Rapporto esplicativo

concernente la modifica dell'ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT; RS *780.11*) e la modifica dell'ordinanza sulle tasse e indennità nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (RS *780.115.1*)

1. Situazione iniziale

Il servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni del Centro servizi informatici CSI-DFGP (di seguito: Servizio) ha il compito di assicurare la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, di restare al passo con l'evoluzione tecnologica adeguando di continuo le pertinenti basi legali.

È incontestato che il mercato dei servizi di telecomunicazione è in costante evoluzione offrendo ai clienti un ventaglio di possibilità sempre più ampio di comunicare nei modi più disparati. La tecnologia Internet in rapida espansione mette viepiù in ombra la tecnologia analogica (servizi a commutazione di circuito quali il telefono a rete fissa, il fax, ecc.). Anche gli autori di reato sfruttano in misura crescente e consapevolmente queste nuove sofisticate prestazioni di telecomunicazione sapendo che le nuove possibilità di comunicare non sono sorvegliate o lo sono soltanto limitatamente. A parere delle autorità di perseguimento penale, quest'evoluzione stride con le disposizioni dell'OSCPT, già da tempo obsolete e quindi di ostacolo a un perseguimento penale efficace nella lotta, ad esempio, contro la pedofilia, l'estremismo, il terrorismo, i reati economici (frode, spionaggio economico) o la narcocriminalità.

La Svizzera ha firmato la Convenzione del Consiglio d'Europa contro la cibercriminalità del 23 novembre 2001, che entrerà in vigore per la Svizzera il 1°gennaio 2012. La Convenzione esige, tra l'altro, il disciplinamento specifico, nel diritto nazionale, della raccolta dei cosiddetti dati informatici in tempo reale. L'obiettivo della presente revisione parziale dell'OSCPT è colmare queste lacune

Per tale motivo e vista l'urgenza di adeguare le disposizioni dell'OSCPT, è stato deciso di attuare questa revisione parziale senza aspettare la conclusione della revisione attualmente in corso della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT; RS *780.1*), che è di natura più sostanziale e disciplinerà il campo d'applicazione, gli obblighi degli offerenti di prestazioni di telecomunicazione (di seguito: offerenti), il sistema informatico per il trattamento dei dati raccolti e altre tematiche. È stata altresì sottoposta al Consiglio federale una proposta nel quadro dell'attuale revisione totale della LSCPT che tratta i quattro temi citati in precedenza.L'articolo 15 dell'attuale LSCPT permette di adeguare da subito l'OSCPT. Nella sua decisione del 23 giugno 2011 (A-8267/2010), in particolare nei considerandi 3.2. e 3.3.4., il Tribunale amministrativo federale giunge alla stessa conclusione sollecitando i legislatori

competenti per l'ordinanza perché avviino al più presto la revisione dell'OSCPT e adeguino i tipi di sorveglianza ai progressi della tecnica. L'ordinanza ha dovuto essere modificata anche a causa dell'entrata in vigore, il 1° gennaio 2011, del Codice di diritto processuale penale svizzero (CPP; RS *312.0*).

Secondo le autorità inquirenti competenti a ordinare misure di sorveglianza e i giudici dei provvedimenti coercitivi che li approvano, l'elenco delle misure di sorveglianza non va considerato esaustivo. Al considerando 3 della decisione del 23 giugno 2011 (A-8267/2010; pag. 7), il Tribunale amministrativo federale conclude che gli offerenti devono eseguire soltanto le misure esplicitamente menzionate nell'ordinanza. In passato questo significava che il Servizio doveva eseguire le misure di sorveglianza non elencate nell'ordinanza a proprie spese e con la propria infrastruttura. A tal fine gli offerenti dovevano unicamente concedere l'accesso alle proprie istallazioni e permettere al Servizio di eseguire la sorveglianza. Questo contraddice il mandato legale esaustivo della LSCPT e provocava per il Servizio, gli offerenti e le autorità inquirenti una notevole incertezza del diritto. Questo si può evitare integrando esplicitamente nell'OSCPT le corrispondenti misure di sorveglianza in materia di sorveglianza di Internet e adeguando l'ordinanza sugli emolumenti e le indennità nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (RS *780.115.2* di seguito: ordinanza sugli emolumenti). In questo modo non s'intende tuttavia estendere la cerchia degli offerenti rientranti nel campo d'applicazione. Sono assoggettati all'obbligo soltanto i fornitori di accesso a Internet. In particolare, non è previsto di assoggettare gli offerenti di applicazioni che non siano contemporaneamente fornitori di accesso a Internet all'obbligo derivante dalla sezione 6 AP-OSCPT. Questo vale sia per i servizi di messaggistica elettronica asincrona (ad es. e-mail) sia per i servizi di messaggistica elettronica sincrona (ad es. chat). Tuttavia, se i fornitori di accesso a Internet offrono questi servizi, soggiacciono agli obblighi di cui alla sezione 6.

In altre parole, gli offerenti di servizi Internet (quali chat, community e altri servizi a valore aggiunto) sono soggetti all'obbligo di sorveglianza soltanto se sono anche fornitori di accesso a Internet. L'OSCPT definisce le misure di sorveglianza divenute imprescindibili per le autorità inquirenti negli ultimi anni e riconosciute dalla giurisprudenza, mentre l'ordinanza sugli emolumenti stabilisce gli emolumenti e le indennità corrispondenti. Si tratta in particolare delle cosiddette ricerche per zona di copertura dell'antenna, della ricerca e del salvataggio di persone disperse (ricerca di emergenza) nonché della sorveglianza con implicazioni internazionali di persone sospette.

Va infine sottolineato che le misure di sorveglianza citate in precedenza secondo gli standard internazionali (ETSI)[1] sono concretizzate nelle direttive tecniche e amministrative del Servizio in applicazione dell'articolo 33 capoverso 1bis. Di conseguenza, anche l'esecuzione della sorveglianza di Internet sarà standardizzata, sia per il Servizio sia per gli offerenti, il che

[1] Istituto europeo delle norme di telecomunicazione, responsabile per l'armonizzazione della telecomunicazione.

comporterà una riduzione delle spese, poiché secondo l'articolo 16 LSCPT gli offerenti soggetti all'obbligo di notificazione dovranno essere in grado di attuare questi standard e assumersi i costi degli investimenti necessari a tal fine. Le autorità di perseguimento penale potranno quindi sorvegliare in modo più efficace anche la comunicazione tra gli autori di reato che si servono delle nuove tecnologie di telecomunicazione anche per la comunicazione transfrontaliera.

2. Commento alle singole disposizioni dell'ordinanza sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT; RS *780.11*)

Art. 1 cpv. 2 lett. e

Questa modifica concerne soltanto il testo italiano e quello tedesco. La versione francese vigente reca l'espressione «fournisseurs d'accès à Internet» (fornitori di accesso a Internet). La precisazione linguistica intende chiarire il campo d'applicazione. Sono soggetti all'obbligo di sorveglianza soltanto gli offerenti che soggiacciono all'obbligo di notificazione ai sensi della legge sulle telecomunicazioni e che forniscono l'accesso a Internet. I fornitori di chat, blog, community o servizi a valore aggiunto devono assicurare la sorveglianza di Internet soltanto se offrono ai loro clienti anche l'accesso a Internet..

I gestori di reti domestiche, reti aziendali e altre reti private (ad es. WLAN, WIFI o reti fisse in stazioni, aeroporti, ristoranti o alberghi) rientrano nel campo d'applicazione, ma secondo l'articolo 1 capoverso 4 LSCPT devono soltanto permettere la sorveglianza da parte del Servizio. Non sono quindi obbligati ad adottare provvedimenti attivamente, a investire o a salvare dati specifici.

Art. 2 Termini e abbreviazioni

L'elenco dei termini e delle abbreviazioni che figurava nell'articolo 2 è stato spostato nell'allegato sul modello dell'ordinanza concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT[2]).

Art. 8 cpv. 1

Riformulando l'articolo 8 capoverso 1 OSCPT, s'intende sottolineare che il sistema di trattamento del Servizio elabora tutti i dati raccolti nel corso della sorveglianza del traffico delle telecomunicazioni nel quadro di misure di sorveglianza ordinate e approvate. Tra questi dati figurano anche quelli raccolti in occasione della sorveglianza del traffico delle telecomunicazioni in Internet.

[2] RS **784.104** (cfr. art. 1 e allegato ORAT).

Art. 9 cpv. 1 e 2

Nel capoverso 1 sono stati adeguati i rinvii alle disposizioni vigenti sulla protezione e sicurezza dei dati.

Il capoverso 2 si fonda sull'attuale normativa in materia di sicurezza dei dati relativi alla trasmissione dei dati risultanti da una sorveglianza. Disciplinando esplicitamente la responsabilità per la sicurezza dei dati fino alla loro consegna al Servizio, il capoverso riflette la prassi adottata finora. Tale responsabilità si desume dall'articolo 15 capoverso 1 LSCPT, che impone agli offerenti di trasmettere al Servizio, su richiesta, il traffico delle telecomunicazioni della persona sorvegliata.

In questa sede si rimanda anche alle direttive CIC[3] sulla sicurezza informatica.

Art. 11 lett. d

Il Codice di diritto processuale penale svizzero, entrato in vigore il 1° gennaio 2011, ha abrogato l'articolo 4 capoverso 3 LSCPT, cui ora subentra l'articolo 271 capoverso 1 CPP. L'adeguamento è quindi puramente formale.

Titolo prima dell'art. 15

Sezione 4 Sorveglianza dei servizi telefonici

Il titolo di questa sezione non corrisponde alla situazione attuale e va pertanto adeguato. È infatti superfluo e fuorviante specificare che la sezione non riguarda Internet quando i nuovi articoli 24, 24*a*, 24*b* e 24*c* della sezione 6 vertono esclusivamente sulla sorveglianza di Internet. Conviene tuttavia sottolineare che rientrano in questa sezione anche i fornitori svizzeri di telefonia VoIP che sfruttano Internet come tecnologia di trasmissione e che quindi anche gli offerenti di simili servizi sono assoggettati agli obblighi cui sottostanno fornitori di servizi di telefonia classica.

Art. 15 cpv. 1 lett. d e i n. 2

Il CPP, entrato in vigore il 1° gennaio 2011, ha abrogato l'articolo 4 capoversi 3 e 4 LSCPT, cui sono subentrati gli articoli 271 capoverso 1 risp. 272 capoversi 2 e 3 CPP. Si tratta di un adeguamento formale.

Art. 16 Forme di sorveglianza (in tempo reale e retroattiva)

Come nelle altre disposizioni elencate qui di seguito, la lettera b è stata integrata con la nozione di «identificativo della cella (Cell ID)», affinché ciascun offerente di telefonia mobile fornisca la reale identificazione della cella secondo gli standard internazionali. Lo stesso vale per le lettere c numero 4 e d numero 3[4]. Il numero SIM, ovvero l'identificativo di ogni cliente, non costituisce un parametro disponibile nella rete. Per questo motivo, il numero SIM non figura più tra i parametri di rete da fornire di cui alle lette-

[3] Consiglio informatico della Confederazione.

[4] Cfr. anche art. 24*a* lett. a e b n. 6 e art. 24*b* lett. a n. 6 per quel che concerne le spiegazioni in merito all'identificazione cellulare (Cell ID).

re c numero 3 e d numero 2. Alla lettera c numero 5 è stata anche soppressa l'espressione «…e la durata del collegamento;» poiché, nel caso di una sorveglianza in tempo reale, questo parametro è già dato dal marcatempo (timestamp).

La nuova lettera e prevede un'ulteriore misura di sorveglianza consolidata nella prassi, ovvero la ricerca per zona di copertura dell'antenna. Questo tipo di ricerca permette di raccogliere retroattivamente i dati relativi al traffico di tutte le comunicazioni effettuate tramite telefonia mobile in una determinata cella di un'antenna e per un determinato periodo. I dati così rilevati possono, tra l'altro, essere analizzati in funzione dei numeri di chiamata in uscita e in entrata. È registrata soltanto la comunicazione realmente avvenuta.

Art. 16a Ricerca e salvataggio di persone disperse

In esecuzione dell'articolo 3 LSCPT, l'articolo 16*a* definisce le modalità di esecuzione delle misure di sorveglianza nel quadro della ricerca e del salvataggio di persone disperse o in situazione di emergenza (la cosiddetta ricerca di emergenza). Lo scopo di tale ricerca è localizzare l'apparecchiatura terminale della persona dispersa. Esistono tre tipi di ricerca di emergenza: (N1) la determinazione dell'ultimo luogo di localizzazione registrato dell'apparecchiatura terminale mobile della persona dispersa, (N2) la trasmissione continua in tempo reale dei dati relativi al traffico dell'apparecchiatura terminale della persona dispersa (per la telefonia mobile: anche la posizione attuale) e (N3) la ricerca e la consegna dei dati storici relativi al traffico dell'apparecchiatura terminale della persona dispersa (per la telefonia mobile: anche le informazioni sulla posizione).

Nell'ambito della telefonia mobile, il fornitore di prestazioni di telecomunicazione trasmette i dati concernenti la o le antenne di telefonia mobile con la quale è o era collegata l'apparecchiatura terminale mobile della persona dispersa. Questi dati possono essere: l'identificativo della cella (Cell ID), la posizione, la direzione di trasmissione e la banda di frequenza dell'antenna. Permettendo di localizzare approssimativamente l'apparecchiatura terminale mobile della persona dispersa, questi dati consentono di circoscrivere il luogo in cui quest'ultima si trova.

Le ricerche di emergenza (N2 e N3) possono essere ordinate anche in riferimento ai collegamenti alla rete fissa.

La ricerca di emergenza N2 attraverso un collegamento alla rete fissa può essere ordinata ad esempio quando l'autorità competente fa sorvegliare i collegamenti alla rete fissa della persona con intenti suicidi per raccogliere maggiori informazioni sul suo attuale luogo di soggiorno.

La ricerca di emergenza N3 attraverso un collegamento alla rete fissa può essere ordinata nel caso in cui l'autorità competente intende localizzare il possibile luogo di soggiorno della persona con intenti suicidi contattando le persone con le quali essa ha comunicato nelle ultime quattro settimane.

Art. 16b Misure di sorveglianza con implicazioni internazionali

Nella sua decisone del 10 marzo 2009 (A 2335/2008), il Tribunale amministrativo federale (TAF) ha stabilito chiaramente che la sorveglianza del traffico delle telecomunicazioni secondo gli articoli 15 capoverso 1 LSCPT e 16 OSCPT (vecchio) non si limita ai collegamenti nazionali con un numero di chiamata nazionale.

L'articolo 16*b* è stato introdotto per precisare l'applicabilità in termini geografici delle forme di sorveglianza di cui all'articolo 16 (misure di sorveglianza con implicazioni internazionali). Il capoverso 1 precisa che, anche se hanno implicazioni internazionali, le forme di sorveglianza sono considerate ordinarie secondo l'articolo 16 lettere a, c numeri 1-3 e 5 e d numeri 1, 2 e 4.

Una sorveglianza ha implicazioni internazionali se la misura di sorveglianza interessa il traffico delle telecomunicazioni da e verso un elemento d'indirizzo internazionale all'estero, un elemento d'indirizzo svizzero all'estero o un elemento d'indirizzo estero in Svizzera. Il traffico delle telecomunicazioni comprende i servizi di telefonia inclusi gli SMS. In tal caso possono essere ordinate anche forme di sorveglianza in tempo reale e retroattive del traffico delle telecomunicazioni, indipendentemente dall'appartenenza di rete dell'elemento d'indirizzo.

La sorveglianza del traffico delle telecomunicazioni con implicazioni internazionali presuppone tuttavia che detto traffico transiti attraverso una rete svizzera.

L'articolo 16*b* capoverso 2 chiarisce che le forme di sorveglianza di cui agli articoli 16 lettere b, c numero 4 e d numero 3 nonché 16*a* sono considerate ordinarie anche se ordinate per un Inbound-Roamer. L'Inbound-Roamer è un utente di telefonia mobile estero collegato in una rete di un offerente svizzero.

Con questa misura non è tuttavia possibile fornire tutti i parametri e tutti i dati nelle svariate situazioni immaginabili assicurando la stessa qualità di quella ottenuta nel quadro di una sorveglianza a carattere puramente nazionale.

Art. 17 cpv. 2, 4, 5, 6 e 7

L'articolo 271 capoverso 1 CPP persegue lo stesso obiettivo dell'articolo 4 capoversi 5 e 6 LSCPT. Il 1° gennaio 2011, con l'entrata in vigore del CPP, gli articoli 3-10 LSCPT sono stati abrogati, ragion per cui s'impone l'adeguamento dell'articolo 17 capoverso 2 OSCPT. Lo scopo è di assicurare la cernita delle informazioni raccolte durante la sorveglianza di una persona assoggettata al segreto professionale che non è oggetto delle indagini in corso. Da un lato, vanno adottate le necessarie misure di protezione e, dall'altro, il Servizio deve regolarmente informare l'autorità che ha ordinato la sorveglianza.

L'articolo 17 capoverso 4 è stato riformulato per precisare l'obbligo degli offerenti di trasmettere il traffico di telecomunicazioni della persona sorvegliata. Il capoverso 4 conferisce inoltre al Servizio la facoltà di stabilire nelle sue direttive i requisiti di tale trasmissione. È precisato che le direttive,

conformi agli standard dell'ETSI, garantiscono la sicurezza d'investimento degli offerenti e agevolano il processo di unificazione della sorveglianza del traffico delle telecomunicazioni secondo gli standard europei.

L'articolo 17 capoverso 5 è stato introdotto per permettere al Servizio di eseguire anche le misure di sorveglianza che non figurano nell'ordinanza, ma che sono state ordinate dalle autorità di perseguimento penale e approvate dai giudici dei provvedimenti coercitivi. Si rimanda in questa sede al commento relativo all'articolo 25 capoverso 5. Secondo la decisione del Tribunale amministrativo federale del 23 giugno 2011 (A-8267/2010), gli offerenti interessati devono permettere l'esecuzione di queste misure di sorveglianza. Non devono tuttavia attivarsi e mettere a disposizione del Servizio soltanto le interfacce già esistenti.

Sul piano materiale, i capoversi 6 e 7 corrispondono ai precedenti capoversi 5 e 6 del medesimo articolo.

Art. 18 cpv. 1, 3, 7 e 8

Il capoverso 1 è stato integrato con il complemento «…o far eseguire da terzi…» per precisare che un offerente interessato da una misura di sorveglianza può certamente coinvolgere terzi o cosiddette *persone ausiliarie* per adempiere il proprio mandato legale. Si tratta essenzialmente di ditte specializzate nel settore dell'intercettazione legale delle telecomunicazioni (lawful interception).

Il capoverso 3 è stato integrato con la congiunzione «anche» per sottolineare l'obbligo degli offerenti di essere in grado di ricevere ordini di sorveglianza in ogni momento e di eseguirli con la massima sollecitudine. Contrariamente a quanto prevedeva il vecchio capoverso 3, quest'obbligo si riferisce anche agli orari di servizio e non soltanto a quelli fuori servizio. Il capoverso 3 specifica inoltre che l'offerente comunica al Servizio per scritto i nominativi delle persone di riferimento. Le modifiche di tali dati devono essere comunicate al Servizio per scritto e senza indugio.

Nel capoverso 7 è stato eliminato l'avverbio «temporaneamente», poiché lo scopo è di offrire al Servizio la possibilità di utilizzare gratuitamente i servizi di telecomunicazione o le linee dell'offerente per verificare in ogni momento la capacità di eseguire misure di sorveglianza e per identificare e risolvere rapidamente i problemi che possono emergere nel corso della sorveglianza delle telecomunicazioni. Sebbene l'avverbio «temporaneamente» sia indefinito, se fosse mantenuto si rischierebbe di pregiudicare l'esecuzione corretta e ininterrotta delle misure sorveglianza. In altri termini, se il Servizio ritiene necessario controllare l'esecuzione di determinate forme di sorveglianza, deve poterlo fare senza essere costretto a negoziare la durata della verifica. Inoltre, nelle relative direttive organizzative e amministrative del Servizio figurano da anni le condizioni alle quali gli offerenti devono mettere gratuitamente a disposizione del Servizio i servizi di telecomunicazione da essi offerti con la specificazione di riferimento «Permanent Testing Environment».

Il nuovo capoverso 8 disciplina l'obbligo degli offerenti di assistere il Servizio nei casi in cui è necessario verificare che i dati risultanti dalla sorveglianza corrispondano effettivamente al traffico delle telecomunicazioni delle perso-

ne sorvegliate. Con questa disposizione non si esige dagli offerenti di salvare i dati in doppio. L'offerente interessato non deve adottare provvedimenti tecnici o organizzativi altri da quelli richiesti dalla LSCPT, dall'OSCPT o dalle direttive.

Titolo prima dell'art. 23

Sezione 6 Sorveglianza di Internet

Il titolo della sezione 6 è stato adeguato in seguito alla riformulazione dell'articolo 24 e all'introduzione degli articoli 24*a*, 24*b e* 24*c*. Negli articoli 23 lettera g numero 1, 24 capoverso 1 lettera b – f, 24 capoverso 2 lettera a e b, 24*b* lettera b numero 5 e 24*b* lettera a numero 5 è stato inserito tra parentesi, dopo la definizione generica (ad es. *elementi d'indirizzo noti* di cui all'art. 23 lett. g n. 1), un elenco non esaustivo di elementi d'indirizzo, di accessi e applicazioni Internet sorvegliabili e di parametri di comunicazione. Questi elenchi non esaustivi non intendono oltrepassare il quadro definito dal termine più generico che li precede né rimandare a qualsivoglia elemento ipotizzabile. I progressi nella tecnologia delle telecomunicazioni e dell'informatica, il crescente numero di applicazioni, di parametri e, in parte, di nomi proprietari rendono difficile elencare in maniera esaustiva questi elementi attribuibili al rispettivo termine generico.

Art. 23 lett. d, f e g

L'articolo 23 lettera d ha subito un adeguamento di carattere formale, visto che l'articolo 4 capoverso 3 LSCPT è stato abrogato il 1°gennaio 2011 con l'entrata in vigore del CPP per essere sostituito dall'articolo 271 capoverso 1 CPP.

La modifica della lettera f concerne il testo italiano e quello tedesco: il termine italiano «offerente Internet» e quello tedesco «Internet-Anbieterin» sono stati sostituiti con «fornitore di accesso a Internet», rispettivamente «Internetzugangsanbieterin»**.** Questa modifica terminologica interessa anche l'articolo 1 capoverso 2 lettera e nonché l'allegato.

In questo modo si chiarisce che gli obblighi definiti nella sezione 6 in riferimento alle applicazioni Internet valgono soltanto per gli offerenti soggetti all'obbligo di notificazione i quali sono nel contempo fornitori di accesso a Internet.

Senza essere esaustivo, l'elenco degli elementi d'indirizzo di cui alla lettera g numero 1 completa quello attuale. Lo scopo è di ottenere dalle autorità di perseguimento penale i dati dei relativi elementi d'indirizzo per eseguire le misure di sorveglianza di Internet da esse ordinate.

Art. 24 Forme di sorveglianza

L'articolo 24 è stato completamente riveduto, poiché non risponde più allo stato attuale della tecnica. La disposizione in vigore lascia intendere che la comunicazione in Internet avvenga soltanto per e-mail. È incontestato che i settori della tecnologia e dei servizi Internet abbiano subito e continueranno a subire importanti sviluppi. Nell'ambito di tale evoluzione, la comunicazione per e-mail riveste un ruolo marginale. L'adeguamento di questa parte

dell'OSCPT si è quindi imposto anche per motivi legati alla certezza del diritto e per mettere di nuovo a disposizione delle autorità di perseguimento penale uno strumento efficace per lottare contro la criminalità, in particolare nel campo della cibercriminalità. Oltre a riformulare l'articolo 24, si è provveduto a introdurre gli articoli 24*a*, 24*b* e 24*c*.

La suddivisione in quattro articoli ha lo scopo di conformare la sorveglianza di Internet alle disposizioni internazionali dell'ETSI sulla sorveglianza del traffico delle telecomunicazioni e di far confluire nell'ordinanza la giurisprudenza del TAF in materia di misure di sorveglianza con implicazioni internazionali. A tal fine, l'articolo 24 disciplina in prima linea gli accessi a Internet e le applicazioni che possono essere sorvegliate. Come già illustrato in riferimento all'articolo 23 lettera f, soltanto i fornitori di accesso a Internet sono assoggettati all'obbligo di sorveglianza delle applicazioni Internet. Questo obbligo concerne soltanto le applicazioni offerte ai clienti dagli offerenti soggetti all'obbligo di notificazione che sono nel contempo fornitori di accesso a Internet. Gli articoli 24*a* e 24*b*, invece, definiscono le singole forme di sorveglianza. Più precisamente, l'articolo 24*a* verte sulla sorveglianza in tempo reale e l'articolo 24*b* sulla sorveglianza retroattiva. L'articolo 24*c*, infine, disciplina le misure di sorveglianza con implicazioni internazionali.

L'articolo 24 definisce in modo dettagliato i diversi canali di comunicazione fornendo un elenco corredato di esempi delle svariate tecnologie attuali per la trasmissione di dati Internet.

Il capoverso 1 stila un elenco dei seguenti canali di comunicazione:

a. l'accesso a Internet via un Network Access Server su linea commutata è il primo tipo di accesso a Internet offerto al pubblico, ovvero l'accesso attraverso un collegamento telefonico. Questo tipo di accesso è usato ancora oggi per garantire accesi remoti sicuri;

b. l'accesso a Internet a banda larga è il tipo di accesso più diffuso. Si tratta, in particolare, della tecnologia ADSL e degli accessi VDSL o via cavo;

c. la tipologia descritta corrisponde all'accesso a Internet attraverso una rete mobile (ad es. GPRS o LTE). Questo accesso avviene tramite onde radio per mezzo di un cellulare o di un altro apparecchio mobile quale, ad esempio, un portatile o un notepad (la connessione a Internet è continua, indipendentemente dagli spostamenti dell'apparecchio terminale mobile);

d. l'accesso a Internet senza fili è effettuato tramite onde radio, principalmente tramite Wi-Fi, a disposizione del pubblico nella maggior parte dei luoghi liberamente accessibili;

e. la tipologia descritta corrisponde all'accesso a fibra ottica, direttamente a domicilio dell'utente finale (ad es. Ethernet con accesso Fiber To The Home). Si tratta ancora di una tecnologia di punta nel campo delle connessioni, ma entro il 2020 sarà di uso comune;

f. la tipologia descritta corrisponde agli accessi effettuati attraverso lo strato 3 OSI (ad es. accesso IP a banda larga).

Il capoverso 2 elenca in prima linea i servizi Internet (applicazioni) che possono essere sorvegliati presso i fornitori di accesso a Internet, nella misura in cui li offrano ai loro clienti. Alla lettera a sono citati, da un lato, i servizi di messaggistica elettronica asincrona (ad es. e-mail), che non forniscono all'utente le informazioni in tempo reale, dall'altro, i servizi di messaggistica elettronica sincrona (ad es. Instant Messaging o Chat), che permettono lo scambio d'informazioni in tempo reale.

La lettera b disciplina la possibilità di sorvegliare servizi di telecomunicazione che si basano su media digitali quali la trasmissione di comunicazioni vocali, dati e contenuti (ad es. testi, grafica, animazioni, dati audio e video) in quanto parte integrante della telecomunicazione.

Art. 24a Forme di sorveglianza (in tempo reale)

L'articolo 24*a* descrive i tipi d'informazioni che possono essere sorvegliati in tempo reale. Le lettere a e b disciplinano le forme di sorveglianza per l'accesso a Internet e le lettere c e d quelle per le applicazioni Internet.

a. La sorveglianza secondo la lettera a è effettuata direttamente sull'accesso a Internet. In questo modo è sorvegliato in tempo reale l'intero traffico di dati in transito attraverso quest'accesso;

b. la lettera b si riferisce a tutti i dati che non riguardano il contenuto della comunicazione, bensì la configurazione e l'amministrazione della connessione. Segue un elenco di parametri:

   1. i parametri usuali dell'offerente in merito all'inizio e alla fine di una sessione Internet, ordinati per ora e data,
   2. il tipo di connessione a Internet quali, ad esempio, ADSL o UMTS,
   3. le tracce lasciate dall'utente al momento dell'accesso quali, ad esempio, il nome d'utente, la parola chiave, l'ora del login,
   4. tutti gli elementi d'indirizzo, in particolare quelli in merito all'origine della comunicazione (ad es. il numero di telefono del cellulare con il quale è stata stabilita la connessione a Internet),
   5. i parametri di comunicazione e quelli d'identificazione degli utenti. I primi sono costituiti dai parametri direttamente collegati all'apparecchiatura terminale quali, ad esempio, l'indirizzo MAC e il numero IMEI, i secondi dagli ulteriori criteri d'identificazione a disposizione dell'offerente, non per forza direttamente riferiti all'apparecchiatura terminale (ad es. il numero IMSI),
   6. la sorveglianza del traffico Internet generato da un telefono cellulare attraverso una rete mobile. Le informazioni raccolte consentono di localizzare l'apparecchiatura terminale. La posizione dell'apparecchio terminale è dedotta da tutti i parametri da fornire in base al numero 6,
   7. le informazioni che possono essere richieste durante una connessione di comunicazione. In tal caso l'autorità di perseguimento penale ha la possibilità di chiedere un rapporto tecnico

su tutti i cambiamenti originati dal sorvegliato o dall'offerente (ad es. cambio di abbonamento, modifiche della rete);

c. la lettera c disciplina la sorveglianza del contenuto di un'applicazione (ad es. il contenuto di un'e-mail);

d. la lettera d si riferisce a tutti i dati che non riguardano il contenuto di un'applicazione, bensì la configurazione e l'amministrazione della connessione. Segue un elenco di parametri:

1. i parametri usuali dell'offerente relativi all'inizio e alla fine di una sessione Internet, ordinati per ora e data,
2. tutti gli elementi d'indirizzo, in particolare quelli in merito all'origine e alla destinazione della comunicazione,
3. gli elementi che riguardano l'accesso a un servizio Internet (ad es. nome d'utente, parola chiave),
4. le informazioni della busta secondo il protocollo impiegato (ad es. il protocollo SMTP). Si tratta di protocolli standard per inviare e ricevere le e-mail,
5. altri parametri di comunicazione generati e conservati presso il fornitore di accesso a Internet in caso di utilizzo di un servizio Internet, quali ad esempio l'indirizzo di porta dell'origine e della destinazione della comunicazione,
6. le informazioni che possono essere richieste durante una comunicazione attraverso un servizio Internet. In tal caso l'autorità di perseguimento penale ha la possibilità di chiedere un rapporto tecnico su tutti i cambiamenti originati dal sorvegliato o dal fornitore di accesso a Internet (ad es. cambio di abbonamento, modifiche del login del sorvegliato che accede a Internet).

Art. 24b Forme di sorveglianza (retroattiva)

L'articolo 24*b* si riferisce alla cosiddetta sorveglianza retroattiva, ossia ai dati registrati e conservati dal fornitore di accesso a Internet.

La lettera a riguarda la trasmissione dei dati relativi al traffico riguardanti l'attribuzione di almeno uno dei parametri specificati qui di seguito.

1. Il numero 1 impone la consegna dei seguenti elementi: data e ora d'inizio e fine della connessione. Nello specifico, il termine *connessione* definisce l'intera sessione Internet e non ogni singola azione effettuata nel quadro di una simile sessione;
2. il numero 2 chiede informazioni sul tipo di connessione o di collegamento, ad esempio una connessione ADSL o un collegamento analogico;
3. il numero 3 riguarda i dati di accesso noti (nomi d'utente e parole chiave);
4. il numero 4 si riferisce agli elementi d'indirizzo noti dell'accesso Internet sorvegliato, in particolare quelli relativi all'origine della comunicazione (ad es. l'indirizzo IP, il numero telefonico del collegamento ADSL;

5. il numero 5 riguarda le informazioni note al momento dell'impiego di un apparecchio per accedere a Internet. L'elenco non è esaustivo e si riferisce, ad esempio, all'accesso tramite computer o cellulare («smartphone»);

6. tra le informazioni menzionate al numero 6 si annoverano anche quelle relative all'identificativo della cella (Cell ID)[5] durante la sorveglianza di un cellulare usato per accedere a Internet.

La lettera b si riferisce, in particolare, all'ottenimento d'informazioni retroattive risultanti dalla sorveglianza di un servizio di messaggistica elettronica asincrona. Si tratta propriamente di dati riguardanti la sorveglianza di e-mail. In questi casi devono essere trasmessi alle autorità di perseguimento penale i dati seguenti:

1. i dati di base generati presso il fornitore di accesso a Internet in occasione dell'invio e della ricezione di messaggi mediante servizi di messaggistica elettronica asincrona, ossia la data e l'ora dell'invio e della ricezione;

2. i parametri registrati e conservati dal fornitore di accesso a Internet durante l'impiego di un protocollo, necessari, ad esempio, per inviare o ricevere e-mail;

3. gli indirizzi IP impiegati per l'invio e la ricezione di messaggi trasmessi mediante servizi di messaggistica elettronica asincrona (ad es. e-mail);

4. tutti gli altri elementi d'indirizzo disponibili registrati dal fornitore di accesso a Internet in occasione dell'invio o della ricezione di messaggi della persona sorvegliata.

Art. 24c Misure di sorveglianza con implicazioni internazionali

Con decisione del 10 marzo 2009 (A 2335/2008), il TAF ha statuito che la sorveglianza del traffico delle telecomunicazioni secondo gli articoli 15 capoverso 1 LSCPT e 16 OSCPT (vecchio) non si limita ai collegamenti nazionali con un numero di chiamata nazionale. Il ricorso alla base di questa decisione verteva sulla sorveglianza di un collegamento telefonico situato all'estero. Di conseguenza, la decisione del TAF interessa i servizi di telefonia.

Le conclusioni giudiziarie si applicano tuttavia anche alla sorveglianza di Internet. Il TAF ha di fatto concluso che la sorveglianza del traffico delle telecomunicazioni tra un elemento d'indirizzo estero e qualsiasi elemento d'indirizzo situato nella rete di un offerente svizzero non è contraria allo spirito della LSCPT. Come previsto dall'articolo 15 capoverso 1 OSCPT, un collegamento simile permette di sorvegliare il traffico delle telecomunicazioni di una determinata persona e, come nel caso della sorveglianza di un elemento d'indirizzo nazionale, l'oggetto della sorveglianza è un determinato elemento d'indirizzo. Dall'articolo 15 capoverso 1 LSCPT non è possibile dedurre che la sorveglianza sia limitata a un elemento d'indirizzo nazionale con un accesso nazionale.

[5] Cfr. quanto esposto in precedenza in merito all'art. 16 OSCPT.

L'articolo 24*c* è stato introdotto per precisare l'applicabilità in termini geografici delle forme di sorveglianza di cui agli articoli 24, 24*a* e 24*b* (misure di sorveglianza con implicazioni internazionali). L'articolo 24*c* precisa quindi che le misure di sorveglianza, anche se hanno implicazioni internazionali, costituiscono forme di sorveglianza ordinarie secondo gli articoli 24 capoverso 1 lettere c e d, 24*a* lettere a e b e 24*b* lettera a.

Si hanno implicazioni internazionali quando una misura di sorveglianza interessa il traffico Internet da e per un elemento d'indirizzo estero all'interno del Paese, chiamato Inbound Roamer. Il traffico delle telecomunicazioni comprende il traffico in Internet attraverso una rete telefonica mobile svizzera o un accesso senza fili in Svizzera. L'elemento d'indirizzo da sorvegliare può essere, ad esempio, un numero MSISDN o un numero IMSI. Nel caso specifico possono essere ordinate anche forme di sorveglianza in tempo reale e retroattive, indipendentemente dall'appartenenza di rete dell'elemento d'indirizzo.

Con questa misura non è tuttavia possibile fornire tutti i parametri e tutti i dati nelle svariate situazioni immaginabili assicurando la stessa qualità di quella garantita nel quadro di una sorveglianza a carattere puramente nazionale.

Art. 25 Esecuzione della sorveglianza

Integrato con due capoversi nuovi (4 e 5), questo articolo ora ne comprende sette.

Il capoverso 1 lettera a è mantenuto nella sua forma attuale. Soltanto il capoverso 1 lettera b è integrato con l'espressione «se necessario», affinché il Servizio possa continuare a decidere se contattare il fornitore di accesso a Internet nei casi menzionati al capoverso 1 lettera b. Contrariamente alla versione francese, in quelle italiana e tedesca è stato necessario modificare i termini «offerente Internet» e «Internet-Anbieterin» sostituendoli con «fornitore di accesso a Internet» e «Internetzugangsanbieterinnen».

Il capoverso 2, tenendo conto dell'entrata in vigore del CPP il 1° gennaio 2011 e della conseguente abrogazione degli articoli 3-10 LSCPT, rinvia all'articolo 271 capoverso 1 CPP, che persegue lo stesso obiettivo dell'articolo 4 capoversi 5 e 6 LSCPT. Il capoverso è stato adeguato anche perché la sorveglianza non interessa più soltanto le applicazioni e-mail, ma anche gli accessi e le applicazioni Internet (rinvio agli articoli 24, 24*a* e 24*b*).

Il capoverso 3 ha subito lo stesso adeguamento linguistico del capoverso 1 lettera b: i termini impiegati ora sono «fornitori di accesso a Internet» per l'italiano e «Internetzugangsanbieterinnen» per il tedesco.

Il capoverso 4 è stato introdotto per precisare l'obbligo degli offerenti Internet di trasmettere il traffico delle telecomunicazioni delle persone sorvegliate. Questo capoverso conferisce inoltre al Servizio la facoltà di stabilire, nelle sue direttive, i requisiti di tale trasmissione. Viene specificato che le direttive si fondano sugli standard ETSI per garantire la sicurezza d'investimento degli offerenti e per promuovere l'unificazione della sorveglianza del traffico delle telecomunicazioni secondo gli standard europei.

Il capoverso 5 è stato introdotto per disciplinare in via separata la facoltà del Servizio di ordinare ai fornitori di servizi di telecomunicazione interessati l'esecuzione di misure di sorveglianza che, pur non figurando esplicitamente nell'ordinanza, sono state ordinate dalle autorità di perseguimento penale e approvate dai giudici dei provvedimenti coercitivi. In questa sede si rimanda altresì a quanto esposto in merito all'articolo 17 capoverso 5. Secondo la decisione del Tribunale amministrativo federale del 23 giugno 2011 (A-8267/2010), gli offerenti interessati devono permettere l'esecuzione di simili misure di sorveglianza mettendo a disposizione del Servizio soltanto le interfacce già esistenti.

Nell'articolo 25 capoverso 6, nelle versioni italiana e tedesca, i termini «offerente Internet» e «Internet-Anbieterin» sono stati sostituiti con «fornitore di accesso a Internet» e «Internetzugangsanbieterin».

Il contenuto dei capoversi 4 e 5 è stato spostato ai capoversi 5 e 6.

Art. 26 Obblighi dei fornitori di accesso a Internet

L'articolo è stato riformulato e conformato al nuovo articolo 18 OSCPT. Ora comprende sette capoversi anziché cinque. In aggiunta, nelle versioni italiana e tedesca, nel titolo e nei capoversi 1, 2, 3, 5, 6 e 7 i termini «offerente Internet» e «Internet-Anbieterin» sono stati sostituiti con «fornitore di accesso a Internet» e «Internetzugangsanbieterin».

Queste modifiche sono dovute alla nuova terminologia dell'articolo 1 capoverso 2 lettera e.

Il rinvio obsoleto del capoverso 1 al vecchio articolo 24 OSCPT è stato eliminato e sostituito con un nuovo rinvio alla sezione 6. Il capoverso 1 dell'articolo 18 è stato inoltre integrato con l'espressione «…o far eseguire da terzi…» per precisare che un offerente interessato da una misura di sorveglianza può certamente coinvolgere terzi o cosiddette *persone ausiliarie* per l'adempimento del proprio mandato legale. Si tratta essenzialmente di ditte specializzate nel settore dell'intercettazione legale delle telecomunicazioni (lawful interception). Il capoverso 3, oltre ad essere stato armonizzato terminologicamente nelle tre lingue ufficiali è stato conformato al nuovo articolo 18 capoverso 3 OSCPT. Viene inoltre precisato che i fornitori di accesso a Internet devono comunicare al Servizio per scritto e senza indugio i nominativi delle persone di riferimento e gli eventuali cambiamenti degli stessi. Il rinvio obsoleto del capoverso 4 al vecchio articolo 24 OSCPT è stato soppresso e sostituito con un rinvio agli articoli 24-24*c*. Il capoverso è stato inoltre adeguato al fatto che la sorveglianza non verte più soltanto sulle applicazioni e-mail, ma anche sugli accessi e le applicazioni Internet (rinvio agli art. 24, 24*a*, 24*b* e 24*c*).

Il vecchio contenuto del capoverso 5 è stato abrogato, poiché trattava aspetti di natura organizzativa e amministrativa già disciplinati nelle direttive organizzative e amministrative del Servizio[6]. Il nuovo tenore disciplina l'obbligo dei fornitori di accesso a Internet di collaborare tra di loro per sor-

[6] Direttive OAR (Organsiational and Administrative Requirements) del Servizio, che sono a disposizione degli offerenti.

vegliare il traffico di telecomunicazioni che transita attraverso le reti di diversi fornitori di accesso a Internet.

Il contenuto del capoverso 6 corrisponde a quello dell'articolo 18 capoverso 8.

Il nuovo capoverso 7 disciplina l'obbligo degli offerenti di assistere il Servizio nel verificare, caso per caso, che i dati risultanti dalla sorveglianza corrispondano effettivamente al traffico delle telecomunicazioni della persona sorvegliata.

Art. 27 cpv. 1 e cpv. 2

Nella parte introduttiva del capoverso 1 delle versioni italiana e tedesca, i termini «offerente Internet» e «Internet-Anbieterin» sono stati sostituiti con «fornitore di accesso a Internet» e «Internetzugangsanbieterin» (cfr. quanto esposto in precedenza riguardo all'art.1 cpv. 2 lett. e).

Il capoverso 1 lettera a è stato adeguato affinché questo articolo, in quanto disposizione esecutiva dell'articolo 14 capoverso 4 LSCPT (identificazione dell'autore del reato commesso mediante Internet), non si applichi soltanto agli utenti di indirizzi IP attribuiti in modo definitivo (indirizzi IP statici), ma anche all'identificazione degli utenti di indirizzi IP dinamici. La disposizione è stata inoltre integrata con i dati usati per la procedura d'identificazione (login) e gli altri indirizzi IP che i fornitori di accesso a Internet hanno attribuito agli utenti. È stata inoltre adeguata, a livello terminologico, alla parte introduttiva dell'articolo 27 capoverso 1.

La modifica del capoverso 1 lettera b riguarda soltanto il testo italiano e quello tedesco, in cui i termini «offerente Internet» e «Internet-Anbieterin» sono stati sostituiti con «fornitore di accesso a Internet» e «Internetzugangsanbieterin».

Il capoverso 1 lettera c è stato modificato affinché l'obbligo di identificare i clienti non si limiti ai servizi e-mail, bensì venga esteso a tutti i servizi di messaggistica elettronica, nella misura in cui siano stati messi a disposizione della clientela da parte dei fornitori di accesso a Internet. L'adeguamento terminologico interessa il termine «fornitore di accesso a Internet» nella versione italiana e «Internetzugangsanbieterin» in quella tedesca.

Contrariamente alla versione francese, anche nel capoverso 2 delle versioni italiana e tedesca è stato necessario sostituire il termine «offerente Internet» rispettivamente «Internet-Anbieterin» con «fornitore di accesso a Internet» e «Internetzugangsanbieterin».

Art. 36b

L'articolo 36*b* statuisce che i fornitori di accesso a Internet da rete fissa e da rete mobile devono essere in grado, al più tardi entro 12 mesi dall'entrata in vigore della presente modifica, di adempiere gli obblighi ed eseguire i tipi di sorveglianza definiti nella sezione 6. Considerata la portata dei lavori preparatori che grava sui fornitori per il calcolo del preventivo, l'acquisizione dell'*hardware*, l'attuazione e l'esame degli aggiornamenti del *software* e l'adeguamento dei processi amministrativi, un termine transitorio di 12 mesi appare appropriato. Inoltre, nella decisione del Tribunale amministrativo

federale del 10 marzo 2009 (A-2335/2008), a un offerente è stato concesso un termine di attuazione di 12 mesi per dotarsi delle capacità necessarie per effettuare le misure di sorveglianza con implicazioni internazionali. Se agli offerenti fosse imposto un termine transitorio più breve, la maggior parte di essi sarebbe in ritardo nell'adempiere gli obblighi e attuare i tipi di sorveglianza ora definiti nella sezione 6. Il termine di un anno per dotarsi delle capacità necessarie per eseguire i tipi di sorveglianza di cui alla sezione 6 consente di implementare i processi per la sorveglianza delle e-mail secondo l'articolo 24 OSCPT e di adeguarli agli standard dell'Istituto europeo per le norme di telecomunicazione (ETSI).

È tuttavia fatta un'eccezione per l'articolo 25 capoverso 5 AP OSCPT.

Sebbene la questione sia anche disciplinata nella sezione 6, il termine transitorio non è concesso nel caso in cui l'offerente permette la sorveglianza mettendo semplicemente a disposizione le interfacce esistenti. La disposizione transitoria non si applica nemmeno ai tipi di sorveglianza definiti nella sezione 4 ed eseguiti già da anni (in specie: la ricerca per zona di copertura dell'antenna secondo l'art. 16 lett. e AP OSCPT, la ricerca e il salvataggio di persone disperse secondo l'art. 16*a* AP OSCPT e le misure di sorveglianza con implicazioni internazionali secondo l'art. 16*b* AP OSCPT).

Allegato Termini e abbreviazioni

Fondandosi sull'articolo 2, l'allegato riporta l'elenco dei termini e delle abbreviazioni in uso nel settore della sorveglianza delle telecomunicazioni.

3. Modifica dell'ordinanza sulle tasse e indennità nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (RS 7*80.115.1*)

3.1. Introduzione

La revisione parziale dell'ordinanza ha lo scopo, da un lato, di definire gli emolumenti e le indennità per le misure di sorveglianza emerse nella prassi. Si tratta in particolare di tre misure: la trasmissione di dati relativi a misure di sorveglianza con implicazioni internazionali (art. 16*b* AP OSCPT), la ricerca per zona di copertura dell'antenna (art. 16 lett. e AP OSCPT) e la ricerca e il salvataggio di persone disperse (ricerca di emergenza; art 16*a* AP OSCPT). Dall'altro, la revisione è tesa a definire gli emolumenti e le indennità per la sorveglianza di Internet. L'articolo 4 non risponde più alle attuali esigenze legali in materia di emolumenti. Per colmare questa lacuna sono stati quindi introdotti due articoli nuovi (art. 4 e 4*a* OEm-SCPT). Il testo dell'ordinanza ha inoltre subito qualche modifica di lieve entità al fine di eliminare alcune imprecisioni.

3.2 Commento alle singole disposizioni

Titolo

Il titolo «Ordinanza sulle tasse e indennità nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni» è sostituito con «Ordinanza sugli emolumenti e le indennità per la sorveglianza

della corrispondenza postale e del traffico delle telecomunicazioni (OEm-SCPT)».

Art. 1 cpv. 2bis

Il nuovo capoverso 2bis specifica che, per la sorveglianza di un elemento d'indirizzo, di formato svizzero o estero, sono riscossi una sola indennità e un solo emolumento.

Art. 2 Emolumenti e indennità

A. Servizi a commutazione di circuito

Occorre innanzitutto sottolineare che è rimasta immutata la strutturazione delle differenti misure di sorveglianza in base agli articoli 16, 16*a* e 16*b* OSCPT (traffico a commutazione di circuito [Circuit Switched, CS]) o agli articoli 24, 24*a* e 24*b* (traffico a commutazione di pacchetto [Paket Switched, PS]). In linea di massima restano invariati gli emolumenti e le indennità per le misure di sorveglianza figuranti già nell'ordinanza attuale. L'introduzione, nella rubrica CS, dei nuovi articoli 16 lettera e, 16*a* e 16*b* non ha comportato alcun adeguamento degli emolumenti o delle indennità delle altre misure di sorveglianza figuranti nella tabella. L'unica novità consiste nel fatto che le rubriche CS 5, CS 6 nonché N 1-3 (ricerca di emergenza) sono state integrate con la prassi del Servizio in materia di riscossione degli emolumenti e di versamento delle indennità.

B. Servizi a commutazione di pacchetto

1. Osservazioni preliminari

Nel diritto vigente le rubriche PS 1-5 e 8 contemplano soltanto la sorveglianza del traffico e-mail. Come illustrato all'inizio del presente rapporto (cfr. n. 1), la revisione parziale dell'OSCPT ha, tra l'altro, l'obiettivo di disciplinare in modo esaustivo la sorveglianza di Internet. Per tale motivo, svariate rubriche alla lettera B vanno sostituite o adeguate sulla scorta delle modifiche nella sezione 6 OSCPT.

2. Rubriche PS 1-4

La nuova struttura della sezione 6 OSCPT, e in particolare degli articoli 24, 24*a*, 24*b* e 24*c*, differenzia tra la sorveglianza dell'accesso a Internet e quella delle singole applicazioni Internet. Opera inoltre una netta distinzione tra la sorveglianza in tempo reale dell'accesso a Internet e delle applicazioni (art. 24*a*) e quella retroattiva dell'accesso a Internet e dei servizi di messaggistica elettronica asincrona (art. 24*b*).

Concretamente, le misure di sorveglianza di cui all'articolo 24*a* figurano nelle rubriche PS 1-4 e quelle secondo l'articolo 24*b* nelle rubriche PS 5-6.

Per lo stesso motivo è stato necessario sostituire la terza colonna, che finora conteneva l'elemento d'indirizzo da sorvegliare, con le informazioni relative all'accesso e alle applicazioni Internet o ai servizi di messaggistica elettronica asincrona, ora soggetti a sorveglianza. Sempre nella stessa

colonna (rubriche PS 1-4) viene precisato il tipo d'informazioni che i fornitori di accesso a Internet devono trasmettere, ovvero:

- **il contenuto e i dati relativi al traffico** (PS 1) o soltanto **i dati relativi al traffico** di un accesso a Internet (PS 2),
- **il contenuto e i dati relativi al traffico** (PS 3) o soltanto **i dati relativi al traffico** di un'applicazione Internet (PS 4).

La rubrica PS 1 contempla la sorveglianza in tempo reale di un accesso a Internet e la trasmissione dei dati relativi al traffico.

Gli emolumenti per tale servizio ammontano a 4 160 franchi.

L'importo indicato si compone della quota di emolumento per il Servizio (1 080 fr.; cfr. CS 1-3) e della quota d'indennità a favore dei fornitori di accesso a Internet (1 330 fr.) e si riallaccia all'indennità per l'esecuzione di una misura secondo la rubrica CS 1-3 dell'attuale ordinanza sugli emolumenti. La differenza tra questo importo di base, pari a 2 410 franchi, e l'importo complessivo di 4 160 franchi è riconducibile alle spese di conservazione dei dati presso il centro di trattamento del Servizio.

Il calcolo parte dal presupposto di un costo di 50 franchi per anno e gigabyte (GB) di dati (su un sistema di stoccaggio ad alta disponibilità e ridondante), di un fabbisogno supplementare medio di 20 GB al mese e di una permanenza media di circa sei mesi dei dati nel sistema. Applicando la seguente formula si arriva quindi a un totale di 1 750 franchi per ciascuna misura di sorveglianza:

$$20\,GB \times \frac{6\,(6+1)}{2}\,mesi \times \frac{50\ fr.}{12\,mesi \times GB} = 1\,750\ fr.$$

La rubrica PS 2 indica l'indennità da versare a un collaboratore di un servizio di telecomunicazione per mezza giornata di lavoro (quattro ore) o a un collaboratore del Servizio per un'ora di lavoro. Ad entrambi è applicata la stessa tariffa oraria. La medesima base di calcolo si applica alla riscossione degli emolumenti e al versamento dell'indennità della rubrica PS 4.

La rubrica PS 3, vertente sulla sorveglianza in tempo reale di un'applicazione Internet di un fornitore di accesso a Internet e la consegna dei dati relativi al traffico, corrisponde all'onere di lavoro delle attuali rubriche 1-5, che comprendono la sorveglianza in tempo reale di un'e-mail (contenuto e dati relativi al traffico).

3. Rubriche 5 e 6

La rubrica 5 riprende le attuali rubriche 6 e 7. I dati relativi al traffico richiesti corrispondono a quelli degli articoli 24 lettere f e g nonché 16 lettera d (CS 4) per gli accessi a Internet mediante una rete mobile.

La rubrica P6 si rifà all'attuale rubrica PS 8. I dati da trasmettere non si limitano tuttavia a quelli dell'attuale articolo 24 lettera h OSCPT, ma comprendono anche quelli spediti o ricevuti tramite i servizi di messaggistica elettronica asincrona.

Considerato quanto detto, gli emolumenti e le indennità sono conformi alla prassi attuale e corrispondono agli importi previsti dall'attuale ordinanza sugli emolumenti.

4. Rubriche A 0.1 e A 0.2

La rubrica A 0.1 ricalca l'attuale rubrica A 0 mantenendo invariati gli emolumenti e l'indennità. L'unica novità è la creazione di una nuova rubrica (A 0.2) che contempla, invece dell'attuale rubrica PS 6, l'identificazione degli utenti di indirizzi IP dinamici secondo l'articolo 14 LSCPT capoverso 4 mantenendo invariati gli emolumenti e l'indennità (cfr. quanto illustrato in merito all'art. 27 cpv. 1 lett. a).

Art. 3 frase introduttiva Forfait supplementari per prestazioni fornite al di fuori degli orari d'ufficio ordinari

Nello specifico, si tratta di un semplice adeguamento all'attuale denominazione del Servizio.

Per l'applicazione del forfait per prestazioni fornite al di fuori degli orari d'ufficio ordinari, il termine «provvedimento» è stato sostituito con il termine «mandato». Tale importo forfettario viene fatturato una sola volta per mandato e offerente, precisato che un mandato può comprendere svariate misure di sorveglianza o richieste d'informazione.

Art. 3a Altre prestazioni

Questo articolo si riferisce alla prassi consolidata e incontestata del Servizio di fatturare all'autorità di perseguimento penale un emolumento pari a 125 franchi per ogni copia supplementare di un DVD o di un disco rigido.

Art. 4 Emolumenti per prestazioni non previste

Il capoverso 1, che permette al Servizio di riscuotere emolumenti per prestazioni che non figurano nell'elenco dell'OSCPT, riprende la seconda frase dell'attuale articolo 4. Il capoverso 2 fissa l'indennità oraria. L'importo di 160 franchi corrisponde alla tariffa oraria media dei collaboratori del Servizio e tiene conto delle loro qualifiche e conoscenze tecniche. Si riallaccia inoltre alla prassi di fatturazione del Servizio, già confermata dal Tribunale federale (cfr. Tribunale federale, decisione del 20 marzo 2007, 1A.255/2006), e tiene conto sia delle tariffe previste da determinate ordinanze sugli emolumenti della Confederazione[7] sia del fatto che il Servizio è chiamato a eseguire oltre 10 000 misure di sorveglianza l'anno. Dal momento che ogni misura di sorveglianza coinvolge uno o più collaboratori del Servizio (giuristi, ingegneri, personale amministrativo), non appare ragionevole riportare le singole tariffe orarie dei singoli collaboratori. Tale differenziazione nel calcolare gli emolumenti comporterebbe un grave sovraccarico amministrativo del Servizio Il capoverso 3 definisce la base di calcolo per scaricare le spese supplementari legate all'acquisto di apparecchi e quelle riconducibili agli inve-

[7] In particolare l'ordinanza sugli emolumenti del Controllo federale delle finanze (RS **172.041.17**) e l'ordinanza sugli emolumenti per le prestazioni dell'Ufficio federale di giustizia (RS **172.041.14**)

stimenti tecnici. Secondo la prassi adottata finora, l'emolumento comprende sia l'indennità da versare all'offerente sia quella spettante al Servizio per ciascun mandato di sorveglianza. La tariffa oraria pari a 160 franchi si applica sia ai collaboratori dell'offerente sia a quelli del Servizio.

Art. 4a Indennità per prestazioni non previste

Il capoverso 1, corrispondente al capoverso 1 dell'articolo 4 per quanto riguarda le indennità non elencate nell'ordinanza, stabilisce che l'indennità è parte integrante dell'emolumento riscosso dalle autorità di perseguimento penale. L'emolumento si compone quindi dell'indennità per il Servizio e di quella per gli offerenti. L'importo dell'indennità destinata al Servizio si ottiene sottraendo dall'emolumento l'indennità da versare agli offerenti.

Il capoverso 2 dell'articolo 4*a* fissa la tariffa oraria a 160 franchi (cfr. quanto esposto in merito all'art. 4).

Il capoverso 3 definisce in modo dettagliato le modalità di fatturazione per gli offerenti di servizi postali e di telecomunicazione, affinché il Servizio possa indennizzarli correttamente e in conformità con l'articolo 4*a*.

Il capoverso 4 stabilisce che le indennità coprono l'80 per cento dell'onere complessivo[8].

Art. 5a Emolumenti per provvedimenti non approvati

L'articolo 5 sancisce il principio secondo il quale gli emolumenti e le indennità sono dovuti anche se la misura di sorveglianza ordinata ed eseguita non è stata autorizzata o non ha portato ai risultati auspicati.

Art. 5b Applicabilità dell'ordinanza generale sugli emolumenti

Si tratta di un semplice rinvio all'ordinanza generale sugli emolumenti[9].

4. Conseguenze finanziarie e sull'effettivo del personale

In una prima fase, molto verosimilmente, i due avamprogetti di ordinanza non genereranno costi supplementari per la Confederazione, nemmeno in termini di personale.

In virtù degli articoli 15 e 16 LSCPT in combinato disposto con gli articoli 18 e 26 OSCPT, gli offerenti si assumono le spese d'investimento per garantire la capacità di eseguire misure di sorveglianza. Dopo l'entrata in vigore della revisione parziale dell'OSCPT, o al termine del periodo transitorio, gli offerenti dovranno sostenere tali spese anche per le nuove tecnologie di telecomunicazione che hanno immesso e immetteranno sul mercato (sorveglianza di Internet).

[8] Si tratta di una percentuale di copertura introdotta a suo tempo dal DATEC e consolidatasi nella prassi.
[9] RS **172.041.1**

A medio termine il Servizio dovrà quindi effettuare meno «misure speciali» potendo ricorrere a processi di sorveglianza standardizzati anche per la sorveglianza di Internet. Si vedrà pertanto ridurre l'onere in termini di mezzi tecnici nel settore della sorveglianza di Internet.

Riguardo al settore del personale, le possibilità di operare risparmi sono praticamente inesistenti. I due progetti di revisione parziale non accrescono tuttavia il fabbisogno di personale del Servizio.

Le autorità di perseguimento penale della Confederazione e dei Cantoni avranno a disposizione nuove possibilità d'indagine nel settore del traffico della telecomunicazione in Internet in rapida crescita e che richiede un impegno considerevole per contrastare la cibercriminalità. Questa lotta imprescindibile contro le nuove forme di criminalità cagionerà spese, che tuttavia dovrebbero aggirarsi entro limiti sostenibili vista l'efficacia delle possibilità d'indagine derivanti dalle nuove misure di sorveglianza.