Berna, 16 febbraio 2022

Revisione parziale di quattro ordinanze di esecuzione della LSCPT (OSCPT, OEm-SCPT, OE-SCPT, OST-SCPT)

Rapporto esplicativo per l'avvio della consultazione

Indice

1 Situazione iniziale

In occasione della modifica del 22 marzo 2019 della LTC[1] è stato aggiunto un nuovo capoverso 2 all'articolo 2 della LSCPT[2]. Il nuovo capoverso[3] autorizza il Consiglio federale a precisare le categorie di persone obbligate a collaborare (POC), segnatamente quelle di cui all'articolo 2 lettere b, c ed e LSCPT. I lavori di attuazione si concentrano sulla revisione parziale dell'OSCPT[4], che a sua volta implica revisioni parziali dell'OEm-SCPT[5], dell'OE-SCPT[6] e dell'OST-SCPT[7]. Nel marzo 2021 sono stati consultati una prima volta gli uffici federali. Il 29 aprile 2021 il Tribunale federale ha emanato una sentenza[8] qualificante un fornitore quale fornitore di servizi di comunicazione derivati (FSCD; art. 2 lett. c LSCPT) e non, come deciso dal Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio SCPT), quale fornitore di servizi di telecomunicazione (FST; art. 2 lett. b LSCPT). Per avere il tempo necessario per analizzare in modo approfondito le conseguenze di tale sentenza sulla prassi del Servizio SCPT, si è deciso di suddividere le revisioni in due progetti. Il presente primo progetto di revisione (OSCPT, OEm-SCPT, OE-SCPT e OST-SCPT) contiene tutte le disposizioni che non disciplinano le definizioni delle POC. Tali disposizioni, che adeguano l'OSCPT alla tecnologia 5G, devono entrare in vigore in tempi brevi. Le definizioni delle POC (soprattutto la delimitazione tra FST e FSCD) saranno oggetto di un secondo progetto di revisione parziale.

Il 19 marzo 2021, nell'ambito della legge federale concernente agevolazioni amministrative e misure di sgravio del bilancio della Confederazione, il Parlamento ha deciso una modifica della LSCPT che permette di calcolare le indennità e la partecipazione alle spese per singolo caso o sotto forma di importi forfettari (art. 38*a* LSCPT)[9]. Tale modifica implica una revisione dell'OEm-SCPT in un progetto separato.

Va infine menzionato l'attuale progetto di revisione nel quadro dell'ordinanza sulle misure di polizia per la lotta al terrorismo (OMPT)[10]. La possibilità di ordinare una

1 Legge del 30 aprile 1997 sulle telecomunicazioni (**LTC**; RS **784.10)**
2 Legge del 18 marzo 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**LSCPT**; RS **780.1**; cfr. RU **2020** 6180)
3 RU **2020** 6180. Il 18 novembre 2020 il Consiglio federale ha deciso che la modifica del 22 marzo 2019 della LTC entra in vigore il 1° gennaio 2021, eccetto l'art. 2 cpv. 1 lett. b e 2 LSCPT, che entrerà in vigore in un secondo momento (RU **2020** 6177).
4 Ordinanza del 15 novembre 2017sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**OSCPT**; RS **780.11**)
5 Ordinanza del 15 novembre 2017 sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**OEm-SCPT**; RS **780.115.1**
6 Ordinanza del DFGP del 15 novembre 2017 sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**OE-SCPT**; RS **780.117)**
7 Ordinanza del 15 novembre 2017 sul sistema di trattamento per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**OST-SCPT**; RS **780.12**)
8 2C_544/2020
9 FF **2021** 669, pag. 5/6
10 Procedure di consultazione =>Procedure di consultazione concluse =>2021 => DFGP =>Entrata in vigore parziale della legge federale sulle misure di polizia per la lotta al terrorismo; ordinanza sulle misure di polizia per la lotta al terrorismo =>Progetto posto in consultazione concernente OE-SCPT e Progetto posto in consultazione-2 (OMPT) concernente OSCPT (pag. 12), OEm-SCPT (pag. 14) e OST-SCPT (pag. 14)

localizzazione ai sensi dell'articolo 23*q* nLMSI[11] per individuare il luogo in cui si trova o soggiorna una persona richiede una adeguamento dell'OSCPT, dell'OEm-SCPT, dell'OE-SCPT e dell'OST-SCPT. Questi adeguamenti implicheranno a tempo debito lavori di coordinamento con il presente progetto.

2 Procedura preliminare, in particolare procedura di consultazione

[*sarà redatto dopo la procedura di consultazione*]

Testo …

3 Punti essenziali del progetto

3.1 Adeguamenti dell'OSCPT

Dall'entrata in vigore della LSCPT e delle sue ordinanze d'esecuzione il 1° marzo 2018, la tecnologia si è ulteriormente sviluppata. La telefonia mobile è per esempio arrivata alla quinta generazione (5G). È pertanto necessario adeguare l'OSCPT ai nuovi identificativi (elementi d'indirizzo, numeri degli apparecchi, numeri degli utenti, ecc.) della tecnologia 5G e all'uso di nuovi identificativi temporanei. Ne risultano due nuovi tipi di informazione: IR_53_ASSOC_PERM (informazioni su identificativi assegnati a lungo termine) nel nuovo articolo 48*a* e IR_54_ASSOC_TEMP (informazioni immediate su identificativi assegnati per breve tempo) nel nuovo articolo 48*b*.

La presente revisione prevede tre ulteriori nuovi tipi di informazione:

- il tipo di informazione IR_51_EMAIL_LAST, informazioni su servizi di posta elettronica (art. 42*a*), che fornisce il momento dell'ultima attività rilevante per l'accesso a un servizio di posta elettronica e serve a determinare il momento in cui un processo di comunicazione è concluso;
- il tipo di informazione IR_52_COM_LAST, informazioni su altri servizi di telecomunicazione o servizi di comunicazione derivati (art. 43*a*), che fornisce dati sull'ultima attività rilevante di un altro servizio di telecomunicazione o servizio di comunicazione derivato;
- il tipo d'informazione IR_55_TEL_ADJ_NET, determinazione delle reti immediatamente adiacenti per i servizi di telefonia e multimedia (art. 48*c*), che risolve problemi specifici nell'identificazione degli autori di reato nel caso di numeri di telefono falsificati (spoofing) o sconosciuti.

Per sfruttare le nuove possibilità tecniche del «lawful access to location services» (LALS) volto a determinare la posizione nelle reti mobili, sono previsti quattro nuovi

[11] Nel progetto di legge federale del 25 settembre 2020 sulle misure di polizia per la lotta al terrorismo (**MPT**; FF **2020** 6795, in particolare 6801)

tipi di sorveglianza che permettono la determinazione univoca o periodica della posizione mediante la rete nell'ambito della sorveglianza in tempo reale e della ricerca d'emergenza (art. 56*a* e 56*b* nonché, per la ricerca d'emergenza, art. 67 cpv. 1 lett. b e c).

Va inoltre menzionato il nuovo articolo 4*a* (inizio e fine della sorveglianza retroattiva) che ridisciplina il calcolo, controverso nella prassi, del termine di sei mesi. L'articolo 20 vigente (registrazione dei dati degli utenti dei servizi di telefonia mobile) è completato e suddiviso in disposizioni per persone fisiche (art. 20*a*) e persone giuridiche (art. 20*b*). L'articolo 20*a* capoverso 5 prevede ora una deroga alla verifica dell'identità e al rilevamento dei dati per le autorità di polizia, il Servizio delle attività informative della Confederazione (SIC) e altri gruppi di persone, se sussiste una base legale che permette loro di non rivelare la vera identità delle persone in questione.

Sono infine previsti singoli adeguamenti in varie disposizioni e l'allegato è completato con nuove definizioni e abbreviazioni.

3.2 Adeguamenti dell'OEm-SCPT

In seguito all'introduzione nell'OSCPT dei cinque tipi di informazione e dei quattro tipi di sorveglianza summenzionati, è necessario adeguare anche l'allegato dell'OEm-SCPT. Gli emolumenti e le indennità degli altri tipi di informazione e di sorveglianza restano immutati.

Vi sono inoltre singole modifiche negli articoli 3, 15, 17 capoverso 3, 18 e 19 capoverso 1 OEm-SCPT.

3.3 Adeguamenti dell'OE-SCPT

Con la presente revisione l'OE-SCPT si applica, oltre che alle POC, anche alle autorità secondo l'articolo 1 capoverso 2 lettere a–f OSCPT. Di conseguenza è modificato anche l'articolo 3 OE-SCPT, che disciplina la comunicazione sicura.

In seguito all'introduzione dei tipi di informazione menzionati sopra, sono adeguati anche i termini di trattamento per la fornitura di informazioni previsti dall'articolo 14 OE-SCPT.

Le autorità che hanno diritto alle informazioni ritengono che nella prassi il termine di un giorno lavorativo previsto dal vigente articolo 14 capoverso 2 lettera b OE-SCPT sia troppo lungo, soprattutto nel caso in cui presentano la richiesta di informazioni durante il fine settimana o in un giorno festivo e ne hanno urgentemente bisogno. Per questo motivo, per i FST e i FSCD «grandi» è ora fissato un termine più breve di sei ore nel caso di domande d'informazione al di fuori degli orari d'ufficio ordinari o nei giorni festivi (servizio di pronto intervento). Tale termine corrisponde a quello per le sorveglianze retroattive urgenti. L'esperienza insegna che durante il servizio di pronto intervento le domande di informazioni e gli ordini di sorveglianza sono pochi e quindi molto probabilmente le POC non si troveranno di fronte a un carico eccessivo di la-

voro. D'altronde le autorità di perseguimento penale devono poter raccogliere informazioni urgenti anche durante il fine settimana e nei giorni festivi affinché le indagini di polizia e il perseguimento penale non risulti ostacolato.

Anche nell'articolo 14 capoverso 3 il termine per le informazioni semplici da parte delle «piccole» POC è stato ridotto da due a un giorno lavorativo, al fine di tenere conto dell'urgente bisogno delle autorità di perseguimento penale di termine più corti.

Sono inoltre previste singole modifiche negli articoli 10 capoverso 4 (nuovo), 11 capoverso 2, 12 nonché 18 capoversi 2 e 3 OE-SCPT.

3.4 Adeguamenti dell'OST-SCPT

Il presente progetto offre l'opportunità di sottoporre a revisione parziale anche l'OST-SCPT. Oltre agli accessi all'indicazione della situazione operativa delle parti del sistema di trattamento (dashboard PTSS), che visualizza lo stato delle componenti della sorveglianza, sono ora 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). Inoltre, l'articolo 3 capoverso 2 lettere a–c è completato con il rimando alla prima sezione del capitolo 3 dell'OSCPT, poiché vi rientrano soprattutto le informazioni e le sorveglianze particolari (art. 25 OSCPT) e i tipi d'informazioni con ricerca flessibile dei nomi (art. 27 OSCPT, cfr. n. 5.4). È infine adeguato un termine nell'articolo 11.

4 Ripercussioni per la Confederazione, i Cantoni e le POC

Secondo le stime attuali, gli adeguamenti delle quattro ordinanze (OSCPT, OEm-SCPT, OE-SCPT e OST-SCPT) probabilmente non avranno ripercussioni finanziarie e sull'effettivo del personale di rilievo per la Confederazione e i Cantoni nonché per le POC. Ciononostante occorre menzionare le seguenti ripercussioni finanziarie di minima entità:

- i nuovi tipi di informazione e sorveglianza e gli adeguamenti alla tecnologia 5G nell'OSCPT possono implicare conseguenze finanziarie ed economiche per le POC a seconda degli adeguamenti tecnici a cui devono provvedere nei loro sistemi in seguito a queste revisioni parziali. Le POC dovranno affrontare spese d'investimento in particolare per poter realizzare i nuovi tipi di informazione e sorveglianza. Versando delle indennità le autorità di perseguimento penale partecipano alle spese d'esercizio delle POC;
- l'integrazione dei nuovi tipi di informazione e sorveglianza nelle relative componenti del sistema di trattamento del Servizio SCPT implicherà determinati adeguamenti del sistema (processi aggiuntivi, modifica delle funzio-

nalità, eventuali nuovi server, ecc.). Sono pertanto prevedibili spese aggiuntive per il Servizio SCPT che possono però essere affrontate con le risorse attuali;

- i nuovi tipi di informazione e di sorveglianza saranno probabilmente usati relativamente poco o molto meno di altri tipi. È pertanto prevedibile un carico relativamente esiguo per i bilanci dei Cantoni. Gli emolumenti per i nuovi tipi di informazione e sorveglianza sono simili a quelli per i tipi attuali. Le spese a carico delle autorità cantonali di perseguimento penale dipenderanno dal numero di questi tipi di informazione e di sorveglianza richiesto o ordinato, che non è né prevedibile né influenzabile,
- per questo motivo, con i nuovi emolumenti e le nuove indennità, il grado di copertura della Confederazione dovrebbe restare praticamente invariato;
- secondo il nuovo articolo 15 capoverso 2 OEm-SCPT la Confederazione può versare un'indennità anche alle POC che, pur non essendo tenute a fornire informazioni o eseguire sorveglianze, sostengono il Servizio SCPT nell'esecuzione. Questa nuova disposizione non avrà praticamente ripercussioni finanziarie per le POC e la Confederazione poiché si tratta di una costellazione assai rara nella prassi.

5 Commento a singoli articoli

5.1 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». Queste espressioni sottintendono che il relativo disciplinamento va considerato nel rispettivo contesto e riguardano parametri e funzioni opzionali oppure determinati standard o determinate versioni di standard i cui dettagli non possono essere approfonditi nell'OSCPT. Su richiesta del Servizio SCPT, i fornitori devono descrivere in modo dettagliato, in osservanza del loro obbligo di collaborazione, il motivo per cui determinati parametri, dati e funzioni non sono disponibili o non possono essere forniti.

Sostituzione di espressioni

Capoverso 1: 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. L'espressione «punto di accesso WLAN» è pertanto sostituita con l'espressione generale «accesso WLAN» poiché essa implica sia i punti di accesso che gli hotspot.

Capoverso 2: la revisione offre l'opportunità di introdurre nell'OSCPT l'abbreviazione *FSCD*, già usata nella prassi insieme all'abbreviazione *FST* (cfr. anche la modifica dell'art. 1 cpv. 2 lett. j).

Art. 1 cpv. 1 e cpv. 2 lett. j

Il *capoverso 1* subisce una lieve modifica redazionale. Nella versione italiana l'espressione «come pure» è sostituita da «nonché».

Nel *capoverso 2 lettera j* è introdotta l'abbreviazione *FSCD* (cfr. l'abbreviazione *FST* già usata nella lettera 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, da una parte per evitare un'inutile ripetizione nell'ordinanza e, dall'altra, perché è stato introdotto un nuovo articolo (art. 2*b*) che descrive in modo dettagliato la categoria dei *FSCD*. Sotto il profilo materiale la disposizione non è modificata.

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 possibile registrazione mediante procedura di richiamo delle autorizzazioni alla sorveglianza e di 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).

Le *lettere b* e *c* non contengono modifiche materiali.

Poiché attualmente si applica di norma l'accesso in linea, 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 si trova nella sezione 2 «ordine di sorveglianza».

La durata massima di una sorveglianza retroattiva è definita nella legge. L'autorità che ordina la sorveglianza può anche ordinare una durata più breve. I metadati possono essere chiesti con effetto retroattivo fino a sei mesi, indipendentemente dalla durata della sorveglianza (art. 273 cpv. 3 CPP[12]). A tale scopo i fornitori 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. 2 OSCPT in combinato disposto con gli art. 21 cpv. 2 e 22

12 Codice di procedura penale svizzero (Codice di procedura penale, **CPP**; RS **312.0**)

cpv. 2 LSCPT). Finora non è stato stabilito in un'ordinanza cosa significa precisamente nella prassi il termine di sei mesi per l'inizio e la fine della sorveglianza retroattiva e come va calcolato, il che è stato causa di discussioni.

Il *capoverso 1* stabilisce il «dies a quo» per il calcolo del termine di sei mesi per le sorveglianze retroattive. Tale giorno corrisponde al giorno della ricezione dell'ordine da parte del Servizio SCPT. Non è pertanto determinante la data dell'ordine o della trasmissione[13] da parte dell'autorità ordinante.

Per il calcolo del termine di sei mesi il momento della ricezione è preferito al momento della trasmissione dell'ordine per i seguenti motivi: in caso di trasmissione mediante WMC[14], che è il caso normale, il fatto che il momento determinante si fondi sul momento della trasmissione o della ricezione non fa alcuna differenza. La distanza temporale tra la trasmissione dell'ordine da parte dell'autorità ordinante e la ricezione da parte del Servizio SCPT è trascurabile, poiché si tratta di pochi secondi. Solo in caso di invio per corrispondenza dell'ordine, ossia 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). Questa differenza è problematica poiché i fornitori sono tenuti anche a cancellare i dati storici. Nell'esempio 4 sussisterebbe un rischio maggiore che i dati richiesti dall'autorità ordinante siano già stati cancellati dal fornitore. Scegliendo il momento della ricezione il tempo trascorso tra la ricezione dell'ordine da parte del Servizio SCPT e l'incarico al fornitore può essere mantenuto in termini ridotti.

Va osservato che il giorno della trasmissione da parte dell'autorità ordinante 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[15].

Se l'ordine è caricato nel sistema di trattamento del Servizio SCPT (WMC), tale momento è considerato il giorno della trasmissione e della ricezione da parte del Servizio SCPT (cfr. sotto es. 2). Se l'ordine è trasmesso per telefono è determinante il momento della telefonata e non quello della ricezione successiva dell'ordine scritto (cfr. sotto es. 3).

La sorveglianza inizia pertanto al più presto sei mesi prima del giorno della ricezione da parte del Servizio SCPT. La sorveglianza inizia non prima di mezzanotte (ore 00.00 e 0 secondi[16], ora svizzera), all'inizio di tale giorno. Preme ricordare che l'articolo 273 capoverso 3 CPP prevede un termine espresso in mesi e non in ore.

13 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).

14 Warrant Management Component (WMC): una componente del sistema di trattamento del Servizio SCPT, operativa dal 18 marzo 2019.

15 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»)

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

Il calcolo del termine di sei mesi si fonda sulla dottrina[17] e sulla giurisprudenza[18]: «Il termine fissato in mesi scade il giorno che nel calendario corrisponde al giorno dell'evento, ossia allo stesso numero del giorno che ha fatto decorrere il termine oppure, in mancanza del giorno corrispondente, all'ultimo giorno del mese.»[19] Per la sorveglianza retroattiva questo significa che un termine fissato in mesi decorre il giorno il cui numero corrisponde a quello del giorno della ricezione 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. Se ad esempio il Servizio SCPT riceve l'ordine il 31 del mese, il giorno dell'inizio della sorveglianza retroattiva è il giorno 31 di sei mesi prima. Se però il 31 non esiste in tale mese (p. es. il 31 aprile), si prende l'ultimo giorno del mese (30 aprile, cfr. sotto esempi 2-3).

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[20] ora svizzera di tale giorno (cfr. sotto es. 1-4). Se la sorveglianza retroattiva è eseguita lo stesso giorno – ossia prima delle ore 23.59 e 59 secondi – le autorità legittimate ricevono soltanto i dati risultanti fino al momento dell'esecuzione della sorveglianza retroattiva. Non vi è quindi una seconda trasmissione successiva dei dati restanti (metadati risultanti dal periodo tra il momento dell'esecuzione della sorveglianza e la fine del giorno). Ciò è rilevante soprattutto se una sorveglianza retroattiva è stata dichiarata urgente (cfr. es. 5). Anche i dati rilevanti presso il fornitore che sono a disposizione solo successivamente a causa di ritardi usuali (p. es. dati del roaming), non devono essere trasmessi posteriormente. Se tali dati sono importanti per l'autorità ordinante, questa dovrebbe prendere in considerazione un'ulteriore sorveglianza retroattiva in un momento successivo (cfr. sotto es. 5).

I fornitori tenuti a conservare i metadati devono garantire la conservazione sufficientemente lunga dei dati, tenendo conto della suddetta regola per il calcolo del momento iniziale della sorveglianza retroattiva e dei termini di trattamento di cui agli articoli 17 e 18 OE-SCPT (cfr, anche i commenti all'art. 21 cpv. 4 OSCPT). Il fornitore esegue la sorveglianza retroattiva entro tre giorni lavorativi, in casi urgenti entro sei ore (art. 17 cpv. 3 OE-SCPT).

Qui di seguito sono elencati alcuni esempi per il calcolo del termine di sei mesi. Va osservato che i valori standard dell'ora dell'inizio e della fine della sorveglianza sono rispettivamente le ore 00.00 e 0 secondi e le ore 23.59 e 59 secondi, tranne se l'esecuzione della sorveglianza avviene lo stesso giorno dell'ordine; in tal caso l'ora della fine della sorveglianza corrisponde a quella dell'inizio più 59 secondi. Vanno forniti i dati disponibili al momento dell'esecuzione.

17 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.

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

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

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

Esempio 1: ordine datato martedì, 10 novembre 2020, ricevuto dal Servizio SCPT mediante messaggio elettronico criptato del **12 novembre 2020** alle ore 09.00**.**
→ **GG** inizio **= 12**, MM: 11 - 6 = 5 → **MM = 5**, **AAAA = 2020**
Inizio non prima del 12 maggio 2020, ore 00.00;
fine non oltre il 12 novembre 2020, ore 23.59.

Esempio 2: ordine caricato in WMC lunedì, **31 agosto 2020** alle ore 18.00.
→ **GG** inizio **= 31**, MM: 8 - 6 = 2 → **MM = 02**, **AAAA = 2020**
Poiché il 31 febbraio 2020 non esiste, si prende l'ultimo giorno di febbraio 2020.
Inizio non prima del 29 febbraio 2020, ore 00.00;
fine non oltre il 31 agosto 2020, ore 23.59.

Esempio 3: ordine orale per telefono al Servizio SCPT domenica, **31 maggio 2020** alle ore 16.50.
→ **GG** inizio **= 31**, MM: 5 - 6 = -1 + 12 → **MM** = **11** dell'anno precedente, AAAA: 2020 - 1 → **AAAA = 2019**
Poiché il 31 novembre 2019 non esiste, si prende l'ultimo giorno di novembre 2019.
Inizio non prima del 30 novembre 2019, ore 00.00;
fine non oltre il 31 maggio 2020, ore 23.59.

Esempio 4: ordine datato mercoledì, 8 aprile 2020, inviato per posta giovedì, 9 aprile 2020 (timbro postale), nessun avviso telefonico. Ricevuto dal Servizio SCPT il **14 aprile 2020** (dopo il lunedì di Pasqua) alle ore 09.00. Ordine di sorveglianza trasmesso al fornitore il 14 aprile 2020 alle ore 09.50.
→ **GG** inizio **= 14**, MM: 4 - 6 = -2 + 12 → **MM** = **10** dell'anno precedente, AAAA: 2020 - 1 → **AAAA = 2019**
Inizio non prima del 14 ottobre 2019, ore 00.00;
fine non oltre il 14 aprile 2020, 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).

Esempio 5: ordine di sorveglianza retroattiva urgente, caricato in WMC dall'autorità ordinante venerdì, **28 agosto 2020, ore 16.00**, incarico trasmesso alla POC dal Servizio SCPT alle ore 16.30.
→ **GG** inizio **= 28**, MM: 8 - 6 = 2 → **MM = 02**, **AAAA = 2020**
Inizio non prima del 28 febbraio 2020, ore 00.00;
fine non oltre il 28 agosto 2020.

L'ora risulta dal momento dell'esecuzione da parte della POC (ha al massimo 6 ore di tempo dopo la ricezione dell'incarico, ossia non più tardi delle ore 22.30). Per motivi tecnici i metadati più recenti presso la POC non sono ancora pronti per essere forniti. L'autorità ordinante deve effettuare una ponderazione tra la velocità della fornitura e la disponibilità dei metadati. I metadati retroattivi sono disponibili presso la POC soltanto con alcune ore di ritardo. Occorrerebbe prendere in considerazione una sorveglianza retroattiva in un momento ulteriore (attenzione: perdita di metadati più vecchi) o, in caso di sorveglianze urgenti, una sorveglianza in tempo reale limitata ai metadati.

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

Il presente articolo disciplina le prestazioni del Servizio SCPT e delle POC menzionate al di fuori degli orari d'ufficio ordinari, ossia da lunedì a venerdì tra le ore 17.01 e le ore 07.59 nonché durante il fine settimana e i giorni festivi (cfr. art. 10). Durante questi orari il Servizio SCPT e le POC mettono a disposizione un servizio di pronto intervento. I termini di trattamento per le prestazioni del Servizio SCPT e delle POC durante il servizio di pronto intervento sono disciplinati, come quelli per il trattamento negli orari d'ufficio, nell'OE-SCPT.

Il capoverso 1 è adeguato e strutturato in modo nuovo. Non vi sono modifiche materiali sostanziali per il Servizio SCPT, le autorità e le POC. In particolare, per le POC la soluzione di eventuali problemi è già prevista nell'articolo 11 vigente (cpv. 1 lett. e in combinato disposto con il cpv. 2) come pure la reperibilità 24 ore su 24 e 7 giorni su 7 («in ogni momento», fine cpv. 2). I FST, eccetto quelli con obblighi di sorveglianza ridotti secondo l'articolo 51, e i FSCD con obblighi di sorveglianza supplementari (art. 52) devono fornire tutti i servizi di pronto intervento di cui al capoverso 1 lettere a–e. Non devono invece fornite un servizio di pronto intervento 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.

Le lettere a–e enumerano in modo esaustivo le prestazioni durante il servizio di pronto intervento. Va notato che durante il servizio di pronto intervento il Servizio SCPT fornisce soltanto una consulenza limitata. La *lettera a* disciplina la trasmissione delle informazioni standardizzate menzionate. La *lettera b* elenca altre informazioni standardizzate. La *lettera c* disciplina i tipi di sorveglianza in tempo reale da attivare durante il servizio di pronto intervento, mentre la *lettera d* determina i tipi di sorveglianza retroattiva dichiarati urgenti da eseguire durante tale servizio. La lettera e elenca i tipi di ricerche di emergenza e di condannati da eseguire durante il servizio di pronto intervento.

Il *capoverso 2* sancisce la prassi attuale secondo cui le autorità annunciano gli incarichi di cui al capoverso 1 per telefono al servizio di pronto intervento del Servizio SCPT. Sono eccettuate soltanto le informazioni fornite in modo automatizzato. Solo in questo modo è garantito che i collaboratori del Servizio SCPT siano resi attenti tempestivamente agli incarichi e possano trattarli entro i termini previsti nonché informare a loro volta dell'incarico le POC in questione.

Il capoverso 3 non subisce modifiche materiali rispetto al vigente capoverso 3. 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 richieste di informazioni e gli ordini di sorveglianze particolari (art. 25) sono escluse dalle prestazioni fornite durante il servizio di pronto intervento. Si tratta di informazioni o sorveglianze che non corrispondono ad alcun tipo di informazione o sorveglianza dell'ordinanza (cosiddette informazioni o sorveglianze non standardizzate) e la cui esecuzione spetta al Servizio SCPT o a una persona da esso incaricata. La fornitura di queste informazioni o l'esecuzione di queste sorveglianze sono molto

più complesse dei 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 pronto intervento presso il Servizio SCPT o terzi da esso incaricati implicherebbe spese sproporzionatamente elevate.

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

Ai fini di una migliore leggibilità il vigente articolo 18 è suddiviso in quattro articoli (art. 18, 18*a*, 18*b* e 18*c*). Gli articoli illustrano in dettaglio gli obblighi connessi alla fornitura di informazioni.

L'*articolo 18 capoverso 1* sancisce il principio secondo cui le seguenti categorie di POC devono fornire le informazioni mediante l'interfaccia d'interrogazione del sistema di trattamento del Servizio SCPT (IRC[21]):

- i FST, eccetto quelli con obblighi di sorveglianza ridotti (art. 51);
- i FSCD con obblighi di informazione supplementari (art. 22); e
- i FSCD con obblighi di sorveglianza supplementari (art. 52);

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

Il *capoverso 2* precisa che le POC menzionate nel capoverso 1 devono fornire in forma automatizzata le informazioni elencate, mentre per le altre informazioni possono scegliere se fornirle manualmente o in forma automatizzata. L'obbligo della forma automatizzata riguarda spesso informazioni urgenti o semplici. La possibilità di scegliere tra forma automatizzata e manuale va vista nell'ottica della libertà economica delle POC in questione, poiché l'automatizzazione delle informazioni implica spese d'investimento, ma d'altra parte consente di risparmiare costi operativi rispetto all'informazione manuale. Questa possibilità di scelta implica che alcune POC forniscono le informazioni di un determinato tipo in forma manuale, mentre altre POC le forniscono in forma automatizzata. Dei cinque nuovi tipi di informazione quelle di cui all'articolo 42*a* (IR_51_EMAIL_LAST), 43*a* (IR_52_COM_LAST), 48*a* (IR_53_ASSOC_PERM) e 48*b* (IR_54_ASSOC_TEMP) devono essere fornite in forma automatizzata, mentre per le informazioni secondo l'articolo 48*c* (IR_55_TEL_ADJ_NET) le POC possono scegliere tra la trasmissione manuale e quella automatizzata. La trasmissione delle informazioni in forma automatizzata si svolge senza intervento umano del Servizio SCPT e delle POC; l'autorità legittimata inserisce la sua domanda d'informazione nella componente per le domande d'informazione IRC del sistema di trattamento e riceve entro un'ora una risposta dai sistemi delle POC. Per la trasmissione manuale dell'informazione mediante l'IRC, l'autorità legittimata inserisce la sua domanda d'informazione nell'IRC e la POC riceve la comunicazione che ha ricevuto una domanda d'informazione. Il collaboratore della POC entra nell'IRC e compila a mano la relativa maschera di risposta. L'autorità legittimata

21 IRC: Information request component del sistema di trattamento del Servizio SCPT; operativo dal 18 marzo 2019.

riceve la risposta nell'IRC. Per la trasmissione manuale dell'informazione al di fuori del sistema di trattamento, l'autorità legittimata inserisce la sua domanda d'informazione nell'IRC e il Servizio SCPT la trasmette alla POC mediante un mezzo di trasmissione scritto autorizzato dal DFGP. La POC può fornire l'informazione senza requisiti di forma e trasmette la risposta al Servizio SCPT mediante un mezzo di trasmissione scritto autorizzato dal DFGP. Il Servizio SCPT trasmette la risposta in modo sicuro all'autorità legittimata.

Secondo il *capoverso 3* i FSCD con obblighi d'informazione supplementari (art. 22) sono esentati dall'obbligo d'informazione di cui all'articolo 48*b*. L'attuazione di questo tipo di informazione da fornire in tempo reale richiede da parte delle POC investimenti in una nuova interfaccia d'interrogazione e nel sistema per la trasmissione automatizzata delle informazioni. Per ragioni di proporzionalità questi oneri supplementari devono essere imposti soltanto ai «grandi» FST e ai «grandi» FSCD (art. 52). Inoltre, il capoverso 3 prevede che, nel caso di informazioni secondo gli articoli 38, 39 e 48*c*, i FSCD con obblighi d'informazione supplementari (art. 22) devono fornire soltanto le informazioni loro disponibili, poiché secondo l'articolo 21 capoverso 6 lettere b e c non sono tenuti a conservare i relativi metadati. Devono fornire tali informazioni durante gli orari di lavoro normali e possono fornirle durante il servizio di pronto intervento (art. 11).

Il *capoverso 4* concerne la fornitura di informazioni da parte dei FST con obblighi di sorveglianza ridotti (art. 51). Anche loro sono esentati, per i motivi illustrati sopra (cfr. il commento al cpv. 3), dall'obbligo di fornire le informazioni di cui all'articolo 48*b*. La condizione minima è la trasmissione manuale delle informazioni al di fuori del sistema di trattamento (cfr. il commento al cpv. 2). Vi è tuttavia anche la possibilità di fornire le informazioni manualmente mediante il sistema di trattamento (IRC, cfr. il commento al cpv. 2). Un FST con obblighi di sorveglianza ridotti (art. 51) può sempre esprimere il desiderio di fornire determinate informazioni in forma automatizzata. In tal caso il Servizio SCPT decide, previa consultazione, se ciò può essere attuato nell'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 di trasmissione di informazioni da parte dei FSCD senza obblighi supplementari, vale a dire 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.

Secondo il *capoverso 1,* nel fornire informazioni, essi non sono tenuti a rispettare i tipi previsti dalla presente ordinanza. Poiché non devono garantire la disponibilità a fornire informazioni, devono fornire soltanto i dati a loro disposizione.

Il *capoverso 2* disciplina la trasmissione delle informazioni. I FSCD senza obblighi supplementari e i gestori di reti di telecomunicazione interne sono tenuti almeno a fornire le informazioni disponibili, per scritto e al di fuori del sistema di trattamento, tramite un mezzo di trasmissione sicuro approvato dal DFGP.

Secondo il *capoverso 3* i FSCD senza obblighi supplementari e i gestori di reti di telecomunicazione hanno anche la possibilità di fornire manualmente o, d'intesa con il Servizio SCPT, in forma automatizzata i dati a loro disposizione mediante l'interfaccia d'interrogazione del sistema di trattamento.

Art. 18b Ricorso a terzi per fornire informazioni

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

Art. 18c Comunicazione del numero di pacchetti di dati in occasione della fornitura di informazioni

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

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

Per i servizi di telefonia mobile i requisiti per l'identificazione sono più severi rispetto ad altri servizi quali ad esempio WLAN (cfr. art. 19). La presente disposizione si fonda, come pure gli articoli 20*a* e 20*b*, sulle norme di delega al Consiglio federale degli articoli 21 capoverso 1 lettera d, 22 capoverso 2 e 23 capoverso 1 LSCPT. Le disposizioni divergenti per persone fisiche (art. 20*a*) e 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 questi sono utilizzabili soltanto dopo l'attivazione da parte dell'utente, alla loro prima attivazione, i FST o i rivenditori (cpv. 2) devono verificare, nel caso di persone fisiche, l'identità dell'utente (lett. a) e, nel caso di persone giuridiche, i dati di quest'ultime (lett. b).

Per attivazione 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 fissa nell'apparecchio (embedded SIM; eSIM), di regola il fornitore attiva il relativo profilo o può attivare il servizio anche eliminando un eventuale blocco all'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 installato nel tablet ed è «consegnato» 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 della sua attivazione e quindi dell'utilizzabilità nella rete di telefonia mobile. È inoltre importante chi deve procedere all'identificazione dell'utente e alla registrazione dei dati relativi alla persona. Poiché, nel suddetto esempio, non procede all'attivazione del mezzo di accesso alla telefonia mobile, il negozio di elettronica non deve neppure procedere alla

registrazione dei 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 compito del fornitore di telefonia mobile in quanto FST, quando 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 o dei dati della persona giuridica incombe ai rivenditori professionali (art. 2 lett. f LSCPT), se la consegna dei mezzi d'accesso o la prima attivazione è effettuata da questi ultimi. Ad esempio, al momento della consegna di un mezzo d'accesso in un negozio di un rivenditore professionale quest'ultimo procede all'identificazione dell'utente, copia il suo mezzo d'identificazione (p. es. documento d'identità) e trasmette successivamente al FST i dati richiesti relativi alla persona nonché la copia elettronica del mezzo d'identificazione conformemente all'articolo 20*a* capoverso 4. In questo caso il FST non deve procedere a un'ulteriore verifica dei dati dell'utente. La registrazione e l'identificazione secondo regola dell'utente da parte del rivenditore professionale nonché la trasmissione dei dati al FST deve essere verificata e imposta in maniera idonea dal FST, poiché quest'ultimo deve essere in grado di fornire le informazioni richieste e non può far valere eventuali omissioni del rivenditore professionale.

Nel caso di nuovi contatti con i clienti nel corso della relazione commerciale, si può presumere che di norma il FST aggiorni ed eventualmente verifichi i loro dati poiché ciò è nel suo interesse. 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 d'informazioni, oltre ai dati prescritti del cliente vanno forniti anche 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. Non è quindi richiesta la registrazione successiva di dati relativi alla persona temporaneamente modificati. Se viene a conoscenza di una modifica dei dati del cliente, il FST deve comunicarli nel quadro di un'eventuale informazione.

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

Il *capoverso 1* enumera in modo esaustivo i mezzi d'identificazione ammessi per fornire la prova dell'identità. Altri mezzi, quali la licenza di condurre, non sono ammessi. 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 i mezzi d'identificazione menzionati è obbligatoria. Ciò corrisponde al disciplinamento precedente per servizi di telefonia prepagati (prepaid), che con la revisione totale della OSCPT è stata estesa a tutti i servizi di telefonia mobile, a prescindere dal metodo di pagamento (p. es. abbonamento, prepagato, gratuito)[22]. Nella prassi i fornitori di servizi di telefonia mobile chiedono da tempo la presentazione di un documento d'identità per contrarre un abbonamento. Il fornitore o il rivenditore professionale non deve verificare in modo dettagliato l'autenticità del

22 La sentenza della Corte EDU del 30 gennaio 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 secondo l'art. 8 CEDU.

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 sono soltanto tenuti ad accettare documenti d'identità la cui autenticità risulta plausibile. Se accetta un documento d'identità manifestamente riconoscibile come falsificazione o manifestamente 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 intende farsi identificare con uno di questi documenti, di regola il cliente li presenta in loco. Poiché la procedura di verifica dell'identità non è disciplinata, è possibile anche la verifica per video o online[23]. In tal caso occorre rispettare le norme inerenti alla sicurezza e alla qualità della circolare della FINMA 2016/7 «Video identificazione e identificazione online»[24] per l'identificazione online nel settore bancario.

Il documento d'identità (lett. a–c) deve essere valido al momento della registrazione, che corrisponde al momento 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 errate con documenti d'identità scaduti.

I dati menzionati 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 sono responsabili della registrazione corretta 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 sono disponibili in lettere latine (traslitterazione) possono essere usati direttamente per la normale (ossia letterale) ricerca del nome (cfr. art. 35).

Per i seguenti dati relativi alla persona o al documento, invece di una registrazione manuale dovrebbero essere registrati i dati MRZ:

- 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 registrate secondo le indicazioni del cliente verificandone la plausibilità (nessuna indicazione inventata o manifestamente errata).

23 Cfr. anche l'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**)

24 finma.ch =>Documentazione => Circolari

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 indicazioni. Non sono contemplate le semplici carte telefoniche che non sono carte SIM o simili. Questi ulteriori dati devono essere rilevati affinché si possa individuare chi abbia fatto eventuali registrazioni errate (cfr. la corrispondente disposizione penale dell'art. 39 cpv. 1 lett. c LSCPT). Va osservato che in caso di rilevamento errato della relazione con il cliente senza abbonamento (prepaid o gratuito), il FST deve bloccare l'accesso ai servizi di telecomunicazione (art. 6*a* LTC). Per momento ai sensi della *lettera a* s'intende la data e l'ora. Il nome e l'indirizzo di cui alla *lettera b* devono essere registrati integralmente e il rilevamento dipende da chi lo effettua (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 anche il cognome e il nome 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 le indicazioni 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 sinora, una copia elettronica del documento d'identità. Ciò continua a essere necessario perché in passato si sono verificati molti rilevamenti errati di dati personali. La copia del documento d'identità è per il momento il mezzo più idoneo per evitare tali rilevamenti errati. Deve essere allestita una copia elettronica ben leggibile (fotografie, scansione). Le copie cartacee non soddisfano più i nuovi requisiti. La durata di conservazione per le FST è disciplinata dall'articolo 21 capoverso 3. Il *secondo periodo* introduce un termine entro cui i rivenditori professionali devono trasmettere al FST tutti i dati rilevati conformemente ai capoversi 2 e 3 e la copia del documento d'identità. Il termine è di 14 giorni, ragionevolmente esigibile anche da piccoli rivenditori. Il capoverso intende delimitare le responsabilità in modo più chiaro (cfr. anche la corrispondente disposizione penale dell'art. 39 cpv. 1 lett. c LSCPT).

Il nuovo *capoverso 5* prevede una nuova deroga alla verifica dell'identità e al rilevamento dei dati, da una parte per le autorità di polizia e il Servizio delle attività informative della Confederazione (SIC) e, dall'altra per altri gruppi di persone, qualora sussista una base legale che permetta loro di non rendere nota la loro vera identità. La deroga può essere chiesta dalle autorità di polizia federali e cantonali e dal SIC.

Secondo il diritto vigente la verifica dell'identità ai sensi del capoverso 1 è prevista per tutti gli utenti e quindi anche per i membri delle autorità di polizia e i collaboratori del SIC. Tuttavia, negli ultimi anni tale disciplinamento si è rilevato particolarmente problematico per le suddette autorità. Presso i FST e i rivenditori professionali un gran numero di persone non controllabile ha accesso ai sistemi e quindi ai dati necessari per fornire informazioni. Per questo motivo, nei sistemi odierni la protezione dell'identità degli utenti è insufficiente, soprattutto se si tratta di membri delle autorità di polizia o di collaboratori del SIC.

Gli agenti in incognito (art. 298*a* segg. CPP) hanno il compito legale di chiarire crimini e delitti. A tale scopo possono concludere transazioni fittizie o fingere di volerle concludere (art. 298*a* cpv. 1 CPP). La legge prevede che durante il loro impiego la vera identità degli agenti in incognito non sia individuabile. Oltre a essere contraria agli scopi del loro compito (chiarire reati gravi), la rivelazione dell'identità di un agente in incognito può costituire anche un notevole pericolo per la vita e l'integrità dell'agente stesso, soprattutto nei casi in cui i reati sono stati commessi da un'organizzazione criminale ai sensi dell'articolo 260ter CP. Le attuali lacune relative alla sicurezza nel quadro dei diritti d'accesso dei FST implicano proprio queste situazioni pericolose.

Agli agenti infiltrati (art. 151 e 285*a* segg. CPP) è assegnata un'identità fittizia. Per contro, agli agenti in incognito non può essere assegnata un'identità fittizia (art. 298*a* cpv. 2) per motivi legati alla proporzionalità, dato che le indagini mascherate sono permesse soltanto per chiarire reati particolarmente gravi elencati all'articolo 286 capoverso 2 CPP.

I collaboratori del SIC agiscono in diverse funzioni in situazioni in cui rendere nota la loro vera identità e la loro appartenenza al SIC può implicare una minaccia diretta alla loro integrità e a quella di persone del loro ambiente oppure mettere a repentaglio l'esecuzione del loro compito. Questo perché possono essere minacciate direttamente dalle persone che hanno contattato oppure perché nel loro lavoro di controspionaggio possono subire svantaggi, fino all'arresto, se più tardi si recano in un Paese contro cui era diretta l'attività di controspionaggio del SIC.

I collaboratori del SIC devono poter utilizzare collegamenti telefonici anonimi costantemente modificati o da usare solo una volta soprattutto quando reclutano e istruiscono informanti. I titolari dei collegamenti non devono quindi essere identificabili. Anche nel caso di osservazioni di persone nel quadro dei servizi informativi il SIC deve modificare periodicamente i collegamenti telefonici utilizzati in modo da ridurre la possibilità che siano individuati. La controparte potrebbe usare – illegalmente – i cosiddetti IMSI-catcher e tentare di identificare i titolari di determinati numeri di cellulare.

La possibilità prevista dalla legge per il SIC di lavorare con identità fittizie non è sufficiente per provvedere al necessario gran numero di collegamenti di telefonia mobile anonimizzati. Il SIC deve avere la possibilità di procurarsi presso i fornitori un numero sufficiente di collegamenti telefonici anonimizzati, vale a dire fino a parecchie centinaia all'anno. Secondo l'articolo 18 della legge federale sulle attività informative (LAIn) oltre che per i collaboratori del SIC, le identità fittizie sono previste anche per i collaboratori delle autorità d'esecuzione cantonali e, in determinate circostanze, per fonti umane del SIC.

Non tutti i FST possono garantire che i loro sistemi attuali non vengano sfruttati da criminali per identificare agenti infiltrati e mettere a repentaglio la vita e l'incarico di questi ultimi. È pertanto necessario che implementino soluzioni tecniche affinché le autorità di polizia e i collaboratori del SIC non siano ostacolati o addirittura messi in pericolo nell'adempimento dei loro compiti. Anche dall'assenza di un documento d'identità nel sistema del FST si può a volte dedurre che si tratta di un utente di un'autorità preposta alla sicurezza.

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

Il *capoverso 1* disciplina le indicazioni da rilevare delle persone giuridiche. Le indicazioni corrispondono a quelle del vigente articolo 20 capoverso 3. Di norma le indicazioni sono rilevate 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. La persona utente dei servizi menzionata nella *lettera c* 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. 21 Termini di conservazione

Il presente articolo è stato ampiamente riveduto al fine di strutturare meglio, completare e precisare il disciplinamento dei termini di conservazione delle singole categorie di dati. Per i FSCD con obblighi di informazione (art. 22) e di sorveglianza (art. 52) supplementari la presente revisione usa l'espressione compatta *FSCD con obblighi supplementari*. I termini di conservazione principali non sono modificati: come finora, 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 3), i dati relativi all'uso (usage data) devono essere conservati per sei mesi (cpv. 2 e 4) e i dati per l'identificazione degli utenti di accessi WLAN pubblici gestiti professionalmente durante l'intera durata della relazione commerciale nonché per sei mesi dopo il suo termine (cpv. 5).

Nel *capoverso 1* sono state inserite anche le indicazioni sugli identificativi assegnati a lungo termine secondo l'articolo 48*a*.

Il *capoverso 2* è nuovo e disciplina i termini di conservazione per i dati di utenza relativi all'ultima attività rilevante per l'accesso ai servizi di posta elettronica nonché ad altri servizi di telecomunicazione e comunicazione derivati, necessari per i nuovi tipi di informazione di cui agli articoli 42*a* e 43*a*.

L'espressione generale *indicazioni ai fini dell'identificazione* è ora precisata nei singoli capoversi. Nella maggior parte dei casi si tratta di dati sull'utente (cpv. 1 e 3), In altri si può tuttavia trattare anche di dati relativi all'uso (cpv. 2, 4 e 5). In seguito alla precisazione delle *indicazioni ai fini dell'identificazione* è stato inserito il nuovo *capoverso 3* in modo da disciplinare esplicitamente il termine di conservazione delle indicazioni sugli utenti e della copia della prova d'identità nel settore della telefonia mobile. Ne fanno parte i dati relativi alla persona rilevati in occasione della registrazione e, nel caso di persone fisiche, anche la copia elettronica della prova dell'identità. Nel diritto vigente ciò è disciplinato implicitamente nel capoverso 1.

Nel diritto vigente i dati sull'attribuzione e la traduzione di indirizzi IP e numeri di porta sono contenuti nel capoverso 2 lettera b. Nel presente progetto di revisione il disciplinamento è suddiviso a seconda dell'attribuzione univoca o dell'attribuzione

plurivoca: i dati sull'attribuzione univoca di indirizzi IP sono disciplinati nel nuovo *capoverso 4* e i dati sull'attribuzione e traduzione plurivoca (NAT) di indirizzi IP e numeri di porta nel nuovo *capoverso 6 lettera b*. Per gli indirizzi assegnati in modo univoco occorre distinguere tra indirizzi IP assegnati in modo fisso e indirizzi IP assegnati in modo dinamico. Il termine di conservazione per i dati sull'attribuzione di indirizzi IP fissi include l'intera durata della relazione commerciale e ulteriori sei mesi. Per gli indirizzi IP assegnati in modo dinamico il termine di conservazione è di soli sei mesi, poiché fanno parte dei dati che dipendono dall'uso.

Il tenore del *capoverso 5* corrisponde al secondo periodo del capoverso 1 vigente ed è semplicemente completato sotto il profilo redazionale («accesso WLAN» invece di «punto di accesso WLAN»; cfr. il commento alla sostituzione di espressioni, cpv. 1).

I dati di cui al *capoverso 6* sono quelli di identificazione secondo l'articolo 22 capoverso 2 secondo periodo LSCPT. Il *capoverso 6* si fonda sul vigente capoverso 2 ed è stato completato con la *lettera c,* che disciplina il termine di conservazione dei metadati per la determinazione delle reti immediatamente adiacenti per le informazioni di cui all'articolo 48*c* (cfr. il relativo commento). Lo stralcio dell'espressione *essere in grado di trasmettere* chiarisce che, nella misura in cui si tratta di metadati, questi dati devono essere conservati ma non devono essere trasmessi nell'ambito di informazioni. Le POC devono servirsi di questi metadati soltanto per l'identificazione degli utenti e trasmettere le indicazioni richieste secondo la domanda di informazioni. I metadati stessi possono essere trasmessi dalle POC soltanto nell'ambito di sorveglianze (in tempo reale o retroattive). Occorre tuttavia tenere conto del fatto che i metadati di cui alla lettera b non sono parte dei tipi di sorveglianza standardizzati.

Il *capoverso 7* corrisponde al vigente capoverso 3 con l'aggiunta del rinvio al capoverso 6 (invece che cpv. 2) e disciplina, come sinora, la distruzione dei metadati contemplati nel capoverso 6.

Osservazione: non devono essere conservate indicazioni sugli identificativi assegnati a breve termine di cui all'articolo 48*b*. A causa dello svolgimento molto dinamico dell'attribuzione, questo tipo di informazione è possibile solo in tempo reale (cfr. il commento all'art. 48*b*).

Art. 26 Tipi di informazioni in generale

Il *capoverso 1* è rielaborato sotto il profilo formale. L'enumerazione in cifre è sostituita da un'enumerazione un po' più ampia in lettere. Inoltre, sono inclusi in questo elenco i quattro nuovi tipi di informazione. La *lettera b* è completata dagli articoli 42*a* (IR_51_EMAIL_LAST: informazioni su servizi di posta elettronica) e 43*a* (IR_52_COM_LAST: informazioni su altri servizi di telecomunicazione o servizi di comunicazione derivati). La nuova *lettera h* menziona gli articoli 48*a* (IR_53_ASSOC_PERM, informazioni su identificativi assegnati a lungo termine) e 48*b* (IR_54_ASSOC_TEMP: informazioni immediate su identificativi assegnati per breve tempo) e la nuova *lettera i* l'articolo 48*c* (IR_55_TEL_ADJ_NET: determinazione delle reti immediatamente adiacenti per i servizi di telefonia e multimedia). Inoltre, nella *lettera d* il termine specifico «copia del documento d'identità» è sostituto da quello più generale «prova dell'identità» poiché possono ora essere usate anche identità elettroniche.

Il *capoverso 2* contiene una modifica redazionale. È opportuno usare l'espressione «persone obbligate a collaborare» in sostituzione 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 i quattro nuovi tipi di sorveglianza sulla determinazione della posizione (due per la sorveglianza in tempo reale e la ricerca di condannati, due per la ricerca d'emergenza) e sono adeguati alcuni titoli di tipi di sorveglianza già esistenti.

Le *lettere a–c* del *capoverso 1* restano fondamentalmente invariate. La *lettera d* è nuova 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 lettera d vigente diventa la *lettera e*.

Nel *capoverso 2 lettera c* la formulazione scelta è ora *la determinazione della posizione per l'ultima attività* (cfr. anche il commento all'art. 63).

Nel *capoverso 3 lettera a* il titolo della ricerca d'emergenza è stato modificato come segue: *la determinazione della posizione per l'ultima attività* (cfr. art. 67 cpv. 1 lett. a). La *lettera b* è nuova 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). Le *lettere c–e* restano invariate e corrispondono alle lettere b–d vigenti. Sono adeguati soltanto i rimandi tra parentesi alle pertinenti disposizioni.

Nel *capoverso 4 lettera a* la formulazione scelta è ora *la determinazione della posizione per l'ultima attività* (cfr. anche il commento all'art. 63). La *lettera b* è nuova 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). Le *lettere c–e* restano invariate e corrispondono alle lettere b–d vigenti. Sono adeguati soltanto i rimandi tra parentesi alle pertinenti disposizioni. Nella *lettera f* è aggiunto il rimando alla ricerca per zona di copertura dell'antenna nell'ambito della ricerca di condannati (art. 68 cpv. 1 lett. g, finora lett. d).

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. Quest'integrazione è necessaria poiché vi sono casi in cui le POC non sono in grado di effettuare i collegamenti test come disciplinato nel primo periodo. In questi casi i collegamenti test sono effettuati 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 devono garantire la disponibilità alla sorveglianza). I collegamenti test possono essere effettuati anche per le sorveglianze particolari (art. 25), i cosiddetti casi speciali. Oltre a tollerare la sorveglianza eseguita dal Servizio SCPT o da persone da esso incaricate

(art. 26 cpv. 2 lett. b LSCPT), alle POC incombe l'obbligo accessorio (cfr. messaggio del 27 febbraio 2013 concernente la LSCPT, ad art. 26 cpv. 2, FF *2013* 2283 2337) di permettere al Servizio SCPT l'esecuzione di collegamenti test in relazione all'ordine di una sorveglianza, al fine di verificare il corretto funzionamento di quest'ultima. Per l'esecuzione dei collegamenti test, le POC devono garantire senza indugio al Servizio SCPT o alle persone da esso incaricate l'accesso ai loro impianti (cfr. art. 53 cpv. 1).

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

Nel *capoverso 1 lettera b numero 1* sono adeguati i rimandi ai dati finora disciplinati nell'articolo 20. In tale articolo è ora disciplinata la verifica dei dati degli utenti dei servizi di telefonia mobile, nell'articolo 20*a* la relativa prova dell'identità per le persone fisiche e nell'articolo 20b la prova dell'identità delle persone giuridiche. Nel *numero 2,* agli «ulteriori dati di contatto» è aggiunto il loro periodo di validità. Per periodo di validità s'intende il periodo di tempo (data di inizio ed eventualmente di fine) in cui gli «ulteriori dati di contatto» sono o erano disponibili presso la POC. Come «ulteriori dati di contatto» la POC può ad esempio fornire ulteriori indirizzi, numeri di telefono e indirizzi di posta elettronica a essa noti. La POC rende noti i dati a sua disposizione. Non ha l'obbligo di rilevare senza lacune e aggiornare i dati di contatto attuali dei loro clienti.

Il *capoverso 1 lettera c* subisce per analogia le stesse modifiche della lettera b. 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 forniti i dati rilevati per l'identificazione degli utenti con mezzi adeguati conformemente all'articolo 19. La prassi ha evidenziato che, in considerazione della molteplicità delle possibilità d'identificazione e di rilevamento dei dati, non si può prestabilire una struttura di dati fissa. Le indicazioni possono quindi essere trasmesse senza una struttura, ma devono essere provviste di una designazione adeguata affinché le autorità legittimate capiscano meglio il significato delle informazioni trasmesse, ad esempio MSISDN, numero della carta di credito, numero del documento d'identità, numero ID, boarding pass, MRZ, nome utente IPASS.

La versione tedesca della frase introduttiva del *capoverso 1 lettera d* è adeguata sotto il profilo redazionale in modo da rispettare la parità di genere nella lingua («von der oder dem Teilnehmenden»).

Il *capoverso 1 lettera d numero 2* subisce due modifiche. 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 carte SIM che possono essere usate contemporaneamente in diverse apparecchiature terminali (cosiddette offerte multiSIM o multidevice). Ne risulta una gerarchia all'interno dell'abbonamento: un *master* (numero principale) e ulteriori *slave* (numeri secondari). In alcuni abbonamenti questa gerarchia può essere modificata dall'utente stesso, vale a dire che quest'ultimo può decidere quale carta SIM usa il numero principale. Ne consegue che a un'IMSI sono assegnati più MSISDN. Nel caso semplice a un'IMSI è assegnato soltanto un MSISDN. I numeri secondari sono numeri tecnici di regola non noti all'utente. Se vi è soltanto una carta SIM, quest'ultima è il numero principale e non vi

sono numeri secondari. Le offerte multiSIM o multidevice si ripercuotono sulla fornitura di informazioni, sulla sorveglianza, sulla ricerca d'emergenza e sulla ricerca di condannati.

Inoltre, un nuovo identificativo del sistema 5G, il *Generic Public Subscription Identifier* (GPSI), che sta diventando sempre più importante, sostituisce l'*identificativo DSL* menzionato finora a titolo di esempio per gli accessi Internet a banda larga nella rete fissa. Negli esempi della presente ordinanza l'*identificativo DSL* è sostituito ovunque con il *GPSI* poiché gli esempi dovrebbero essere per quanto possibile tipici e attuali. Questo però non significa che l'*identificativo DSL* non debba più essere fornito (questo vale anche per tutti gli altri esempi sostituiti). Il *GPSI* è un identificativo pubblico usato sia all'interno che al di fuori di un sistema 3GPP. Si tratta o di un MSISDN (p. es. +41791234567) o di 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, invece della rete di telefonia mobile, un hotspot WLAN. L'aggiunta 3GPP significa che si tratta di un sistema di telefonia mobile o di un servizio standardizzato secondo il 3GPP (*sistema 3GPP* o servizio *3GPP*).

Un altro identificativo non menzionato negli esempi, ma che, se del caso, deve essere fornito è l'OTO-ID, che designa in modo univoco un accesso domiciliare in fibra ottica (fiber to the home).

Il contenuto del *numero 9* resta invariato. L'espressione «numero SIM» è semplicemente sostituita dall'abbreviazione tecnica universale ICCID (definita 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 con numero SIM. L'abbreviazione ICCID è invece chiara per tutte le forme di SIM.

Nel *numero 10*, accanto all'IMSI dell'ordinanza vigente, è aggiunto l'identificativo SUPI del sistema 5G. Nel sistema 5G a ogni utente è assegnato un Subscription Permanent Identifier (SUPI). Il *SUPI* è univoco su scala mondiale ed è installato nella banca dati dell'utente della rete domestica (UDM/UDR). Il *SUPI* è usato soltanto all'interno del sistema 3GPP. Come *SUPI* può ad esempio essere usato l'*IMSI*. L'apparecchiatura terminale comunica il proprio *SUPI* alla rete esclusivamente in forma criptata (p. es. in occasione dell'annuncio alla rete). 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 (il *GPSI* o il *SUPI* può essere richiesto mediante i tipi di informazione di cui agli art. 36 o 41).

Nel *numero 11* viene corretto un errore. A causa di una svista nella traduzione dello standard ETSI 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 spiegato sopra per il numero 2, possono esservi ulteriori elementi d'indirizzo o identificativi del servizio appartenenti a un servizio di accesso alla rete (p. es. abbonamento di telefonia mobile) oggetto di una richiesta. Questi vanno comunicati in questo campo sotto forma di elenco o di settore (range, da … a). Va inoltre ora indicata anche la durata 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 richiesto. Può ad esempio trattarsi della denominazione dell'abbonamento venduto. A fronte della molteplicità dei servizi disponibili sul mercato, le autorità di perseguimento penale hanno chiesto di aggiungere questo elemento.

Le due frasi introduttive del *capoverso 2* sono state riprese senza modifiche dal capoverso 2 vigente. La *lettera g* precisa che l'IDI è un identificativo nazionale e che la domanda può ora essere presentata anche con il Legal Entity Identifier (LEI, cfr. il commento all'art. 20*b* cpv. 1 lett. b) internazionale. Nella *lettera i* l'*identificativo DSL* è sostituito da *GPSI* (cfr. il commento al cpv. 1 lett. d n. 2). La *lettera j* prevede un nuovo identificativo del sistema 5G (SUPI; cfr. il commento al 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 al cpv. 1 lett. d n. 9).

Il *capoverso 3* primo periodo corrisponde fondamentalmente al terzo periodo del capoverso 2 vigente. Si procede soltanto a una correzione: il criterio secondo la lettera e (numero del documento d'identità) non è più previsto dalla nuova disposizione, poiché si tratta di un criterio univoco e quindi non è necessario aggiungere un secondo criterio. Il *secondo periodo* corrisponde al quarto periodo del capoverso 2 vigente.

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

Nella frase introduttiva del *capoverso 1* si precisa che vanno fornite le indicazioni valide durante il periodo a cui si riferisce la richiesta. Il momento della richiesta può riguardare il presente e il passato, ma non il futuro. Poiché le indicazioni di questo tipo di informazione sono dati dipendenti dall'utilizzazione, le POC con obbligo d'informazione devono conservare soltanto i dati degli ultimi sei mesi. Se la domanda d'informazione riguarda un periodo di più di sei mesi nel passato, le POC devono fornire soltanto gli eventuali dati ancora a loro disposizione.

Per motivi redazionali, il secondo periodo del vigente *capoverso 1* è spostato al *capoverso 2*.

Il *capoverso 1 lettera a* resta invariato.

Nelle *lettere b e c*, in considerazione delle offerte multiSIM e multidevice, gli identificativi sono messi al plurale (cfr. art. 35 cpv. 1 lett. d n. 2) e si precisa che si tratta di identificativi relativi al servizio di accesso alla rete richiesto.

La *lettera c* prevede nuovi identificativi del sistema 5G: SUPI e GPSI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10 «SUPI» e art. 35 cpv. 1 lett. d n. 2 «GPSI»).

Nella *lettera d* è aggiunto un nuovo identificativo del sistema 5G: il *PEI*. Il *Permanent Equipment Identifier* (*PEI*) serve all'identificazione univoca su scala mondiale delle apparecchiature terminali nelle reti di telefonia mobile 5G. Il *PEI* è costituito da un'*IMEI* o un'*IMEISV*. Si precisa inoltre che queste indicazioni sono disponibili soltanto per gli ultimi sei mesi poiché si tratta di dati dipendenti dall'utilizzazione (usage).

Nella *lettera e* 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).

Nella *lettera f,* alla comunicazione del codice PUK (PUK e PUK2) è aggiunta l'indicazione del relativo periodo di validità (cfr. per analogia l'art. 35 cpv. 1 lett. b n. 2). L'indicazione del periodo di validità serve alla distinzione nel caso in cui siano comunicati vari codici PUK. Vanno forniti i codici PUK relativi alla carta SIM oggetto della richiesta.

Per motivi redazionali il secondo periodo del capoverso 1 vigente costituisce ora il nuovo *capoverso 2*. Il contenuto resta invariato. Il capoverso 2 vigente diventa il *capoverso 3*.

Negli esempi del *capoverso 3 lettera a* l'identificativo DSL, meno usuale, è sostituito da GPSI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2).

Nelle *lettere b e c* sono aggiunti i nuovi identificativi SUPI del sistema 5G (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10) e PEI (cfr. art. 36 cpv. 1 lett. d).

La *lettera d* resta invariata.

La *lettera e* è nuova e permette in particolare di rendere più efficiente l'interrogazione del codice PUK. Finora a tal fine erano necessarie due domande di informazione: IR_4_NA e IR_6_NA. Ora, per individuare il codice PUK è necessaria soltanto una domanda di informazioni IR_6_NA.

La *lettera f* è nuova e permette di inoltrare la domanda di informazioni con il criterio del 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 che si può comprare 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 di richiesta 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 è stata accolta e inserita nello standard. Pertanto la disposizione può ora essere integrata.

Art. 37 cpv. 1, frase introduttiva (concerne soltanto il testo tedesco) e lett. b

La versione tedesca della *frase introduttiva* del *capoverso 1* è adeguata sotto il profilo redazionale in modo da rispettare la parità di genere nella lingua.

L'identificativo univoco del servizio (p. es. nome utente, username) nella *lettera b* si riferisce al fornitore. All'occorrenza, serve alle autorità legittimate come criterio di ricerca per altre domande di informazione. Per quanto possibile, l'identificativo del

servizio deve essere accompagnato da una designazione idonea se il suo significato non è chiaro.

Negli esempi della *lettera b* l'identificativo DSL è sostituito da un identificativo del sistema 5G (GPSI; cfr. il commento all'art. 35 cpv. 1 lett. d n. 2).

Art. 38 Tipo di informazione IR_8_IP (NAT): identificazione dell'utenza in caso di indirizzi IP non assegnati univocamente (NAT)

La prassi ha evidenziato che, nel caso di cosiddetti carrier-grade NAT (cgNAT), le domande d'informazione relative all'identificazione dell'utenza per mezzo dell'indirizzo IP e di altri criteri non conducono sempre a risultati univoci. Ciò è dovuto al fatto che nel caso dei cgNAT il fornitore di accesso a Internet (carrier) usa la Network Address Translation (NAT) per tutti o per la maggior parte dei suoi clienti. Di conseguenza è possibile che vari clienti navighino contemporaneamente in Internet con lo stesso indirizzo IP sorgente pubblico e probabilmente anche con lo stesso numero di porta sorgente pubblico (criteri obbligatori della richiesta di informazioni). Come per gli altri tipi di informazione, deve pertanto essere possibile permettere più risultati. La possibilità di risultati plurivoci nel caso di NAT è già stata illustrata nel rapporto esplicativo dell'OSCPT vigente (pag. 39 seg.).

Per tenere conto di quanto illustrato, il *capoverso 1* nonché le *lettere a e b* subiscono adeguamenti redazionali: utente, identificativo dell'utente, identificativo del servizio e servizio di accesso alla rete sono messi al plurale. Inoltre, la versione tedesca del *capoverso 1* è adeguata sotto il profilo redazionale in modo da rispettare la parità di genere nella lingua.

Negli esempi della *lettera b* l'identificativo DSL, meno usato, è sostituito da GPSI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 2).

Le modifiche del *capoverso 2 lettera f* ridefiniscono il momento (ora: momento determinante). Secondo la sentenza del Tribunale amministrativo federale A-6807/2019 il FST deve memorizzare i metadati sull'attribuzione e la traduzione degli indirizzi IP e dei numeri di porta (cfr. art. 21 cpv. 6 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 ricercato (n. 4.5.1 pag. 24). La presente integrazione 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 non deve quindi trovarsi necessariamente all'inizio del contesto di traduzione NAT richiesto (osservato).

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

Nel presente articolo le modifiche sono analoghe a quelle dell'articolo 38 (cfr. sopra). Inoltre le due possibilità di richiesta d'informazioni sono descritte in modo più preciso:

a) se la traduzione NAT si è svolta con l'elemento d'indirizzo sorgente (originating IP address),

b) se la traduzione NAT si è svolta con l'elemento d'indirizzo di destinazione (destination IP address).

L'elemento d'indirizzo sorgente (originating IP address) deve sempre essere fornito nella domanda.

Art. 40 cpv. 1 lett. b, c e d, frase introduttiva (concerne soltanto il testo tedesco) nonché 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 degli ulteriori dati di contatto (cfr. il commento alla modifica analoga dell'art. 35 cpv. 1 lett. b e c).

La *lettera d 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 extra (p. es. multidevice, multiSIM) che hanno più di un identificativo (p. es. MSISDN). Gli altri identificativi sono contemplati dal numero 7.

Secondo la *lettera d numero 6* possono ora essere comunicati i periodi di validità degli stati del servizio, analogamente a quanto previsto per il tipo d'informazione IR_4_NA (art. 35 cpv. 1 lett. d n. 6 vigente). Poiché lo standard ETSI definisce differenti formati di dati per i servizi di accesso alla rete (NA) e i servizi multimedia (TEL), per definire il parametro del periodo di validità, già applicato per i servizi di accesso alla rete (NA), anche per i servizi multimedia era necessario presentare una richiesta di modifica all'ETSI. Ora che l'ETSI ha adeguato lo standard, la presente modifica può essere introdotta.

Nel *numero 7* è inserita l'aggiunta «o assegnati» per segnalare che si tratta anche degli elementi d'indirizzo e degli identificativi assegnati (associated) nell'ambito del servizio, ad esempio per i servizi di telefonia mobile con carte SIM extra. Ne fanno parte anche gli elementi d'indirizzo e gli identificativi aggiunti dopo la registrazione, qualora si tratti di dati sull'utente (subscriber data). Gli elementi d'indirizzo e gli identificativi assegnati temporaneamente in relazione all'utilizzazione (usage data) non sono contemplati qui, bensì dal nuovo tipo d'informazione di cui all'articolo 48*b*. Va ora indicato il periodo di validità degli elementi d'indirizzo e degli indentificativi.

Nel *numero 10* è inserito il nuovo identificativo SUPI del sistema 5G (cfr. il commento all'art. cpv. 1 lett. d n. 10). Inoltre si parla ora dei «relativi» IMSI o SUPI per esprimere che si può trattare di varie IMSI o SUPI (p. es. servizi di telefonia mobile con carte SIM extra).

Nel *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 «relativi» per esprimere che si può trattare di varie ICCID (p. es. servizi di telefonia mobile con carte SIM extra).

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 dell'elaborazione dell'OSCPT del 17 novembre 2017 il corrispondente standard ETSI non conteneva ancora il parametro necessario. Nel frattempo lo standard è stato adeguato e pertanto la trasmissione del «tipo di relazione commerciale» è ora possibile.

Nel *numero 13* è inserito un campo per la trasmissione della «denominazione 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 presentata anche con il criterio del Legal Entity Identifier internazionale (LEI, cfr. il commento all'art. 20*b* cpv. 1 lett. b).

Nella lettera j è inserito un nuovo identificativo del sistema 5G (SUPI) (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 contenuto del *capoverso 3* corrisponde al terzo e al quarto periodo del capoverso 2 vigente, i quali sono spostati nel presente capoverso per motivi redazionali.

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

Nel *capoverso 1* si aggiunge che le richieste si riferiscono a un determinato periodo. Di conseguenza, le risposte sono valide soltanto per il periodo a cui si riferisce la richiesta. Va ricordato che soltanto le POC con obblighi di sorveglianza sono tenute a conservare i metadati degli ultimi sei mesi (obbligo di conservazione dei metadati). Metadati più vecchi possono essere forniti soltanto se disponibili presso la POC. Le POC senza obblighi di sorveglianza forniscono le indicazioni a loro disposizione poiché non hanno l'obbligo di conservare i metadati.

Il *capoverso 1 lettera a* resta invariato.

Nella *lettera b* è aggiunto il termine «relativi» al fine di esprimere che si tratta degli elementi d'indirizzo e degli identificativi assegnati (associated) al servizio richiesto, ad esempio nel caso di servizi di telefonia mobile con carte SIM extra (p. es. multidevice, multiSIM), poiché esse hanno più di un identificativo (p. es. MSISDN).

Nella *lettera c* sono inseriti i nuovi identificativi del sistema 5G: SUPI e GPSI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10 «SUPI» e n. 2 «GPSI»). È inoltre aggiunto il termine «relativi» al fine di esprimere che può trattarsi di vari IMSI e SUPI e che vanno forniti i relativi MSISDN o GPSI (p. es. servizi di telefonia mobile con carte SIM extra).

Nella *lettera d* è inserito un nuovo identificativo del sistema 5G: *PEI* (cfr. art. 36 cpv. 1 lett. d). Si precisa inoltre che le indicazioni sono disponibili per gli ultimi sei mesi, poiché si tratti di dati relativi all'uso (usage).

Nella *lettera e* 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). È inoltre aggiunto il termine «relativi» al fine di esprimere che si può trattare di vari ICCID (p. es. servizi di telefonia mobile con carte SIM extra).

Nella *lettera f,* in riferimento alla comunicazione dei codici PUK e PUK2 è aggiunta l'indicazione del periodo di validità (cfr. il commento alla modifica analoga dell'art. 36 cpv. 1 lett. f).

Il *capoverso 2* corrisponde al secondo periodo del capoverso 1 vigente, che è spostato in questa posizione per motivi redazionali.

Nel *capoverso 3 lettera a* gli esempi vengono 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), poiché s'intendono menzionare soltanto pochi esempi attuali. Ciò non significa tuttavia che il numero di telefono e *TEL URI* non possano più essere usati come criteri di richiesta.

Nella lettera b 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. d).

Le *lettere d* ed *e* restano invariate.

Nelle *lettere f* e *g* sono aggiunti il numero SIM (ICCID) e il codice per la ricarica del credito o per il pagamento del servizio (cfr. il commento all'art. 36 cpv. 2 lett. e ed f).

Art. 42 cpv. 1 lett. c, frase introduttiva e n. 6 e lett. d, cpv. 2, frase introduttiva, lett. g e j nonché cpv. 3

Come per gli altri tipi di informazione su servizi di comunicazione (art. 35, 40 e 43) nel *capoverso 1 lettera c numero 6* è aggiunto un campo per la trasmissione della denominazione del servizio (cfr. il commento all'art. 35 cpv. 1 lett. d n. 13). Nella *lettera d* è inserito un nuovo identificativo del sistema 5G (GPSI; cfr. il commento all'art. 35 cpv. 1 lett. d n. 2).

Nel *capoverso 2 lettera g* si precisa che l'IDI è un identificativo nazionale e che la domanda può contenere anche il Legal Entity Identifier internazionale (LEI, cfr. il commento 20*b* cpv. 1 lett. b). La *lettera j* prevede 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 capoverso 2 vigente.

Art. 42a **Tipo d'informazione IR_51_EMAIL_LAST: informazioni su servizi di posta elettronica**

Il presente tipo d'informazione è nuovo e ha lo scopo di individuare *l'ultima attività rilevante per l'accesso a un servizio di posta elettronica* (per la definizione cfr. n. 39 dell'allegato OSCPT). Da una parte, ciò serve a identificare l'utente del servizio. Dall'altra, il momento dell'ultimo accesso al servizio di posta elettronica è determinante per la cosiddetta conclusione del processo di comunicazione. Infatti, per tutti i messaggi giunti e salvati nella casella di posta elettronica il processo di comunicazione è considerato concluso. Secondo l'articolo 265 CPP, il pubblico ministero può ingiungere di consegnare i messaggi salvati nella casella di posta elettronica il cui processo di comunicazione è concluso. I messaggi che arrivano dopo l'ultimo accesso possono essere individuati dalle autorità legittimate soltanto nell'ambito di una sorveglianza in

tempo reale secondo l'articolo 58 (RT_26_EMAIL_IRI) o l'articolo 59 (RT_27_EMAIL_CC_IRI).

Nella domanda non può essere indicato un momento determinante. Per il presente tipo di informazione le POC devono fornire informazioni soltanto sull'ultima attività rilevante per l'accesso negli ultimi sei mesi prima del momento della domanda. Non devono invece fornire informazioni su attività che hanno preceduto l'ultima attività rilevante. Nel quadro di questa informazione non è previsto il rilevamento retroattivo delle attività di accesso al servizio di posta elettronica (cronologia). La cronologia e i metadati storici possono essere rilevati soltanto mediante la sorveglianza retroattiva HD_30_EMAIL (art. 62, cfr. il commento all'art. 62).

Il *capoverso 1* disciplina le indicazioni da fornire. Secondo la *lettera a* deve essere comunicato l'identificativo univoco dell'utente nel contesto del fornitore (p. es. il numero cliente), sempreché il fornitore ne abbia assegnato uno. L'«identificativo univoco del servizio» di cui alla *lettera b* designa in modo univoco il servizio di posta elettronica (casella di posta elettronica) a cui si riferisce la risposta. La *lettera c* enumera le indicazioni da fornire sull'origine del collegamento in occasione dell'ultima attività rilevante per l'accesso.

Il *capoverso 2* disciplina il contenuto della domanda di informazioni. A titolo di esempio sono menzionati l'indirizzo di posta elettronica e il nome utente. Questo criterio deve essere sufficientemente preciso affinché il fornitore possa individuare il servizio di posta elettronica (mailbox) in questione.

Art. 43 cpv. 1 lett. c, frase introduttiva e n. 6, cpv. 2, frase introduttiva lett. g, i ed 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), nel *capoverso 1 lettera c numero 6* è aggiunto un campo per la trasmissione della denominazione del servizio (cfr. il commento all'art. 35 cpv. 1 lett. d n. 13).

Nel *capoverso 2 lettera g* è aggiunta la possibilità della domanda mediante il Legal Entity Identifier internazionale (LEI, cfr. il commento all'art. 20*b* cpv. 1 lett. b).

Nella *lettera i* si precisa che si tratta di un elemento d'indirizzo o di un identificativo del servizio oggetto della richiesta (servizio di telecomunicazione o servizio di comunicazione derivato). La domanda d'informazione può ad esempio riguardare un determinato push token che va qui indicato. Il push token è un identificativo specifico dell'applicazione e dell'apparecchiatura usato per i messaggi di un'applicazione. Con il push token si garantisce che la comunicazione del servizio in questione possa essere inviata a una determinata applicazione su un determinato apparecchio (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 richiesta. 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 capoverso 2 vigente

Art. 43a Tipo di informazione IR_52_COM_LAST: informazioni su altri servizi di telecomunicazione o servizi di comunicazione derivati

Questo tipo d'informazione è nuovo e permette di chiedere le indicazioni sull'ultima *attività rilevante per l'accesso a un altro servizio di telecomunicazione o di comunicazione derivato* (per la definizione cfr. n. 41 dell'allegato OSCPT). Da una parte, ciò serve a identificare l'utente del servizio. Dall'altra il momento dell'ultimo accesso al servizio è determinante per la cosiddetta conclusione del processo di comunicazione. Infatti, in analogia alla posta elettronica, al momento dell'ultimo accesso al servizio, il processo di comunicazione di tutti i messaggi giunti e salvati precedentemente è considerato concluso.

Secondo l'articolo 265 CPP, il pubblico ministero può ingiungere di consegnare i messaggi salvati dal relativo servizio il cui processo di comunicazione è concluso.

Nella domanda non può essere indicato un momento determinante. Per il presente tipo di informazione le POC devono fornire informazioni soltanto sull'ultima attività rilevante per l'accesso negli ultimi sei mesi prima del momento della domanda.

Non devono invece fornire informazioni su attività che hanno preceduto l'ultima attività rilevante. Nel quadro di questa informazione non è previsto il rilevamento retroattivo delle attività di accesso al servizio di posta elettronica (cronologia).

Il *capoverso 1* disciplina le indicazioni da fornire. Secondo la *lettera a* deve essere comunicato l'identificativo univoco dell'utente nel contesto del fornitore (p. es. il numero cliente), sempreché il fornitore ne abbia assegnato uno. L'«identificativo univoco del servizio» di cui alla *lettera b* designa in modo univoco nel contesto del fornitore il servizio di telecomunicazione o di comunicazione derivato a cui si riferisce la risposta. La *lettera c* enumera le indicazioni da fornire sull'origine del collegamento in occasione dell'ultima attività rilevante per l'accesso.

Il *capoverso 2* disciplina il contenuto della domanda di informazioni. A titolo di esempio sono menzionati l'indirizzo dell'utente, lo pseudonimo e il push token (cfr. il commento all'art. 43 cpv. 2 lett. i). Il criterio deve essere sufficientemente preciso affinché il fornitore possa individuare il servizio di telecomunicazione o di comunicazione derivato in questione.

Art. 44 cpv. 1, frase introduttiva, lett. c e f nonché cpv. 3 lett. c e d

Nella versione italiana nella frase introduttiva «informazioni» è sostituito da «indicazioni», in adeguamento alla terminologia di altri articoli dell'OSCPT. Le altre modifiche concernono soltanto la versione tedesca, adeguata sotto il profilo redazionale in modo da rispettare la parità di genere nella lingua.

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

Il *capoverso 1* è adeguato alla terminologia dell'articolo 20*a* («documento» invece di «documento d'identità»).

Nel capoverso 2 è inserito un nuovo identificativo del sistema 5G (SUPI; cfr. il commento all'art. 35 cpv. 1 lett. d n. 10). Il contenuto del resto del capoverso resta invariato. L'abbreviazione *ICCID* è spiegata nell'allegato dell'OSCPT.

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 Tipo di informazione IR_20_CONTRACT: copia del contratto

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 un nuovo identificativo del sistema 5G (SUPI; cfr. il commento all'art. 35 cpv. 1 lett. d n. 10). Il contenuto del resto del capoverso resta invariato. L'abbreviazione *ICCID* è spiegata nell'allegato dell'OSCPT.

Art. 48 Tipo di informazione IR_21_TECH: dati tecnici

Il *capoverso 1* precisa che questa domanda d'informazione si riferisce agli elementi di rete «nella localizzazione richiesta».

Nel *capoverso 2 lettera a* l'enumerazione a titolo esemplificativo degli identificativi degli elementi di rete è sostituita dall'espressione generale «identificativi della cella o della zona». Il nuovo termine «identificativo della cella» comprende gli esempi del testo vigente CGI (2G e 3G), ECGI (4G) e NCGI[25] (5G). I tre esempi di identificativi della zona (SAI[26], RAI[27] e TAI[28]) sono sostituiti dall'iperonimo «identificativo della zona». Tali modifiche redazionali non si ripercuotono tuttavia sulla fornitura di CGI, ECGI, SAI, RAI e TAI. Se disponibili, essi vanno tuttora forniti.

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. Per questo motivo, in alternativa agli identificativi degli elementi

25 **NCGI** (New Radio Cell Global Identity): identificativo non modificato di una cella nelle reti di telefonia mobile di quinta generazione (5G), secondo 3GPP TS 23.003, Clause 19.6A. Il NCGI è costituito dalla concatenazione dell'identificativo PLMN (MCC + MNC) nonché del NR Cell Identity (NCI) ed è univoco su scala mondiale.

26 **SAI** (Service Area Identity): identificativo non modificato della zona di copertura di un servizio (Service Area), usato in reti di telefonia mobile per il mobility management (cfr. 3GPP TS 23.003, Clause 12.5).

27 **RAI** (Routing Area Identity): identificativo non modificato per una zona di routing (Routing Area), usato in reti di telefonia mobile nel settore della trasmissione di pacchetti di dati per il mobility management (cfr. 3GPP TS 23.003, Clause 4.2).

28 **TAI** (Tracking Area Identity identificativo non modificato per una zona di tracciamento (Tracking Area), usato in reti di telefonia mobile della quarta generazione per il mobility management (cfr. 3GPP TS 23.003, Clause 19.4.2.3).

di rete è aggiunta un'altra designazione idonea (p. es. nome dell'hotspot in alternativa a 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 esplicativodato 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 nel quale si ricevono indicazioni sul fornitore dell'hotspot. Se il nome dell'hotspot non è sufficientemente chiaro e può quindi dare adito a confusione, possono essere usate altre designazioni sufficientemente chiare, ad esempio una breve designazione della localizzazione. La presente modifica non significa che il BSSID non debba essere fornito. Se noto, esso deve infatti essere fornito. 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 provvisti di marche temporali.

Nel *capoverso 3 lettera a* in riferimento alla localizzazione è aggiunta l'espressione «richiesta» per precisare che la domanda può essere fatta indicando le coordinate geografiche della localizzazione, vale a dire che la richiesta si riferisce a tutti gli elementi di rete della POC di tale localizzazione. Secondo la *lettera b* è possibile anche una richiesta riguardante un determinato elemento della rete di tale localizzazione. Si aggiunge che per tale richiesta, invece di un identificativo standardizzato, può essere usata anche un'altra designazione idonea (p. es. nome dell'hotspot). Inoltre, come nel capoverso 2, è usata l'espressione generale identificativo della cella o della zona (cfr. sopra).

Art. 48a Tipo di informazione IR_53_ASSOC_PERM: informazioni su identificativi assegnati a lungo termine

Per la fornitura di servizi di telecomunicazione dell'IP Multimedia Subsystem (IMS), invece degli identificativi permanenti del servizio o dell'apparecchio, possono essere usati anche identificativi assegnati a lungo termine. È pertanto introdotto questo nuovo tipo di informazione che permette di richiedere gli identificativi assegnati a lungo termine (IMPI per l'IMPU pubblica 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 OSCPT 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).

Art. 48b Tipo di informazione IR_54_ASSOC_TEMP: informazioni immediate su identificativi assegnati per breve tempo

Nel caso di servizi di telefonia mobile 5G, invece degli identificativi permanenti del servizio o dell'apparecchio, possono essere usati sussidiariamente anche identificativi

assegnati a breve termine (temporanei). Questo nuovo tipo di informazione è introdotto per poter chiedere in tempo reale gli identificativi permanenti assegnati a un identificativo temporaneo.

I dettagli sono disciplinati nell'allegato 1 dell'OE-SCPT. Esempio: SUPI per SUCI e viceversa.

I casi di applicazione più importanti sono i seguenti.

Per 5G, un'autorità legittimata rileva con i propri apparecchi radiotecnici (p. es. false base station) un identificativo temporaneo (p. es. 5G-S-TMSI/5G-GUTI o un SUCI criptato), dopodiché presenta una domanda secondo il presente nuovo tipo di informazione in modo da ricevere subito il relativo identificativo permanente, ossia un SUPI.

Il tempo di risposta di questo nuovo tipo di informazione deve essere molto breve (entro alcuni secondi), poiché gli identificativi temporanei cambiano spesso (p. es. almeno in occasione di ogni service request o paging occasion oppure ancora più spesso). Questa informazione deve pertanto essere chiesta e fornita mediante una nuova interfaccia d'interrogazione del tipo LI_HIQR. La richiesta (domanda di informazione) può contenere soltanto un singolo identificativo (cpv. 2 lett. a). Poiché si tratta di un'informazione in tempo reale non può essere indicato un momento determinante. Si applica quindi il momento dell'inoltro della richiesta. Richieste retroattive non sono possibili.

L'indicazione della localizzazione (cpv. 2 lett. b) è necessaria poiché l'identificativo temporaneo è univoco solo localmente. In un altro luogo, lo stesso identificativo temporaneo nello stesso momento può risultare assegnato a un altro identificativo permanente.

Esempi per richieste: SUCI, 5G-S-TMSI o 5G-GUTI.

Art. 48c Tipo di informazione IR_55_TEL_ADJ_NET: determinazione delle reti immediatamente adiacenti per i servizi di telefonia e multimedia

Questo tipo di informazione è introdotto per risolvere problemi specifici degli identificativi degli autori di reati in presenza di numeri di telefono falsificati (spoofing) o sconosciuti di chi telefona o del mittente di una comunicazione. Ciò può essere utile, nel caso ad esempio di una minaccia anonima di bomba, per potere seguire la traccia della chiamata o del messaggio anonimi.

I metadati storici (HD) di comunicazioni e tentativi di comunicazioni conservati ai fini della sorveglianza retroattiva contengono gli elementi di indirizzo dei partecipanti alla comunicazione (chi con chi). Se tuttavia il numero di telefono è falsificato o sconosciuto, le autorità legittimate hanno bisogno di un mezzo per poter ricostruire la chiamata o la comunicazione.

Il fornitore deve trasmettere le indicazioni sulla rete immediatamente adiacente «da» e da quella immediatamente adiacente «a», nella misura in cui tali reti erano coinvolte nella comunicazione o nel tentativo di comunicazione oggetto della richiesta. Non deve tuttavia fornire indicazioni su eventuali altre reti precedenti o successive di una comunicazione. Esempio: una chiamata è stata effettuata dalla rete del fornitore A

mediante la rete di transito del fornitore B alla rete del fornitore C. Se è il destinatario della richiesta, il fornitore B deve indicare i fornitori A («da») e C («a») come reti immediatamente adiacenti. Se il destinatario della richiesta è A, esso deve indicare il fornitore B («a»; non esiste una rete «da»). Se il destinatario della richiesta è C, esso deve indicare il fornitore B («da», non esiste una rete «a»).

Il presente tipo di informazione istituisce per i FST con obblighi integrali (ovvero FST che il Servizio SCPT non qualifica come fornitori con obblighi di sorveglianza ridotti) e i FSCD con obblighi di sorveglianza supplementari (art. 52) un obbligo di conservazione di sei mesi dei relativi metadati (cfr. anche art. 21 cpv. 6 lett. c e art. 61 lett. j). Poiché ogni fornitore può controllare soltanto 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 tal modo l'autorità legittimata può ricostruire o seguire la comunicazione in questione mediante la richiesta di informazioni ai singoli fornitori.

Questo nuovo tipo di informazione istituisce una procedura standardizzata per la ricostruzione di comunicazioni o tentativi di comunicazione. L'emolumento e le indennità sono fissati nell'OEm-SCPT. I tempi di trattamento sono disciplinati nell'articolo 14 OE-SCPT.

Art. 50 cpv. 5-10

Il *capoverso 5* resta materialmente invariato.

Capoverso 6: nel caso di servizi di telefonia mobile con carte SIM extra (p. es. multidevice o multiSIM per ulteriori apparecchiature quali smartphone, tablet, smartwatch) devono essere sorvegliati tutti gli apparecchi terminali, i numeri e le SIM associati all'identificativo principale sorvegliato (Target ID); ad esempio, 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). Sono eccettuati gli identificativi accessori del target (p. es. numeri tecnici) associati solo a una determinata apparecchiatura terminale o a una determinata SIM. Per le apparecchiature terminali supplementari e per i numeri o le SIM aggiuntivi non sono riscossi emolumenti o versate indennità. Se necessario, per le relative sorveglianze il fornitore può chiedere ulteriori LIID (lawful interception identifier, ossia identificativi assegnati specificamente per la sorveglianza) al Servizio SCPT. Se non auspica la sorveglianza globale di tutte le apparecchiature, di tutti numeri e di tutte le SIM associati all'identificativo principale, l'autorità ordinante deve menzionarlo esplicitamente nell'ordine.

Se, nel caso di una sorveglianza in tempo reale già attiva o di una determinazione periodica della posizione, al servizio sorvegliato si aggiunge una nuova apparecchiatura, un nuovo numero o una nuova SIM, devono essere sorvegliati anche questi. Per queste sorveglianze aggiuntive non sono riscossi ulteriori emolumenti o versate ulteriori indennità, Se necessario, il fornitore può chiedere un ulteriore LIID al Servizio SCPT.

Il *capoverso 7* precisa l'obbligo dei FST di sopprimere i criptaggi attuati da o per loro (art. 26 cpv. 2 lett. c LSCPT). Per «criptaggi attuati per loro» s'intendono criptaggi che sono stati effettuati mediante la chiave pubblica del fornitore. Anche se in senso

stretto non è stato il fornitore ad apportare il criptaggio, esso è in grado di sopprimerlo poiché dispone della chiave privata adeguata. Si chiarisce inoltre che anche i FSCD con obblighi di informazione o sorveglianza supplementari secondo gli articoli 22 o 52 sono tenuti a sopprimere i criptaggi attuati da o per loro. Questi FSCD hanno pertanto i medesimi obblighi dei FST. L'obbligo menzionato nell'articolo 26 capoverso 2 lettera c LSCPT di sopprimere i criptaggi attuati si applica pertanto anche ai FSCD con obblighi d'informazione supplementari.

In caso di procedure di criptaggio asimmetriche (criptaggio con chiave pubblica del destinatario e decriptaggio con chiave privata del destinatario), di regola un fornitore non può più sopprimere un criptaggio da esso stesso apportato. I dati criptati possono essere decriptati soltanto dai destinatari con la cui chiave pubblica sono stati criptati. Un'eventuale chiave pubblica aggiuntiva del fornitore non deve tuttavia rivelare il fatto della sorveglianza.

Se per l'invio ricorre a una procedura di criptaggio asimmetrica, il fornitore deve rilevare i dati da sorvegliare e trasmetterli prima di attuare il criptaggio.

Viceversa, nel ricevere i dati criptati con la propria chiave pubblica, il fornitore deve rilevare i dati da sorvegliare e decriptarli con la propria chiave privata prima di trasmetterli al Servizio SCPT o all'autorità.

Per «punti idonei» s'intendono tutti i punti in cui il fornitore ha il controllo fattuale e giuridico della comunicazione o del salvataggio dei dati e in cui i dati da sorvegliare possono essere rilevati senza criptaggio o in cui il fornitore può sopprimere il criptaggio.

Il *capoverso 8* amplia gli obblighi nel contesto della sorveglianza in tempo reale di servizi di telefonia mobile estendendoli alla sorveglianza delle banche dati tecniche degli utenti (p. es. HLR[29], HSS[30] e UDM[31]), ai fini del rilevamento e della fornitura di metadati importanti dell'identificativo sorvegliato. Le banche dati contengono in particolare informazioni sulla rete che fornisce il servizio, sulle modifiche degli identificativi del servizio e dell'apparecchio assegnati, sugli eventi relativi alla localizzazione, sul cambio dell'elemento di rete che fornisce il servizio nonché sugli eventi di identificazione e di autenticazione.

Secondo il *capoverso 9,* per la sorveglianza in tempo reale nell'IMS va, se del caso, attivata la determinazione da parte della rete dei dati di localizzazione dell'identificativo sorvegliato.

Il *capoverso 10* stabilisce che le modifiche di apparecchiature terminali o di SIM connesse all'abbonamento o al prepaid sorvegliato devono essere osservate dalle POC e che queste ultime devono adeguare autonomamente la sorveglianza alle modifiche. Questo lavoro supplementare delle POC non è indennizzato. Nemmeno il Servizio

29 **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 degli utenti (p. es. IMSI, MSISDN, configurazione, profili del servizio) e la rete attuale che fornisce il servizio.

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

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

SPCT può chiedere un emolumento supplementare per il lavoro aggiuntivo. Se necessario, il fornitore può chiedere un ulteriore LIID per installare altre sorveglianze necessarie.

Art. 53 cpv. 1

Questa disposizione precisa che nel caso delle POC che hanno soltanto l'obbligo di tollerare l'accesso ai propri impianti è possibile eseguire i collegamenti test necessari. I collegamenti test sono disciplinati dall'articolo 30. Un collegamento test è necessario in particolare quando occorre preparare una sorveglianza ordinata o controllare la qualità di una sorveglianza in corso, anche se sotto il profilo tecnico questa è attuata dal Servizio SCPT.

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

Il *capoverso 1* resta invariato.

5G rende possibili registrazioni multiple (multiple registrations) o connessioni multiple (multiple attachments) nelle stesse o in diverse reti che forniscono il servizio, il che rende possibile anche un cambio dell'obiettivo della sorveglianza (target) tra le diverse reti e tecnologie[32].

Il *capoverso 2 lettera a* è completato affinché nel quadro della sorveglianza in tempo reale le autorità siano in futuro informate sulla tecnologia usata da un 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 per la connessione e la sconnessione 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.

Le *lettere b e d* restano invariate.

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. d «PEI»).

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 in particolare la modifica del supporto al servizio (service support), ad esempio modifiche del PDP context, del bearer o della sessione PDU, e l'aggiornamento della posizione del target, ad esempio location update e mobility registration update. Della gestione della mobilità fanno ad esempio parte GMM, EMM e mobility registration.

32 Cfr. 3GPP TS 33.501 sezione 6.3.2.

Nella *lettera h* si procede a un adeguamento redazionale al tenore dell'articolo 56 capoverso 2 lettera e numero 9 e alla sostituzione di «momentanea» con «attuale». Inoltre si precisa che i dati di localizzazione devono essere determinati per quanto possibile dalla rete e contrassegnati in modo corrispondente. I dati di localizzazione determinati dalla rete sono più affidabili di quelli determinati dall'apparecchiatura terminale, poiché questi ultimi potrebbero essere falsificati. Vanno tuttavia forniti tutti i dati di localizzazione disponibili, anche quelli dell'apparecchiatura terminale, contrassegnati in modo corrispondente. La caratterizzazione «determinati dalla rete» o «determinati dall'apparecchiatura terminale» aiuta le autorità a valutare quanto possano fidarsi dei dati di localizzazione. Nel caso dei sistemi di telefonia mobile di quarta (EPS) e di quinta generazione (5GS) possono essere disponibili marche temporali e indicazioni sull'età dei dati di localizzazione. Se del caso, vanno trasmesse anche queste. Per *età* s'intende il periodo intercorso tra la determinazione effettiva della posizione e la trasmissione dell'informazione.

La nuova *lettera i* disciplina la trasmissione di metadati importanti rilevati in occasione della sorveglianza di banche dati tecniche degli utenti quali HLR, HSS e UDM (cfr. il commento all'art. 50 cpv. 8). Si tratta di:

- informazioni sulla rete precedente e quella attuale che ha fornito o fornisce il servizio, ossia eventi del tipo «serving system» (*rete che fornisce il servizio*, p. es. Serving PLMN, VPLMN ID);
- informazioni sulla modifica degli identificativi dei servizi e delle apparecchiature terminali assegnate (p. es. IMSI, MSISDN, IMEI, SIP-URI, IMPI), ossia eventi del tipo susbcriber record change;
- informazioni sugli eventi relativi alla localizzazione e, se del caso, il loro motivo, ad esempio eventi del tipo register location / cancel location / register termination;
- informazioni sul cambio dell'elemento di rete che fornisce il servizio (p. es. SGSN, MME, MSC, AMF);
- informazioni sugli eventi di identificazione e di autenticazione del target (p. es. diritto d'accesso a un PWLAN ricevuto).

Il *capoverso 3* subisce una modifica redazionale in quanto il «tipo di tecnologia di telefonia mobile», sinora contenuto in ogni lettera del capoverso, è menzionato nella frase introduttiva.

Nella *lettera a* si procede a due modifiche, analogamente all'articolo 48 capoverso 2 lettera a (cfr. il relativo commento): invece di elencare a titolo esemplificativo i singoli identificativi è inserita l'espressione generale «identificativo della cella o della zona» e, in alternativa a BSSID, è aggiunta «un'altra designazione idonea» (p. es. nome dell'hotspot). È sufficiente una designazione sufficientemente precisa dell'accesso WLAN, ossia la designazione trasmessa deve identificare senza ombra di dubbio l'accesso WLAN della localizzazione (cfr. anche il commento all'art. 48 cpv. 2 lett. a e cpv. 3 lett. b). Il nome dell'hotspot deve essere trasmesso nel parametro *SSID.*

Il contenuto delle *lettere b* e *c* resta invariato. Nella lettera c ci si limita a sostituire «punto di accesso WLAN» con «accesso WLAN» (cfr. il commento alla sostituzione di espressioni, cpv. 1).

Le integrazioni delle *lettere d* ed *e* riguardano i dati di localizzazione in caso di accesso non 3GPP inaffidabile (ingl. «untrusted», *lett. d*) e affidabile (ingl. «trusted», *lett. e*) alla rete di telefonia mobile. Con «inaffidabile» e «affidabile» si distingue il tipo di accesso dal punto di vista del fornitore del servizio di telefonia mobile.

Il fornitore di telefonia mobile non si fida degli accessi designati come inaffidabili. Si tratta perlopiù di accessi di terzi, ossia di accessi gestiti da altri fornitori di cui il fornitore di telefonia mobile conosce soltanto i dati di connessione IP (cfr. anche le spiegazioni nell'allegato «Definizioni e abbreviazioni»). Tra l'apparecchiatura terminale del target e il gateway (evolved packet data gateway) del fornitore di telefonia mobile è istituita una connessione sicura (criptata, VPN). Il fornitore di telefonia mobile comunica l'indirizzo IP sorgente pubblico visibile e, se del caso, il numero di porta sorgente dell'apparecchiatura terminale del target.

L'aggiunta «affidabile» significa che il fornitore si fida di questo accesso poiché è perlopiù gestito da lui stesso. Un tale accesso è designato anche come trusted WLAN access network (TWAN). Se, oltre alla designazione dell'accesso alla rete (identificativo TWAN), è noto anche l'indirizzo postale, va comunicato anche quest'ultimo.

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

Il *capoverso 1* è semplificato ed è ora costituito soltanto dal primo periodo del capoverso 1 vigente. Definisce i servizi interessati dal tipo di sorveglianza RT_24_TEL_IRI.

Il nuovo *capoverso 2* è costituito dal secondo periodo del capoverso 1 vigente e specifica i metadati da trasmettere in tempo reale. La *lettera a* corrisponde all'attuale capoverso 1 lettera a. Nella *lettera b* è inserito un nuovo identificativo del sistema 5G: SUPI (cfr. il commento all'art. 35 cpv. 1 lett. d n. 10). Le *lettere c* e *d* corrispondono alle lettere c e d del capoverso 1 con un adeguamento redazionale della lettera c della versione tedesca in modo da rispettare la parità di genere nella lingua.

I numeri 1, 3, 5, 6, 7 e 8 della *lettera e* corrispondono a quelli del vigente capoverso 1 lettera e. Nei *numeri 2* e *4* sono inseriti nuovi identificativi del sistema 5G: GPSI e PEI (cfr. il commento agli art. 35 cpv. 1 lett. d n. 2 «GPSI» e 36 cpv. 1 lett. d «PEI»). Il *numero 9* precisa che la disposizione e applicabile solo alla telefonia mobile e a WLAN. Inoltre, sancisce che i dati di localizzazione devono essere determinati per quanto possibile dalla rete e contrassegnati in modo corrispondente (cfr. il commento all'art. 54 cpv. 2 lett. h). Nel caso di EPS e 5GS i dati di localizzazione devono essere completati dalla marca temporale connessa e dall'età dei dati di localizzazione (cfr. il commento all'art. 54 cpv. 2 lett. h). Infine «punto di accesso WLAN è sostituto da «accesso WLAN» (cfr. il commento alla sostituzione di espressioni, cpv. 1).

La *lettera f* disciplina la trasmissione di importanti metadati che possono essere rilevati in occasione della sorveglianza di banche dati tecniche degli utenti (cfr. il commento agli art. 54 cpv. 2 lett, i) quali HLR, HSS e UDM (cfr. il commento all'art. 50 cpv. 8).

Invece di ripetere qui in un capoverso 3 i dati di localizzazione identici a quelli dell'articolo 54 capoverso 3, il capoverso 2 lettera e numero 9 rinvia a tale disposizione. Si può quindi rinunciare a un capoverso 3 nell'articolo 56.

Art. 56a Tipo di sorveglianza RT_56_POS_IMMED: determinazione unica e immediata della posizione mediante la rete

Nella presente ordinanza *localizzazione* e *posizione* hanno un significato diverso. Finora vi erano solo dati di localizzazione (location information). Per *localizzazione* s'intende la cella o la zona in cui si trova l'obiettivo della sorveglianza (target). La *localizzazione* è di norma solo un'individuazione approssimativa del luogo in cui si trova effettivamente il target (apparecchiatura terminale) e corrisponde perlopiù al luogo in cui si trova l'antenna con cui è collegato o era collegato l'ultima volta il target. I dati di localizzazione possono essere molto imprecisi e dipendono dalla portata dell'antenna. Nelle zone di campagna la posizione effettiva del target può divergere fino a 30 km da quella dell'antenna. Spesso la *localizzazione* è già nota alla rete di telefonia mobile e in tal caso non deve essere determinata. Può tuttavia succedere che la localizzazione debba essere determinata dalla rete mobile, ad esempio nel caso di una ricerca d'emergenza EP_35_PAGING o di una sorveglianza HD_31_PAGING.

Per *posizione* s'intende invece il luogo preciso in cui si trova effettivamente il target (apparecchiatura terminale) al momento della determinazione della posizione. La determinazione della posizione è una nuova funzione nella rete di telefonia mobile. La determinazione della posizione ai sensi della LSCPT (LALS, Lawful Access to Location Services) costituisce una novità ed è considerata una sorveglianza ai sensi dell'articolo 269 CPP. È eseguita soltanto su ordine delle autorità legittimate a ordinare una sorveglianza. L'ordine deve essere approvato dal giudice delle misure coercitive. Sono introdotti 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 effettuare la determinazione unica e immediata della posizione mediante una corrispettiva funzione della rete (LALS). Vanno determinate le posizioni di tutte le apparecchiature terminali associate all'identificativo sorvegliato (Target ID).

Le prescrizioni tecniche di esecuzione sono emanate dal DFGP nell'OE-SCPT e nel suo allegato (*cpv. 2*). Finora non sono ancora state fatte esperienze pratiche con questa nuova determinazione unica della posizione mediante LALS. 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 ritardi le posizioni delle apparecchiature terminali.

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

Secondo la *lettera d,* se la posizione non è stata determinata va comunicato il motivo della mancata determinazione (codice d'errore) e, se possibile, l'ultima localizzazione

nota nel momento in questione della cella dell'apparecchiatura terminale, ossia la localizzazione dell'antenna della cella che fornisce il servizio.

Art. 56*b* Tipo di sorveglianza RT_57_POS_PERIOD: determinazione periodica della posizione mediante la rete

Le osservazioni preliminari sull'articolo 56*a* valgono anche per il presente articolo. Si tratta del secondo tipo di sorveglianza della determinazione della posizione mediante LALS: la determinazione periodica della posizione mediante la rete.

Secondo il *capoverso 1,* il fornitore del servizio di telefonia mobile deve effettuare la determinazione periodica della posizione mediante una funzione di determinazione della posizione della rete (LALS). Vanno determinate le posizioni di tutte le apparecchiature terminali mobili associate all'identificativo sorvegliato (Target ID).

Le prescrizioni tecniche di esecuzione sono emanate dal DFGP nell'OE-SCPT e nel suo allegato (*cpv. 2*). Il DFGP può ad esempio prevedere che la posizione sia determinata a intervalli fissi predefiniti. Poiché finora non sono state fatte esperienze pratiche con la nuova determinazione periodica della posizione mediante LALS, in particolare per quanto riguarda le risorse e il tempo necessario per la determinazione della posizione, non si possono ancora stabilire prescrizioni concrete in merito a parametri tecnici quali frequenza, periodicità e distanza temporale minima tra due determinazioni 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 ritardi le posizioni delle apparecchiature terminali.

Secondo il *capoverso 3 lettera d* se la posizione non è stata determinata va comunicato il motivo della mancata determinazione (codice d'errore) e, se possibile, l'ultima localizzazione nota nel momento in questione della cella dell'apparecchiatura terminale, ossia la localizzazione dell'antenna della cella che fornisce il servizio.

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

Le *lettere a–d, f* e *i* restano materialmente invariate.

Nelle *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. d «PEI»).

Secondo la *lettera g numero 1* vanno trasmesse, se disponibili, le marche temporali connesse ai dati di localizzazione nel sistema delle tecnologie di telefonia mobile di quarta (EPS) e quinta generazione (5GS). I *numeri 2 e 3* restano invariati.

In considerazione delle esperienze maturate nella prassi, nella *lettera h* è inserita la possibilità di un'altra designazione idonea quale «il nome dell'hotspot», anche se non si tratta di identificativi univoci. È tuttavia sufficiente una designazione sufficientemente precisa dell'accesso WLAN, vale a dire che la designazione trasmessa deve

identificare l'accesso WLAN nel luogo in questione in maniera sufficientemente precisa (cfr. anche il commento all'art. 48 cpv. 2 lett. a). Il nome dell'hotspot va trasmesso con il parametro *SSID*.

La *lettera i* riprende 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 lettera i vigente.

Le nuove *lettere k* e *l* disciplinano la trasmissione dei dati di localizzazione nel caso di accessi non 3GPP sia inaffidabili che affidabili alla rete di telefonia mobile e corrispondono alle modifiche dell'articolo 54 capoverso 3 lettere d ed e (cfr. il relativo commento).

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

Nelle *lettere b* e *d* 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. d «PEI»).

Per la precisazione nella frase introduttiva della *lettera g* riguardante «i dati di localizzazione, determinati per quanto possibile dalla rete e contrassegnati in modo corrispondente», si veda il commento all'art. 56 capoverso 1 lettera e n. 9. Nel *numero 1*, in analogia all'articolo 60 lettera g numero 1, sono aggiunte «le marche temporali connesse» (cfr. il relativo commento). I *numeri 2* e *3* restano invariati. Il nuovo *numero 4* disciplina la trasmissione dei dati di localizzazione nel caso di un cosiddetto accesso non 3GPP inaffidabile alla rete di telefonia mobile ed è paragonabile alla modifica dell'articolo 54 capoverso 3 lettera d (cfr. il relativo commento).

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

La *lettera i* resta invariata sotto il profilo materiale. Il *primo punto del numero 4* subisce una modifica redazionale per chiarire che il rimando alla lettera g si riferisce ai dati di localizzazione. Nel *secondo punto* il termine generale «accesso WLAN» sostituisce «punto di 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). Il nome dell'hotspot va trasmesso con il parametro *SSID.*

Secondo la lettera j devono ora essere trasmesse anche le indicazioni sulle reti immediatamente adiacenti «da» e «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 all'art. 48*c*). Questa procedura è tuttavia difficilmente eseguibile nel caso della sorveglianza in tempo reale e non è compatibile con gli standard di ETSI e 3GPP. Per questo si rinuncia a una disposizione analoga nell'articolo 56 capoverso 1 lettera e.

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

Nella *lettera a* a complemento dell'indirizzo IP è aggiunto il numero di porta, al fine di rendere possibile l'identificazione del server e del client in caso di network address translation.

L'obbligo di memorizzare i metadati di servizi di posta elettronica (cronologia) incombe soltanto alle POC con obblighi integrali di sorveglianza, vale a dire i FST non esentati secondo l'articolo 51 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 dell'ultima attività

Il *capoverso 1* precisa che non si tratta dell'ultima attività rilevata bensì dell'ultima attività rilevabile. Se necessario, la POC deve pertanto localizzare l'ultima attività. Inoltre, l'intera frase è messa al plurale poiché va rilevata la localizzazione dell'ultima attività di tutte le apparecchiature terminali associate all'identificativo sorvegliato (e quindi non solo di uno).

Il *capoverso 2* elenca, con una nuova struttura, i dati da trasmettere. Non sono tuttavia previsti nuovi dati rispetto alla versione vigente, ad eccezione dei nuovi parametri del sistema 5G la cui designazione è cambiata (p. es. GPSI per MSISDN, SUPI per IMSI, PEI per IMEI). Inoltre, nella *lettera h numero 1* l'elenco esemplificativo di identificativi è accorciato, analogamente all'articolo 48 capoverso 2 lettera a (cfr. il relativo commento). Sono inoltre aggiunte le «marche temporali connesse» (cfr. il commento all'art. 54 cpv. 2 lett. h) e le celle coinvolte sono messe al plurale (anche nel *n. 3*), poiché nelle reti 4G e 5G un'apparecchiatura terminale può essere servita da più celle (master node e uno o più secondary node). Ciò serve ad aumentare l'ampiezza di banda in quanto le celle procedono a una cosiddetta «carriers aggregation».

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. 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). Il nome dell'hotspot va trasmesso con il parametro *SSID*.

Art. 65 cpv. 2, frase introduttiva e cpv. 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). Il nome dell'hotspot va trasmesso con il parametro *SSID*.

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

È modificata la struttura del *capoverso 1*. Inoltre sono introdotti due nuovi tipi di sorveglianza per la ricerca d'emergenza. Gli altri tipi di ricerca d'emergenza restano invariati.

Vanno osservate le modifiche relative ai servizi di telefonia mobile con carte SIM extra, illustrate all'articolo 50 capoverso 6 (p. es. multidevice o multiSIM per ulteriori apparecchi 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 tutte le apparecchiature terminali mobili della persona dispersa o di terzi associate all'identificativo sorvegliato (Target ID). Questa precisazione riguarda soprattutto gli abbonamenti di telefonia mobile con carte SIM extra (cosiddette offerte multidevice o multiSIM, cfr. anche il commento all'art. 50 cpv. 6). Questo tipo di ricerca d'emergenza, applicato da parecchi anni, riguarda la localizzazione di apparecchiature terminali mobili mediante le celle radio mobili. Va fornita l'ultima localizzazione disponibile della corrispondente apparecchiatura mobile, a prescindere dalla tecnologia e dal tipo di accesso alla rete usati con l'apparecchiatura.

Il tipo EP_58_POS_IMMED, definito nella *lettera b*, è nuovo. Si tratta della determinazione unica e immediata della posizione mediante la rete di tutte le apparecchiature terminali mobili della persona dispersa o di terzi associate all'identificativo sorvegliato (Target ID) nell'ambito di una ricerca d'emergenza. Sotto il profilo tecnico questo tipo corrisponde al nuovo tipo di sorveglianza RT_56_POS_IMMED (cfr. anche il commento all'art. 56*a*).

Anche il tipo EP_59_POS_PERIOD, definito nella *lettera c*, è nuovo. Si tratta della determinazione periodica della posizione mediante la rete di tutte le apparecchiature terminali mobili della persona dispersa o di terzi associate all'identificativo sorvegliato (Target ID) nell'ambito di una ricerca d'emergenza. Sotto il profilo tecnico questo tipo corrisponde al nuovo tipo di sorveglianza RT_57_POS_PERIOD (cfr. anche il commento all'art. 56*b*).

Rispetto alla localizzazione di cui alla lettera a, la determinazione della posizione di cui alle lettere b e c è molto più precisa. È effettuata da funzioni specifiche della rete che richiedono un onere 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 implicano una perdita di tempo nelle operazioni di salvataggio delle persone nonché un maggiore impiego di personale e materiale (auto della polizia, elicotteri), il che comporta 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 lettera b vigente e disciplina la sorveglianza in tempo reale di contenuto e metadati nell'ambito di una ricerca d'emergenza. L'autorità ordinante trasmette al Servizio SCPT un ordine per ciascuna POC e per ciascun numero principale sorvegliato e il Servizio SCPT trasmette l'incarico della ricerca d'emergenza alla POC. Ogni POC incaricata installa i tipi di sorveglianza di cui agli articoli 55 e 57 in modo tale che siano contemplati tutti i servizi da essa forniti delle categorie TEL e NA per i numeri accessori appartenenti al numero principale ricercato. Questo pacchetto permette di tenere conto dell'urgenza di una ricerca d'emergenza, poiché si tratta di ritrovare quanto prima una persona la cui vita e integrità fisica sono in pericolo. Nella ricerca d'emergenza si perderebbe troppo tempo con singoli incarichi, conferiti di norma nell'ambito delle sorveglianze per ogni servizio di telefonia o multimedia (TEL) e per ogni servizio di accesso alla rete (NA). Anche in questo caso vanno sorvegliati eventuali numeri accessori del numero principale (p. es. abbonamenti con SIM extra, cosiddette offerte multidevice o multiSIM). Un esempio: la POC riceve l'incarico di una ricerca d'emergenza del tipo EP_36_RT_CC_IRI (lett. b) per il MSISDN x. Supponiamo che presso la POC l'utente con il MSISDN x abbia un abbonamento mobile con accesso alla telefonia e a Internet che comprende una SIM extra con il MSISDN y per l'accesso alla rete. In tal caso per il servizio di telefonia la POC installa una sorveglianza in tempo reale di contenuto e metadati di servizi di telefonia e multimedia (art. 57) per il MSISDN x e, per il servizio di accesso alla rete, una sorveglianza in tempo reale di contenuto e metadati di servizi di accesso alla rete (art. 55) per il MSISDN x nonché un'ulteriore sorveglianza per il MSISDN y. Anche nell'ambito di una ricerca d'emergenza le sorveglianze in tempo reale restano attive fintanto che il Servizio SCPT non conferisca alle POC l'incarico di sospenderle.

La *lettera e* corrisponde alla lettera c vigente e definisce la sorveglianza in tempo reale senza dati sul contenuto, ossia solo la sorveglianza dei metadati, nell'ambito di una ricerca d'emergenza. La procedura corrisponde a quella descritta per la lettera d, con la differenza che questo tipo di sorveglianza si fonda sui tipi di cui all'articolo 54 e 56.

La *lettera f* disciplina la ricerca d'emergenza retroattiva, ad esempio nel caso in cui l'apparecchiatura terminale non è più accesa o non è più coperta dalla rete. La procedura corrisponde a quella descritta per la lettera d. Rispetto a quest'ultima vi sono le seguenti differenze: si tratta di sorveglianze retroattive, ogni POC incaricata installa i corrispondenti tipi di sorveglianza di cui agli articoli 60 e 61, di modo che siano contemplati tutti i servizi da essa forniti per il numero sorvegliato e per i numeri a esso associati, e, visto che si tratta di una sorveglianza retroattiva, non è necessario conferire l'ordine di sospendere la sorveglianza.

L'indennità per le POC dipende dal numero di ricerche d'emergenza ordinato dalle autorità per ciascuna POC e per ciascun numero e non dal numero di sorveglianze effettivamente svolte.

In varie disposizioni sono inseriti i nuovi identificativi del sistema 5G (GPSI, SUPI, PEI; cfr. i commenti agli art. 35 cpv. 1 lett. d n. 2 «GPSI» e n. 10 «SUPI» nonché 36 cpv. 1 lett. d «PEI»).

Il *capoverso 2* precisa che per il tipo di sorveglianza secondo il capoverso 1 lettera f l'inizio e la fine della sorveglianza sono retti dall'articolo 4*a* (cfr. il relativo commento).

Art. 68 Ricerca di condannati

Per la ricerca di condannati, le lettere a–c prevedono tre nuovi tipi di sorveglianza.

La lettera a introduce il cosiddetto paging nell'ambito della 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 unico e immediato nell'ambito della 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 periodico nell'ambito della ricerca di condannati, ossia la determinazione periodica della posizione mediante la rete secondo l'articolo 56*b* (cfr. il relativo commento).

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

Il *capoverso 2* precisa che per il tipo di sorveglianza secondo il capoverso 1 lettera f l'inizio e la fine della sorveglianza sono retti dall'articolo 4*a* (cfr. il relativo commento).

Art. 74a Disposizione transitoria della modifica del xx.xx.xxxx

Per sincronizzare l'introduzione dei nuovi tipi di informazione e sorveglianza tra le POC e il Servizio SCPT è opportuno prevedere disposizioni transitorie dettagliata per le singole modifiche. Entro i termini menzionati le POC 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 forma standardizzata il più presto possibile o al più tardi entro i termini previsti.

Il capoverso 1 prevede per le POC in questione un termine transitorio di 12 mesi dopo l'entrata in vigore della presente modifica per i seguenti quattro tipi di informazione:

1. IR_51_EMAIL_LAST (informazioni su servizi di posta elettronica; art. 42*a*),
2. IR_52_COM_LAST (informazioni su servizi di comunicazione derivati; art. 43*a*)
3. IR_53_ASSOC_PERM (informazioni su identificativi assegnati a lungo termine; Art. 48*a*),
4. IR_55_TEL_ADJ_NET (determinazione delle reti immediatamente adiacenti per i servizi di telefonia e multimedia; Art. 48*c*).

Il *capoverso 2* conferisce alle POC con obblighi integrali un termine transitorio più lungo pari a 24 mesi dopo l'entrata in vigore della presente modifica per il quinto nuovo tipo di informazione IR_54_ASSOC_TEMP *(*informazioni immediate su iden-

tificativi assegnati per breve tempo; art. 48*b),* poiché esso richiede adeguamenti maggiori (cfr. anche il commento all'art. 18 cpv. 3). Per l'attuazione dei due nuovi tipi della determinazione unica e immediata della posizione secondo gli articoli 56*a* (RT_56_POS_IMMED) e 67 capoverso 1 lettera b (EP_58_POS_IMMED) è invece concesso un periodo transitorio relativamente breve di 12 mesi dopo l'entrata in vigore della presente revisione. In considerazione della loro prevista utilità, questi nuovi tipi di sorveglianza devono essere a disposizione delle autorità di perseguimento penale il più presto possibile.

Il *capoverso 3* 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): primo, le POC con obblighi integrali devono garantire la memorizzazione dei dati necessari a tal fine entro 12 mesi dall'entrata in vigore della presente revisione e, secondo, devono essere in grado di fornire i nuovi dati retroattivi (art. 61 lett. j) entro 18 mesi dall'entrata in vigore della revisione.

Il *capoverso 4* disciplina il periodo transitorio per le POC con obblighi integrali per quanto riguarda i due nuovi tipi di determinazione periodica della posizione secondo gli articoli 56*b* (RT_57_POS_PERIOD) e 67 capoverso 1 lettera c (EP_59_POS_PERIOD). L'implementazione di questi nuovi tipi di sorveglianza nell'attuale componente relativa alla sorveglianza in tempo reale del sistema di trattamento del Servizio SCPT (ISS) non è opportuna né dal punto di vista economico né da quello temporale, poiché la componente è ormai arrivata alla fine del suo ciclo di vita e sarà presto sostituita. L'implementazione dovrebbe quindi essere effettuata due volte: una volta nella componente attuale e una seconda volta nella nuova componente. Non è inoltre sicuro che l'implementazione nella componente attuale sia possibile, poiché questa versione non è più stata ulteriormente sviluppata dal produttore. 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. Dopo la messa in esercizio completa della nuova componente, le POC avranno ancora 18 mesi di tempo per i necessari lavori di adeguamento e per eseguire i test con il Servizio SCPT.

Il *capoverso 5* è la controparte della prima parte del capoverso 1 e del capoverso 2 e definisce lo stesso termine transitorio relativamente breve di 12 mesi dopo l'entrata in vigore della presente revisione per il Servizio SCPT in relazione ai corrispondenti tipi di informazione e di sorveglianza. I due nuovi tipi della determinazione unica e immediata della posizione secondo gli articoli 56*a* (RT_56_POS_IMMED) e 67 capoverso 1 lettera b (EP_58_POS_IMMED) saranno implementati anch'essi nella nuova componente per la sorveglianza in tempo reale del sistema di trattamento del Servizio SCPT.

Analogamente al capoverso 3, il *capoverso 6* disciplina il termine transitorio di 18 mesi per il Servizio SCPT per essere in grado di ricevere i dati storici corrispondenti.

Il *capoverso 7* corrisponde alla seconda parte del capoverso 1.

Il *capoverso 8* costituisce la controparte riguardante il Servizio SCPT del capoverso 4.

5.2 Ordinanza sugli emolumenti e le indennità per la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OEm-SCPT)

Art. 3 cpv. 4 lett. a e b, 4bis e 5

Il *capoverso 4 lettera a* è completato con il nuovo tipo di informazione IR_53_ASSOC_PERM (art. 48*a* OSCPT). Nella *lettera b* sono aggiunti quattro nuovi tipi di informazione IR_51_EMAIL_LAST (art. 42*a* OSCPT), IR_51_COM_LAST (art. 43*a* OSCPT), IR_54_ASSOC_TEMP (art. 48*b* OSCPT) e IR_55_TEL_ADJ_NET (art. 48*c* OSCPT).

Il *capoverso 4bis* è completato con il nuovo tipo di informazione IR_53_ASSOC_PERM (art. 48*a* OSCPT).

Il *capoverso 5* precisa l'espressione «in tempi brevi». Affinché si applichi questa regola, le ricerche per zona di copertura dell'antenna devono essere ordinate entro 24 ore. Come sinora, il Servizio SCPT allestisce un calcolo secondo gli articoli 13 e 17 (emolumento e indennità per prestazioni non previste).

Art. 15 **Diritto**

Nella *rubrica* «Diritto all'indennità» è sostituito da «Diritto». Secondo l'articolo 38 capoverso 2 LSCPT[33] le POC ricevono dal Servizio SCPT un'equa indennità[34] per le spese cagionate per l'esecuzione delle sorveglianze e la fornitura delle informazioni secondo gli articoli 21 e 22.

Il *capoverso 1* non subisce modifiche materiali. Hanno diritto a un'indennità le POC di cui all'articolo 2 lettere a–e LSCPT, ossia tutte le POC, eccetto i rivenditori professionali (art. 2 lett. f LSCPT), se adempiono i loro obblighi d'informazione e di sorveglianza secondo la LSCPT e l'OSCPT, a prescindere dal fatto che siano in possesso di un attestato (art. 33 cpv. 6 LSCPT, art. 31 OSCPT). Le POC che non adempiono i loro obblighi d'informazione e di sorveglianza secondo la LSCPT e l'OSCPT non hanno diritto a un'indennità. Le POC che adempiono parzialmente i loro obblighi, sostenendo ad esempio il Servizio SCPT, possono essere indennizzate conformemente all'articolo 19 capoverso 2.

Il *capoverso 2* prevede un'indennità anche per le POC che sostengono il Servizio SCPT nella fornitura di informazioni o nell'esecuzione delle sorveglianze, pur non essendo tenute esse stesse a fornire informazioni o eseguire sorveglianze. Si tratta ad esempio di organizzare l'accesso a Internet, consentire al Servizio SCPT l'accesso senza problemi ai server o adeguare l'infrastruttura. Al contrario del capoverso 1, il capoverso 2 non prevede un diritto all'indennità (disposizione potestativa). È possibile non indennizzare determinate spese delle POC, ad esempio quelle per l'energia

33 Versione in vigore dal 1° dicembre 2022
34 «equa indennità»; cfr. la sentenza del Tribunale federale del 27 luglio 2021 (2C_650/2020)

elettrica supplementare. Sono contemplati soprattutto i FST con obblighi di sorveglianza ridotti (art. 51 OSCPT), i FSCD senza obblighi d'informazione o di sorveglianza supplementari (cfr. art. 22 e 52 OSCPT), ma anche i gestori di reti di telecomunicazione interne o persone che mettono a disposizione di terzi il loro accesso a una rete di telecomunicazione pubblica.

Il nuovo *capoverso 3* riprende il disciplinamento dell'articolo 16 vigente.

Art. 16 Abrogato

Il disciplinamento di questa disposizione è ripreso nel capoverso 3 dell'articolo 15. L'articolo 16 è pertanto abrogato.

Art. 17 cpv. 3 e 3bis

Il vigente capoverso 4, che comprende il disciplinamento riguardante l'80 per cento per l'indennità, coincide con la fine del capoverso 3. Per questo motivo nel *capoverso 3* il sintagma «unicamente dell'80 per cento» è stralciato.

Il *capoverso 3bis* disciplina l'importo massimo dell'indennità in modo simile all'articolo 19 capoverso 2 terzo periodo.

Art. 18 Casi di assunzione delle spese

In seguito agli adeguamenti formali nell'OSCPT in riferimento alla categoria dei FSCD, anche nella presente ordinanza si usa l'espressione «FSCD con obblighi supplementari di cui agli articoli 22 e 52 OSCPT (cfr. p. es. art. 11 cpv. 1 lett. a e art. 19 cpv. 1 OSCPT).

Art. 19 cpv. 1

Il *capoverso 1* rimanda all'articolo 13 (emolumento per prestazioni non previste). Con questo rimando il Servizio SCPT fissa l'emolumento per le spese che ha dovuto sostenere in seguito alla cooperazione insufficiente di una POC, poiché il Servizio SCPT deve svolgere al posto della POC un lavoro supplementare che supera l'emolumento ordinario. L'osservazione «in funzione del tempo impiegato» rende troppo restrittivo il rimando all'articolo 13 poiché in tal caso sarebbe applicabile soltanto il capoverso 1. Con la presente modifica (stralcio di «in funzione del tempo impiegato») il rimando riguarda ora anche il capoverso 2 dell'articolo 13. Può pertanto ora essere fatturata direttamente in base all'OEm-OSCPT anche la messa a disposizione di materiale usato una volta sola. In tal caso il Servizio SCPT decide di volta in volta se dopo la fine della misura di sorveglianza il materiale può essere consegnato alla POC o meno. Il materiale usato più volte è fatturato per ore. Applicando questo metodo di fatturazione, un caso speciale presso una POC può causare spese elevate. Si raccomanda pertanto all'autorità abilitata a ordinare la sorveglianza di sentire prima il Servizio SCPT in merito all'ammontare delle spese.

Allegato
L'allegato dell'OEm-SCPT è costituito da una tabella che comprende tutti i tipi di informazione e sorveglianza e i rispettivi emolumenti definiti nell'ordinanza stessa. Riporta sia l'emolumento per il Servizio SCPT sia le indennità per le POC coinvolte. La tabella consente a tutte le autorità abilitate di calcolare in anticipo i costi di una misura di sorveglianza prevista. Se sono necessari parametri quali il numero delle POC coinvolte, può essere consultato il Servizio SCPT. In linea di massima le autorità abilitate devono versare al Servizio SCPT sia l'«emolumento Servizio SCPT» sia l'«indennità per persone obbligate a collaborare». Per le informazioni di cui agli articoli 27, 35, 37, 40, 42, 43 e (nuovo) 48*a* OSCPT, dal 1° luglio 2020 alle autorità abilitate a chiedere informazioni non è più fatturato un emolumento globale (composto dall'«emolumento Servizio SCPT» e dall'«indennità per persone obbligate a collaborare»). Alle POC continua a essere versata l'«indennità per persone obbligate a collaborare» pari a tre franchi. Su raccomandazione del gruppo di lavoro «Finanziamento SCPT» le entrate che vengono a mancare al Servizio SCPT sono compensate da un aumento dell'emolumento per le sorveglianze in tempo reale e retroattive[35].

Nel quadro della revisione parziale dell'OSCPT sono istituiti cinque nuovi tipi di informazione e quattro nuovi tipi di sorveglianza:

1) il tipo di informazione IR_51_EMAIL_LAST: informazioni su servizi di posta elettronica (art. 42*a* OSCPT);
2) il tipo di informazione tipo di informazione IR_52_COM_LAST: informazioni su altri servizi di telecomunicazione o servizi di comunicazione derivati (art. 43*a* OSCPT);
3) il tipo di informazione IR_53_ASSOC_PERM: informazioni su identificativi assegnati a lungo termine (art. 48*a* OSCPT);
4) il tipo di informazione IR_54_ASSOC_TEMP: informazioni immediate su identificativi assegnati per breve tempo (art. 48*b* OSCPT);
5) il tipo di informazione IR_55_TEL_ADJ_NET: determinazione delle reti immediatamente adiacenti per i servizi di telefonia e multimedia (art. 48*c* OSCPT);
6) il tipo di sorveglianza (sorveglianza in tempo reale) RT_56_POS_IMMED: determinazione unica e immediata della posizione mediante la rete (art. 56*a* OSCPT);
7) il tipo di sorveglianza (sorveglianza in tempo reale) RT_57_POS_PERIOD, determinazione periodica della posizione mediante la rete (art. 56*b* OSCPT);
8) il tipo di sorveglianza (ricerca d'emergenza) EP_58_POS_IMMED: determinazione unica e immediata della posizione mediante la rete (art. 67 cpv. 1 lett. b OSCPT); e
9) il tipo di sorveglianza (ricerca d'emergenza) EP_59_POS_PERIOD: determinazione periodica della posizione mediante la rete (art. 67 cpv. 1 lett. c OSCPT).

Questo rende necessaria una corrispondente revisione parziale dell'OEm-SCPT.

35 Cfr. revisione parziale dell'OEm-SCPT del 20 maggio 2020, in vigore dal 1° luglio 2020 (RU **2020** 2061) e rapporto esplicativo.

Nel fissare gli emolumenti e le indennità per i nuovi tipi di informazione e sorveglianza questi ultimi sono messi fondamentalmente in relazione con i tipi di informazione e sorveglianza vigenti. L'importo dell'emolumento è inoltre influenzato da altri criteri quali le spese di manutenzione, ammortizzamento e investimento per il sistema di trattamento. Si tiene infine conto anche della frequenza d'uso dei nuovi tipi di informazione e sorveglianza.

Gli emolumenti e le indennità per i nuovi tipi di informazione corrispondono agli importi vigenti. Tra i nuovi tipi di informazione soltanto il tipo IR_53_ASSOC_PERM (art. 48*a* OSCPT) può essere considerato un'informazione «semplice» per cui il Servizio SCPT non riscuote un emolumento, ma alla POC è versata un'indennità. Gli altri nuovi tipi di informazione sono considerati informazioni «complesse» e per ogni richiesta d'informazione è fissato un emolumento di 75 franchi per il Servizio SCPT e versata un'indennità di 125 franchi alla POC.

Per i nuovi tipi di sorveglianza sussistono meno corrispondenze con quelli vigenti. I due nuovi tipi di sorveglianza per la determinazione della posizione della rete (LALS) offrono una funzione del tutto nuova. L'emolumento e l'indennità per la determinazione unica e immediata della posizione RT_56_POS_IMMED (art. 56*a* OSCPT) si fondano pertanto su quelli del tipo lontanamente paragonabile HD_31_PAGING (art. 63 OSCPT) e sono maggiori di 50 franchi, poiché il lavoro del Servizio SCPT e delle POC sarà maggiore. Grazie alla determinazione molto più precisa della posizione, questo nuovo tipo di sorveglianza offre un valore aggiunto notevole rispetto a HD_31_PAGING.

Il secondo nuovo tipo di sorveglianza per la determinazione della posizione mediante la rete (LALS), RT_57_POS_PERIOD (art. 56*b* OSCPT), corrisponde a una tipica sorveglianza in tempo reale dall'attivazione alla disattivazione. A scadenze periodiche regolari la rete determina la posizione precisa dell'apparecchiatura terminale della persona sorvegliata e trasmette immediatamente la posizione al sistema di trattamento. L'emolumento globale è leggermente più alto rispetto a quello del tipo di sorveglianza in tempo reale «solo metadati» ed è un multiplo di quello per la determinazione unica e immediata della posizione RT_54_POS_IMMED (fr. 2800.- rispetto a fr. 600.-), poiché il sistema di trattamento deve essere adeguato per poter ricevere e trattare le indicazioni sulla posizione.

Poiché la ricerca d'emergenza può essere un elemento fondamentale per salvare una vita ed è impiegata soltanto in casi in cui è messa in pericolo la vita e l'integrità fisica di una persona, l'emolumento e le indennità sono, come anche in altri tipi di sorveglianza per la ricerca d'emergenza, inferiori rispetto ad altri tipi di sorveglianza comparabili. Inoltre, per l'emolumento si rinuncia a un supplemento per la determinazione della posizione (unica o periodica) nell'ambito della ricerca d'emergenza. Pertanto l'emolumento per EP_58_POS_IMMED (art. 67 lett. b OSCPT), pari a 50 franchi, equivale a quello degli altri tipi di sorveglianza per la ricerca d'emergenza. L'indennità (fr. 350.-) si fonda su quello della sorveglianza analoga RT_56_POS_IMMED, ma è ridotto di 50 franchi.

L'importo dell'emolumento per EP_59_POS_PERIOD (art. 67 lett. c OSCPT) equivale a quello degli altri tipi di sorveglianza per la ricerca d'emergenza. Come per la

sorveglianza, anche per la ricerca d'emergenza l'indennità per la determinazione periodica della posizione è più elevata rispetto alla determinazione unica. Con un importo di 750 franchi è tuttavia inferiore rispetto alla sorveglianza dello stesso tipo RT_57_POS_PERIOD ed equivale a quella per le altre sorveglianze in tempo reale per la ricerca d'emergenza EP_36_RT_CC_IRI (art. 67 lett. d OSCPT) ed EP_37_RT_IRI (Art. 67 lett. e).

Per le ripercussioni finanziarie dei nuovi tipi di informazione e sorveglianza si veda il numero 4.

Infine, per il tipo d'informazione IR_18_ID «copia del documento» è sostituito da «prova dell'identità», come nell'articolo 45 OSCPT. Nella colonna «caso» di IR_21_TECH è aggiunto «tipo di informazione», analogamente ai quattro tipi di informazione precedenti.

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

Art. 1 Campo d'applicazione

Poiché la comunicazione sicura è disciplinata nell'ordinanza dipartimentale anche per le autorità (cfr. art. 3), il campo d'applicazione va esteso anche a quest'ultime. Pertanto l'OE-SCPT si applica, oltre che al Servizio SCPT e alle POC, 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 deve essere esteso anche alla comunicazione tra il Servizio SCPT e le autorità.

Il *capoverso 1* disciplina ora anche la comunicazione sicura tra il Servizio SCPT e le autorità di cui all'articolo 1 capoverso 2 lettere a–f OSCPT. Sono considerati mezzi di trasmissione sicuri i mezzi di trasmissione elettronici del sistema di trattamento del Servizio SCPT (*lett. a*), le soluzioni di criptaggio per messaggi di posta elettronica, disciplinate nell'allegato 1 dell'OE-SCPT, o, d'intesa con il Servizio SCPT, un altro mezzo equivalente (*lett. c*).

La lettera a vigente, riguardante la comunicazione confidenziale tra le POC e il Servizio SCPT è spostata nel *capoverso 2* senza subire modifiche sostanziali.

Art. 10 cpv. 4

In analogia al disciplinamento del termine per la trasmissione delle domande di informazioni (art. 14 cpv. 1) e dei mandati per l'esecuzione della sorveglianza del traffico delle telecomunicazioni (art. 16 cpv. 1, 17 cpv. 1 e 18 cpv. 1) da parte del Servizio

SCPT alle POC, il nuovo capoverso 4 prevede lo stesso termine anche per la sorveglianza della corrispondenza postale. Il termine per la trasmissione del mandato di esecuzione della sorveglianza in tempo reale della corrispondenza postale al fornitore è fissato anch'esso a un'ora. Le sorveglianze della corrispondenza postale sono ordinate e eseguite esclusivamente durante gli orari normali di lavoro.

Art. 11 cpv. 2

Analogamente agli articoli 10 capoverso 4, 14 capoverso 1, 16 capoverso 1, 17 capoverso 1 e 18 capoverso 1, il nuovo *capoverso 2* disciplina il termine per la trasmissione del mandato di esecuzione di una sorveglianza retroattiva della corrispondenza postale (cfr. il commento all'art. 10 cpv. 4).

Art. 12 **Fornitura di informazioni**

I primi due periodi restano invariati. Il terzo periodo è aggiunto in seguito agli adeguamenti degli articoli 35 capoverso 1 lettera b e c nonché 40 capoverso 1 lettere b e c OSCPT, secondo cui per i tipi di informazione IR_4_NA e IR_10_Tel deve ora essere indicato il periodo di validità. Presso i fornitori sono spesso memorizzati, oltre all'indirizzo al momento della registrazione, anche indirizzi successivi dopo un trasloco e altre indicazioni relative ai clienti, ad esempio l'indirizzo o il nome e il cognome di un'altra persona validi come indirizzo postale. Il fornitore deve trasmettere tutti gli indirizzi e le indicazioni disponibili per l'intero periodo di validità di tali informazioni.

Art. 14 cpv. 2, 3 e 4

Il *capoverso 2* disciplina i tempi di trattamento per le POC «grandi» e «medie». Vi rientrano i FST («grandi»), eccetto quelli con obblighi di sorveglianza ridotti secondo l'articolo 51 OSCPT, i FSCD con obblighi d'informazione supplementari (art. 22 OSCPT, «medi») e i FSCD con obblighi di sorveglianza supplementari (art. 52 OSCPT, «grandi»).

La *lettera a* precisa che alle domande d'informazione di cui all'articolo 48*b* OSCPT va risposto immediatamente. Il tempo di risposta per questo nuovo tipo di informazione deve essere molto breve (pochi secondi) poiché gli identificativi temporanei cambiano spesso. L'informazione deve pertanto essere richiesta e fornita mediante un'interfaccia d'interrogazione del tipo LI_HIQR. Un momento determinante non è indicato poiché si tratta di una richiesta in tempo reale ed è quindi determinante il momento della richiesta. Non sono possibili richieste retroattive. Va osservato che i FSCD con obblighi d'informazione supplementari (art. 22 OSCPT, «di grandezza media») sono esentati dal fornire le informazioni di cui all'articolo 48*b* OSCPT (cfr. art. 18 cpv. 3 OSCPT) e quindi la lettera a non è loro applicabile.

Nella *lettera b* il termine di un'ora per il trattamento da parte del fornitore delle informazioni menzionate resta invariato. Poiché i tipi di informazione elencati sono forniti in forma automatizzata (cfr. art. 18 cpv. 2 OSCPT), i tempi di reazione per la risposta sono relativamente brevi. Si tratta dei seguenti tipi di informazione: IR_4_NA (art. 35 OSCPT), IR_5_NA_FLEX (art. 27 OSCPT in combinato disposto con l'art. 35

OSCPT), IR_6_NA (art. 36 OSCPT), IR_7_IP (art. 37 OSCPT), IR_10_TEL (art. 40 OSCPT), IR_11_TEL_FLEX (art. 27 OSCPT in combinato disposto con l'art. 40 OSCPT), IR_12_TEL (art. 41 OSCPT), IR_13_EMAIL (art. 42 OSCPT) e IR_14_EMAIL_FLEX (art. 27 OSCPT in combinato disposto con l'art. 42 OSCPT). Il termine di un'ora si applica anche ai seguenti nuovi tipi di informazione: IR_51_EMAIL_LAST (informazioni su servizi di posta elettronica; art. 42*a* OSCPT), IR_52_COM_LAST (informazioni su servizi di telecomunicazione o servizi di comunicazione derivati; art. 43*a* OSCPT) e IR_53_ASSOC_PERM (informazioni su identificativi assegnati a lungo termine; art. 48*a* OSCPT).

Anche nella *lettera c numero 1* il termine di risposta di un giorno lavorativo per le domande d'informazioni pervenute al fornitore durante gli orari d'ufficio ordinari resta invariato. Questo termine concerne, come sinora, i seguenti tipi d'informazione: IR_8_IP (NAT) (art. 38 OSCPT), IR_9_NAT (art. 39 OSCPT), IR_15_COM (art. 43 OSCPT), IR_16_COM_FLEX (art. 27 OSCPT in combinato disposto con l'art. 43 OSCPT), IR_17_PAY (art. 44 OSCPT), IR_18_ID (art. 45 OSCPT), IR_19_BILL (art. 46 OSCPT), IR_20_CONTRACT (art. 47 OSCPT), IR_21_TECH (art. 48 OSCPT). A questi si aggiunge il nuovo tipo d'informazione IR_55_TEL_ADJ_NET (determinazione delle reti immediatamente adiacenti per i servizi di telefonia e multimedia; art. 48*c* OSCPT).

Entro un giorno lavorativo significa che la risposta deve essere trasmessa al Servizio SCPT o all'autorità richiedente entro le ore 17:00 del giorno lavorativo successivo alla richiesta (cfr. es. 1 qui appresso).

Nella prassi il termine di un giorno lavorativo è stato giudicato troppo lungo dalle autorità autorizzate a ricevere le informazioni nel caso in cui la loro richiesta è inoltrata durante il fine settimana o in un giorno festivo ed è quindi urgente. Per questo motivo il *numero 2* stabilisce per i grandi FST e FSCD un nuovo termine più breve di sei ore nel caso di richiesta al di fuori degli orari d'ufficio ordinari o nei giorni festivi. Il termine corrisponde a quello per le sorveglianze retroattive urgenti. L'esperienza insegna che durante il servizio di pronto intervento vi sono relativamente poche domande d'informazioni e pochi ordini di sorveglianza e pertanto non è prevedibile 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 i giorni festivi. Va osservato che i FSCD con obblighi di informazione supplementari (art. 22 OSCPT, «grandezza media») non devono fornire un servizio di pronto intervento (cfr. art. 11 cpv. 1 OSCPT) e quindi la lettera c numero 2 non è applicabile a questi ultimi.

Una domanda d'informazioni non automatizzata alla POC durante il servizio di pronto intervento presuppone che il Servizio SCPT sia avvisato dall'autorità legittimata (art. 15 LSCPT, cfr. art. 11 cpv. 2 OSCPT), affinché possa contattare successivamente la POC in questione per conferirle il corrispondente incarico.

Il tempo di trattamento di sei ore significa che entro sei ore dalla ricezione della richiesta la POC deve inserire la risposta nell'IRC o, in caso di guasto dell'IRC, trasmetterla in modo sicuro (cfr. art. 3) al Servizio SCPT. Qui di seguito presentiamo alcuni esempi.

Esempio 1: una domanda d'informazioni è inserita nell'IRC lunedì alle ore 16.10 e giunge alla POC entro pochi secondi. In questo caso il termine è di un giorno lavorativo. Per rispondere alla domanda, il fornitore ha tempo fino alla fine del giorno lavorativo successivo, ossia fino a martedì, ore 16.59.

Esempio 2: una domanda d'informazioni è inserita nell'IRC lunedì alle ore 17.05 e giunge alla POC entro pochi secondi. Poiché il momento dell'inserimento è al di fuori degli orari d'ufficio ordinari, l'autorità legittimata deve avvisare il Servizio SCPT. Il Servizio SCPT informa senza indugio la POC. Il tempo di trattamento concesso alla POC è di sei ore dalla ricezione del mandato. Per rispondere il fornitore ha quindi tempo fino alle ore 23.05 dello stesso giorno. L'autorità deve versare un emolumento supplementare (servizio di pronto intervento). Alla POC è versata un'indennità supplementare (indennità per il servizio di pronto intervento; cfr. art. 6 OEm-SCPT).

Esempio 3: se la domanda d'informazione è inoltrata sabato alle ore 18.50 (al di fuori degli orari d'ufficio ordinari). Il fornitore ha tempo fino a domenica alle ore 00.50 per rispondere alla domanda. La procedura è simile all'esempio 2.

Il *capoverso 3* disciplina i tempi di trattamento per le POC «piccole». Si tratta dei FST con obblighi di sorveglianza ridotti (art. 51 OSCPT).

Analogamente al capoverso 2 lettera a e b, in riferimento ai termini di trattamento si procede a una distinzione in base alla complessità della fornitura delle informazioni. Per le informazioni elencate nella *lettera a,* rispetto al diritto vigente il termine è ridotto da due a un giorno lavorativo. Per le informazioni menzionate nella *lettera b* il termine resta invariato (due giorni lavorativi).

Il *capoverso 4* disciplina i termini di trattamento per i FSCD senza obblighi supplementari secondo gli articoli 22 e 52 OSCPT e per i gestori di reti di telecomunicazione interne, che devono fornire soltanto le indicazioni di cui dispongono (cfr. art. 22 cpv. 3 LSCPT). Nel fornire le informazioni, queste POC non devono attenersi ai tipi standardizzati previsti dall'OSCPT (art 18*a* OSCPT).

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

Art. 18 cpv. 2 e 3

In seguito alle lettere nuove degli articoli 67 capoverso 1 e 68 capoverso 1 OSCPT devono essere adeguati i rimandi nei *capoversi 2* e *3*.

Allegato 1

Nel quadro della revisione parziale dell'OSCPT sono istituiti cinque nuovi tipi di informazione e quattro nuovi tipi di sorveglianza:

1) il tipo di informazione IR_51_EMAIL_LAST: informazioni su servizi di posta elettronica (art. 42*a* OSCPT);
2) il tipo di informazione tipo di informazione IR_52_COM_LAST: informazioni su altri servizi di telecomunicazione o servizi di comunicazione derivati (art. 43*a* OSCPT);
3) il tipo di informazione IR_53_ASSOC_PERM: informazioni su identificativi assegnati a lungo termine (art. 48*a* OSCPT);
4) il tipo di informazione IR_54_ASSOC_TEMP: informazioni immediate su identificativi assegnati per breve tempo (art. 48*b* OSCPT);
5) il tipo di informazione IR_55_TEL_ADJ_NET: determinazione delle reti immediatamente adiacenti per i servizi di telefonia e multimedia (art. 48*c* OSCPT);
6) il tipo di sorveglianza (sorveglianza in tempo reale) RT_56_POS_IMMED: determinazione unica e immediata della posizione mediante la rete (art. 56*a* OSCPT);
7) il tipo di sorveglianza (sorveglianza in tempo reale) RT_57_POS_PERIOD, determinazione periodica della posizione mediante la rete (art. 56*b* OSCPT);
8) il tipo di sorveglianza (ricerca d'emergenza) EP_58_POS_IMMED: determinazione unica e immediata della posizione mediante la rete (art. 67 cpv. 1 lett. b OSCPT); e
9) il tipo di sorveglianza (ricerca d'emergenza) EP_59_POS_PERIOD: determinazione periodica della posizione mediante la rete (art. 67 cpv. 1 lett. c OSCPT).

Questo rende necessaria una corrispondente revisione dell'allegato 1 dell'OE-SCPT riguardante le prescrizioni tecniche in materia di interfacce per l'esecuzione della sorveglianza delle telecomunicazioni. Sono inoltre inseriti i parametri e le designazioni della tecnologia 5G.

5.4 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 dell'OSCPT, di modo che risulti chiaramente che anche per gli articoli ivi contenuti, quali gli articoli 25 (informazioni e sorveglianze particolari) e 27 (tipi di informazioni con ricerca flessibile dei nomi) OSCPT, è possibile il trattamento dei dati nel sistema di trattamento per la sorveglianza del traffico delle telecomunicazioni. La nuova componente per la sorveglianza in tempo reale permette di trasmettere alle autorità di perseguimento penale anche mediante il sistema di trattamento un numero sempre maggiore di dati da sorveglianze particolari («special cases»). Il contenuto vigente della disposizione resta tuttora valido. Il capoverso 2 lettera d resta invariato.

Art. 8 cpv. 3-6

Secondo il *capoverso 3* singoli collaboratori (cosiddetti «OrgAdmin»), soprattutto della polizia, possono essere autorizzati dal Servizio SCPT a concedere ulteriori accessi. Finora potevano assegnare gli accessi soltanto all'interno della propria autorità o alle persone interessate e ai loro rappresentanti legali. La modifica prevede che possano concedere l'accesso anche alle autorità d'approvazione, tra cui in particolare il giudice dei provvedimenti coercitivi. Le autorizzazioni previste dal numero 2.7 «autorità d'approvazione» non sono modificate. Finora tali autorizzazioni potevano essere concesse soltanto dal Servizio SCPT. Con la presente modifica potranno concederle anche le OrgAdmin. L'autorità d'approvazione riceve accesso soltanto alla componente per la gestione dei mandati WMC (Warrant Management Component) e non ha quindi accesso ai dati risultanti dalla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

I nuovi *capoversi 4 e 5* illustrano l'accesso ai dati da parte del Servizio SCPT. I collaboratori del Servizio SCPT e altri possibili ausiliari non hanno in linea di massima accesso ai dati risultanti da singole sorveglianze. Di solito i dati sono semplicemente scansionati da un software. Di regola non è previsto che una persona possa venire a conoscenza dei dati («privacy by design»). Ciononostante, sia per i collaboratori del Servizio SCPT sia per altre persone che sostengono il Servizio SCPT è di regola effettuato un controllo di sicurezza. L'intervento di altre persone può rendersi ad esempio necessario se specialisti dell'esercente dell'hardware o del fornitore del software devono aiutare a risolvere problemi complessi. Possono tuttavia essere considerati ausiliari anche le persone che sostengono il Servizio SCPT in caso di carico di lavoro elevato. Secondo gli articoli 18 capoverso 1 LSCPT e 29 OSCPT, il Servizio SCPT ha il compito di adottare misure per controllare la qualità dei dati della sorveglianza 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. Ciò può essere il caso in presenza di problemi constatati dalle autorità stesse che ordinano la sorveglianza, ad esempio una telefonata in cui si sente soltanto uno dei due utenti.

Oltre che per il controllo della qualità, l'accesso ai dati della sorveglianza e quindi la conoscenza di singoli contenuti possono essere necessari anche per fornire consulenza all'autorità che ordina 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 tal caso il Servizio SCPT deve sempre procurarsi il consenso scritto dell'autorità investita del procedimento. La forma scritta ai sensi del capoverso 4 è necessaria perché il consenso deve essere attestabile. In maniera analoga anche l'articolo 11 capoverso 1 lettera b OTDI[36] prevede il consenso scritto dell'autorità competente. I requisiti della forma scritta previsti dall'articolo 14 CO[37] non devono essere

36 Ordinanza del 25 novembre 2020 sul coordinamento della trasformazione digitale e la governance delle TIC in seno all'Amministrazione federale (Ordinanza sulla trasformazione digitale e l'informatica, **OTDI**; RS **172.010.58**)

37 Codice delle obbligazioni, **CO**; RS **220**

rispettati e pertanto il consenso non deve essere corredato di firma autografa o di 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. Affinché il Servizio SCPT possa svolgere questo compito in modo sicuro, il capoverso 5 prevede delle deroghe al capoverso 4. Il Servizio SCPT è responsabile della sicurezza del sistema di trattamento e deve pertanto adottare le pertinenti misure (art. 12 LSCPT, art. 11 OST-SCPT), per le quali non è sempre necessario il consenso delle autorità investite del procedimento (cfr. cpv 5). Può trattarsi sia di misure preventive, quali i test di funzionalità, sia dell'osservazione statistica delle attività nel sistema sia di interventi per rimediare a guasti della funzionalità. A tale scopo il Servizio SCPT svolge un monitoraggio ai fini del controllo della qualità: verifica che il sistema funzioni correttamente ed esamina se ciò che è rappresentato è plausibile (leggibilità, usufruibilità e utilizzabilità del contenuto). I collaboratori del Servizio SCPT ed eventuali ausiliari (p. es. specialisti di un fornitore di software) hanno bisogno di accedere a diversi dati (metadati, dati di login e di contenuto) della sorveglianza. Può darsi che debbano prendere conoscenza anche del contenuto della sorveglianza, sebbene questo non sia il loro obiettivo principale o non sia nelle loro intenzioni. In altre parole, il collaboratore del Servizio SCPT si concentra sul problema che deve risolvere e scorge solo spezzoni del contenuto. Di regola si procede ad accessi automatizzati per verificare regolarmente la qualità dei dati e la stabilità del sistema nonché per eliminare tempestivamente eventuali errori. Si analizzano in particolare l'ampiezza dell'errore (riguarda solo un singolo caso?), le conseguenze (la fornitura dei dati ha subito ritardi, è erronea o non è stata effettuata?), la durata e i fattori caratterizzanti (quali tipi di sorveglianze, quali tipi di provider sono coinvolti?).

Il *capoverso 5* contiene le deroghe al capoverso 4 ed elenca i casi in cui si può rinunciare al consenso dell'autorità investita del procedimento.

Se sussistono o se vi è il rischio di gravi guasti nel funzionamento (*lett. a n. 1),* l'accesso è necessario urgentemente per assicurare il funzionamento regolare del sistema di trattamento (cfr. anche art. 11). È sufficiente anche un rischio imminente per il sistema poiché anch'esso costituisce un caso d'emergenza in cui è necessario intervenire immediatamente. Se ad esempio una sorveglianza di un'autorità rende necessario un enorme spazio di memoria e l'autorità in questione non può essere raggiunta perché è reperibile soltanto durante gli orari d'ufficio, occorre poter accedere ai dati già in caso di rischio imminente per il sistema di trattamento, in modo da risolvere il problema e garantire la stabilità del sistema.

Anche nei casi in cui individuare la sorveglianza che causa problemi è impossibile o comporterebbe un onere sproporzionato (*lett. a n. 2*), il Servizio SCPT deve avere la possibilità di poter adottare le misure per assicurare il funzionamento regolare del sistema di trattamento. Deve poterlo fare anche se l'autorità competente non può essere raggiunta in tempo utile (p. es. nei giorni festivi) o se raggiungerla comporterebbe un onere sproporzionato. Anche una piccola modifica nella trasmissione di prodotti e formati può portare a una rappresentazione errata o diversa nel sistema di trattamento, il che implica a sua volta difficoltà nella valutazione dei dati da parte dell'autorità competente. L'immissione o la trasformazione di dati di buona qualità forniti dalle

POC può causare una perdita di qualità o addirittura problemi per l'intero sistema di trattamento. A seconda delle circostanze, questi problemi sono constatabili soltanto per mezzo di un'ampia analisi dei dati e non possono quindi essere imputati a una sorveglianza concreta prima dell'analisi, di modo che non può essere individuata l'autorità cui chiedere il consenso.

Proprio per individuare il mandato di sorveglianza o i formati che causano un problema o per rendere il sistema in generale più stabile (come nel monitoraggio summenzionato), occorre spesso confrontare numerosi dati per scoprire anomalie. Se le comunicazioni di errore riguardano un gran numero di sorveglianze deve essere verificata ciascuna di esse. Individuare in un caso del genere tutte le autorità competenti e contattarle singolarmente è praticamente impossibile o causa un onere di lavoro sproporzionato. È pertanto previsto che il consenso non è necessario neanche nel caso di un gran numero di sorveglianze coinvolte (*lett. b*).

Secondo il *capoverso 6,* il Servizio SCPT adotta misure contrattuali, organizzative e tecniche appropriate per impedire la divulgazione dei dati. In tal modo s'intende impedire a tutti, e quindi non soltanto a terzi (p. es. ausiliari del Servizio SCPT), bensì anche ai collaboratori del Servizio SCPT che per adempiere i loro compiti devono essere a conoscenza di dati della sorveglianza, di trasmettere tali dati ad altre persone.

Art. 10 cpv. 4

I termini di conservazione dei dati nel sistema di trattamento sono disciplinati dall'articolo 11 LSCPT. L'*articolo 10 capoverso 4* disciplina la durata di conservazione dei verbali. Nella versione tedesca il termine «Speicherdauer» è sostituito da quello più appropriato di «Aufbewahrungsdauer».

Nella versione vigente manca tuttavia un disciplinamento sulla durata di conservazione dei verbali relativi alla cancellazione dei dati. Tale disciplinamento permette soprattutto di sapere quando sono stati cancellati dati conservati a lungo con funzioni di trattamento ridotte. In questo caso l'articolo 10 OLPD[38] non può servire da base.

Art. 11 Misure per la sicurezza del sistema

L'espressione un po' imprecisa e troppo restrittiva «esercizio regolare» è sostituita dall'espressione «funzionamento regolare», usata anche nell'articolo 8 capoverso 4.

Allegato lett. af

La «Segnalazione dello stato di esercizio delle parti del sistema di trattamento a cui la persona ha accesso», il cosiddetto dashboard PTSS, è un'applicazione che serve a visualizzare lo stato delle componenti della sorveglianza in cui sono pubblicati ticket e comunicazioni (p. es. comunicazioni di guasti e il loro stato, indicazioni dello stato delle componenti del sistema, stabilità della rete) nonché determinati termini (p.es. periodi di manutenzione delle componenti del sistema e di altri sistemi quali I-Net di Teldas). Il dashboard PTSS tratta in particolare anche dati relativi allo stato attuale

38 Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (**OLPD**; RS **235.11**)

della componente per la sorveglianza in tempo reale (ISS) ed è in grado di rappresentarli in un grafico. Questa integrazione della matrice disciplina l'accesso delle autorità legittimate e del Servizio SCPT al dashboard PTSS. L'accesso a quest'ultimo e i dati indicati dipendono in linea di massima dai diritti d'accesso effettivi della persona in questione alle componenti del sistema di trattamento.

Allegato

Tabelle «Panoramica tempi di trattamento»

Tabella «Panoramica tempi di trattamento»

Incarico	Art. OSCPT	Tipi di incarichi	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 lavorativi
Disattivazione solo durante gli orari d'ufficio	16 lett. a	PO_1_RT_INTERCEPTION	≤ 1 ora	≤ 1 giorno lavorativo

Incarico	Art. OSCPT	Tipi di incarichi	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 42 27, 42 42*a* 43*a* 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_13_EMAIL IR_14_EMAIL_FLEX IR_51_EMAIL_LAST IR_52_COM_LAST IR_53_ASSOC_PERM	≤ 1 ora	≤ 1 ora	≤ 1 giorno lavorativo

	48*b*	IR_54_ASSOC_TEMP	subito	subito (eccetto i FSCD con obblighi d'informazione supplementari, art. 22 OSCPT)	--
	38 39 43 27, 43 44 45 46 47 48 48*c*	IR_8_IP (NAT) IR_9_NAT IR_15_COM IR_16_COM_FLEX IR_17_PAY IR_18_ID IR_19_BILL IR_20_CONTRACT IR_21_TECH IR_55_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 in giorni festivi: ≤ 6 ore (eccetto i FSCD con obblighi d'informazione supplementari, art. 22 OSCPT)	≤ 2 giorni lavorativi

Incarico	**Art. OSCPT**	**Tipi di incarichi**	**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	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 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	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI	≤ 1 ora	Da installare al momento indicato nell'incarico (> 1 ora)
Sorveglianza in tempo reale durante il servizio di pronto intervento	54 55 56	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI	≤ 1 ora	≤ 2 ore

	56*a* 56*b* 57 58 59	RT_56_POS_IMMED RT_57_POS_PERIOD RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI		
Sorveglianza retroattiva durante gli orari d'ufficio	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	≤ 3 giorni lavorativi
Sorveglianza retroattiva in casi urgenti (durante gli orari d'ufficio e il servizio di pronto intervento)	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 pronto intervento	67 cpv. 1 lett. a 67 cpv. 1 lett. b 67 cpv. 1 lett. c 67 cpv. 1 lett. d 67 cpv. 1 lett. e	EP_35_PAGING EP_58_POS_IMMED EP_59_POS_PERIOD EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 ora	≤ 1 ora
	67 cpv. 1 lett. f	EP_38_HD	≤ 1 ora	≤ 4 ore
Ricerca di condannati durante gli orari d'ufficio e il servizio di pronto intervento	68 cpv. 1 lett. a 68 cpv. 1 lett. e 68 cpv. 1 lett. d 68 cpv. 1 lett. e 68 cpv. 1 lett. e 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_56_POS_IMMED RT_57_POS_PERIOD	≤ 1 ora	≤ 1 ora
Ricerca di condannati durante gli orari d'ufficio e il servizio di pronto intervento	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 58 59 67 cpv. 1 lett. c 67 cpv. 1 lett. d 67 cpv. 1 lett. e	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_57_POS_PERIOD RT_25_TEL_IRI_CC RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI EP_59_POS_PERIOD EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 ora	≤ 1 giorno lavorativo

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

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