Il *capoverso 2 lettera a* è completato in modo tale che le autorità siano in futuro informate, nell'ambito della sorveglianza in tempo reale, sulla tecnologia usata dal target e su un cambio della rete o della tecnologia da parte del target. Per la telefonia mobile vanno trasmesse anche le informazioni sulle procedure di connessione e disconnessione dell'accesso alla rete secondo la tecnologia usata (p. es. GPRS, EPS, 5GS). Nel caso di GPRS in particolare gli eventi GPRS attach, GPRS detach, PDP context activation e PDP context deactivation; nel caso di EPS gli eventi E-UTRAN attach, E-UTRAN detach, bearer activation e bearer deactivation; nel caso di 5GS gli eventi registration, deregistration, PDU session establishment e PDU session release.

La *lettera b* resta invariata.

Nelle *lettere c* ed *e* sono rispettivamente cancellate le precisazioni ridondanti «per le reti mobili» e «per la telefonia mobile» in quanto l'intero articolo si riferisce solamente al settore della telefonia mobile.

Nelle *lettere c, e* ed *f* sono aggiunti i nuovi identificativi del sistema 5G (SUPI, GPSI, PEI; cfr. il commento all'art. 35 cpv. 1 lett. d n. 2 «GPSI» e n. 10 «SUPI» nonché all'art. 36 cpv. 1 lett. b n. 4 «PEI»).

L'aggiunta «dispositivi associati» alla *lettera d* precisa che vanno trasmessi anche gli indirizzi IP assegnati degli apparecchi multidevice. Inoltre non sono più menzionati i settori di indirizzi IP non rilevanti in questo caso.

La *lettera g* precisa che si tratta di eventi che modificano le caratteristiche tecniche del servizio di accesso alla rete sorvegliato o la sua gestione della mobilità (mobility management). Rientrano nelle modifiche delle caratteristiche tecniche ad esempio:

- le modifiche del supporto al servizio (service support);

31 Cfr. 3GPP TS 33.501 sezione 6.3.2.

- le modifiche del PDP context, del bearer o della sessione PDU;
- i NAS signalling messages del target;
- l'aggiornamento della posizione del target, ad esempio location update e mobility registration update.

I NAS signalling messages sono messaggi di segnalazione che il dispositivo e il nucleo centrale della rete di telefonia mobile si scambiano mediante l'interfaccia NAS (NAS = Non Access Stratum). Il mobility management comprende ad esempio GMM, EMM e mobility registration.

Analogamente all'articolo 56 capoverso 2 lettera e numero 9, la *lettera h* precisa ora che si tratta di dati di localizzazione «attuali» e non «momentanei» sottolineando inoltre che questi dati devono essere determinati, se possibile, dalla rete e contrassegnati come tali. I dati di localizzazione determinati dalla rete sono più affidabili di quelli determinati dal dispositivo, poiché questi ultimi potrebbero essere falsificati. Vanno tuttavia forniti tutti i dati di localizzazione disponibili, anche quelli del dispositivo che vanno contrassegnati come tali. La dicitura «determinati dalla rete» o «determinati dal dispositivo» aiuta le autorità a valutare quanto siano affidabili questi dati. Adesso vanno trasmessi anche i dati di localizzazione, riguardanti il target, dedotti dai messaggi di segnalazione NAS e, per i sistemi di telefonia mobile di quarta (EPS) e di quinta generazione (5GS), anche le marche temporali e le indicazioni sull'età dei dati di localizzazione se disponibili. Per «età dei dati di localizzazione» s'intende il periodo intercorso tra l'effettiva determinazione del dato di localizzazione e la trasmissione dell'informazione.

Le *lettere i–k* disciplinano la trasmissione di importanti metadati rilevati in occasione della sorveglianza di banche dati tecniche degli utenti quali HLR, HSS e UDM (cfr. il commento all'art. 50 cpv. 7).

La *lettera i* concerne le informazioni sulla rete che fornisce attualmente il servizio e su quella che lo forniva precedentemente, ossia eventi del tipo «serving system» (*rete che fornisce il servizio*, p. es. serving PLMN, VPLMN ID).

La *lettera j* concerne:

- le informazioni sulla modifica degli identificativi del servizio e del dispositivo attribuiti (p. es. IMSI, MSISDN, IMEI, SIP-URI, IMPI), ossia eventi del tipo «susbcriber record change». Vanno trasmessi in particolare gli identificativi temporanei, anche se la loro durata di vita è breve;
- le informazioni sugli eventi relativi alla localizzazione e, se del caso, il loro motivo, ad esempio eventi del tipo «register location / cancel location / register termination»;
- le informazioni sul cambio dell'elemento di rete che fornisce il servizio (p. es. SGSN, MME, MSC, AMF);
- le informazioni sugli eventi di identificazione e autenticazione del target (p. es. ottenimento di un diritto di accesso a un PWLAN).

La *lettera k,* riguardante esclusivamente la tecnologia 5G, prevede la trasmissione anche di informazioni sull'attribuzione di nuovi identificativi temporanei. Ciò riguarda in particolare l'occultamento («concealing») di identificativi degli utenti (p. es. SUCI

anziché SUPI). Gli identificativi temporanei vanno sempre forniti in caso di nuove attribuzioni, anche se la loro durata di vita è breve.

Il *capoverso 3* subisce una modifica redazionale: al posto della nozione di «tecnologia di telefonia mobile» (nelle vigenti lett. a-c), viene impiegata la nozione più generale di «tecnologia di accesso alla rete», poiché anche le tecnologie di accesso non 3GPP, come l'accesso WLAN, sono interessate dalla disposizione. Analogamente all'articolo 48 capoverso 2 lettera a (cfr. il relativo commento), alla *lettera a* viene utilizzata la nozione generale di identificativi della cella o della zona. Adesso la disposizione comprende anche il caso in cui il target utilizza un gruppo di celle radio («combined cell», cella radio composta da più antenne distribuite geograficamente). Vista la complessità di questa normativa, si rimanda all'allegato OE-SCPT. I dati di localizzazione nel caso dell'accesso WLAN (adesso: acceso non 3GPP) non sono più disciplinati alla lettera a bensì alla nuova lettera d. Il contenuto della *lettera b* resta invariato. Alla *lettera c* non è più menzionata l'indicazione concernente la localizzazione dell'accesso WLAN che ora è disciplinata alla nuova lettera d. La *lettera d* precisa i dati di localizzazione da trasmettere in caso di un accesso non 3GPP alla rete di telefonia mobile. Sono previste due varianti: numero 1 per l'accesso WLAN e numero 2 per l'accesso da rete fissa.

Art. 56 Tipo di sorveglianza RT_24_TEL_IRI: sorveglianza in tempo reale dei metadati per servizi di telefonia e multimedia

A seguito delle numerose modifiche l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Il vigente capoverso 1 è suddiviso in due capoversi.

Il *capoverso 1* corrisponde al vigente capoverso 1, primo periodo.

La frase introduttiva del *capoverso 2* corrisponde al vigente capoverso 1, secondo periodo. La *lettera a* è invariata e corrisponde al vigente capoverso 1 lettera a. Alla *lettera b* l'espressione «reti mobili» è sostituita da «servizi di telefonia mobile» e come alternativa all'IMSI è introdotto il nuovo identificativo SUPI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10). Il contenuto della vigente lettera b^{bis} è aggiunto, senza modifiche, alla fine della lettera b. Le *lettere c* e *d* non sono modificate e corrispondono alle vigenti lettere c e d del capoverso 1 con un adeguamento redazionale alla lettera c nella versione tedesca in modo da rispettare la parità di genere nella lingua.

La *lettera e* è stata adeguata sotto il profilo redazionale per migliorarne la leggibilità. L'espressione «tecnologia di accesso alla rete» sostituisce l'espressione «tecnologia di telefonia mobile», poiché anche il passaggio del target a un accesso non 3GPP va comunicato. I *numeri 1–9* corrispondono ai numeri della vigente lettera e del capoverso 1 con le modifiche seguenti: al *numero 2* si precisa attraverso l'introduzione dell'aggettivo «specifico» che deve essere indicato il ruolo di ogni partecipante alla comunicazione. Inoltre viene aggiunto l'identificativo 5G GPSI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2). Al *numero 4* è inserito l'identificativo 5G PEI (cfr. il commento all'art. 36 cpv. 1 lett. b n. 4). Al *numero 9* l'espressione, poco utilizzata, «servizi mobili» è sostituita con «servizi di telefonia mobile». Inoltre, adesso è previ-

sto che i dati di localizzazione del target debbano essere determinati per quanto possibile dalla rete e contrassegnati come tali (determinato dalla rete/non determinato dalla rete; cfr. il commento all'art. 54 cpv. 2 lett. h). La nozione «dati di localizzazione momentanea» è ora sostituita con «dati attuali di localizzazione». Per definire più precisamente i dati di localizzazione si rimanda ora all'articolo 54 capoverso 3. Il vigente capoverso 2 è pertanto soppresso. Poiché il target può utilizzare contemporaneamente anche più celle, si inserisce «celle utilizzate» al plurale. Anziché «punto di accesso WLAN» si utilizza adesso l'espressione più generale «accesso non 3GPP». Secondo il numero 9 adesso vanno trasmessi anche i dati di localizzazione riguardanti il target dedotti dai messaggi di segnalazione NAS e, per i sistemi EPS e 5GS, i dati di localizzazione integrati, se disponibile, dalla marca temporale associata o dall'età dei dati di localizzazione (cfr. il commento all'art. 54 cpv. 2 lett. h).

La nuova *lettera f* disciplina la trasmissione di importanti metadati che possono essere rilevati in occasione della sorveglianza di banche dati tecniche degli utenti come HLR, HSS e UDM (cfr. il commento all'art. 50 cpv. 7 e all'art. 54 cpv. 2 lett. i, j e k).

Art. 56a Tipo di sorveglianza RT_54_POS_ONCE: determinazione unica e immediata della posizione mediante la rete

La determinazione della posizione ai sensi della LSCPT (LALS, lawful access to location services) è una funzione delle reti mobili di recente introduzione ed è a tutti gli effetti una sorveglianza ai sensi dell'articolo 269 CPP, pertanto deve soddisfare gli stessi rigorosi requisiti di una sorveglianza in tempo reale. Questa disposizione disciplina il primo tipo di sorveglianza della nuova determinazione della posizione mediante LALS: determinazione unica («ONCE») e immediata della posizione mediante la rete.

Nella presente ordinanza *localizzazione* e *posizione* hanno un significato diverso. Finora c'erano solo i dati di localizzazione («location information»). Per *localizzazione* si intende la localizzazione dell'antenna della cella che fornisce il servizio possibilmente integrata con altre indicazioni come la direzione principale d'irradiazione dell'antenna. La localizzazione è dunque solo un'individuazione approssimativa del luogo in cui si trova effettivamente il target (dispositivo). La cella che fornisce il servizio è la cella dove è situata l'antenna con cui è collegato o era collegato l'ultima volta il target. Maggiore è la portata di questa antenna e più ampia sarà la distanza tra il luogo in cui si trova effettivamente il target e la localizzazione indicata. Nelle zone rurali tale distanza può superare i 30 chilometri e nei casi estremi, ossia nelle zone di montagna, può essere ancora maggiore. In caso di sorveglianze in tempo reale, la localizzazione attuale del target è costantemente comunicata. In caso di sorveglianza retroattiva, sono incluse le indicazioni di localizzazione relative all'inizio e alla fine delle comunicazioni e delle sessioni di accesso alla rete. Inoltre l'ultima localizzazione conosciuta del target può essere chiesta ad hoc con una ricerca d'emergenza EP_35_PAGING o con una sorveglianza HD_31_PAGING.

Per *posizione* si intende invece il luogo preciso in cui si trova effettivamente il target (dispositivo) al momento della determinazione della posizione. L'attuale revisione introduce due tipi di sorveglianza per la determinazione della posizione mediante LALS:

1) determinazione unica e immediata della posizione (presente articolo),

2) determinazione periodica della posizione (cfr. art. 56*b*).

Secondo il *capoverso 1,* il fornitore del servizio di telefonia mobile deve procedere a una determinazione unica e immediata della posizione utilizzando una funzione apposita della rete (LALS). Vanno determinate le posizioni di tutti i dispositivi mobili associati al target ID. Se il target ID sorvegliato è un numero di dispositivo, sarà determinata la posizione soltanto di quel dispositivo. Se invece il target ID sorvegliato è un elemento d'indirizzo (p. es. MSISDN/GPSI) o un numero identificativo di un utente (p. es. IMSI/SUPI), i dispositivi utilizzati possono essere diversi (smartphone, tablets e smartwatch) tutti con la stessa relazione commerciale (abbonamento o prepaid), in particolare se vi sono associate più SIM. Poiché di regola non si conosce quale dispositivo abbia con sé la persona sorvegliata, vanno rilevate tutte le posizioni dei dispositivi associati (cfr. commenti all'art. 50 cpv. 6).

Secondo il *capoverso 2,* le prescrizioni tecniche di esecuzione sono emanate dal DFGP nella OE-SCPT e nell'allegato 1 di quest'ultima. Finora non sono ancora state fatte esperienze pratiche con questa nuova determinazione unica e immediata della posizione. A secondo dell'implementazione tecnica la determinazione della posizione può richiedere un certo tempo. Una volta determinate, il fornitore del servizio di telefonia mobile deve tuttavia trasmettere immediatamente e senza indugio le posizioni dei dispositivi.

Il *capoverso 3* precisa le indicazioni da trasmettere. Le indicazioni di cui alle *lettere a* e *b* nonché alla *lettera c numeri 1–3* devono essere obbligatoriamente trasmesse; le altre (*lettera c numero 4)* vanno trasmesse se disponibili o se possono essere determinate.

Secondo la *lettera d*, se non è stato possibile determinare la posizione, ne va comunicato il motivo (codice d'errore). Affinché l'autorità ordinante riceva almeno i dati di localizzazione nel caso in cui non sia stato possibile determinare la posizione, il fornitore deve effettuare, come piano alternativo, un «paging» ai sensi dell'articolo 63.

Art. 56b Tipo di sorveglianza RT_55_POS_PERIOD: determinazione ricorrente e periodica della posizione mediante la rete

Le osservazioni introduttive fatte per l'articolo 56*a* valgono anche per il presente articolo riguardante il secondo tipo di sorveglianza della determinazione della posizione mediante LALS: la determinazione ricorrente e periodica della posizione mediante la rete («PERIOD»).

Il *capoverso 1* prevede che il fornitore del servizio di telefonia mobile effettui una determinazione periodica e ricorrente della posizione utilizzando un'apposita funzione della rete (LALS). Vanno determinate le posizioni di tutti i dispositivi mobili associati all'identificativo sorvegliato (target ID; cfr. il commento all'art. 56*a* cpv. 1).

Secondo il *capoverso 2,* le prescrizioni tecniche di esecuzione sono emanate dal DFGP nella OE-SCPT e nell'allegato 1 di quest'ultima. Il DFGP può ad esempio prevedere che la posizione vada determinata a intervalli di tempo fissi predeterminati. Poiché finora non sono ancora state fatte esperienze pratiche con questa nuova determinazione periodica e ricorrente della posizione, in particolare per quanto riguarda le

risorse o il tempo necessario per ogni singola determinazione, non è ancora possibile stabilire prescrizioni concrete in merito a parametri tecnici come frequenza, periodicità e intervallo minimo tra due determinazioni successive della posizione. A seconda dell'implementazione tecnica, la determinazione della posizione può richiedere un certo tempo. Una volta determinate, il fornitore di telefonia mobile deve tuttavia trasmettere immediatamente e senza indugio le posizioni dei dispositivi.

Secondo il *capoverso 3 lettera d,* se non è stato possibile determinare la posizione, ne va comunicato il motivo (codice d'errore). Vista l'esecuzione automatizzata di questo tipo di sorveglianza, non è possibile, stando all'attuale stato delle conoscenze, uno scenario alternativo come nel caso dell'articolo 56*a*.

Art. 60 Tipo di sorveglianza HD_28_NA: sorveglianza retroattiva dei metadati per i servizi di accesso alla rete

A seguito delle numerose modifiche, l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Il contenuto delle *lettere a-c* e *j* (prima i) è invariato. La lettera c subisce una leggera modifica redazionale nella versione tedesca.

Alla *lettera d* è cancellata l'espressione «settori d'indirizzo» in quanto in questo caso si tratta dell'indirizzo IP effettivamente assegnato al target in quel preciso momento. Sono ora aggiunte le indicazioni nel caso di un accesso non 3GPP poiché è possibile accedere alla rete di telefonia mobile anche senza passare da un'antenna di telefonia mobile (accesso 3GPP), ad esempio mediate il WLAN di casa o un WLAN pubblico. Se non è coinvolta nessuna antenna di telefonia mobile, si omettono anche i relativi dati di localizzazione (lett. g) in quanto è possibile determinare la localizzazione dell'accesso mediante questo indirizzo IP sorgente e il numero di porta.

Alle *lettere e* ed *f* è stralciata la condizione «se disponibile» in quanto si tratta di parametri obbligatori. Inoltre alle *lettere e* e *g* l'espressione «telefonia mobile» è sostituita con «servizi di telefonia mobile».

Alle *lettere e, g* e *h* sono inseriti i nuovi identificativi del sistema 5G (PEI, SUPI, GPSI; cfr. i commenti all'art. 35 cpv. 1 lett. d n. 2 «GPSI» e n. 10 «SUPI» nonché all'art. 36 cpv. 1 lett. b n. 4 «PEI»).

Secondo la *lettera g* vanno ora trasmesse anche le marche temporali, eventualmente disponibili nei sistemi di telefonia mobile di quarta (EPS) e quinta generazione (5GS), associate alle indicazioni relative alla localizzazione. I singoli dati di localizzazione non sono più descritti in modo dettagliato in questa lettera poiché sono diventati troppo complessi per essere inseriti in una disposizione di un atto normativo. Si rimanda invece alle prescrizioni applicabili del DFGP riportate nell'allegato 1 della OE-SCPT.

La *lettera h* precisa che la disposizione vale soltanto per gli accessi alla rete mediante WLAN pubblici gestiti professionalmente. In base alle esperienze pratiche, viene ora introdotta la possibilità di indicare, al posto di un identificativo univoco, un'altra designazione idonea come il nome dell'hotspot. È sufficiente una definizione abbastanza precisa dell'accesso WLAN, ciò significa che la designazione trasmessa deve designare in modo sufficientemente preciso l'accesso WLAN nel luogo in questione (cfr. il commento all'art. 48 cpv. 2 lett. a).

La *lettera i* riprende e riunisce in un'unica lettera il disciplinamento riguardante le informazioni relative alla localizzazione provenienti dalla navigazione marittima e aerea, che nel diritto vigente sono previste alla fine delle lettere g e h.

La *lettera j* corrisponde alla vigente lettera i.

Art. 61, frase introduttiva e lett. b, d, g, g^{bis}, i e j

Nelle *lettere b* e *d* sono aggiunti i nuovi identificativi del sistema 5G (PEI, SUPI, GPSI; cfr. i commenti all'art. 35 cpv. 1 lett. d n. 2 «GPSI» e n. 10 «SUPI» nonché all'art. 36 cpv. 1 lett. b n. 4 «PEI»).

Alla *lettera g* i singoli dati di localizzazione non sono più descritti in modo dettagliato poiché sono diventati troppo complessi per essere inseriti in una disposizione di un atto normativo. Si rimanda invece alle prescrizioni applicabili del DFGP riportate nell'allegato 1 della OE-SCPT.

La *lettera g^{bis}* riprende, analogamente all'articolo 60 lettera i, il disciplinamento riguardante le informazioni relative alla localizzazione provenienti dalla navigazione marittima e aerea, che si trova alla fine della frase introduttiva della vigente lettera g.

Materialmente la *lettera i* resta invariata; al *numero 4* si rimanda alle prescrizioni applicabili del DFGP riportate all'allegato 1 della OE-SCPT.

Secondo la *lettera j* adesso vanno trasmesse anche le indicazioni sulla rete immediatamente adiacente lungo il percorso di comunicazione ossia quella da cui provengono le indicazioni («da») e quella a cui sono dirette («a»), sempreché queste siano coinvolte nella comunicazione o nel tentativo di comunicazione. In tal modo, in caso di numero di telefono sconosciuto o falsificato («spoofing»), le autorità di perseguimento penale hanno la possibilità di tracciare la comunicazione o i tentativi di comunicazione (cfr. anche il commento e l'esempio all'art. 48*c*). Ciò può essere utile, nel caso ad esempio di una minaccia anonima dinamitarda, per potere tracciare la comunicazione e quindi risalire alla provenienza della comunicazione o del tentativo di comunicazione. I metadati storici delle connessioni e dei tentativi di connessione, conservati per gli scopi della sorveglianza retroattiva, contengono gli elementi d'indirizzo dei partecipanti alla comunicazione (chi con chi). Tuttavia, se il numero di provenienza è falsificato o sconosciuto, le autorità legittimate hanno bisogno di altre indicazioni per rintracciare o tracciare la chiamata o la comunicazione.

Per ottenere indicazioni affidabili e dal momento che il fornitore può controllare solamente le proprie interfacce di rete, quest'ultimo deve conservare solamente le indicazioni sulle reti «da» e «a» immediatamente adiacenti alla sua, sempreché queste fossero coinvolte nella comunicazione o nel tentativo di comunicazione oggetto della domanda. La durata di conservazione dei metadati è di sei mesi (art. 26 cpv. 5 LSCPT) e concerne solo i fornitori con obblighi di sorveglianza.

In particolare il fornitore non è tenuto a conservare indicazioni su eventuali altre reti a monte o a valle di una connessione. Su richiesta vanno tuttavia trasmessi altri metadati di cui dispone (art. 26 cpv. 6, art. 27 cpv. 2, art. 28 cpv. 2 e art. 29 cpv. 2 LSCPT). Tali indicazioni supplementari non rientrano nel presente tipo di sorveglianza standardizzato e possono essere richieste come sorveglianza particolare ai sensi dell'articolo 25 OSCPT.

Fornire indicazioni sulle reti immediatamente adiacenti è tuttavia difficile per la sorveglianza in tempo reale e non è compatibile con gli standard di ETSI e 3GPP. Pertanto si rinuncia a una disposizione analoga all'articolo 56 capoverso 2 lettera e.

Art. 62 Tipo di sorveglianza HD_30_EMAIL: sorveglianza retroattiva dei metadati per i servizi di posta elettronica

A seguito delle numerose modifiche, l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Alla *lettera a* sono stati aggiunti all'indirizzo IP i numeri di porta per permettere l'identificazione del server e del client in caso di network address translation (NAT).

Soltanto le POC con obblighi integrali di sorveglianza devono conservare i metadati di servizi di posta elettronica (cronologia), ossia i FST con obblighi integrali e i FSCD con obblighi di sorveglianza supplementari (art. 52). Tutte le altre POC forniscono soltanto i dati a loro disposizione.

Art. 63 Tipo di sorveglianza HD_31_PAGING: determinazione della localizzazione al momento dell'ultima attività

A seguito delle numerose modifiche, l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Il capoverso 1 precisa che non si tratta dell'ultima attività rilevata bensì dell'ultima attività rilevabile. Se occorre, la POC deve dunque rilevare la localizzazione dell'ultima attività. Inoltre, l'intera frase è al plurale poiché va rilevata la localizzazione dell'ultima attività di ciascun dispositivo associato al target ID (e quindi non solo di uno; cfr il commento all'art. 56*a* cpv. 1).

Il capoverso 2 disciplina in dettaglio, secondo una nuova struttura, le indicazioni da trasmettere cui non se ne aggiungono di nuove rispetto alla versione vigente; ad eccezione dei nuovi parametri equivalenti del sistema 5G le cui designazioni sono cambiate (p. es. GPSI per MSISDN, SUPI per IMSI, PEI per IMEI). Inoltre alla *lettera h* si rimanda alle prescrizioni applicabili del DFGP, ossia all'allegato 1 della OE-SCPT.

Art. 64 cpv. 2

Nel *capoverso 2* si usa l'espressione generale «identificativi della cella o della zona» (cfr. il commento all'art. 48 cpv. 2 lett. a), invece di elencare a titolo esemplificativo i singoli identificativi. Si precisa inoltre che la disposizione interessa soltanto gli accessi WLAN pubblici gestiti professionalmente. Inoltre «punto di accesso WLAN» è sostituito dal termine più generale «accesso WLAN» (cfr. il commento alla sostituzione di espressioni, cpv. 1). Invece dell'identificativo dell'accesso WLAN può essere fornita anche un'altra designazione idonea (p. es. nome dell'hotspot; cfr. il commento all'art. 48 cpv. 2 lett. a).

Art. 65 cpv. 2, frase introduttiva, e 3

La frase introduttiva del *capoverso 2* subisce una modifica redazionale.

Nel *capoverso 3* il termine più generale «accesso WLAN» sostituisce «punto di accesso WLAN» (cfr. il commento alla sostituzione di espressioni, cpv. 1). È inoltre

usata l'espressione generale «identificativi della cella o della zona» (cfr. il commento all'art. 48 cpv. 2 lett. a), invece di elencare a titolo esemplificativo i singoli identificativi. Invece dell'identificativo dell'accesso WLAN può essere fornita anche un'altra designazione idonea (p. es. nome dell'hotspot; cfr. il commento all'art. 48 cpv. 2 lett. a).

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

A seguito delle numerose modifiche, l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. La disposizione ha una nuova impostazione. Sono stati inoltre aggiunti due nuovi tipi di sorveglianza in tempo reale per la ricerca d'emergenza. Gli altri tipi di ricerca d'emergenza restano invariati.

Si devono tenere presenti i commenti alle modifiche di cui all'articolo 50 capoverso 6, relative ai servizi di telefonia mobile con carte SIM supplementari (p. es. multidevice o multiSIM per dispositivi supplementari quali smartphone, tablet, smartwatch).

La *lettera a* definisce, come finora, la ricerca d'emergenza del tipo «paging» che corrisponde al tipo di sorveglianza HD_31_PAGING (cfr. il commento all'art. 63). Ora si precisa che le POC devono determinare anche la localizzazione al momento dell'ultima attività di tutti i dispositivi mobili, associati al target ID, della persona dispersa o di terzi. Questa precisazione riguarda soprattutto gli abbonamenti di telefonia mobile con carte SIM supplementari (cosiddette offerte multidevice o multiSIM, cfr. il commento all'art 56*a* cpv. 1). Questo tipo di ricerca d'emergenza, utilizzato da parecchi anni, corrisponde alla localizzazione dei dispositivi mobili sulla base delle celle radio. La POC fornisce l'ultima localizzazione disponibile di ciascun dispositivo mobile a prescindere dalla tecnologia e dal tipo di accesso alla rete utilizzati.

Il tipo EP_56_POS_ONCE di cui alla *lettera b* è nuovo. Si tratta della determinazione unica e immediata mediante la rete della posizione di tutti i dispositivi mobili, associati al target ID, della persona dispersa o di terzi nell'ambito di una ricerca d'emergenza. Sotto il profilo tecnico questo tipo corrisponde al nuovo tipo di sorveglianza RT_54_POS_ONCE (cfr. anche il commento all'art. 56*a*).

Anche il tipo EP_57_POS_PERIOD di cui alla *lettera c* è nuovo. Si tratta della determinazione ricorrente e periodica mediante la rete della posizione di tutti i dispositivi mobili, associati al target ID, della persona dispersa o di terzi nell'ambito di una ricerca d'emergenza. Sotto il profilo tecnico questo tipo corrisponde al nuovo tipo di sorveglianza RT_55_POS_PERIOD (cfr. anche il commento all'art. 56*b*).

Rispetto alla determinazione della localizzazione di cui alla lettera a, la determinazione della posizione di cui alle lettere b e c è molto più precisa e viene effettuata da funzioni specifiche della rete che richiedono un onore tecnico maggiore. Le nuove funzioni di determinazione della posizione permettono di ottenere dati più precisi sulla posizione del telefono cellulare della persona cercata. Dati di localizzazione imprecisi ritardano il salvataggio della persona dispersa e comportano il massiccio impiego di personale e materiale (p. es. auto della polizia, elicotteri), il che implica a sua volta maggiori spese. Una localizzazione più precisa della persona cercata permette di eseguire le operazioni di salvataggio in modo più mirato e di salvare vite umane.

La *lettera d* corrisponde alla vigente lettera b e disciplina la sorveglianza in tempo reale di contenuti e metadati nell'ambito di una ricerca d'emergenza. L'autorità che dispone la sorveglianza trasmette al Servizio SCPT un ordine per ciascuna POC e per ciascun numero principale sorvegliato e il Servizio SCPT inoltra l'incarico di ricerca d'emergenza alle POC corrispondenti. Ogni POC incaricata implementa il tipo di sorveglianza che fa al caso secondo gli articoli 55 e 57, in modo tale da coprire tutti i servizi da essa forniti delle categorie TEL e NA per i numeri secondari associati al numero principale ricercato. Questo abbinamento tiene conto dell'urgenza di una ricerca d'emergenza tesa a trovare il più rapidamente possibile persone la cui vita e integrità fisica sono in pericolo. Assegnare singoli mandati per ogni servizio di telefonia o multimedia (TEL) e per ogni servizio di accesso alla rete (NA) sorvegliato, come avviene normalmente per le sorveglianze, richiederebbe troppo tempo per le ricerche d'emergenza. Anche in questo caso vanno sorvegliati eventuali numeri secondari associati al numero principale sorvegliato (p. es. abbonamenti con SIM supplementari, cosiddette offerte multidevice o multiSIM). Un esempio: la POC riceve un mandato per la ricerca d'emergenza del tipo EP_36_RT_CC_IRI (lett. d) per il MSISDN x. Supponiamo che l'utente con il MSISDN x abbia presso la POC un abbonamento mobile con accesso alla telefonia e a Internet comprendente una SIM supplementare con il MSISDN y per l'accesso a Internet. In questo caso la POC effettua una sorveglianza in tempo reale dei contenuti e dei metadati per i servizi di telefonia e multimedia (art. 57) per il MSISDN x e due sorveglianze in tempo reale dei contenuti e dei metadati per i servizi di accesso alla rete (art. 55), una per il MSISDN x e l'altra per il MSISDN y. Anche nel caso di una ricerca d'emergenza, le sorveglianze in tempo reale restano attive fintanto che il Servizio SCPT non impartisce alla POC l'ordine di revoca.

La *lettera e* corrisponde alla vigente lettera c e definisce la sorveglianza in tempo reale senza dati sul contenuto, ossia solo dei metadati nell'ambito di una ricerca d'emergenza. Il procedimento corrisponde a quello descritto alla lettera d con la differenza che questo tipo di sorveglianza si fonda sui tipi di sorveglianza di cui agli articoli 54 e 56.

La *lettera f* disciplina la ricerca d'emergenza retroattiva, ad esempio nel caso in cui il dispositivo non sia più acceso o non abbia alcuna copertura di rete e quindi non sono disponibili dati aggiornati. Il procedimento corrisponde a quello descritto alla lettera d con la differenza che si tratta di sorveglianze retroattive e che ogni POC incaricata implementa il tipo di sorveglianza che fa al caso secondo gli articoli 60 e 61 di modo che siano coperti tutti i servizi da essa forniti per il numero sorvegliato e per quelli a esso associati (cfr. il commento all'art. 50 cpv. 6). Valgono le solite regole per le sorveglianze retroattive (nessun ordine di revoca della sorveglianza, inizio e fine secondo l'art. 4*a*). L'indennità per le POC dipende dal numero di ricerche d'emergenza disposte dalle autorità per POC e per numero sorvegliato e non dal numero di sorveglianze effettivamente svolte.

In varie disposizioni sono ora aggiunti i nuovi identificativi del sistema 5G (GPSI, SUPI, PEI; il commento all'art. 35 cpv. 1 lett. d n. 2 «GPSI» e n. 10 «SUPI» nonché art. 36 cpv. 1 lett. b n. 4 «PEI»).

Art. 68 Ricerca di condannati

A seguito delle numerose modifiche, l'articolo è stato interamente rivisto per migliorarne la leggibilità e la comprensibilità. Le *lettere a–c* prevedono tre nuovi tipi di sorveglianza per la ricerca di condannati.

La *lettera a* introduce il cosiddetto «paging» nell'ambito di una ricerca di condannati, ossia la determinazione della localizzazione dell'ultima attività secondo l'articolo 63 (cfr. il relativo commento).

La *lettera b* introduce il LALS una tantum nell'ambito di una ricerca di condannati, ossia la determinazione unica e immediata della posizione mediante la rete secondo l'articolo 56*a* (cfr. il relativo commento).

La *lettera c* introduce il LALS ricorrente e periodico nell'ambito di una ricerca di condannati, ossia la determinazione ricorrente e periodica della posizione mediante la rete secondo l'articolo 56*b* (cfr. il relativo commento).

Le altre lettere restano invariate e sono semplicemente spostate più sotto (la *lett. a* diventa la *lett. d*, la *lett. b* diventa la *lett. e*, ecc.).

Il *capoverso 2* precisa che l'inizio e la fine di una sorveglianza retroattiva di cui al capoverso 1 lettera f sono retti dalle disposizioni dell'articolo 4*a* (cfr. il relativo commento).

Art. 74b Disposizione transitoria della modifica del 15 novembre 2023

Per garantire un'introduzione impeccabile dei nuovi tipi di informazione e sorveglianza presso i FST e il Servizio SCPT, è opportuno prevedere disposizioni transitorie dettagliate per le singole modifiche. Entro i termini menzionati i FST e il Servizio SCPT devono effettuare gli adeguamenti tecnici e i relativi test affinché i nuovi tipi di informazione e sorveglianza possano essere svolti in modo standardizzato il più presto possibile o al più tardi entro i termini previsti. Per i FSCD non vanno previsti termini transitori poiché i nuovi tipi di informazione e sorveglianza valgono esclusivamente per i FST. I FSCD ne sono esplicitamente esentati (cfr. il commento agli art. 18 cpv. 4 e 50 cpv. 1).

Il *capoverso 1* prevede per tutti i FST un periodo transitorio di 24 mesi dall'entrata in vigore della presente revisione per i nuovi tipi di informazioni di cui agli articoli 48*a* (IR_51_ASSOC_PERM: informazioni su identificativi attribuiti a lungo termine) e 48*c* (IR_53_TEL_ADJ_NET: determinazione delle reti adiacenti di servizi di telefonia e multimedia). Va ricordato che i FST con obblighi di sorveglianza ridotti (art. 51) non sono tenuti a conservare i corrispondenti metadati di cui all'articolo 48*c*; quindi forniscono le informazioni di cui all'articolo 48*c* sulla base delle informazioni di cui dispongono. Se forniscono informazioni al di fuori del sistema di trattamento, non devono adeguare i loro sistemi.

Il *capoverso 2* non prevede alcun termine transitorio espresso in mesi ma fa dipendere il termine per la disponibilità a fornire informazioni dall'effettivo utilizzo commerciale della nuova funzione della tecnologia 5G che nasconde l'identificativo permanente dell'utente sull'interfaccia radio dell'accesso alla rete mobile (il cosiddetto accesso 3GPP). La disposizione interessa quei fornitori di servizi di telefonia mobile che

gestiscono una rete 5G. Dall'attivazione del primo accesso commerciale alla rete mobile che nasconde gli identificativi permanenti sull'interfaccia radio, possibilità offerta dalla futura tecnologia 5G autonoma (la cosiddetta 5G *standalone*), detti fornitori dovranno essere in grado di attuare il nuovo tipo di informazione di cui all'articolo 48*b* (IR_52_ASSOC_TEMP: informazioni immediate su identificativi attribuiti per breve tempo). In altre parole, dovranno fornire le informazioni di cui all'articolo 48*b* in forma automatizzata solamente dal momento in cui la nuova funzione della tecnologia 5G è effettivamente utilizzata. Il presente capoverso riguarda esclusivamente i FST con obblighi integrali, quelli con obblighi di sorveglianza ridotti (art. 51) sono esentati dal fornire questo tipo di informazione (cfr. art. 18 cpv. 4).

Per l'attuazione dei due nuovi tipi relativi alla determinazione unica e immediata della posizione secondo gli articoli 56*a* (RT_56_POS_IMMED) e 67 lettera b (EP_58_POS_IMMED), il *capoverso 3* prevede, come al capoverso 1, un periodo transitorio di 24 mesi dall'entrata in vigore della presente modifica. In considerazione del valore aggiunto che ci si aspetta da questi due nuovi tipi di sorveglianza, queste sorveglianze devono essere a disposizione delle autorità di perseguimento penale il più presto possibile. Il capoverso riguarda esclusivamente i FST con obblighi integrali, quelli con obblighi ridotti (art. 51) non devono attuare alcun tipo di sorveglianza (cfr. art. 50 cpv. 1).

Il *capoverso 4* prevede due termini per la modifica del tipo di informazione HD_29_TEL concernente la designazione della rete immediatamente adiacente della comunicazione o del tentativo di comunicazione (art. 61 lett. j): anzitutto i FST con obblighi integrali devono garantire la memorizzazione dei dati necessari a tal fine entro 18 mesi dall'entrata in vigore della presente modifica e in secondo luogo devono essere in grado di fornire i nuovi dati retroattivi entro 24 mesi dall'entrata in vigore della presente revisione. L'obbligo di memorizzare inizia dunque sei mesi prima dell'obbligo di consegna questo per garantire che, dall'inizio dell'obbligo di consegna, il fornitore disponga già dei pertinenti dati storici degli ultimi sei mesi. Il capoverso riguarda esclusivamente i FST con obblighi integrali, quelli con obblighi di sorveglianza ridotti (art. 51) non devono attuare alcun tipo di sorveglianza (cfr. art. 50 cpv. 1).

Il *capoverso 5* definisce il termine transitorio per i FST con obblighi integrali per quanto riguarda i due nuovi tipi relativi alla determinazione periodica della posizione di cui agli articoli 56*b* (RT_55_POS_PERIOD) e 67 lettera c (EP_57_POS_PERIOD). Implementare questi due nuovi tipi di sorveglianza nell'attuale componente del sistema di trattamento del Servizio SCPT relativa alla sorveglianza in tempo reale (ISS) non è opportuno né sul piano economico né sotto il profilo della tempistica, poiché la componente è ormai arrivata alla fine del suo ciclo di vita e sarà presto sostituita. Si rinuncia pertanto all'implementazione nell'attuale componente (ISS). Inoltre non è sicuro che l'implementazione sia fattibile poiché il produttore non sviluppa più questa versione della componente. Per questo motivo questi tipi di sorveglianza saranno attuabili in forma standardizzata soltanto dopo l'introduzione e l'adeguamento della nuova componente per la sorveglianza in tempo reale. Una volta che la nuova componente sarà operativa («FLICC[32] 2.0»), i FST con obblighi

[32] Federal Lawful Interception Core Component (FLICC)

integrali avranno ancora 24 mesi di tempo per adattare i loro sistemi e procedere ai test necessari con il Servizio SCPT. Il capoverso riguarda esclusivamente i FST con obblighi integrali, quelli con obblighi ridotti (art. 51) non devono attuare alcun tipo di sorveglianza (cfr. art. 50 cpv. 1).

Il *capoverso 6* è la controparte dei capoversi 1, 3 e 4 e fissa, per il Servizio SCPT, lo stesso termine transitorio di 24 mesi dall'entrata in vigore della presente revisione per quanto riguarda i tipi di informazione e sorveglianza corrispondenti (cfr. cpv. 1, 3 e 4). La *lettera a* riguarda l'implementazione nella IRC dei nuovi tipi di informazione di cui agli articoli 48*a* e 48*c* e l'implementazione, nella nuova componente del sistema di trattamento del Servizio SCPT relativa alla sorveglianza in tempo reale, dei nuovi tipi di sorveglianza relativi alla determinazione unica e immediata della posizione di cui agli articoli 56*a* (RT_54_POS_ONCE) e 67 lettera b (EP_56_POS_ONCE), affinché i mandati possano essere trasmessi e i dati possano essere ricevuti e messi a disposizione degli utenti. Inoltre le informazioni e le sorveglianze devono poter essere rilevate nelle statistiche del Servizio SCPT. Analogamente al capoverso 4, la *lettera b* fissa un termine transitorio di 24 masi per il Servizio SCPT, affinché quest'ultimo possa ricevere i dati storici corrispondenti.

Analogamente al capoverso 2 (art. 48*b*), il *capoverso 7* prevede per il Servizio SCPT lo stesso termine per adattare il sistema di trattamento, affinché i nuovi dati possano essere ricevuti praticamente in tempo reale e le informazioni possano essere rilevate nelle statistiche.

Il *capoverso 8* è la controparte del capoverso 5 (art. 56*b* e 67 lett. c) e fissa lo stesso termine transitorio per il Servizio SCPT.

Allegato

Nell'allegato OSCPT sono state aggiunte alcune nozioni e abbreviazioni utilizzate nell'ordinanza, quelle obsolete sono state cancellate e alcune sono state opportunamente modificate. L'ordine delle nozioni e delle abbreviazioni viene modificato in quanto ora si basa sulla loro prima occorrenza nell'ordinanza.

4.2 Ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT)

Sostituzione di espressioni

Le abbreviazioni FST e FSCD sono utilizzate anche nella OE-SCPT, pertanto le relative disposizioni sono adeguate.

Art. 1 Campo d'applicazione

Poiché la comunicazione sicura è ora disciplinata anche per le autorità a livello di ordinanza dipartimentale (cfr. art. 3), il campo di applicazione va esteso in tal senso. Ciò significa che la OE-SCPT con gli allegati si applica non solo al Servizio SCPT e

alle persone obbligate a collaborare, ma anche alle autorità di cui all'articolo 1 capoverso 2 lettere a-f OSCPT.

Art. 3 Sicurezza della comunicazione

Nella versione vigente questa disposizione disciplina esclusivamente la comunicazione tra le POC e il Servizio SCPT. La modifica dell'articolo 3 OSCPT, secondo cui i mezzi di trasmissione sicuri devono essere approvati dal DFGP, implica che l'articolo 3 OE-SCPT vada esteso anche alla comunicazione tra il Servizio SCPT e le autorità.

Adesso il *capoverso 1* disciplina anche la comunicazione sicura tra il Servizio SCPT e le autorità di cui all'articolo 1 capoverso 2 lettere a-f OSCPT. La disposizione vale anche per la comunicazione sicura tra il Servizio SCPT e le POC (secondo l'art. 2 LSCPT) come anche tra queste ultime e le autorità. Sono considerati mezzi di trasmissione sicuri il sistema di trattamento del Servizio SCPT (*lett. a*), le soluzioni di criptaggio per messaggi di posta elettronica (*lett. b*), definite più in dettaglio nell'allegato 1 della OE-SCPT, e, d'intesa con il Servizio SCPT, anche un altro mezzo equivalente (*lett. c*).

La vigente lettera a, riguardante le comunicazioni confidenziali tra le POC e il Servizio SCPT, è spostata al nuovo *capoverso 2* senza subire alcuna modifica materiale.

Art. 10 cpv. 2bis

Il nuovo capoverso applica ai mandati di sorveglianza della corrispondenza postale lo stesso termine di inoltro previsto per le domande di informazioni (art. 14 cpv. 1) e i mandati di sorveglianza del traffico delle comunicazioni (art. 16 cpv. 1, 17 cpv. 1 e 18 cpv. 1) destinati alle POC. Il che significa che il Servizio SCPT deve trasmettere al fornitore di servizi postali il mandato di esecuzione di una sorveglianza in tempo reale della corrispondenza postale entro un'ora dalla ricezione dell'ordine. Le sorveglianze della corrispondenza postale sono ordinante ed eseguite esclusivamente durante gli orari d'ufficio ordinari.

Art. 11 Sorveglianza retroattiva

Il nuovo *capoverso 1* disciplina il termine per la trasmissione del mandato di esecuzione di una sorveglianza retroattiva della corrispondenza postale (cfr. il commento all'art. 10 cpv. 2bis) analogamente agli articoli 10 capoverso 2bis, 14 capoverso 1, 16 capoverso 1, 17 capoverso 1 e 18 capoverso 1.

Il *capoverso 2* corrisponde al vigente articolo 11.

Art. 14 cpv. 2, 3 e 4

Il *capoverso 2* disciplina i termini di trattamento per i FST, eccetto quelli con obblighi di sorveglianza ridotti (art. 51 OSCPT), e i FSCD con obblighi supplementari (art. 22 o 52 OSCPT). Il capoverso prevede ora che le norme indicate valgano solamente nella misura in cui le POC siano tenute a fornire le informazioni secondo l'articolo 18 OSCPT. I FSCD con obblighi supplementari secondo l'articolo 22 o 52 OSCPT sono

esentati ai sensi dell'articolo 18 capoverso 4 OSCPT dal fornire i tre nuovi tipi di informazioni di cui agli articoli 48*a*-48*c* OSCPT.

La *lettera a* precisa che il tipo di informazione di cui all'articolo 48*b* OSCPT va trattato immediatamente. Il tempo di risposta per questo nuovo tipo di informazione deve essere molto breve (frazioni di secondo) poiché gli identificativi temporanei cambiano frequentemente. L'informazione deve pertanto essere consultata e fornita in forma automatizzata tramite una nuova interfaccia di consultazione. Trattandosi di una consultazione in tempo reale, non è possibile indicare un momento determinante: vale il momento della consultazione. Consultazioni nel passato non sono possibili. Va osservato che i FST con obblighi di sorveglianza ridotti, come anche indicato nella frase introduttiva, e i FSCD con obblighi supplementari secondo l'articolo 22 o 52 OSCPT sono esentati dal fornire le informazioni di cui all'articolo 48*b* OSCPT (cfr. art. 18 cpv. 3 e 4 OSCPT) per ragioni di proporzionalità; a queste categorie di POC non si applica la lettera a.

Nella *lettera b* il termine di un'ora per il trattamento delle informazioni menzionate da parte del fornitore resta invariato. Poiché i tipi di informazioni elencati sono forniti in forma automatizzata (cfr. art. 18 cpv. 2 OSCPT), i tempi di reazione per le risposte sono di conseguenza brevi. Si tratta dei seguenti tipi di informazione disciplinati nella OSCPT: IR_4_NA (art. 35), IR_5_NA_FLEX (art. 27 in combinato disposto con l'art. 35), IR_6_NA (art. 36), IR_7_IP (art. 37), IR_10_TEL (art. 40), IR_11_TEL_FLEX (art. 27 in combinato disposto con l'art. 40), IR_12_TEL (art. 41). Il termine di un'ora vale anche per il nuovo tipo di informazione di cui all'articolo 48*a* (IR_51_ASSOC_PERM: informazioni su identificativi attribuiti a lungo termine). Va osservato che in caso di domande di informazioni trasmesse in forma automatizzata, il Servizio SCPT non procede a notificarle durante il servizio di picchetto.

Alla *lettera c numero 1* il termine di un giorno lavorativo per rispondere alle domande di informazioni ricevute dal fornitore negli orari d'ufficio ordinari non cambia. Il termine riguarda, come nel testo vigente, i seguenti tipi di informazione disciplinati nella OSCPT e trasmessi manualmente: IR_8_IP (NAT) (art. 38), IR_9_NAT (art. 39), IR_15_COM (art. 43), IR_16_COM_FLEX (art. 27 in combinato disposto con l'art. 43). Adesso il termine di trattamento per i tipi di informazione IR_13_EMAIL (art. 42) e IR_14_EMAIL_FLEX (art. 27 in combinato disposto con l'art. 42) è rispettivamente di un giorno lavorativo e di sei ore anziché di un'ora (cfr. il vigente cpv. 2 lett. a), poiché queste informazioni adesso possono essere fornite anche manualmente (cfr. commento all'art. 18 cpv. 2 OSCPT). Inoltre è stato aggiunto il nuovo tipo di informazione IR_53_TEL_ADJ_NET (determinazione delle reti adiacenti di servizi di telefonia e multimedia; art. 48*c* OSCPT). «Entro un giorno lavorativo» significa che la risposta deve arrivare al Servizio SCPT e all'autorità richiedente entro le 17.00 del giorno successivo (cfr. es. 1 qui appresso).

Le autorità legittimate che trasmettono una domanda urgente durante il fine settimana o in un giorno festivo ritengono il termine di un giorno lavorativo troppo lungo. Per questa ragione, il *numero 2* riduce il termine di risposta a sei ore per domande di informazioni al di fuori degli orari d'ufficio ordinari o nei giorni festivi. Questo termine corrisponde a quello per le sorveglianze retroattive urgenti. L'esperienza insegna che

le domande di informazioni e gli ordini di sorveglianza che giungono durante il servizio di picchetto sono pochi, ma per lo più urgenti e non possono aspettare il giorno lavorativo successivo; la presente disposizione non comporterà dunque un sovraccarico per le POC. D'altra parte, affinché le indagini di polizia e quindi il perseguimento penale non siano ostacolati, le autorità di perseguimento penale devono poter ricevere le informazioni urgentemente necessarie anche durante il fine settimana e nei giorni festivi. Va osservato che il numero 2 si applica solamente alle POC tenute ai sensi dell'articolo 11 capoverso 1 OSCPT a fornire un servizio di picchetto, il che non è il caso dei FST con obblighi di sorveglianza ridotti (art. 51 OSCPT) e dei FSCD con obblighi di informazione supplementari (art. 22 OSCPT); a queste categorie di POC non si applica la lettera c numero 2.

Se una domanda di informazioni trasmessa in forma non automatizzata deve essere inoltrata alla POC interessata durante il servizio di picchetto, l'autorità legittimata (cfr. art. 15 LSCPT) avverte previamente il Servizio SCPT (cfr. art. 11 cpv. 2 OSCPT) affinché quest'ultimo possa a sua volta informare la POC interessata in merito al mandato in oggetto.

Il termine di trattamento pari a sei ore comporta che la POC ha sei ore di tempo, dalla ricezione della domanda, per immettere la risposta nella componente IRC (cfr. il commento all'art. 18 OSCPT) o, in caso di un guasto della IRC, per trasmetterla in modo sicuro (cfr. art. 3) al Servizio SCPT. Seguono alcuni esempi concernenti le domande di informazioni secondo la lettera c.

Esempio 1: una domanda di informazioni è caricata nella IRC lunedì alle 16.10 e la POC la riceve qualche secondo dopo. In questo caso, il termine di trattamento corrisponde a un giorno lavorativo. Il fornitore ha tempo fino alla fine del giorno lavorativo successivo, ossia fino a martedì alle 16.59, per fornire le informazioni richieste.

Esempio 2: una domanda di informazioni è caricata nella IRC lunedì alle 17.05 e la POC la riceve qualche secondo dopo. Poiché la domanda è stata carica al di fuori degli orari d'ufficio ordinari, l'autorità legittimata deve previamente avvisare il Servizio SCPT se desidera che la domanda sia trattata durante il picchetto. Il Servizio SCPT informa senza indugio la POC. Il termine di trattamento concesso alla POC è di sei ore dalla ricezione dell'ordine. Il fornitore ha quindi tempo fino alle 23.05 dello stesso giorno per fornire le informazioni richieste.

Esempio 3: se la domanda di informazioni è trasmessa sabato alle 18.50 (nel fine settimana), il fornitore ha tempo fino alle 00.50 di domenica per trattarla. La procedura è la stessa descritta nell'esempio 2.

Anche il termine di trattamento per le informazioni in forma manuale (*lett. d)* è di un giorno lavorativo. Poiché le informazioni secondo gli articoli 44-48 OSCPT non vanno necessariamente trasmesse durante il servizio di picchetto, non sono disciplinate nella precedente lettera c, ma separatamente. Rispetto al vigente articolo 14 capoverso 2 lettera b, il termine per fornire le informazioni IR_17_PAY (art. 44), IR_18_ID (art. 45), IR_19_BILL (art. 46), IR_20_CONTRACT (art. 47) e IR_21_TECH (art. 48) resta invariato.

Il *capoverso 3* disciplina i termini di trattamento per le POC «piccole», ossia i FST con obblighi di sorveglianza ridotti (art. 51 OSCPT).

Analogamente al capoverso 2 lettere a e b, i termini di trattamento sono differenti in funzione della complessità delle informazioni da fornire. Per le informazioni di cui alla *lettera a*, il termine di due giorni lavorativi previsto dalla disposizione vigente viene ridotto a uno, mentre per le informazioni di cui alla lettera b il termine resta invariato (due giorni lavorativi).

Il *capoverso 4* disciplina i termini di trattamento per i FSCD senza obblighi supplementari secondo l'articolo 22 o 52 OSCPT e per i gestori di reti di telecomunicazione interne; queste due categorie di POC devono fornire solamente le indicazioni di cui dispongono (cfr. art. 22 cpv. 3 LSCPT) e, nel farlo, non sono tenute a rispettare i tipi standardizzati previsti dalla OSCPT (art. 18*a* OSCPT).

Per i termini di trattamento si veda anche la tabella dell'allegato «Panoramica termini di trattamento».

Art. 18 cpv. 2 e 3

In seguito all'introduzione delle nuove lettere agli articoli 67 e 68 capoverso 1 OSCPT vanno anche adeguati i rimandi nei *capoversi 2* e *3*.

Allegato 1

Nel quadro della revisione parziale della OSCPT, sono istituiti tre nuovi tipi di informazione e quattro nuovi tipi di sorveglianza:

1) il tipo di informazione IR_51_ASSOC_PERM, informazioni su identificativi attribuiti a lungo termine (art. 48*a* OSCPT);
2) il tipo di informazione IR_52_ASSOC_TEMP, informazioni immediate su identificativi attribuiti per breve tempo (art. 48*b* OSCPT);
3) il tipo di informazione IR_53_TEL_ADJ_NET, determinazione delle reti adiacenti di servizi di telefonia e multimedia (art. 48*c* OSCPT);
4) il tipo di sorveglianza (sorveglianza in tempo reale) RT_54_POS_ONCE, determinazione unica e immediata della posizione mediante la rete (art. 56*a* OSCPT);
5) il tipo di sorveglianza (sorveglianza in tempo reale) RT_55_POS_PERIOD, determinazione ricorrente e periodica della posizione mediante la rete (art. 56*b* OSCPT);
6) il tipo di sorveglianza (ricerca d'emergenza) EP_56_POS_ONCE, determinazione unica e immediata della posizione mediante la rete (art. 67 lett. b OSCPT); e
7) il tipo di sorveglianza (ricerca d'emergenza) EP_57_POS_PERIOD, determinazione ricorrente e periodica della posizione mediante la rete (art. 67 lett. c OSCPT).

Queste aggiunte impongono una revisione parziale dell'allegato 1 della OE-SCPT al fine di fissare le prescrizioni da applicare alle interfacce per l'esecuzione della sorveglianza delle telecomunicazioni. Sono inoltre inseriti i parametri e le designazioni della tecnologia 5G.

Allegato 2

L'allegato 2 della OE-SCPT definisce i requisiti tecnici delle reti di trasferimento per la sorveglianza delle telecomunicazioni tra le POC e il sistema di trattamento del Servizio SCPT. La revisione parziale di questo allegato è principalmente dovuta alla dismissione della tecnologia ISDN da parte dei FST svizzeri in seguito agli sviluppi tecnici e quindi alla disattivazione dei collegamenti di trasferimento ISDN. L'ISDN si basava ancora sul principio della commutazione a circuito. Nel frattempo solamente le reti a commutazione di pacchetto sono ancora supportate come rete di trasferimento. I capitoli nell'allegato 2 relativi all'ISDN sono stati completamente stralciati. Le interfacce di consegna ISDN (HI2 per CS IRI e HI3 per CS CC), la rete di trasferimento ISDN per CS CC, la rete di trasferimento per CS IRI e le sequenze di segnalazione per la rete di trasferimento a commutazione di circuito (CS) non figurano più nell'allegato. Se una POC desidera consegnare i dati delle sorveglianze ancora tramite reti a commutazione di circuito, li deve convertire in pacchetti IP e trasferirli tramite reti a commutazione di pacchetto.

Inoltre la panoramica delle interfacce di consegna, i dettagli delle singole richieste e componenti del sistema di trattamento nonché il modello svizzero di riferimento per la sorveglianza delle telecomunicazioni (architettura funzionale per la sorveglianza delle telecomunicazioni basata sull'architettura di riferimento ETSI) sono aggiornati.

Infine alcuni termini sono corretti e sono aggiunti l'interfaccia LI_HIQR (per le informazioni secondo l'art. 48*b*) nonché un riferimento alla OST-SCPT.

4.3 Ordinanza sul sistema di trattamento per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OST-SCPT)

Art. 3 cpv. 2 lett. a-c

Nel *capoverso 2* le *lettere a-c* sono completate con il rimando alla sezione 1 del capitolo 3 della OSCPT, in modo da chiarire che il sistema di trattamento per la sorveglianza del traffico delle telecomunicazioni (di seguito «sistema di trattamento») è in grado di trattare anche i dati di cui agli articoli di questa sezione, ad esempio gli articoli 25 (Informazioni e sorveglianze particolari) e 27 (Tipi di informazioni con ricerca flessibile dei nomi) OSCPT. La nuova componente per la sorveglianza in tempo reale permette di consegnare alle autorità di perseguimento penale un volume sempre maggiore di dati concernenti le sorveglianze particolari («special cases») anche mediante il sistema di trattamento. Il contenuto della vigente disposizione continua ad essere valido. Il capoverso 2 lettera d resta invariato.

Art. 8 cpv. 3-6

Secondo il *capoverso 3,* il Servizio SCPT può autorizzare singoli collaboratori (i cosiddetti «OrgAdmin»), soprattutto della polizia, ad assegnare accessi ad altre persone. Detti collaboratori possono continuare a farlo solamente «all'interno della loro autorità» o a persone interessate e ai loro rappresentanti legali. La disposizione consente

ora di assegnare gli accessi anche alla competente autorità d'approvazione (art. 1 cpv. 2 lett. b OSCPT), ossia ai giudici dei provvedimenti coercitivi e, per il SIC, al Tribunale amministrativo federale. Le autorizzazioni previste al numero 2.7 «autorità d'approvazione» dell'allegato non sono modificate. Finora soltanto il Servizio SCPT poteva assegnare queste autorizzazioni, mentre con la presente modifica potranno farlo anche i collaborati nel ruolo di OrgAdmin. L'autorità d'approvazione riceve solamente un accesso alla componente di gestione dei mandati WMC (Warrant Management Component), quindi non ha accesso ai dati veri e propri della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

In sede di consultazione è stato chiesto che i collaboratori autorizzati dal Servizio SCPT (OrgAdmin) e appartenenti alle autorità che valutano, dispongono e approvano le misure siano a loro volta autorizzati ad assegnare gli accessi anche al di fuori dell'autorità per cui lavorano. Questo agevolerebbe la cooperazione e solleverebbe il Servizio SCPT da questo compito amministrativo, soprattutto nei casi urgenti (p. es. in caso di ricerche d'emergenza da eseguire spesso al di fuori degli orari d'ufficio). La richiesta non ha potuto essere soddisfatta in quanto violerebbe l'articolo 9 capoverso 1 LSCPT secondo cui è il Servizio SCPT a concedere gli accessi ai dati raccolti in relazione al procedimento in questione.

Secondo i capoversi 4 e 5, l'accesso ai dati è ora effettuato dal Servizio SCPT. In linea di principio i collaboratori del Servizio SCPT o eventuali ausiliari non hanno accesso ai dati di singole sorveglianze. Di solito i dati sono semplicemente scansionati da un software. Di regola non è previsto che una persona venga a conoscenza dei dati («privacy by design»). Ciononostante, sia i collaboratori del Servizio SCPT sia le altre persone che affiancano il Servizio nell'eseguire il suo mandato sono di regola sottoposti a un controllo di sicurezza sulle persone. Può rivelarsi necessario ricorrere a personale esterno se ad esempio l'hardware o il software presenta un problema che può essere risolto solamente da uno specialista del gestore dell'hardware o del fornitore del software oppure se il Servizio SCPT deve ricorrere ad ausiliari per smaltire una grossa mole di lavoro. Secondo gli articoli 18 capoverso 1 LSCPT e 29 OSCPT, il Servizio SCPT è tenuto ad adottare misure per il controllo della qualità dei dati trasmessi dai fornitori di servizi di telecomunicazione.

Il *capoverso 4* precisa il principio di cui all'articolo 18 capoverso 2 LSCPT, secondo cui, nell'ambito del controllo della qualità, il Servizio SCPT può prendere conoscenza del contenuto dei dati soltanto previo accordo dell'autorità investita del procedimento. Questo può accadere se ci sono dei problemi, ossia se l'autorità che ha disposto la sorveglianza constata ad esempio che in una telefonata si sente soltanto uno dei due partecipanti.

Il controllo della qualità non è l'unico motivo per cui accedere ai dati relativi alla sorveglianza e conoscere il loro contenuto: tale accesso può essere necessario anche per fornire una consulenza all'autorità che dispone la sorveglianza o a un'altra autorità legittimata (art. 16 lett. j LSCPT) nonché per garantire il funzionamento regolare del sistema di trattamento del Servizio SCPT. In questi casi il Servizio SCPT deve sempre procurarsi, se possibile previamente, il consenso scritto dell'autorità investita del procedimento. La forma scritta ai sensi del capoverso 4 è necessaria perché il consenso deve essere comprovabile. In modo analogo, anche l'articolo 11 capoverso 1 lettera b

dell'ordinanza del 25 novembre 2020[33] sulla trasformazione digitale e l'informatica prevede il consenso scritto dell'autorità responsabile. I requisiti della forma scritta di cui all'articolo 14 del Codice delle obbligazioni[34] non si applicano, pertanto il consenso non deve riportare una firma autografa o una firma elettronica qualificata. Anche un semplice messaggio elettronico soddisfa il requisito della forma scritta.

Secondo l'articolo 6 LSCPT, il Servizio SCPT ha il compito di gestire un sistema informatico per il trattamento dei dati relativi alla sorveglianza del traffico delle telecomunicazioni. Al fine di garantire il funzionamento regolare del sistema, il capoverso 5 prevede una serie di deroghe al capoverso 4. Il Servizio SCPT è responsabile della sicurezza del sistema di trattamento e a tal fine deve adottare misure pertinenti (art. 12 LSCPT, art. 11 OST-SCPT) che non richiedono necessariamente il consenso delle autorità investite del procedimento (cfr. cpv 5). Può trattarsi sia di misure preventive, quali test di funzionamento o osservazioni statistiche delle attività del sistema, sia di interventi a posteriori per rimediare a guasti nel funzionamento. A tale scopo il Servizio SCPT esegue un monitoraggio per il controllo della qualità: verifica che il sistema funzioni correttamente e che le indicazioni visualizzate siano plausibili (leggibili, utilizzabili,). I collaboratori del Servizio SCPT ed eventuali ausiliari (p. es gli specialisti del fornitore di un software utilizzato) devono poter accedere a diversi dati (metadati, dati di accesso e dati sul contenuto) della sorveglianza. Può accadere che nel farlo vengano involontariamente a conoscenza del contenuto della sorveglianza anche se non è l'obiettivo principale del loro intervento. Il collaboratore del Servizio SCPT è comunque concentrato sul problema che deve risolvere e coglie, nella maggior parte dei casi, solo spezzoni del contenuto. Di regola gli accessi per verificare periodicamente la qualità dei dati e la stabilità del sistema oppure per eliminare tempestivamente eventuali errori sono automatizzati. In questi casi si analizza in particolare quanto sia esteso l'errore (riguarda un singolo caso?), la sua portata (la trasmissione dei dati è ritardata, incompleta o impossibile?) nonché la durata e i fattori che caratterizzano la tipologia di errore (quali tipi di sorveglianza e quali provider sono stati coinvolti?).

Il *capoverso 5* elenca i casi per i quali, in deroga al capoverso 4, non è necessario il consenso dell'autorità investita del procedimento.

Per assicurare il funzionamento regolare del sistema di trattamento, in caso di gravi malfunzionamenti o di rischio di gravi malfunzionamenti (*lett. a n. 1),* è necessario un rapido accesso per identificare le cause e ripristinare il funzionamento regolare del sistema (cfr. anche art. 11). Anche il rischio di un grave guasto del sistema è considerato un'urgenza che richiede un intervento immediato. Se ad esempio una sorveglianza occupa molto velocemente un enorme spazio di archiviazione e l'autorità che l'ha disposta non è reperibile perché raggiungibile solamente negli orari d'ufficio è necessario poter accedere tempestivamente ai dati, visto il rischio di malfunzionamento, al fine di individuare il problema e quindi preservare il funzionamento del sistema di trattamento.

[33] RS **172.010.58**
[34] RS **220**

Anche nei casi (*lett. a n. 2*) in cui è impossibile, o comporterebbe un onere sproporzionato, individuare in anticipo la sorveglianza che causa problemi o contattare l'autorità responsabile in quanto non disponibile in tempo utile (p. es. nei giorni festivi), il Servizio SCPT deve poter adottare misure opportune per assicurare il funzionamento regolare del sistema di trattamento. Anche una piccola modifica nella trasmissione di prodotti o formati da parte della POC può causare problemi di visualizzazione nel sistema di trattamento (errori o distorsioni) e conseguentemente comportare una serie di difficoltà nella valutazione dei dati per le autorità competenti. Non si possono tuttavia escludere perdite di qualità o addirittura problemi per l'intero sistema di trattamento non possono tuttavia essere esclusi all'atto dell'immissione o della conversione dei dati di buona qualità trasmessi dalla POC. A seconda delle circostanze sono necessarie approfondite analisi dei dati per individuare questi malfunzionamenti ed è impossibile attribuirli a priori a una sorveglianza specifica o a una determinata autorità, pertanto non è possibile, in questi casi, ottenere un consenso a priori.

Secondo la *lettera b* non è necessario il consenso neppure se, vista la mole delle sorveglianze interessate dall'accesso, è sproporzionato contattare tutte le autorità competenti. In questi casi il sistema funziona ancora correttamente, tuttavia potrebbe essere più instabile o non presentare lo stesso livello di qualità. Per individuare il mandato di sorveglianza o i formati che causano un problema oppure per rendere il sistema in generale più stabile (come nel monitoraggio summenzionato), occorre spesso confrontare, per lo più in maniera automatizzata, numerosi dati per scoprire le anomalie. Prima di riuscire a rintracciare eventuali anomalie occorre analizzare i dati in maniera automatizzata, il che solitamente implica un accesso a una grande quantità di sorveglianze disposte mediante diversi ordini e da varie autorità. È praticamente impossibile stabilire a priori quante e quali sorveglianze sono interessate da un problema. Ne consegue che se un problema può essere risolto solamente accedendo a una grande quantità di sorveglianze, il consenso di ciascuna autorità coinvolta non è necessario.

Secondo il *capoverso 6*, il Servizio SCPT adotta adeguate provvedimenti contrattuali, organizzativi e tecnici per impedire una diffusione dei dati. In tal modo s'intende impedire a tutti, non soltanto a terzi (p. es. ausiliari del Servizio SCPT) ma anche ai collaboratori del Servizio SCPT, di divulgare i dati delle sorveglianze cui devono accedere per adempiere i propri compiti.

L'articolo 6 dell'ordinanza del 31 agosto 2022[35] sulla protezione dei dati (OPDa) costituisce una base legale sufficiente affinché il Servizio SCPT possa precisare i capoversi 3-6 in un regolamento sul trattamento dei dati. Non occorre pertanto riprendere nel nuovo articolo 8 il contenuto del vigente capoverso 4.

Art. 10 cpv. 4

I termini di conservazione dei dati nel sistema di trattamento sono illustrati all'articolo 11 LSCPT.

35 **RS 235.11**

Il *capoverso 4* disciplina la durata di conservazione dei verbali. Nella versione tedesca il termine «Speicherdauer» è sostituito da quello più appropriato di «Aufbewahrungsdauer».

Anche la distruzione dei dati va messa a verbale; tuttavia, finora, mancava una disposizione sulla durata di conservazione di detti verbali che ora viene introdotta con il nuovo *secondo periodo*. Lo scopo principale di tale disciplinamento è di sapere quali dati precedentemente conservati per più tempo con funzioni di trattamento ridotte sono stati cancellati e quando. In questo caso l'articolo 4 OPDa non è applicabile.

Art. 11 Misure per la sicurezza del sistema

Nel *primo periodo* l'espressione un po' imprecisa e restrittiva «esercizio regolare» è sostituita con «funzionamento regolare», usata anche nell'articolo 8 capoverso 4. Il *secondo periodo* riprende in linea di massima il disciplinamento vigente secondo cui il Servizio SCPT consulta previamente l'autorità colpita dal guasto, se è possibile contattarla (cfr. art. 8 cpv. 5).

Allegato lett. af

La «visualizzazione dello stato di funzionamento delle parti del sistema di trattamento cui la persona ha accesso», il cosiddetto dashboard PTSS, è un'applicazione che serve a visualizzare lo stato delle componenti della sorveglianza. PTSS è la sigla inglese del Servizio SCPT. In questa applicazione sono pubblicati ticket e comunicazioni (p. es. messaggi di guasti e il loro stato, indicazioni sullo stato delle componenti del sistema, stabilità delle reti) nonché determinate scadenze (p.es. finestre di manutenzione delle componenti del sistema e di altri sistemi quali I-Net di Teldas). Il dashboard PTSS tratta anche i dati relativi allo stato di funzionamento aggiornato della componente relativa alla sorveglianza in tempo reale ed è in grado di rappresentarli in forma di grafico. Questa integrazione della matrice disciplina l'accesso delle autorità legittimate e del Servizio SCPT al dashboard PTSS; l'accesso a quest'ultimo e il numero di dati visualizzati dipendono in linea di massima dai diritti di accesso effettivi di ciascuna persona alle componenti del sistema di trattamento.

5 Ripercussioni

5.1 Ripercussioni per la Confederazione

Allo stato attuale, i previsti adeguamenti delle tre ordinanze esecutive della LSCPT (OSCPT, OE-SCPT e OST-SCPT) non avranno per la Confederazione significative ripercussioni finanziarie né sul personale.

Per integrare i nuovi tipi di informazione e sorveglianza nelle relative componenti del sistema di trattamento del Servizio SCPT sarà necessario effettuare una serie di modifiche del sistema (ulteriori processi, modifiche delle funzionalità, eventuali nuovi server, ecc). Si prevedono dunque spese supplementari per il Servizio SCPT che tuttavia possono essere coperte con i fondi attualmente preventivati.

5.2 Ripercussioni per i Cantoni

Allo stato attuale, neppure i Cantoni avranno significative ripercussioni finanziarie e sul personale riconducibili agli adeguamenti previsti. Gli emolumenti per i nuovi tipi di informazione e sorveglianza sono ripresi negli importi forfettari previsti dalla OF-SCPT (progetto separato).

5.3 Ripercussioni per le POC

I nuovi tipi di informazione e sorveglianza nonché gli adeguamenti alla tecnologia 5G inseriti nella OSCPT possono avere per i FST conseguenze finanziarie ed economiche in funzione delle modifiche tecniche che dovranno apportare ai loro sistemi in seguito a queste revisioni parziali. I FST dovranno sostenere una serie di costi d'investimento soprattutto per implementare i nuovi tipi di informazione e di sorveglianza. L'articolo 74*b* OSCP concede ai FST termini più lunghi (24 mesi invece di 12) per adeguare i loro sistemi.

6 Aspetti giuridici

6.1 Compatibilità con gli impegni internazionali della Svizzera

Il progetto è compatibile con gli impegni internazionali della Svizzera.

6.2 Forma dell'atto

Il progetto costituisce una revisione parziale di un'ordinanza emanata dal Consiglio federale ai sensi dell'articolo 182 Cost.[36].

6.3 Subdelega di competenze legislative

Il progetto non contiene alcuna subdelega di competenze legislative (ma cfr. art. 70 OSCPT e OE-SCPT).

6.4 Protezione dei dati

Le modifiche previste riguardano anche il trattamento di dati personali degni di particolare protezione (art. 4 LSCPT).

36 RS **101**

Allegato

Tabella «Panoramica termini di trattamento»

Tabella «Panoramica termini di trattamento»

Mandato	**Art. OSCPT**	**Tipi di mandato**	**Servizio SCPT**	**Fornitore di servizi postali**
Sorveglianza in tempo reale posta durante gli orari d'ufficio	16 lett. a 16 lett. b	PO_1_RT_INTERCEPTION PO_2_RT_DELIVERY	≤ 1 ora	≤ 1 giorno lavorativo
Sorveglianza retroattiva posta durante gli orari d'ufficio	16 lett. c	PO_3_HD	≤ 1 ora	≤ 3 giorni lavorativo
Disattivazione solo durante gli orari d'ufficio	16 lett. a	PO_1_RT_INTERCEPTION	≤ 1 ora	≤ 1 giorno lavorativo

Mandato	Art. OSCPT	Tipi di mandato	Servizio SCPT	FST con obblighi integrali* FSCD con obblighi d'informazione supplementari (art. 22 OSCPT) FSCD con obblighi di sorveglianza supplementari (art. 52 OSCPT)	FST con obblighi di sorveglianza ridotti (art. 51 OSCPT)
Informazioni	35 27, 35 36 37 40 27, 40 41 48*a*	IR_4_NA IR_5_NA_FLEX IR_6_NA IR_7_IP IR_10_TEL IR_11_TEL_FLEX IR_12_TEL IR_51_ASSOC_PERM**	≤ 1 ora	≤ 1 ora	≤ 1 giorno lavorativo
	48*b*	IR_52_ASSOC_TEMP**	subito	Subito (eccetto i FSCD con obblighi d'informazione supplementari, art. 22 OSCPT)	--
	38 39 42 27, 42 43 27, 43 48*c*	IR_8_IP (NAT) IR_9_NAT IR_13_EMAIL IR_14_EMAIL_FLEX IR_15_COM IR_16_COM_FLEX IR_53_TEL_ADJ_NET**	≤ 1 ora	Inoltro durante gli orari d'ufficio ordinari: ≤ 1 giorno lavorativo Inoltro al di fuori degli orari d'ufficio ordinari e nei giorni festivi: ≤ 6 ore (eccetto i FSCD con obblighi d'informazione supplementari, art. 22 OSCPT)	≤ 2 giorni lavorativi
	44 45 46 47 48	IR_17_PAY IR_18_ID IR_19_BILL IR_20_CONTRACT IR_21_TECH	≤ 1 ora	≤ 1 giorno lavorativo	≤ 2 giorni lavorativi

Mandato	**Art. OSCPT**	**Tipi di mandato**	**Servizio SCPT**	**FST con obblighi integrali*** **FSCD con obblighi di sorveglianza supplementari (art. 52 OSCPT)**
Sorveglianza in tempo reale durante gli orari d'ufficio	54 55 56 56*a* 56*b* 57 58 59 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 1 ora	≤ 1 ora
Sorveglianza in tempo reale per data durante gli orari d'ufficio	54 55 56 56*a* 56*b* 57 58 59 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 1 ora	Da installare al momento indicato nel mandato (> 1 ora)
Sorveglianza in tempo reale durante il servizio di picchetto	54 55 56 56*a* 56*b* 57 58 59 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 1 ora	≤ 2 ore
Sorveglianza retroattiva durante gli orari d'ufficio	60 61 62 63 64 65	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV**** AS_33_PREP_REF	≤ 1 ora	≤ 3 giorni lavorativi

	66	AS_34		
Sorveglianza retroattiva in casi urgenti (durante gli orari d'ufficio e il servizio di picchetto)	60 61 62 63 64 65 66	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 servizio di picchetto	67 lett. a 67 lett. b 67 lett. c 67 lett. d 67 lett. e	EP_35_PAGING EP_56_POS_ONCE*** EP_57_POS_PERIOD*** EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 ora	≤ 1 ora
	67 lett. f	EP_38_HD	≤ 1 ora	≤ 4 ore
Ricerca di condannati durante gli orari d'ufficio e il servizio di picchetto	68 cpv. 1 lett. a 68 cpv. 1 lett. e 68 cpv. 1 lett. d 68 cpv. 1 lett. e 68 cpv. 1 lett. d 68 cpv. 1 lett. e 68 cpv. 1 lett. d 68 cpv. 1 lett. b 68 cpv. 1 lett. c	HD_31_PAGING 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 RT_54_POS_ONCE*** RT_55_POS_PERIOD***	≤ 1 ora	≤ 1 ore
Ricerca di condannati durante gli orari d'ufficio e il servizio di picchetto	68 cpv. 1 lett. f 68 cpv. 1 lett. f 68 cpv. 1 lett. f 68 cpv. 1 lett. g 68 cpv. 1 lett. g 68 cpv. 1 lett. g	HD_28_NA HD_29_TEL HD_30_EMAIL AS_32_PREP_COV**** AS_33_PREP_REF AS_34	≤ 1 ora	≤ 4 ore
Disattivazione solo durante gli orari d'ufficio	54 55 56 56*b* 57	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_55_POS_PERIOD*** RT_25_TEL_IRI_CC	≤ 1 ora	≤ 1 giorno lavorativo

	58 59 67 lett. c 67 lett. d 67 lett. e	RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI EP_57_POS_PERIOD*** EP_36_RT_CC_IRI EP_37_RT_IRI		

* FST, eccetto quelli con obblighi di sorveglianza ridotti (art. 51 OSCPT).

** I FSCD con obblighi supplementari (art. 22 e 52 OSCPT) sono esentati.

*** I FSCD con obblighi di sorveglianza supplementari (art. 52 OSCPT) sono esentati.

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