Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia
Ufficio federale di giustizia

Riassunto dei risultati della procedura di consultazione

sul rapporto e l'avamprogetto

di modifica della legge federale del 6 ottobre 2006

sulla

sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)

Berna, maggio 2011

Indice

Elenco dei partecipanti alla consultazione con abbreviazioni

CANTONI

Regierungsrat Kt. Zürich	ZH
Regierungsrat Kt. Bern	BE
Regierungsrat Kt. Luzern	LU
Regierungsrat Kt. Uri	UR
Regierungsrat Kt. Schwyz	SZ
Regierungsrat Kt. Obwalden	OW
Regierungsrat Kt. Nidwalden	NW
Regierungsrat Kt. Glarus	GL
Regierungsrat Kt. Zug	ZG
Conseil d'Etat du canton de Fribourg	FR
Regierungsrat Kt. Solothurn	SO
Regierungsrat Kt. Basel-Stadt	BS
Regierungsrat Kt. Basel-Landschaft	BL
Regierungsrat Kt. Schaffhausen	SH
Regierungsrat Kt. Appenzell Ausserrhoden	AR
Standeskommission Kt. Appenzell Innerrhoden	AI
Regierungsrat Kt. St. Gallen	SG
Regierungsrat Kt. Graubünden	GR
Regierungsrat Kt. Aargau	AG
Regierungsrat Kt. Thurgau	TG
Consiglio di Stato del Cantone del Ticino	TI
Conseil d'Etat du canton de Vaud	VD
Conseil d'Etat du canton de Valais	VS
Conseil d'Etat du canton de Neuchâtel	NE
Conseil d'Etat du canton de Genève	GE
Gouvernement du canton du Jura	JU

PARTITI POLITICI

PCS Partito cristiano sociale PCS
CSP Christlich-soziale Partei
PCS Parti chrétien-social
PCS Partida cristian-sociala

PPD Partito popolare democratico svizzero PPD
CVP Christlichdemokratische Volkspartei der Schweiz
PDC Parti démocrate-chrétien suisse
PCD Partida cristiandemocrata svizra

PLR. I Liberali PLR
FDP. Die Liberalen.
PLR. Les Libéraux-Radicaux
PLD. Ils Liberals

I Verdi Partito ecologista svizzero Verdi
Les Verts Parti écologiste suisse
GPS. Grüne Partei der Schweiz
La Verda Partida ecologica svizra

Partito pirata svizzero PPS
Piratenpartei Schweiz
Parti Pirate Suisse

PS Partito socialista svizzero PS
SP Schweiz Sozialdemokratische Partei der Schweiz
PS Parti socialiste suisse
PS Partida socialdemocrata da la Svizra

UDC Unione Democratica di Centro UDC
SVP Schweizerische Volkspartei
UDC Union Démocratique du Centre
PPS Partida Populara Svizra

ORGANIZZAZIONI MANTELLO NAZIONALI DEI COMUNI, DELLE CITTÀ E DELLE REGIONI DI MONTAGNA

Unione delle città svizzere UCS
Schweizerischer Städteverband (SSV)
Union des villes suisses

ORGANIZZAZIONI MANTELLO NAZIONALI DELL'ECONOMIA

economiesuisse economiesuisse
Federazione delle imprese svizzere
Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Swiss business federation

Unione sindacale svizzera Schweiz. Gewerkschaftsbund (SGB) Union syndicale suisse (USS)	USS
Unione svizzera degli imprenditori Schweizerischer Arbeitgeberverband (SAG) Union patronale suisse	USI
Unione svizzera dei contadini Schweizerischer Bauernverband (SBV) Union suisse des paysans (USP)	USC

ALTRE ORGANIZZAZIONI, ISTITUZIONI E SINGOLE PERSONE

Cablecom GmbH	Cablecom
Centre Patronal	CP
Chaos Computer Club Zürich	CCC
Cognizant Technology Solutions S.A	COG
Colt Telecom Services AG	Colt
Giuristi e Giuriste Democratici Svizzeri Demokratische Juristinnen und Juristen der Schweiz (DJS) Juristes Démocrates de Suisse (JDS)	GDS
La Posta Svizzera	–
Commissione federale delle case da gioco Eidgenössische Spielbankenkommission (ESBK) Commission fédérale des maisons de jeu (CFMJ)	CFCG
«ePower für die Schweiz» Gruppo parlamentare	ePower
ETH Eidgenössische Technische Hochschule Zürich	ETH
Finecom Telecommunications AG	Finecom
dirittifondamentali.ch grundrechte.ch droitsfondamentaux.ch	gr.ch
Hauser Ralf	HR
Hewlett-Packard (Schweiz) GmbH	hp

ICTSwitzerland Information and Communication Technology	ICT
ifpi Schweiz (organizzazione mantello dei produttori di supporti audio e audiovisivi)	ifpi
Information Security Society Switzerland	ISSS
INT Informatik AG	INT
Komitee für eine freie Gesellschaft	KFG
Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia Konferenz der kantonalen Justiz- und Polizeidirektoren (KKJPD) Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)	CCDGP
Conferenza dei comandanti delle polizie cantonali della svizzera Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS Conférence des commandants des polices cantonales de suisse (CCPCS)	CCPCS
Conferenza della autorità inquirenti svizzere Konferenz der Strafverfolgungsbehörden der Schweiz (KSBS) Conférence des autorités de poursuite pénale de Suisse (CAPS)	CAIS
Konsumentenforum kf	kf
Métille Sylvain	MS
Orange Communications SA	Orange
privatim - Gli incaricati svizzeri della protezione dei dati privatim - Die schweizerischen Datenschutzbeauftragten privatim - Les commissaires suisses à la protection des données	privatim
Rosenthal David	RD
Conferenza svizzera sull'informatica Schweizerische Informatikkonferenz Conférence suisse sur l'informatique	CSI
Società svizzera di diritto penale Schweizerische Kriminalistische Gesellschaft (SKG) Société Suisse de droit pénal (SSDP)	SSDP
SAFE Schweizerische Vereinigung zur Bekämpfung der Piraterie Association Suisse pour la lutte contre le piratage	safe
Federazione svizzera degli avvocati Schweizerischer Anwaltsverband **(**SAV) Fédération suisse des avocats (FSA)	FSA

Associazione Svizzera delle telecomunicazioni Schweizerischer Verband der Telekommunikation Association Suisse des Télécommunications	asut
Istituto svizzero di polizia Schweizerisches Polizei-Institut (SPI) Institut suisse de police (ISP)	ISPo
Sitrox AG	Sitrox
Stiftung für Konsumentenschutz	SKS
Sunrise Communications AG	Sunrise
SWICO (Associazione economica per una Svizzera digitale)	SWICO
SIMSA swiss internet industry association	SIMSA
Swiss Internet User Group	SIUG
SWISS POLICE ICT (Organizzatrice dello «Schweizer Polizei Informatik Kongress» SPIK)	SPICT
Swisscable (Associazione del ramo delle reti di telecomunicazione)	Swisscable
Swisscom (Svizzera) AG	Swisscom
SWITCH Serving Swiss Universities	switch
Switchplus AG	switchplus
United Security Providers AG **Fargate AG** **Futurecom Interactive AG** **OneConsult GmbH** **Stories AG** **Neidhart + Schön Group AG** **Viollier Consulting AG** **midix.com ag** **Open systems ag** **Namics AG** **InVisible GmbH** **Köpfli & Partner AG** **Dinotronic AG** **terreActive** **von salis engineering GmbH** **Dr. Hartwig Thomas** **Icontel AG** **ISPIN AG** **WIRZ Grupppe**	IT(19)

Università di San Gallo	UNISG
Università di Zurigo	UNIZH
Federazione svizzera dei funzionari di polizia Verband Schweizerischer Polizei-Beamter (VSPB) Fédération suisse fonctionnaires de polices (FSFP)	FSFP
Verein Swiss Privacy Foundation	VSPF
Verizon Switzerland AG	Verizon
3D4X Internetagentur & Softwareentwicklung	3D4X

I. Introduzione

Con decisione del 19 maggio 2010[1] il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia (DFGP) di porre in consultazione il rapporto[2] e l'avamprogetto[3] di modifica della legge federale del 6 ottobre 2000[4] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Si tratta di una revisione totale con l'obiettivo primario di adattare la legge agli sviluppi tecnologici degli ultimi anni, soprattutto nell'ambito di Internet.

Con circolare del 19 maggio 2010 il DFGP ha invitato i Cantoni, i partiti rappresentati nell'Assemblea federale e le associazioni e organizzazioni interessate a esprimere il loro parere entro il 18 agosto 2010.

Sono pervenuti 106 pareri, per un totale di circa 700 pagine. 55 dei 93 destinatari invitati a partecipare alla consultazione hanno inviato un parere, quattro di loro hanno esplicitamente rinunciato ad esprimersi sul contenuto dell'oggetto. 51 partecipanti hanno infine sfruttato la possibilità di esprimere un parere di propria iniziativa.

Hanno espresso un parere:

26 Cantoni

6 partiti

74 cerchie interessate

---

1 http://www.bj.admin.ch/content/bj/it/home/dokumentation/medieninformationen/2010/ref_2010-05-19.html

2 http://www.bj.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/vn-ber-i.pdf

3 http://www.bj.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/entw-i.pdf

4 RS **780.1**

II. Panoramica dei risultati

1. Valutazione generale

I partecipanti alla consultazione hanno riconosciuto o perlomeno non hanno messo in dubbio la necessità di adattare la LSCPT agli sviluppi tecnologici degli ultimi anni, soprattutto nell'ambito di Internet. Tuttavia, per quanto riguarda l'attuazione legislativa, diversi partecipanti hanno espresso numerose e ampie riserve, in parte di carattere strutturale, in merito alle singole disposizioni dell'avamprogetto o hanno addirittura proposto una rielaborazione completa. Vari partecipanti[5] criticano inoltre il linguaggio complicato dell'avamprogetto (AP-LSCPT). Qui di seguito elenchiamo dapprima i partecipanti che approvano l'avamprogetto senza riserve (n. 2). Successivamente presentiamo le critiche più importanti (n. 3) e infine riassumiamo i pareri espressi in merito alle singole disposizioni.

2. Approvazione senza riserve

3 Cantoni (UR, OW, GE) e La Posta Svizzera (per quanto riguarda la sorveglianza della corrispondenza postale) approvano l'avamprogetto senza riserve.

3. Le critiche più importanti

Campo d'applicazione personale (art. 2 AP-LSCPT)

Alcuni partecipanti[6] criticano in generale che dal tenore dell'articolo 2 AP-LSCPT non risulti chiaramente chi vada contemplato. Parecchi partecipanti[7] rifiutano l'estensione del campo d'applicazione prevista dall'articolo 2 capoverso 1 lettera b AP-LSCPT e ne chiedono lo stralcio, la restrizione o almeno una nuova formulazione. In merito all'articolo 2 capoverso 2 AP-LSCPT alcuni partecipanti chiedono di chiarire chi sia concretamente contemplato[8] e, in combinazione con l'articolo 26 AP-LSCPT, quali obblighi debbano adempiere[9]. GPS, USS e INT osservano inoltre che l'estensione del campo d'applicazione potrebbe minacciare l'esistenza soprattutto delle piccole imprese. Secondo RD è contrario al sistema estendere il campo d'applicazione della LSCPT oltre la cerchia dei fornitori di telecomunicazioni anche a persone che sono soggette al segreto delle telecomunicazioni.

Sistema informatico per il trattamento dei dati raccolti nel corso della sorveglianza del traffico delle telecomunicazioni (art. 6-13 AP-LSCPT)

Numerosi partecipanti[10] respingono la conservazione centrale e durevole dei dati presso il servizio di sorveglianza (qui appresso: Servizio) e propongono in linea di massima il mantenimento del vecchio sistema (registrazione dei dati, trasferimento su un supporto, trasmissione all'autorità inquirente, cancellazione dei dati presso il Servizio). Alcuni partecipanti[11]

---

5 BE, SZ, NW, SH, LU, PPD, CAIS, SSDP
6 FR, VD, PPD, ISSS, CP, RD.
7 PLR, PPS, SIUG, switch, switchplus, RD, SWICO, hp, COG, ISSS, GDS, gr.ch, SKS, Verdi, USS, KFG, INT, CSI, asut, Finecom, Orange, Swisscom, Colt, Verizon, VSPF.
8 LU, ETH, UNISG, asut, Swisscom, Finecom, Orange, Colt, Sunrise, Verizon, Swisscable, switch.
9 LU, BL, AR, PS, privatim.
10 SO, BE, NW, BL, LU, SZ, SO, SG, SH, SSDP, CAIS.
11 ZH, LU, AG, GL, GR, TG, VS, JU, CCDGP, CCPCS, CCC.

chiedono di stabilire nella legge che le circostanze del singolo caso possono ancora esigere che sia necessario l'invio per posta mediante supporto di dati o documenti (sistema attuale). Altri[12] invece chiedono di prevedere, nel settore della sorveglianza di Internet, a causa dell'enorme quantità di dati, la registrazione centrale e durevole con un accesso esterno, mentre le sorveglianze telefoniche andrebbero registrate e inviate come sinora su supporti di dati. Vari partecipanti[13] ritengono che il nuovo sistema violi i diritti delle parti, poiché secondo il Codice di diritto processuale penale svizzero del 5 ottobre 2007 (CPP)[14] queste ultime devono poter accedere agli atti originali. L'accesso delle parti è respinto per ragioni di sicurezza tecnica. Un cospicuo numero di partecipanti[15] ritiene inutile il disciplinamento del diritto di esaminare gli atti e di quello di accedere agli atti dell'articolo 10 AP-LSCPT, poiché il CPP contiene disposizioni che garantiscono una protezione sufficiente dei dati personali. Infine, diversi partecipanti[16] ritengono troppo complicato e oneroso il disciplinamento dei termini di conservazione dell'articolo 11 AP-LSCPT, che si ricollega ai termini di prescrizione, e si esprimono a favore del vecchio sistema. I termini di conservazione dovrebbero fondarsi esclusivamente sul CPP.

Mancanza di un obbligo di verifica da parte del Servizio e rimedi giuridici

Numerosi partecipanti[17] chiedono l'obbligo del Servizio di verificare la legittimità dell'ordine di sorveglianza (cfr. anche le osservazioni al cap. III n. 3.2.1 ad art. 15 lett. a e cap. III n. 3.3.1 ad art. 16 lett. a) e che di conseguenza nell'articolo 34 AP-LSCPT (rimedi giuridici), per i soggetti che hanno ricevuto l'ingiunzione di eseguire una sorveglianza, va prevista la possibilità di far verificare da un giudice la legittimità di tale ingiunzione. In tale contesto alcuni partecipanti[18] rilevano una contraddizione in relazione all'articolo 33 AP-LSCPT, secondo cui il Servizio deve vigilare sul rispetto della legislazione.

Obblighi connessi all'esecuzione della sorveglianza (art. 21 AP-LSCPT)

Per numerosi partecipanti[19] gli obblighi concreti dei soggetti che devono eseguire una vigilanza sono disciplinati in modo impreciso. Per garantire la certezza del diritto chiedono pertanto, in parte anche con proposte di formulazione concrete, di prevedere un chiaro elenco degli obblighi.

Identificazione degli utenti Internet (art. 22 AP-LSCPT)

Numerosi partecipanti[20] chiedono di stralciare o adattare la disposizione. Un obbligo d'identificazione a tutto campo per gli utenti Internet è ritenuto sproporzionato e impraticabile. Si fa inoltre notare che esistono numerose possibilità di elusione.

---

12 LU, SZ, SO, SG, SH, CAIS.
13 BE, NW, BS, BL, SSDP, FSA, MS.
14 RU **2010** 1881; entrata in vigore il 1° gennaio 2011.
15 LU, NW, BL, SG, GL, TG, VS, JU, CCDGP CAIS, SSDP.
16 BE, SZ, NW, BL, SH, SG, AG, VD, CAIS.
17 ZG, BE, BL, AR, PLR, PS, Swisscable, SWICO, UCS, Cablecom, asut, Orange, Swisscom, Colt, Sunrise, Verizon, CAIS, privatim, economiesuisse, SIUG, hp, COG, ISSS, VSPF, VERDI, SKS, IT(19).
18 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SWICO, hp, COG.
19 PPD, PLR, UDC, VERDI, SKS, economiesuisse, ICT, ePower, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SIUG, SPICT.
20 VD, VERDI, UDC, PLR, ISSS, UCS, privatim, GDS, gr.ch, RD, IT(19), Cablecom, switch e switchplus, CP, FSA, KFG, PPS, ETH, UNISG, UNIZH.

Proroga della durata di conservazione dei dati a 12 mesi (art. 23 AP-LSCPT)

Numerosi partecipanti[21] respingono la disposizione – in parte rinviando ai criteri sviluppati dalla Corte costituzionale tedesca[22] in relazione alla conservazione dei dati – o chiedono di rivederla. In tale contesto alcuni partecipanti[23] osservano che vengono conservati sistematicamente dati di persone non sospette.

Nessun indennizzo per i soggetti che devono eseguire la sorveglianza (art. 30 cpv.. 1 AP-LSCPT)

Vari partecipanti[24] sono contrari allo stralcio dell'indennizzo per l'esecuzione di misure di sorveglianza. La maggior parte di questi partecipanti[25] osserva che il perseguimento penale è un compito statale i cui costi vanno assunti dalla comunità. Alcuni[26] osservano per soddisfare le nuove esigenze della legge è necessario acquistare un'infrastruttura costosa. Vari partecipanti chiedono un disciplinamento diversificato[27].

Intercettazione e decodificazione di dati (art. 270bis CPP); introduzione di programmi informatici in sistemi di elaborazione dei dati altrui

Dieci partecipanti[28] rifiutano del tutto l'introduzione di programmi informatici («Government Software», spesso chiamati «cavalli di Troia federali») in un sistema informatico; un numero maggiore di partecipanti[29] esprime notevoli riserve, rinviando soprattutto alla notevole ingerenza nella sfera privata degli interessati, di cui sono visibili tutti i dati del sistema informatico sorvegliato. Inoltre si critica che non si è tenuto conto in alcun modo della decisione di fondo della Corte costituzionale tedesca[30] sulla «perquisizione online». Numerosi partecipanti[31] esprimono inoltre preoccupazioni generali relative alla sicurezza, che concernono il programma informatico stesso, il suo uso abusivo da parte di criminali e il sistema di elaborazione dei dati o la rete in cui il programma è introdotto. BS, FR, PS e privatim chiedono inoltre di restringere l'elenco dei reati dell'articolo 269 capoverso 2 lettera a CPP per i quali è previsto l'impiego dei «cavalli di Troia federali».

---

21 BL, VERDI, PS, SKS, USS, GDS, gr.ch, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, ISSS, SWICO, hp, privatim, COG, 3D4X, PPS.

22 Cfr. n. 120 e spiegazioni al cap. III. n. 5.4.

23 GDS, gr.ch, VERDI, SKS.

24 PS, PPD, PLR, UDC, VERDI, PPS, GDS, gr.ch, RD, ISSS, MS, SIUG, SIMSA, INT, asut, Finecom, Orange, Swisscom, Sunrise, Colt, Verizon, Cablecom, FSA, SKS, Swisscable, CP, CCC, Sitrox, economiesuisse, IT(19), SWICO, hp, COG.

25 PPD, PLR UDC, VERDI, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, FSA, SKS Swisscable, SIUG, CP, CCC, Sitrox, PPS.

26 PS, Colt, SIUG, SIMSA, INT, ISSS, PPS, VERDI.

27 Il PPD chiede di rimborsare le spese per l'aggiornamento dei sistemi, mentre il PS propone di diversificare a seconda della grandezza dell'impresa o della sostenibilità economica.

28 VERDI, GDS, gr.ch, Cablecom, CCC, SKS, SIUG, KFG, PPS, ISSS.

29 ZH, BL, AR, LU, PS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, privatim, economiesuisse, Swisscable.

30 BVerfG, 1 BvR 370/07 del 27.2.2008, n. di capoversi. (1 - 333); cfr. anche III. n. 11.1.2.

31 VERDI, GDS, gr.ch, SKS, KFG, PPS, SIUG.

III. Pareri in merito alle singole disposizioni dell'AP-LSCPT

1. Disposizioni generali

1.1. Articolo 1 Campo d'applicazione materiale

[1] La presente legge si applica alla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, incluso Internet, ordinata e attuata:

a. nell'ambito di un procedimento penale;

b. nell'ambito dell'esecuzione di una domanda di assistenza giudiziaria;

c. nell'ambito della ricerca di persone disperse;

d. i nell'ambito delle ricerca di persone condannate a una pena detentiva o a una misura privativa della libertà.

[2] Alle informazioni concernenti il traffico dei pagamenti soggetto alla legge del 30 aprile 19973 sulle poste si applicano gli articoli 284 e 285 del Codice di diritto processuale penale del 5 ottobre 2007 (CPP).

1.1.1 Articolo 1 capoverso 1

Alcuni partecipanti[32] ritengono troppo imprecisi i termini «corrispondenza postale e traffico delle telecomunicazioni», nonché «Internet» del capoverso 1. Definire «Internet» come parte del traffico delle telecomunicazioni significa ignorare le potenzialità di questo mezzo sui generis, poiché Internet non è semplicemente un telefono o un fax più potente. UNISG, switch e switchplus ritengono che non sia chiaro se ad esempio l'utilizzazione di servizi basati su TCP[33]/IP[34], quali HTTP[35], FTP[36] e Telnet[37] facciano parte o meno di Internet ai sensi della legge. Lo stesso vale, secondo UNIZH, per servizi quali Skype[38], PPTP[39] e Teredo[40]. asut ritiene che le misure di sorveglianza debbano riguardare soltanto la comunicazione individuale e che quindi si possano sorvegliare soltanto determinati collegamenti. La FSFP è invece dell'opinione che, in considerazione della futura evoluzione tecnologica, i termini summenzionati siano troppo limitativi e che occorrerebbe pertanto una formulazione più agevole, completa e soprattutto flessibile.

Per quanto riguarda la nuova possibilità di ricercare persone condannate (art. 1 cpv. 1 lett. d AP-LSCPT), si vedano le osservazioni del capitolo III numero 6.2 all'articolo 28 AP-LSCPT.

1.1.2 Articolo 1 capoverso 2

Nessuna osservazione.

1.2. Articolo 2 Campo d'applicazione personale

[1] La sorveglianza basata sulla presente legge è effettuata dai seguenti soggetti:

a. fornitori di servizi postali o di telecomunicazione, compresi i fornitori di accesso a Internet, che esercitano la loro attività a titolo professionale;

---

32 VD, UNIZH, PPS, UNISG, switch, switchplus, ETH.
33 Transmission Control Protocol.
34 Internet-Protocol.
35 Hypertext Transfer Protocol.
36 File Transfer Protocol.
37 Telecommunication Network.
38 Software VoIP (Voice over IP) gratuito.
39 Point-to-Point Tunneling Protocol.
40 Teredo è un verbale della comunicazione per la comunicazione di dati mediante Internet.

b. persone che, a titolo professionale, gestiscono dati relativi alla comunicazio-ne per i fornitori di cui alla lettera a, trasferiscono dati di questo genere a terzi o mettono a disposizione l'infrastruttura necessaria per farlo.

[2] I gestori di reti di telecomunicazione interne e di centralini privati, nonché i sogget-ti di cui al capoverso 1 che non esercitano la loro attività nel settore del traffico delle telecomunicazioni a titolo professionale, tollerano la sorveglianza ai sensi della presente legge.

Vari partecipanti[41] chiedono in generale di precisare l'articolo 2, non essendo chiaro chi sia concretamente contemplato.

NE, ETH e UNISG chiedono di sostituire «a titolo professionale» con «a titolo commerciale»; altri partecipanti[42] con «a titolo commerciale e a scopo di lucro».

1.2.1 Articolo 2 capoverso 1 lettera a

Alcuni partecipanti[43] criticano che il termine «fornitori di accesso a Internet» non sia definito nella legge. switch propone di contemplare come «fornitori di accesso a Internet» coloro che offrono servizi di posta elettronica e di telefonia via IP.

1.2.2 Articolo 2 capoverso 1 lettera b

Numerosi partecipanti[44] ritengono urgentemente necessaria la proposta estensione del campo d'applicazione. kf approva il fatto che si definisca con maggior precisione chi è soggetto alla legge.

Per contro, molti partecipanti[45] rifiutano l'estensione del campo d'applicazione e chiedono lo stralcio, la restrizione o perlomeno la riformulazione della lettera b. Secondo alcuni partecipanti[46], con l'estensione del campo d'applicazione sono ora contemplati tutti i fornitori di servizi, contenuti o prestazioni tecniche necessari per usare o gestire contenuti o servizi in Internet oppure, secondo RD e PPS, tutte le imprese che in qualche modo si occupano professionalmente di dati di comunicazione. In tal modo tutte le imprese e persone di un intero settore economico sono tenute a eseguire la sorveglianza attiva, acquistare gli strumenti necessari e mettere a disposizione le risorse di personale – e tutto ciò a proprie spese. Una siffatta estensione del campo d'applicazione è sproporzionata e inaccettabile. Si chiede di continuare a limitare il campo d'applicazione ai fornitori di accesso a Internet a titolo professionale e di non estenderlo agli hosting-provider e ai fornitori di contenuti.

Vari partecipanti[47] chiedono inoltre di limitare il campo d'applicazione alle imprese o persone giuridiche che offrono servizi di telecomunicazione oppure che gestiscono a scopo commerciale e a fini di lucro[48] o a titolo professionale[49] i dati di comunicazione per i fornitori di telecomunicazioni.

---

41 FR, VD, PPD, ISSS, CP, RD.
42 switch, asut, Finecom, Swisscom, Colt, Sunrise, Verizon.
43 SIUG, switch, switchplus, HR, ETH, UNISG.
44 ZH, ZG, LU, SZ, NW, AR, SO, SH, SG, GR, AG, TG, TI, VS, NE, GE, JU, PLR, ICT, ePower, SPICT, CCDGP, CCPCS, CAIS.
45 PLR, SIUG, VSPF, switch, switchplus, RD, PPS, SWICO, hp, COG, ISSS, GDS, gr.ch, SKS, VERDI, USS, KFG, INT, CSI, asut, Finecom, Orange, Swisscom, Colt, Verizon, VSPF.
46 SIUG, VSPF, switch, switchplus, RD, PPS.
47 asut, Finecom, Orange, Swisscom, Colt, Verizon, SWICO, hp, COG, ISSS.
48 asut, Finecom, Orange, Swisscom, Colt, Verizon.
49 Orange, Cablecom.

Secondo SIMSA il criterio determinante per definire i soggetti tenuti ad eseguire la sorveglianza dovrebbe essere l'offerta della comunicazione individuale. Secondo GDS e gr.ch, la tendenza ad assoggettare all'obbligo di sorveglianza tutte le forme di comunicazione si evidenzia chiaramente nell'estensione del campo d'applicazione.

SKS, Verdi, USS e KFG ritengono inaudito che le ripercussioni per i nuovi soggetti della legge non siano state illustrate. Secondo i Verdi e USS, i costi d'investimento necessari per la sorveglianza costituiscono un problema per i piccoli provider locali e, a seconda delle circostanze, ne pregiudicano l'esistenza. In qualità di piccolo fornitore di hosting direttamente interessato, INT ritiene che, visti i costi che ne conseguono, la revisione sia estremamente dannosa per l'economia, poiché toglie soprattutto alle piccole imprese la possibilità di gestire un'infrastruttura di comunicazione conformemente alla legge. Inoltre, con la situazione attuale di Internet qualsiasi utente è in grado di codificare e rendere anonimi i propri dati (p.es. mediante Tor o Freenet) e quindi qualsivoglia sorveglianza di Internet è una farsa. La revisione è pertanto inutile e inoltre sfavorevole alle PMI.

RD osserva inoltre che l'obiettivo di contemplare determinati fornitori, come ad esempio i gestori di mere piattaforme e-mail quali GMX, Hotmail o Gmail, non può essere raggiunto per motivi pratici, giacché l'esperienza insegna che solitamente tali piattaforme si trovano all'estero, ove la LSCPT non può essere applicata. La prevista estensione del campo d'applicazione non risolverebbe inoltre il problema dovuto al fatto che l'utente finale codifica la sua comunicazione e i suoi dati (problema Skype) e non affida il codice al suo fornitore di accesso a Internet (indipendentemente dal fatto che si tratti di un fornitore di servizi di telecomunicazione ai sensi della legge). Non va inoltre dimenticato il motivo per cui esiste la LSCPT: i fornitori di servizi di telecomunicazione sono soggetti al segreto delle telecomunicazioni e quindi occorre disciplinare i casi in cui essi possono rendere note informazioni che sottostanno a tale segreto professionale. Questo tuttavia significa che è contrario al sistema estendere il campo d'applicazione della LSCPT oltre la cerchia di tali fornitori di servizi di telecomunicazione anche a soggetti che non sottostanno al segreto delle telecomunicazioni. Questi ultimi sono soggetti tutt'al più eccezionalmente al segreto delle telecomunicazioni. I loro documenti sono quindi accessibili anche se si applicano gli strumenti usuali della procedura penale e quindi non vi è motivo di assoggettarli alla LSCPT. In caso contrario, è possibile che il compito delle autorità di perseguimento penale venga addirittura ostacolato, in quanto si potrebbe sostenere a buon diritto che il disciplinamento in una legge speciale invalida tutte le altre regole concernenti la consegna di documenti, l'informazione o il sequestro. La prevista estensione del campo d'applicazione è problematica per il solo fatto che gli obblighi sono fatti su misura per i fornitori di servizi di telecomunicazione, per cui non è assolutamente chiaro come possano adempirli i nuovi soggetti contemplati dalla LSCPT. Può ad esempio trattarsi di gestori di un sito Internet che dispone di una funzione che permette alle persone di comunicarsi informazioni. Da un lato gestiscono un server mail per terzi o lo hanno collegato a un server di un fornitore di servizi di telecomunicazione, dall'altro, per ogni processo di comunicazione, trasmettono e-mail di terzi al server del destinatario. Si può quindi senz'altro sostenere che si tratta di imprese che trasmettono dati della comunicazione a terzi a titolo professionale o che mettono a disposizione l'infrastruttura necessaria. Rientrerebbero inoltre nel campo d'applicazione innumerevoli hosting-provider, ad esempio anche quelli che offrono piattaforme di e-commerce, quali eBay o Ricardo, e ogni impresa che sul proprio sito permette a terzi di fare commenti di qualsiasi genere (p.es. in un libro degli ospiti o in un blog). Infatti, anche questi ultimi trasmettono dati della comunicazione (p.es. il contenuto di annunci di vendita) a terzi (gli internauti) o mettono a disposizione l'infrastruttura necessaria. In tale contesto, a pagina 17 il rapporto esplicativo osserva che s'intendono contemplare soltanto gli hosting-provider. Allo stato attuale anche i media elettronici che pubblicano lettere dei lettori o annunci in Internet sono da considerarsi hosting-provider e dovrebbero pertanto essere contemplati dalla LSCPT. Tutte queste imprese dovrebbero creare a proprie spese

un'enorme infrastruttura, in modo da poter adempiere gli obblighi previsti. Per le autorità di perseguimento penale è senza dubbio allettante poter avere accesso in qualsiasi momento a qualsivoglia processo in Internet. Ma ciò non può e non dovrebbe essere l'obiettivo della LSCPT, che dovrebbe servire soltanto alla sorveglianza delle telecomunicazioni e non di tutto il mondo «digitale».

A RD non è noto alcun Paese occidentale che sorvegli Internet in modo così esteso come lo prevede l'avamprogetto. Sebbene siano menzionati separatamente al capoverso 2, in base alla formulazione dell'articolo 2 capoverso 1 lettera b potrebbero addirittura essere ora contemplati i gestori di reti di telecomunicazione interna e di centralini privati, dato che mettono a disposizione l'infrastruttura necessaria per trasmettere dati della comunicazione a terzi. Anche se si affermasse che il traffico delle telecomunicazioni dell'impresa stessa non è coinvolto, potrebbero ciononostante essere contemplate numerose imprese, ossia quelle che permettono ai propri collaboratori di fare telefonate o scrivere e-mail private o quelle che fungono da servizi centrali di IT o telecomunicazione in seno a gruppi di imprese e in tale funzione forniscono servizi di telecomunicazione per altri gruppi. Anche in questo caso le conseguenze del nuovo campo d'applicazione personale dell'AP-LSCPT sono del tutto sproporzionate. Anche le imprese che forniscono servizi nel settore della sicurezza di reti (p.es. managed security service), sorvegliando e gestendo ad esempio reti interne di imprese (p.es. mediante firewall) potrebbero rientrare nel campo d'applicazione. Si potrebbe infatti sostenere che approntando un firewall mettono a disposizione a titolo professionale l'infrastruttura necessaria per poter trasmettere a terzi i dati della comunicazione. Rientrano nel campo d'applicazione della LSCPT anche le imprese che vendono o danno in affitto in Svizzera hardware o software per reti, poiché mettono a disposizione dei fornitori di servizi di telecomunicazione o anche di altre imprese l'infrastruttura necessaria. Secondo RD non sono state ben ponderate le conseguenze dell'estensione del campo d'applicazione della LSCPT. RD chiede pertanto di rinunciare all'estensione o perlomeno di rivedere la disposizione in modo tale che anche in caso di interpretazione ampia siano contemplati soltanto coloro che devono effettivamente essere contemplati.

CSI osserva che, a causa della disposizione in questione, tutti i suoi membri, ossia le amministrazioni di tutti i livelli statali, potrebbero essere soggetti alla LSCPT, poiché di regola gestiscono reti informatiche e telefoniche a cui, per adempiere compiti amministrativi, sono collegati anche terzi (p.es. Cantoni, Comuni, altre autorità). Perciò CSI ritiene in generale problematica la disposizione e in particolare la sua applicazione alle reti dell'amministrazione pubblica. Chiede quindi di stralciare la lettera b.

Nel suo parere VD osserva che l'espressione «dati relativi alla comunicazione» dell'articolo 2 capoverso 1 lettera b non aiuta a chiarire chi rientri nel campo d'applicazione. Secondo la prassi attuale, la maggior parte dei fornitori di servizi di telecomunicazione è disposta a consegnare, direttamente o su richiesta di un giudice, dati alla polizia, perché ritiene di non sottostare al segreto delle telecomunicazioni. Occorre quindi chiedersi se la revisione totale proposta non abbia la conseguenza che in futuro tali servizi possano operare soltanto nell'ambito della LSCPT.

ETH e UNISG rendono attenti alla seguente contraddizione: secondo il rapporto esplicativo le «scuole» sono esentate dall'obbligo di sorveglianza. Ciononostante le spiegazioni all'articolo 22 («Identificazione degli utenti Internet») menzionano le scuole tra coloro che sono soggetti all'obbligo. La lettera b va quindi precisata, chiarendo che rientrano nel campo d'applicazione della LSCPT soltanto coloro che forniscono prestazioni per i soggetti di cui alla lettera a. ETH chiede inoltre che, in quanto istituto pubblico che offre servizi soltanto agli studenti e a organizzazioni affini, il Politecnico non sia soggetto alla LSCPT ai sensi del capoverso 1. Secondo UNIZH il termine «persone» non chiarisce se la legge sia applicabile a

istituti. In base alla formulazione attuale ritiene tuttavia che a essa stessa, in quanto istituto cantonale, la legge non sia applicabile. È inoltre del parere che la caratteristica dell'«esercizio a titolo professionale» non sia per essa pertinente, poiché opera al servizio del lavoro e dello sviluppo scientifico. In tale contesto SWITCH chiede di precisare nella lettera b che le scuole e le università e le istituzioni come SWITCH, incaricate dell'installazione dell'infrastruttura (informatica) di quest'ultime, non rientrino nel campo d'applicazione della LSCPT.

1.2.3 Articolo 2 capoverso 2 in combinazione con l'articolo 26

Art. 2 cpv. 2

[2] I gestori di reti di telecomunicazione interne e di centralini privati, nonché i soggetti di cui al capoverso 1 che non esercitano la loro attività nel settore del traffico delle telecomunicazioni a titolo professionale, tollerano la sorveglianza ai sensi della presente legge.

Art. 26 Gestori di reti di telecomunicazione interne e di centralini privati e soggetti di cui all'articolo 2 capoverso 1 che non esercitano la loro attività nell'ambito del traffico delle telecomunicazioni a titolo professionale

I gestori di reti di telecomunicazione interne e di centralini privati garantiscono l'accesso ai soggetti incaricati dal Servizio. I soggetti di cui all'articolo 2 capoverso 1 che non esercitano la loro attività nel settore del traffico delle telecomunicazioni a titolo professionale garantiscono ai soggetti incaricati dal Servizio l'accesso ai dispositivi da loro utilizzati. I gestori e i soggetti summenzionati forniscono ai soggetti incaricati dal Servizio le informazioni necessarie.

Alcuni partecipanti[50] chiedono, con proposte concrete di formulazione, di precisare il capoverso 2 e l'articolo 26, al fine di chiarire che tutti i tipi di scuole, gli ospedali e gli alberghi non rientrano tra i soggetti dell'articolo 2 capoverso 1. ETH osserva che il Politecnico federale va considerato gestore di una rete di telecomunicazione interna e di un centralino privato secondo il capoverso 2. Non fornisce un servizio di telecomunicazione ai sensi dell'articolo 2 lettera c dell'ordinanza del 9 marzo 2007[51] sui servizi di telecomunicazione (OST) e non è fornitore di accesso a Internet ai sensi dell'articolo 2 lettera a dell'ordinanza del 31 ottobre 2001[52] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OSCPT). I partecipanti propongono di sostituire l'espressione «non a titolo professionale» con «non a titolo commerciale e senza scopo di lucro».

Visto il rischio di conseguenze penali e nell'interesse della certezza giuridica, LU chiede di chiarire chi siano i fornitori di servizi postali o di telecomunicazione che «non esercitano la loro attività […] a titolo professionale» e, insieme a BL, AR, PS e privatim, quali siano gli obblighi concreti che devono adempiere i soggetti di cui al capoverso 2. Secondo SIUG tutti i privati, le organizzazioni e le imprese che offrono a titolo accessorio servizi di Internet sarebbero costretti all'aiuto passivo e a mettere a disposizione i propri locali e i propri sistemi informatici. Ciò potrebbe significare che debbano rendere note parole chiavi e codici di criptaggio e che con l'aiuto di apparecchi privati debbano eseguire misure di intercettazione. Pertanto, gli operatori che non esercitano la loro attività a titolo professionale non dovrebbero essere soggetti all'obbligo di fornire aiuto e informazioni.

Secondo il CCC l'articolo 26 AP-LSCPT crea uno strumento che permette di introdursi in spazi privati ed è quindi contrario all'articolo 13 della Costituzione federale della Confederazione Svizzera del 18 aprile 1999 (Cost.)[53].

Secondo il PPS non vi è utente di Internet che non soddisfi le condizioni dell'articolo 2 capoverso 2. Qualsiasi gestore di un LAN (inclusi i privati) è perciò costretto a permettere la sor-

---

50 ETH, UNISG, asut, Swisscom, Finecom, Orange, Colt, Sunrise, Verizon, Swisscable, switch.
51 RS **784.101.1**
52 RS **780.11**
53 RS **101**

veglianza da parte dell'Internet service provider (ISP).

Cablecom critica che il rinvio dell'articolo 26 all'articolo 2 capoverso 1 AP-LSCPT non è corretto, poiché il capoverso 1 limita chiaramente la cerchia degli interessati a coloro che esercitano l'attività a titolo professionale. L'articolo 26 dovrebbe quindi rinviare all'articolo 2 capoverso 2.

1.3. Articolo 3 Servizio di sorveglianza

[1] La Confederazione gestisce un servizio di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (Servizio).

[2] Il Servizio svolge i propri compiti autonomamente. Non è vincolato da istruzioni ed è annesso al DFGP soltanto sul piano amministrativo.

[3] Nell'ambito dei suoi compiti, il Servizio collabora con le autorità di concessione e di vigilanza competenti per il settore della corrispondenza postale e del traffico delle telecomunicazioni.

1.3.1 Articolo 3 capoverso 1

Nessuna osservazione.

1.3.2 Articolo 3 capoverso 2

Il PPD propone di eliminare la sovrapposizione dell'attività normativa ed esecutiva del Servizio. ICT, ePower e SPICT trovano sconcertante che lo stesso servizio agisca in quanto esecutore degli ordini delle autorità di perseguimento penale e possa nel contempo stabilire e certificare norme esecutive. Propongono pertanto una bipartizione del Servizio. Altri partecipanti[54] osservano che, non essendo vincolato da istruzioni, il Servizio può anche assolvere compiti nell'applicazione del diritto.

1.3.3 Articolo 3 capoverso 3

ZH, LU, AG, CCPCS e PPD mettono in risalto l'importanza di una stretta collaborazione tra il Servizio e le autorità di perseguimento penale. Tale collaborazione è necessaria e va pertanto sancita nella legge. La legislazione dovrebbe progredire in sintonia con l'evoluzione tecnologica. Il capoverso 3 andrebbe pertanto completato con la frase «nonché con le autorità di perseguimento penale». In tale contesto, anche ICT, ePower e SPICT ritengono degno di nota che la collaborazione con le autorità di perseguimento penale non sia menzionata nel capoverso 3. Per Cablecom non è inoltre chiaro perché il Servizio debba avere soltanto il diritto e non l'obbligo di informare in merito ad eventuali questioni tecniche. In quanto centro di competenza il Servizio dovrebbe mettere a disposizione le sue conoscenze anche dei provider. In caso contrario vi è il rischio che, a causa del diverso livello di conoscenze, possano nascere dei malintesi. Cablecom propone quindi di aggiungere un capoverso 4 dal seguente tenore: «È l'interlocutore delle autorità e degli aventi obbligo in relazione alle misure di sorveglianza e li aiuta in caso di domande».

1.4. Articolo 4 Trattamento di dati personali

Le autorità che ordinano o autorizzano la sorveglianza, così come i soggetti che effettuano la sorveglianza in virtù della presente legge, possono trattare i dati personali di cui necessitano per garantire l'esecuzione degli ordini di sorveglianza.

---

54 asut, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

Nove partecipanti[55] ritengono inutile la disposizione sul trattamento di dati personali, essendo ovvio che le autorità di perseguimento penale nonché il Servizio e i fornitori di servizi possano trattare dati personali ai fini del perseguimento penale.

Per ZG, BL, PS e privatim l'articolo 4 costituisce una clausola generale inammissibile che indebolisce il vincolo a un obiettivo. È possibile che nell'ambito della sorveglianza secondo la LSCPT vengano trattati anche dati personali particolarmente degni di protezione. Secondo l'articolo 17 della legge federale del 19 giugno 1992[56] sulla protezione dei dati (LPD) i dati devono essere la qualifica dei dati avviene in riferimento alla loro base legale. L'articolo 4 AP-LSCPT non rispetta tale distinzione. Il trattamento di dati personali particolari o di profili della personalità dovrebbe pertanto essere esplicitamente disciplinato nella legge. Quanto più delicati sono i dati personali, tanto più preciso deve essere il disciplinamento. La clausola generale non esenta quindi dal fondare il trattamento di dati personali particolarmente degni di protezione su una base legale speciale ed esplicita che soddisfi il principio di determinatezza. Anche BS e VD chiedono in generale di precisare la disposizione. NE chiede inoltre di emanare disposizioni sulla distruzione di dati inutili o raccolti erroneamente o perlomeno un rinvio alla legge sulla protezione dei dati.

Nove partecipanti[57] osservano che occorre rispettare i principi elencati all'articolo 4 LPD, quali i principi della proporzionalità, della buona fede e del vincolo allo scopo. La maggior parte di loro[58] propone la seguente formulazione: «Le autorità che ordinano o autorizzano la sorveglianza, così come i soggetti che effettuano la sorveglianza in virtù della presente legge, possono trattare i dati personali di cui necessitano per garantire l'esecuzione degli ordini di sorveglianza *emessi da un giudice e conformi alla legge*. *Vanno rispettati i principi della legge federale sulla protezione dei dati».*

kf teme che vengano sorvegliate persone incensurate e che i loro dati siano conservati per anni.

1.5. Articolo 5 Segreto postale e delle telecomunicazioni

La sorveglianza e tutte le informazioni che la concernono soggiacciono al segreto postale e delle telecomunicazioni ai sensi dell'articolo 321ter CP.

Alcuni partecipanti[59] osservano che il segreto delle telecomunicazioni è già sancito dall'articolo 43 della legge del 30 aprile 1997[60] sulle telecomunicazioni (LTC). La menzione nella LSCPT è pertanto fuorviante, poiché si potrebbe presumere che anche i dati forniti sotto la voce «informazioni su collegamenti» siano soggette al segreto delle telecomunicazioni. Inoltre, a differenza di quanto suggerisce il tenore della disposizione, non è in primo luogo la sorveglianza a essere soggetta al segreto delle telecomunicazioni, bensì in generale qualsiasi comunicazione per mezzo di reti di telecomunicazione pubbliche. Pertanto la sorveglianza non fonda il segreto delle telecomunicazioni, bensì costituisce piuttosto un'ingerenza in quest'ultimo. Secondo RD, la disposizione fa sì che le informazioni che solitamente non sono soggette al segreto delle telecomunicazioni lo diventino.

---

55 LU, NW, GL, GR, TG, VS, JU, CCDGP, CAIS.
56 RS **235.1**
57 USS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
58 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
59 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
60 RS **784.10**

2. Sistema informatico per il trattamento dei dati raccolti nel corso della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni

2.1. Articolo 6 Principio

Il Servizio gestisce un sistema informatico per il trattamento dei dati raccolti nel corso della sorveglianza del traffico delle telecomunicazioni di cui all'articolo 1 capoverso 1 (sistema di trattamento).

SH respinge la conservazione centrale e durevole dei dati presso il Servizio. Per contro ICT ed ePower approvano la conservazione centrale dei dati, ritenendola un progresso che contribuirà a diminuire i costi del processo di sorveglianza.

IT(19) chiedono di completare la disposizione con prescrizioni chiare sui controlli necessari di tutti i dati della sorveglianza e con definizioni chiaramente strutturate dei compiti del Servizio. Se l'introduzione nascosta di programmi informatici è parte del sistema informatico, il PPS chiede di completare la disposizione con il trattamento di sistemi di dati sorvegliati. In caso contrario, è necessaria una definizione specifica e una base legale.

GDS e gr.ch chiedono di elaborare il sistema di trattamento in modo tale da garantire il diritto di consultazione e di informazione. Le spiegazioni del rapporto esplicativo fanno nascere alcuni dubbi in merito.

CP ritiene che il sistema di trattamento debba disporre dei migliori standard di sicurezza, a causa del grande rischio di attacchi informatici.

2.2. Articolo 7 Scopo del sistema di trattamento

[1] Il sistema di trattamento ha lo scopo di:

a. centralizzare la conservazione dei dati raccolti nel corso della sorveglianza del traffico delle telecomunicazioni;

b. permettere la consultazione in rete di tali dati secondo l'articolo 9.

Sei partecipanti[61] approvano un sistema che metta a disposizione i dati in modo centrale. Il nuovo disciplinamento non dovrebbe tuttavia escludere che in caso di necessità i dati possano essere registrati su altri supporti e messi a disposizione delle autorità che hanno ordinato la sorveglianza. Conformemente alla prassi attuale, tale possibilità deve essere in futuro prevista in particolare per l'assistenza giudiziaria internazionale, poiché solo in tal moto resterà possibile la trasmissione ai tribunali.

CAIS ritiene che anche in futuro la conservazione dei dati relativi alla normale sorveglianza telefonica non dovrebbe competere al Servizio. Come oggi, i dati dovrebbero invece essere conservati su supporti nei fascicoli penali e quindi lo scopo del sistema di trattamento andrebbe adeguato.

ZG, BL e privatim ritengono che dal punto di vista costituzionale e della protezione dei dati la conservazione centrale dei dati sia un mezzo e non uno scopo. ZG chiede pertanto di rettificare la lettera a dell'articolo 7. Il Cantone BL chiede di esaminare se la conservazione cen-

61 ZH, GL, VS, JU, CCDGP, CCPCS.

trale non debba essere giustificata da un ulteriore scopo e privatim propone la seguente formulazione: «Nel sistema di trattamento sono conservati in modo centrale i dati raccolti nel corso della sorveglianza del traffico delle telecomunicazioni al fine di permettere l'accesso in rete a tali dati conformemente all'articolo 9 AP-LSCPT».

Alcuni partecipanti[62] criticano che la disposizione proposta non stabilisca che lo scopo del sistema di trattamento sia innanzitutto la ricezione dei dati e presentano una pertinente proposta di formulazione.

ISSS ritiene che, per proteggere i diritti fondamentali e la sfera privata, ma anche a causa del pericolo di un uso abusivo, un sistema centrale necessiti assolutamente di un'autorità di controllo indipendente, quale ad esempio l'Incaricato federale della protezione dei dati e della trasparenza.

2.3. Articolo 8 Contenuto del sistema di trattamento

Il sistema di trattamento contiene:

a. le comunicazioni della persona sorvegliata, comprese quelle ricevute;

b. i dati indicanti quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto, e i dati relativi alle comunicazioni e alla fatturazione.

Vari partecipanti[63] chiedono che l'articolo 8 lettera b elenchi esplicitamente anche i dati geografici. CCPCS ritiene che può essere determinante anche il tentativo di stabilire un collegamento e chiede pertanto di includerlo nella legge. LU, SG, BL, NW e CAIS chiedono di formulare in modo più preciso la lettera b, chiarendo in particolare la differenza tra i cosiddetti dati del collegamento e quelli relativi alla comunicazione e alla fatturazione. Contestualmente NW, SG e CAIS chiedono inoltre una formulazione più chiara dell'articolo 273 CPP e BL anche dell'articolo 16 lettera e AP-LSCPT.

Alcuni partecipanti[64] sono del parere che l'articolo 7 AP-LSCPT sia sufficiente come principio e che quindi si possa stralciare l'articolo 8 AP-LSCPT, ritenuto superfluo. Cablecom critica l'inutilità della lettera a e ritiene che sia formulata in modo ambiguo. Non è ad esempio chiaro il motivo per cui sono espressamente menzionate le comunicazioni ricevute, ma non quelle inviate. L'affermazione della lettera b è da considerarsi irrealistica in riferimento a alla comunicazione mediante Internet.

2.4. Articolo 9 Accesso al sistema di trattamento

[1] Il Servizio permette alle autorità che hanno ordinato la sorveglianza e ai soggetti da queste designati di accedere in rete, nei limiti dell'autorizzazione loro concessa, ai dati raccolti nel corso della sorveglianza contenuti nel sistema di trattamento

[2] L'autorità che ha ordinato la sorveglianza e i soggetti da questa designati secondo il capoverso 1 hanno accesso in rete ai dati raccolti nel corso della sorveglianza per tutto il tempo in cui l'autorità ordinante è incaricata del caso, ma al massimo per un anno dalla fine della sorveglianza. L'autorità che ha ordinato la sorveglianza informa il Servizio di non essere più competente per il caso e della conclusione della sorveglianza; sono fatti salvi gli articoli 274 capoverso 5 e 275 CPP6. L'autorità che ha ordinato la sorveglianza e resta incaricata del caso può chiedere al Servizio di pro-lungare l'accesso ai dati per periodi non eccedenti un anno. Il Servizio informa tale autorità della prossima scadenza dell'accesso in rete ai dati

[3] L'autorità che ha ordinato la sorveglianza cui viene tolto il caso comunica al Servizio, se del caso, la nuova autorità competente.

---

62 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, Cablecom.

63 ZH, AG, TI, GL, TG, VS, JU, CCDGP, CCPCS.

64 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

[4] Il Servizio permette alla nuova autorità incaricata del caso che lo richieda e ai soggetti da questa designati di accedere in rete, nei limiti dell'autorizzazione loro concessa, ai dati raccolti nel corso della sorveglianza contenuti nel sistema di trattamento. La nuova autorità incaricata del caso e i soggetti da questa designati hanno accesso in rete a tali dati per tutto il tempo in cui la nuova autorità incaricata del caso rimane competente, ma al massimo per un anno dalla domanda di accesso indirizzata al Servizio. Per il resto sono applicabili per analogia i capoversi 2 e 3.

[5] Se per ragioni tecniche non è possibile consultare in rete i dati raccolti nel corso della sorveglianza, i dati sono comunicati inviando supporti di dati e documenti per posta.

Nove partecipanti[65] chiedono di stabilire esplicitamente nel capoverso 5 che le circostanze del caso concreto o difficoltà tecniche possono rendere necessario l'invio postale mediante supporto di dati o documenti. Per impedire abusi o ricatti, i partecipanti a un procedimento, in particolare la difesa, dovrebbero inoltre avere accesso ai dati esclusivamente attraverso il collegamento del pubblico ministero o del giudice istruttore. I dati dovrebbero essere protetti dall'accesso di terzi, eventualmente criptandoli. VD approva la consultazione in rete dei dati soltanto a condizione che le parti e i giudici ottengano gli stessi accessi previsti dal sistema attuale.

BE, NW, BL e SSDP chiedono di mantenere il vecchio sistema. Il disciplinamento dell'accesso proposto è complicato, soggetto a errori e inutile. A volte i procedimenti vengono trasferiti, uniti o separati e il nuovo sistema non tiene conto di queste possibilità procedurali. Inoltre, il disciplinamento dell'accesso proposto è in parte anche contrario alle disposizioni del CPP. Infatti, secondo quest'ultimo le parti devono avere accesso agli atti originali. In caso di accesso diretto delle parti al sistema del Servizio, esistono dubbi in merito alla sicurezza tecnica. Il nuovo sistema ha grossi svantaggi senza portare vantaggi degni di nota. Anche LU, SZ, SO, SG, SH e CAIS chiedono di mantenere il vecchio sistema ed eventualmente di valutare se, vista l'enorme quantità di dati, non sia opportuno limitare la conservazione centrale dei dati a quelli di Internet e registrare e inviare, come sinora, i dati della sorveglianza telefonica su supporti di dati. LU si chiede se i dati saranno ancora a disposizione se dovessero essere accessibili in un momento successivo nel quadro della revisione di una sentenza. Secondo il rapporto esplicativo ciò non è garantito. ZG chiede di prendere in considerazione un disciplinamento più semplice. Per BS, FSA e MS il sistema proposto viola i diritti delle parti ed è necessario un meccanismo di controllo per garantire che tutti i dati importanti si trovino anche nel dossier.

Il PPD rende attento al pericolo di abusi nell'ambito di Internet e chiede di garantire che sia possibile accedere soltanto ai dati raccolti nel corso della sorveglianza.

Per parecchi partecipanti[66] la prima menzione della legge sulla protezione dei dati nel capoverso 2 è estremamente tardiva. La protezione dei dati deve iniziare nel momento in cui i dati vengono raccolti. Inoltre, nel capoverso 1 non è specificato chi rilascia l'autorizzazione. In tutto l'articolo manca la menzione di procedure per garantire la protezione dei dati.

2.5. Articolo 10 Diritto di consultare gli atti e diritto di accedere ai dati

[1] Il diritto di consultare gli atti e il diritto di accedere ai dati dell'interessato raccolti nel quadro di un procedimento penale (art. 1 cpv. 1 lett. a) sono retti dagli artico-li 95, 97, 98, 99 capoverso 1, 101 capoverso 1, 102 e 279 CPP.

[2] Il diritto di consultare gli atti e il diritto di accedere ai dati dell'interessato raccolti nell'ambito dell'esecuzione di una domanda di assistenza giudiziaria (art. 1 cpv. 1 lett. b) sono retti dalla legislazione speciale in materia, nonché dalla legge federale del 19 giugno 19928 sulla protezione dei dati (LPD), se l'autorità incaricata della domanda di assistenza giudiziaria è un'autorità della Confederazione, oppure dal diritto cantonale, se tale autorità è il pubblico ministero di un Cantone.

65 ZH, AG, GL, TG, VS, JU, CCDGP, CCPCS, CCC.

66 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

[3] Il diritto di consultare gli atti e il diritto di accedere ai dati dell'interessato raccolti nell'ambito della ricerca di persone disperse (art. 1 cpv. 1 lett. c) o condannate (art. 1 cpv. 1 lett. d) sono retti dal diritto cantonale. È fatto salvo l'articolo 29.

[4] La persona interessata dai dati raccolti nel corso della sorveglianza in questione fa valere i propri diritti presso l'autorità incaricata del caso. Se non vi è più un'autorità incaricata del caso, li fa valere presso l'ultima che lo era o presso quella successiva. L'interessato non può far valere i propri diritti presso il Servizio.

Un numero notevole di partecipanti[67] respinge l'articolo 10, poiché secondo loro il CPP contiene disposizioni sufficienti per proteggere i dati personali. Il principio del capoverso 1, secondo cui il diritto di consultare gli atti e il diritto di accedere ai dati è retto dal CPP è un'ovvietà. Tuttavia gli articoli del CPP menzionati al capoverso 1 non sono pertinenti per la sorveglianza segreta. BL è d'accordo e propone pertanto un adattamento della disposizione. L'introduzione di una competenza svizzera specifica per domande dall'estero, prevista nel capoverso 2, non ha senso. Per la ricerca di persone disperse secondo il capoverso 3 si potrebbe senz'altro dichiarare applicabile per analogia l'articolo 279 CPP. Il rinvio al diritto cantonale del capoverso 3 non ha senso. Per contro SZ si esprime a favore del rinvio. Il capoverso 4 è inutile.

FR è del parere che anche i terzi che non partecipano al procedimento penale debbano avere il diritto di consultare i dati che li riguardano.

PPS critica che, se la sorveglianza è segreta e non è effettuata una comunicazione conformemente all'articolo 279 capoverso 2 CPP, il capoverso 4 sancisce un diritto senza destinatario.

2.6. Articolo 11 Termine di conservazione dei dati

[1] I dati raccolti nel quadro di un procedimento penale (art. 1 cpv. 1 lett. a) sono conservati nel sistema di trattamento fino alla scadenza del termine di prescrizione dell'azione penale. L'autorità incaricata del caso comunica il termine al Servizio.

[2] I dati raccolti nell'ambito dell'esecuzione di una domanda di assistenza giudiziaria (art. 1 cpv. 1 lett. b) sono conservati nel sistema di trattamento finché lo scopo perseguito lo rende necessario, ma al massimo per 30 anni.

[3] I dati raccolti nell'ambito della ricerca di persone disperse (art. 1 cpv. 1 lett. c) sono conservati nel sistema di trattamento finché lo scopo perseguito lo rende necessario, ma al massimo per 30 anni.

[4] I dati raccolti nell'ambito della ricerca di persone condannate a una pena detentiva (art. 1 cpv. 1 lett. d) sono conservati nel sistema di trattamento finché lo scopo perseguito lo rende necessario, ma al massimo fino alla scadenza del termine di prescrizione della pena. L'autorità incaricata del caso comunica il termine al Servi-zio. I dati raccolti nell'ambito della ricerca di persone condannate a una misura privativa della libertà (art. 1 cpv. 1 lett. d) sono conservati nel sistema di trattamento finché lo scopo perseguito lo rende necessario, ma al massimo per 30 anni.

[5] La Confederazione e ciascun Cantone designano un'autorità che il Servizio informa della prossima scadenza del termine di conservazione dei dati in questione. Tale autorità trasmette l'avviso all'autorità incaricata del caso o, se non vi è più un'autorità incaricata del caso, all'ultima che lo era o a quella successiva. Alla scadenza del termine di conservazione dei dati contenuti nel sistema di trattamento, l'autorità che ha ricevuto l'avviso chiede al Servizio di trasferirle tali dati. Una volta effettuato il trasferimento o in mancanza di una tale richiesta, il Servizio distrugge definitivamente i dati in questione conservati nel sistema di trattamento.

Diversi partecipanti[68] respingono l'articolo 11 AP-LSCPT e osservano che mantenendo, come chiedono, il sistema attuale il disciplinamento complicato dei termini di prescrizione e di conservazione sarebbe obsoleto. Il sistema attuale, in cui i dati sono trattari analogamente a tutti gli altri dati di uno stesso dossier, è preferibile rispetto a un disciplinamento specifico. La disposizione è necessaria soltanto perché i dati sono conservati presso il Servizio e non nel fascicolo penale, il che tuttavia non è opportuno. La connessione dei termini di conservazione dei dati al termine di prescrizione dell'azione penale non è chiara e causa inutili oneri

67 LU, NW, BL, SG, GL, TG, VS, JU, CCDGP, CAIS, SSDP.
68 BE, SZ, NW, BL, SH, SG, AG, VD, CAIS.

amministrativi. L'organizzazione della comunicazione proposta è complicata, l'intera procedura è troppo complessa e onerosa. I termini di conservazione dovrebbero essere retti dal CPP, poiché disciplinamenti diversi sono inopportuni. CAIS ritiene che, se s'intende mantenere il sistema proposto, sia sufficiente una disposizione secondo cui, una volta scaduto il termine di conservazione, l'autorità che dispone degli atti garantisce che i dati registrati presso il Servizio siano cancellati. AG chiede di fissare un termine di conservazione uniforme (p.es. 10 o 15 anni).

ZG chiede di precisare il capoverso 1 in modo tale che sia chiaro quale autorità comunica al Servizio il termine di prescrizione dell'azione penale.

PPD, Verdi, GDS e gr.ch criticano i termini di conservazione troppo lunghi dell'articolo 11. Perciò il PPD propone di ridurre i termini di conservazione. Verdi, GDS e gr.ch chiedono di scorporare i dati al più tardi dopo la chiusura del procedimento penale e di conservarli soltanto per la consultazione da parte delle persone coinvolte. Dopo la conclusione del procedimento non vi è infatti più alcun motivo per impedire la consultazione completa degli atti da parte delle persone coinvolte. A queste ultime dovrebbero pertanto essere consegnate automaticamente tutte le registrazioni in un formato d'uso commerciale.

Il PPS chiede che alla scadenza del termine di conservazione previsto al capoverso 1 i dati siano cancellati. Inoltre, per i termini non dovrebbero essere determinanti, come proposto, gli obiettivi perseguiti, bensì la prescrizione.

IT(19), ISSS, SWICO, hp e COG propongono di completare l'articolo 11 con regole che determinino quale autorità decide in merito alla durata effettiva della conservazione dei dati nel singolo caso. Occorre inoltre disciplinare le condizioni e gli obblighi, come pure il modo di procedere per la cancellazione immediata dei dati non più necessari per gli scopi della sorveglianza e prevedere un controllo dell'effettiva cancellazione dei dati.

Otto partecipanti[69] chiedono di completare il capoverso 5 come segue: «... nel sistema di trattamento e da tutti i mezzi di registrazione...».

2.7. Articolo 12 Sicurezza

Il Servizio è responsabile della sicurezza del sistema di trattamento. Il Consiglio federale emana le disposizioni relative ai provvedimenti tecnici e organizzativi di protezione, in particolare contro l'accesso, la modifica, la diffusione non autorizzata e la distruzione accidentale o non autorizzata dei dati. I soggetti che effettuano la sorveglianza in virtù della presente legge rispettano le istruzioni del Servizio in materia di sicurezza dei dati all'atto della trasmissione dei dati raccolti nell'ambito di una sorveglianza.

IT(19) propongono di completare l'articolo 12 con prescrizioni chiare sui controlli necessari di tutti i dati risultanti dalla sorveglianza e con definizioni chiaramente strutturate dei compiti del Servizio.

SWICO, hp e COG si chiedono quali compiti e obblighi saranno previsti, per i fornitori di servizi di telecomunicazione e ISP menzionati nell'articolo 12, dall'ordinanza del Consiglio federale sui provvedimenti di protezione tecnici e organizzativi e quali costi ne risulteranno. Chiedono che tali obblighi non comportino costi aggiuntivi.

Il PPS chiede che, oltre al Servizio e ai soggetti che effettuano la sorveglianza, siano sogget-

[69] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

ti alle norme sui provvedimenti di protezione tecnici e organizzativi anche le autorità che usano il sistema di trattamento e le unità amministrative da queste designate.

2.8. Articolo 13 Responsabilità

Le autorità che hanno accesso al sistema di trattamento (art. 9) fungono da detentori della collezione di dati raccolti nel corso della sorveglianza di loro competenza

Alcuni partecipanti[70] presentano la seguente proposta di modifica: «Le autorità *che hanno ordinato la sorveglianza* e che hanno accesso al sistema di trattamento (art. 9) *sono responsabili dell'uso conforme alla legge* della collezione di dati raccolti nel corso della sorveglianza di loro competenza». Da parte sua Cablecom propone la seguente precisazione: «*Le autorità che hanno ordinato la sorveglianza* fungono da detentori della collezione di dati raccolti nel corso della sorveglianza di loro competenza».

3. Compiti del Servizio

3.1. Articolo 14 Informazioni sui collegamenti di telecomunicazione

Su richiesta, il Servizio fornisce informazioni sui dati di cui all'articolo 20 capoversi 1-3 esclusivamente alle autorità seguenti, per i fini indicati:

a. autorità federali e cantonali che hanno il diritto di ordinare o approvare la sorveglianza del traffico delle telecomunicazioni, allo scopo di determinare i collegamenti e le persone da sorvegliare;

b. Ufficio federale di polizia e comandi di polizia cantonali e municipali, allo scopo di adempiere compiti di polizia;

c. autorità federali e cantonali competenti, allo scopo di trattare cause penali amministrative.

safe osserva che, secondo l'articolo 14 capoverso 2 in combinazione con il capoverso 4 della LSCPT in vigore, per rendere nota l'identità del titolare del collegamento è applicabile la procedura agevolata. A detta del rapporto esplicativo tale disposizione è ripresa in larga misura nell'articolo 14 in combinazione con l'articolo 20 capoverso 3 AP-LSCPT. Secondo l'articolo 14 capoverso 2 lettere b e c della LSCPT in vigore, possono usufruire della procedura agevolata le autorità di polizia e amministrative competenti per compiti di polizia e cause penali amministrative, ma altrimenti, secondo la lettera a, soltanto «*le autorità federali e cantonali che hanno il diritto di ordinare o approvare una sorveglianza del traffico delle telecomunicazioni*» (art. 6 LSCPT vigente; autorità di perseguimento penale), e soltanto «*allo scopo di determinare i collegamenti e le persone da sorvegliare*» Secondo safe, queste informazioni possono pertanto essere usate soltanto per i casi di sorveglianza riguardanti i reati di cui all'articolo 269 capoverso 2 lettera a CPP. Questo tuttavia non può essere stato l'intento del Legislatore. La procedura dovrebbe essere infatti a disposizione di tutte le autorità di perseguimento penale per perseguire tutti i reati commessi per mezzo di Internet – e soprattutto per raccogliere le prove. Inoltre, la rivelazione di dati è spesso anche un presupposto per prevenire in modo efficace gli atti criminali. safe propone pertanto di modificare l'articolo 14 lettera a AP-LSCPT come segue: «a. autorità federali e cantonali di *perseguimento penale, allo scopo del perseguimento penale e della prevenzione di atti criminali*».

3.2. Articolo 15 Compiti generali nell'ambito della sorveglianza

Nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni, il Servizio svolge i seguenti compiti generali:

---

[70] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

a.	*verifica che la sorveglianza concerna un reato che può essere oggetto di una tale misura in virtù del diritto applicabile e che sia stata ordinata dall'autorità competente; se l'ordine di sorveglianza è chiaramente errato o infondato, interpella l'autorità d'approvazione prima che invii o informazioni siano trasmessi all'autorità che ha ordinato la sorveglianza;*
b.	*istruisce i soggetti che effettuano la sorveglianza in virtù della presente legge in merito allo svolgimento della sorveglianza, li esorta ad adottare qualsiasi misura utile a tal fine e ne controlla l'esecuzione;*
c.	*attua le misure di tutela del segreto professionale ordinate dall'autorità d'approvazione;*
d.	*controlla che la sorveglianza non si estenda oltre la durata autorizzata e vi pone fine alla scadenza del termine, sempreché non ne sia stata chiesta la proroga;*
e.	*comunica senza indugio all'autorità d'approvazione la fine della sorveglianza.*

Alcuni partecipanti[71] propongono di completare l'articolo 15 AP-LSCPT con la seguente lettera f: «offre consulenza alle autorità e ai fornitori di servizi di telecomunicazioni nelle questioni tecniche relative alla sorveglianza del traffico delle telecomunicazioni».

Il PPS critica che manca il compito generale del Servizio di creare e gestire un sistema d'infiltrazione (cfr. cap. III n. 11.1.2 ad art. 270bis).

3.2.1 Lettera a

Il PLR propone di disciplinare in generale in modo più chiaro il ruolo del Servizio, soprattutto per quanto riguarda le sue competenze nei confronti delle autorità di perseguimento penale.

Vari partecipanti[72] osservano che manca la competenza del Servizio di verificare l'ammissibilità della sorveglianza. Nella prassi il Servizio si limita a trasmettere l'ordine, anche nel caso in cui quest'ultimo è chiaramente errato. A questo si aggiunge che le persone soggette alla sorveglianza non possono avvalersi di rimedi giuridici per contestare la mancanza di una base legale per le misure di sorveglianza (cfr. le proposte al cap. III n. 9.2 ad art. 34 AP--LSCPT: rimedi giuridici). Inoltre, il Tribunale amministrativo federale, in quanto autorità di ricorso, può esaminare soltanto i fatti già esaminati dall'autorità inferiore, ossia dal Servizio, che tuttavia non procede a tale esame. Viene quindi proposta la seguente formulazione «a. verifica che la sorveglianza sia stata ordinata dall'autorità competente, che il tipo di misura di sorveglianza ordinata sia previsto dalla legge e che il tipo di misura di sorveglianza ordinata possa essere effettuato sotto il profilo tecnico e organizzativo. Non verifica che nel singolo caso concreto l'ordine di sorveglianza soddisfi le condizioni di cui all'articolo 269 lettere b e c del Codice di procedura penale e che l'ordine sia appropriato». BL osserva che se per ricorrere contro l'ordine di sorveglianza secondo l'articolo 34 capoverso 2 AP-LSCPT possono essere avanzati motivi di fattibilità di ordine tecnico o organizzativo, tale fattibilità dovrebbe essere anteriormente verificata. L'articolo 15 lettera a AP-LSCPT va pertanto completato in tal senso (cfr. le spiegazioni al cap. III n. 9.2.2 ad art. 34 cpv. 2 AP-LSCPT).

Alcuni partecipanti[73] propongono inoltre di completare la lettera a con la seguente frase: «In caso di dubbio sull'obbligo di effettuare una sorveglianza, il Servizio delibera mediante decisione applicando le disposizioni legali pertinenti». Gli stessi partecipanti si chiedono in generale se il Servizio possa decidere nei confronti dei fornitori di servizi di telecomunicazione, dato che il termine «decisione» presuppone che chi decide verifichi e motivi dal punto di vista giuridico la propria decisione. Cablecom rileva infine una contraddizione con l'articolo 33 AP-LSCPT, il quale stabilisce che il Servizio vigila sul rispetto della legislazione.

---

71 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

72 Swisscable, SWICO, SKS, Cablecom, asut, Orange, Swisscom, Colt, Sunrise, Verizon, CAIS, economiesuisse, VERDI, SKS, IT(19).

73 asut, Orange, Swisscom, Colt, Sunrise, Verizon.

3.2.2 Lettera b

Vari fornitori di servizi di telecomunicazione[74] propongono di completare la lettera b come segue: «istruisce, *nel quadro delle basi legali pertinenti,* i soggetti che effettuano la sorveglianza in virtù della presente legge in merito allo svolgimento della sorveglianza, li esorta ad adottare qualsiasi misura utile a tal fine e ne controlla l'esecuzione».

3.2.3 Lettera c-e

Nessuna osservazione

3.3. Art. 16 Compiti nell'ambito della sorveglianza del traffico delle telecomunicazioni

Nell'ambito della sorveglianza del traffico delle telecomunicazioni, il Servizio svolge inoltre i compiti seguenti

a. *contatta tempestivamente l'autorità che ha ordinato la sorveglianza e l'autorità di autorizzazione se ritiene che non sia tecnicamente possibile effettuare la sorveglianza o che la sua esecuzione comporti notevoli difficoltà;*

b. *se più soggetti che effettuano la sorveglianza del traffico delle telecomuni-cazioni in virtù della presente legge partecipano alla fornitura del servizio di telecomunicazione da sorvegliare, incarica della sorveglianza il soggetto cui compete la gestione del numero o quello che può effettuare la sorveglianza con il minor onere tecnico possibile;*

c. *riceve dai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge le comunicazioni deviate della persona sorvegliata, le registra e permette all'autorità che ha ordinato la sorveglianza di consultarle;*

d. *se per ragioni tecniche non è in grado di ricevere, registrare o trasmettere all'autorità che ha ordinato la sorveglianza le comunicazioni della persona sorvegliata, ordina ai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge di trasmettere dette comunicazioni direttamente al servizio di polizia designato dall'autorità che ha ordinato la sorveglianza;*

e. *riceve dai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge i dati che consentono di individuare quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione; li registra e permette all'autorità che ha ordinato la sorveglianza di consultarli;*

f. *su richiesta dell'autorità che ha ordinato la sorveglianza, ordina ai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge di trasmettergli soltanto determinati tipi di dati del flusso di dati in questione.*

3.3.1 Lettera a

CAIS approva esplicitamente il meccanismo pragmatico. Per ZH e CCPCS la formulazione della lettera a non garantisce che il Servizio verifichi in modo approfondito la sorveglianza possa essere effettivamente eseguita sotto il profilo tecnico. Propongono pertanto la seguente formulazione: «se dopo un esame approfondito ritiene che...».

Vari partecipanti[75] ritengono che con una pertinente formulazione dell'articolo 15 lettera a (cfr. cap. III. n. 3.2.1 ad art. 15 lett. a AP-LSCPT) la lettera a dell'articolo 16 AP-LSCPT diventi superflua.

Cablecom si chiede se il Servizio sia in grado di possedere conoscenze approfondite di tutte le tecnologie possibili, necessarie per valutare se l'esecuzione di una sorveglianza comporti notevoli difficoltà. Propone pertanto di coinvolgere in casi speciali tutti gli interessati per discutere le possibilità e le conseguenze della sorveglianza.

---

74 asut, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
75 asut, Orange, Swisscom, Colt, Sunrise, Finecom.

3.3.2 Lettera b

Secondo privatim l'espressione «gestione del numero» non è applicabile a Internet e propone quindi di sostituirla con «gestione del collegamento».

Sei partecipanti[76] chiedono, con una proposta concreta di formulazione, di impartire l'ordine di sorveglianza al fornitore dell'utente da sorvegliare.

Cablecom osserva che secondo questa disposizione un provider può essere obbligato ad assolvere i compiti di un altro avente obbligo, se il Sevizio ritiene che il provider possa eseguire meglio tale compito. Non sono tuttavia chiari i criteri in base ai quali il Servizio possa prendere questa decisione. Visto che le sorveglianze non sono rimborsate, si rischi di creare uno squilibrio economico, in quanto è molto probabile che, essendo dal punto di vista tecnico meglio in grado di effettuare la sorveglianza, i grandi provider dovranno eseguire incarichi per conto di quelli più piccoli. Cablecom propone quindi di impartire l'ordine di sorveglianza al soggetto che fornisce il servizio di telecomunicazione all'utente da sorvegliare.

3.3.3 Lettera c

Nessuna osservazione.

3.3.4 Lettera d

Alcuni partecipanti[77] approvano esplicitamente la disposizione. Per contro alcuni partecipanti appartenenti al ramo dei servizi di telecomunicazione[78] si esprimono a favore dello stralcio della lettera d, poiché il Servizio di sorveglianza deve essere in grado in qualsiasi momento di ricevere il traffico delle telecomunicazioni, giacché anche i servizi di telecomunicazione hanno l'obbligo vincolante di adempiere il proprio compito. Secondo la FSA la trasmissione diretta deve assolutamente rimanere un'eccezione.

3.3.5 Lettera e

Vari partecipanti[79] ritengono che anche in futuro i dati del collegamento non dovrebbero passare attraverso il sistema di sorveglianza ISS[80]. La soluzione finora adottata, che consiste nella trasmissione diretta dei dati da parte dei fornitori di servizi di telecomunicazione all'autorità competente, presenta il solo problema che, a seconda del fornitore di servizi di telecomunicazione, non viene usato un formato uniforme. Tale problema può tuttavia facilmente essere risolto mediante istruzioni tecniche. Anche BL si esprime a favore di un formato uniforme per la trasmissione dei dati e chiede inoltre di chiarire nella legge quale sia la differenza – ammesso che ve ne sia una – tra i cosiddetti «dati del collegamento» e i «dati relativi alle comunicazioni e alla fatturazione»

---

76 asut, Finecom, Orange, Swisscom, Colt, Sunrise.
77 AG, GL, GR, TG, JU, CAIS, CCDGP.
78 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Cablecom.
79 NW, AG, GL, GR, TG, JU, CCDGP.
80 Interception System Svizzera.

3.3.6 Lettera f

Vari partecipanti appartenenti al ramo dei servizi di telecomunicazione[81] ritengono che l'eliminazione di determinati dati da un flusso di dati debba essere esclusivamente compito dell'autorità che ha ordinato la sorveglianza o del Servizio e chiedono pertanto di stralciare la disposizione (cfr. anche cap. III n. 5.2.3 ad art. 21 cpv. 3 AP-LSCPT). Anche Cablecom chiede di stralciare la disposizione e osserva che in caso di cernita da parte del fornitore di servizi di telecomunicazione vi è il rischio di una lacuna nella sorveglianza e ne potrebbe conseguire la perdita irrimediabile di dati importanti. La cernita dovrebbe essere quindi effettuata dalle autorità inquirenti, che conoscono il caso.

3.4. Articolo 17 Controllo della qualità

[1] Il Servizio adotta in via preventiva e a posteriori misure di controllo della qualità dei dati forniti dai soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge.

[2] Se a tal fine il Servizio deve venire a conoscenza del contenuto dei dati, il controllo della qualità può essere effettuato soltanto previo accordo dell'autorità che ha ordinato la sorveglianza.

La FSFP ritiene la disposizione molto importante. Il controllo della qualità deve essere garantito e avvenire periodicamente. Propone pertanto che in caso di non adempimento dello standard previsto siano adottati provvedimenti quali ad esempio la revoca della concessione.

KFG, invece, non vede la necessità della disposizione. Il controllo della qualità ha senso soltanto in riferimento alla verifica della completezza. La disposizione andrebbe pertanto precisata o stralciata.

3.5. Articolo 18 (in combinazione con l'art. 24) Certificazione

Art. 18:

A pagamento, il Servizio rilascia ai fornitori di servizi di telecomunicazione un certificato attestante la loro idoneità a effettuare correttamente la sorveglianza. Il Servizio fissa le modalità della certificazione.

Art. 24:

I fornitori di servizi di telecomunicazione che non dispongono di certificazione si assumono le spese dovute all'eventuale necessità di ricorrere al Servizio o a un terzo per la corretta esecuzione della sorveglianza. In questo caso, tali fornitori devono adottare immediatamente le misure per ottenere la certificazione da parte del Servi-zio, secondo le modalità di cui all'articolo 18.

Vari partecipanti[82] ritengono la certificazione in linea di massima opportuna. Propongono tuttavia di prevedere un obbligo di certificazione secondo cui servizi nuovi possono essere offerti soltanto se la loro sorveglianza è garantita.

VD ritiene che l'obiettivo della certificazione sia poco chiaro. Occorre pertanto chiedersi se non sia opportuno precisare che il valore di un mezzo di prova non è connesso alla certificazione.

Con riferimento alla Repubblica federale di Germania ZH e CCPCS propongono la certificazione dei produttori di apparecchi di telecomunicazione. Da un lato la certificazione dei fornitori di servizi di telecomunicazione è molto onerosa, dall'altro, è più semplice riprendere un certificato già esistente nell'ambito della cooperazione europea. Secondo la CCPCS, la certificazione dei produttori significherebbe maggiore certezza giuridica per i fornitori e protezione

---

81 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

82 LU, NW, BL, SG, AG, GL, GR, TG, JU, CCDGP, CAIS, FSFP, CP.

dell'innovazione.

Vari partecipanti appartenenti al ramo dei servizi di telecomunicazione[83] osservano che una certificazione non è opportuna fintanto che gli obblighi dei fornitori di servizi di telecomunicazione sono descritti in modo insoddisfacente e tendono a crescere senza limiti a causa della mancanza di rimedi giuridici efficienti contro nuovi metodi di sorveglianza. Visti questi presupposti, l'ottenimento di un certificato non è che lo specchio di una situazione momentanea e non ha alcun valore per il futuro. Propongono pertanto la seguente nuova formulazione dell'articolo 18 AP-LSCPT: «Il Servizio rilascia ai fornitori di servizi di telecomunicazione un certificato attestante la loro idoneità *di massima* a effettuare la sorveglianza *prevista dalla presente legge*. *Attesta in particolare che i fornitori di servizi di telecomunicazione tenuti a eseguire la sorveglianza dispongono degli interfaccia necessari compatibili con il sistema di trattamento della Confederazione*». Richiamandosi al principio della proporzionalità, Verizon propone inoltre di concedere ai fornitori di servizi di telecomunicazione la possibilità di ricorrere nel singolo caso a terzi, senza che ciò comporti un obbligo immediato di certificazione. I partecipanti menzionati rifiutano l'assunzione dei costi da parte degli aventi obbligo di sorveglianza. Anche HR chiede di stralciare l'assunzione dei costi da parte degli aventi obbligo di sorveglianza e rinvia inoltre al significato politico-economico del disciplinamento**.** In Svizzera, il settore di Internet ha permesso la nascita di numerose e vivaci nuove imprese (start-up) che hanno creato numerosi posti di lavoro a lungo termine. Inoltre, numerose imprese rinomate del settore si sono insediate in Svizzera (p.es. Google a Zurigo). Costi difficilmente prevedibili e certificazioni onerose costituiscono un ostacolo che riduce in particolare le probabilità di successo delle start-up e l'interesse di insediamento di imprese internazionali. Anche CCC, INT e PPS ritengono l'assunzione dei costi della certificazione un onere sproporzionato per i fornitori di accesso a Internet. Cablecom, infine, osserva che in qualsiasi altra relazione commerciale i costi per i test d'integrazione di interfaccia tecnici sono a carico del mandante o perlomeno ciascuna parte si assume i propri costi. È quindi incomprensibile che il Servizio impieghi ausiliari per la certificazione e se li faccia per giunta pagare dai fornitori di servizi di telecomunicazione. Per queste ragioni Cablecom rifiuta l'assunzione totale dei costi della certificazione da parte dei fornitori di servizi di telecomunicazione, chiedendo di stralciare gli articoli 18 e 24 AP-LSCPT. Secondo SIUG, un intero settore economico è costretto a tenersi al passo con l'istruzione penale ed eseguirla autonomamente per conto dello Stato. Chi non si fa certificare dovrà, se del caso, prendersi a carico i costi imprevisti di una sorveglianza. Per molte imprese ciò costituisce un danno finanziario difficilmente superabile. Per contro, è possibile che i fornitori che si sottopongono alla procedure di certificazione non debbano mai eseguire una sorveglianza. In tal caso il perseguimento penale non trarrà beneficio dai costi e dal lavoro investito. Anche SIUG chiede pertanto di stralciare gli articoli 18 e 24 AP-LSCPT.

IT(19), SWICO, hp e COG chiedono di precisare e descrivere in modo più chiaro l'oggetto e la procedura della certificazione**.** Inoltre, l'articolo 18 AP-LSCPT dovrebbe contenere un elenco che chiarisca chi deve ottenere un certificato. Secondo SWICO, hp e COG i costi della certificazione devono inoltre essere assunti dal Servizio.

GDS e gr.ch si esprimono a favore dello stralcio degli articoli 18 e 24 AP-LSCPT, poiché in caso contrario la libertà di offrire forme moderne di comunicazione è sostituita da un sistema d'autorizzazione e di controllo statale.

Anche switch e switchplus sono contrati a un obbligo (di fatto) di certificazione. Occorre stabilire chiaramente che le persone soggette alla LSCPT devono superare un test di «com-

---

[83] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

pliance» che le esenta dall'obbligo di certificazione. Altrimenti, i requisiti della certificazione vanno adeguati a quelli previsti dalle direttive concernenti l'«acceptance testing», affinché il lavoro non sia raddoppiato.

ISSS osserva che l'oggetto e le procedure della certificazione sono formulate in modo molto vago e che quindi occorre chiedersi in generale se sia possibile accertare mediante una procedura di certificazione l'idoneità di un fornitore di servizi di telecomunicazione a effettuare la sorveglianza conformemente alla legge Non è inoltre chiaro se l'ISP e le persone menzionate nell'articolo 2 capoverso 1 lettera b AP-LSCPT debbano ottenere un certificato.

4. Obblighi nell'ambito della sorveglianza della corrispondenza postale

4.1. Articolo 19

[1] Entro i limiti previsti dall'ordine di sorveglianza, i soggetti che effettuano la sorveglianza della corrispondenza postale in virtù della presente legge trasmettono all'autorità che ha ordinato la sorveglianza gli invii postali e i dati che consentono di individuare quando e con quali persone la persona sorvegliata è stata o è in contatto postale e i dati relativi alle comunicazioni e alla fatturazione. Su richiesta dell'autorità che ha ordinato la sorveglianza, le forniscono informazioni complementari sulla corrispondenza postale della persona sorvegliata.

[2] Tali soggetti conservano i dati di cui al capoverso 1 per dodici mesi.

4.1.1 Capoverso 1

Secondo vari partecipanti[84] la disposizione non chiarisce che nell'ambito della sorveglianza della corrispondenza postale non si deve garantire soltanto che i fornitori trasmettano gli invii postali, ma anche che, dopo il controllo da parte della polizia, li riprendano in consegna e li inviino senza indugio al destinatario. Chiedono una precisazione in tal senso nella legge.

La Posta Svizzera osserva che non è registrata tutta la corrispondenza postale e che pertanto non è possibile fornire successivamente informazioni sul contenuto o i dati secondari della corrispondenza per ogni singolo invio. In particolare gli invii imbucati in una buca delle lettere per strada o in un ufficio postale e tutti gli altri invii (di lettere) non raccomandati non sono registrati da alcun sistema di trattamento e di trasporto della Posta Svizzera, per cui non è disponibile alcun dato secondario che potrebbe essere successivamente richiesto e comunicato. Ciò non vale per tutte le lettere e i pacchi raccomandati e per alti invii che sono rintracciabili per mezzo del sistema «Track & Trace» della Posta Svizzera. In questi casi possono essere successivamente fornite le informazioni trasmesse finora. La Posta Svizzera constata che la revisione della LSCPT non prevede nuove possibilità o nuovi obblighi per la Posta Svizzera.

Per Verdi, GDS e gr.ch la trasposizione della definizione di dati secondari alla sorveglianza della corrispondenza postale è addirittura assurda. Rilevano che il numero di sorveglianze della corrispondenza postale è diminuito in proporzione all'aumento delle forme elettroniche di comunicazione e, al posto del raddoppio della durata di conservazione, propongono lo stralcio della disposizione e la revoca della prassi su di essa fondata. In tale contesto i Verdi rinviano all'enorme quantità di dati accumulati, di minima importanza per il perseguimento di reati. Secondo GDS e gr.ch non esiste alcuna garanzia per l'esattezza delle indicazioni del mittente (qualora queste sussistano), tranne nel caso in cui si richieda un documento d'identità in occasione della consegna in un ufficio postale. In considerazione delle conse-

84 ZH, LU, NW, GL, GR, TG, VS, JU, CCDGP, CAIS.

guenze di un'applicazione letterale, anche SIUG e VSPF ritengono la disposizione insufficiente.

4.1.2 Capoverso 2

Un numero notevole di partecipanti[85] accoglie esplicitamente con favore l'estensione della durata di conservazione dei dati della corrispondenza postale da sei a 12 mesi. Undici di loro[86] chiedono di esaminare se non sia possibile estendere in misura notevolmente maggiore la durata di conservazione, visto che di regola i fornitori conservano i dati per dieci anni. SZ è tuttavia d'accordo con l'estensione della durata di conservazione soltanto a condizione che si prevedano nel contempo misure legislative che garantiscano la sicurezza dei dati, la protezione dall'uso abusivo e la trasparenza della trasmissione dei dati.

Per la Posta Svizzera la prevista estensione della durata di conservazione dei dati secondari da sei a 12 mesi non costituisce un problema.

Cablecom e SKS respingono il prolungamento della durata di conservazione. SKS osserva che la comunicazione postale è costantemente diminuita in proporzione all'aumento di quella elettronica e che i dati raccolti sono in genere poco utili per il perseguimento penale.

5. Obblighi nell'ambito della sorveglianza del traffico delle telecomunicazioni

Vari partecipanti appartenenti al ramo dei servizi di telecomunicazione[87] propongono di modificare il titolo della sezione 5 come segue: «Obblighi dei fornitori di servizi di telecomunicazione», poiché nel caso delle informazioni sui collegamenti di telecomunicazione (art. 20 AP-LSCPT) non si tratta di una sorveglianza né di un'ingerenza nel segreto delle telecomunicazioni.

Swisscom propone di prevedere nella sezione 5 le tre categorie di prestazioni seguenti, ponendo dei limiti chiari a ciascuna categoria: informazioni su collegamenti, sorveglianze in tempo reale e conservazione dei dati relativi ai collegamenti. Inoltre, le disposizioni dovrebbero essere coordinate con il CPP. Da quest'ultimo si evince chiaramente che dovrebbe essere lecita solo la sorveglianza di determinati collegamenti usati da persone sospette. La ricerca generale di elementi di sospetto è pertanto illecita. Secondo Swisscom si tratta quindi di evitare che – com'è stato il caso sinora – sia emanato un ordine che secondo il nuovo CPP non sarebbe ammesso.

5.1. Articolo 20 Informazioni sui collegamenti di telecomunicazione

[1] I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge forniscono al Servizio i seguenti dati concernenti determinati collegamenti di telecomunicazione:

a. il cognome, il nome, la data di nascita, l'indirizzo e, se disponibile, la professione dell'utente;

b. gli elementi dell'indirizzo di cui all'articolo 3 lettera f della legge del 30 aprile 1997 sulle telecomunicazioni;

c. i tipi di collegamento.

[2] I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge devono essere in grado di fornire per almeno due anni dopo l'avvio di un rapporto commerciale nel settore della telefonia

---

85 ZH, LU, NW, GL, GR, TG, VS, JU, SZ, UR, OW, FR, SO, AG, GE, CCDGP, CAIS.
86 ZH, LU, NW, GL, GR, TG, VS, JU, SZ, CCDGP, CAIS.
87 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

mobile e di Internet con clienti che non hanno sottoscritto un abbonamento le informazioni di cui al capoverso 1 relative a tale rapporto.

[3] Se un reato è commesso mediante Internet, i soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge forniscono al Servizio qualsiasi indicazione che consenta di identificarne l'autore.

[4] Il Consiglio federale disciplina la forma delle richieste e la loro conservazione. Può consentire alle autorità di cui all'articolo 14 di accedere a elenchi non pubblici. Può inoltre permettere al Servizio di accedere a tali dati mediante consultazione online. Può prevedere che la comunicazione dei dati sia gratuita e abbia luogo 24 ore su 24.

IT(19), SWICO, hp e COG propongono di prevedere un'autorità di controllo esterna, che sorvegli e controlli il Servizio in qualsiasi momento. Come motivazione SWICO, hp e COG osservano che il prescritto accesso a tutti i dati della comunicazione e il conseguente accertamento dell'identità dell'utente garantisce alle autorità federali ampie possibilità di sorveglianza.

5.1.1 Capoverso 1

UNISG e UNIZH chiedono di menzionare esplicitamente nella legge i «collegamenti Internet» che secondo il rapporto esplicativo fanno parte dei «collegamenti di telecomunicazione». switch e switchplus rilevano che il termine «collegamenti di telecomunicazione» non è definito né nell'OSCPT né nella LTC. Se ne parla soltanto nell'ordinanza dell'Ufficio federale delle comunicazioni del 9 dicembre 1997[88] sui servizi di telecomunicazione e gli elementi d'indirizzo, in cui il termine intende la telefonia mediante GSM[89]/UMTS[90], PSTN[91]/ISDN[92] e IP (VoIP). Chi fornisce servizi di VoIP per il pubblico è tenuto a rendere noti tali dati. I servizi di VoIP non pubblici non sono contemplati.

Lettera a

Dieci partecipanti[93] accolgono esplicitamente con favore il fatto che sia in futuro necessario indicare anche la data di nascita. ZH, LU, CCPCS e BL propongono inoltre che per garantire l'identificazione di clienti, soprattutto nel settore delle registrazione delle carte prepagate nell'ambito delle telefonia mobile, siano rilevati anche il tipo e il numero di documento. In tale contesto BL fa notare gli abusi esistenti nella prassi per cui molte relazioni con clienti sono aperte in base a dati personali che non esistono oppure, dopo una registrazione corretta di una carta SIM prepagata, un impiegato del punto vendita registra ancora altre carte SIM a nome dello stesso utente.

Altri partecipanti[94] chiedono di stralciare l'indicazione della data di nascita.

UNISG e UNIZH osservano che nel settore di Internet, ad esempio quando viene utilizzato un computer pubblico, l'utente non può essere individuato.

Secondo HR dalla lettera a consegue che un indirizzo di posta elettronica non può più essere assegnato anonimamente. Si chiede se i fornitori di un valore aggiunto che non assegnano indirizzi di posta elettronica propri debbano garantire il collegamento tra indirizzo di posta elettronica e persona fisica o se possono limitarsi a rinviare al proprietario del domain secondo il protocollo «whois». Si chiede inoltre se la nuova disposizione renda punibile la pub-

---

88 SR 784.101.113
89 Global System for Mobile Communications.
90 Universal Mobile Telecommunications System.
91 Public Switched Telephone Network.
92 Integrated Services Digital Network.
93 ZH, LU, SO, GL, GR, TG, VS, JU, CCDGP, CCPCS.
94 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

blicazione di un contributo a un forum o a un blog senza chiedere la data di nascita dell'autore.

Lettera b

Nove partecipanti[95] chiedono di riformulare la lettera b come segue: «Gli elementi dell'indirizzo di cui all'articolo 3 *lettere f e g* della legge del 30 aprile 1997 sulle telecomunicazioni;»., poiché negli articoli 270ter e 274 capoverso 4 lettera d CPP sono elencati soltanto gli apparecchi di telefonia mobile. I computer portatili con carte SIM per la comunicazione mediante la rete di telefonia mobile sono pertanto esclusi.

VD chiede un chiarimento nella legge in merito all'identificazione di indirizzi IP. Tale identificazione è oggi considerata una semplice misura ai sensi dell'articolo 14, il che consente alla polizia di ottenere i dati senza l'autorizzazione di un giudice. Secondo VD con l'AP-LSCPT tale prassi non può essere mantenuta senza problemi. Chiede pertanto di chiarire che, come per un numero telefonico, per l'accesso a un indirizzo IP non è necessaria una procedura d'autorizzazione, bensì è sufficiente, come attualmente, una procedura semplice.

Lettera c

Nessuna osservazione.

5.1.2 Capoverso 2

BL ritiene poco chiaro il disciplinamento previsto per la durata dell'obbligo d'informazione. Non è ad esempio chiaro perché il termine sia fissato a due anni indipendentemente da un rapporto commerciale attivo con il cliente. Un fornitore di servizi di telecomunicazione deve essere in grado di fornire le informazioni di cui al capoverso 1 in merito a tutti i rapporti commerciali attivi con clienti. Propone pertanto la seguente formulazione: «*[…] per almeno due anni dallo scioglimento del rapporto commerciale o dalla disattivazione del collegamento […]"*. Inoltre, il tenore dell'articolo 20 capoverso 2 AP-LSCPT va completato con l'aggiunta che durante il termine previsto i fornitori di servizi di telecomunicazione devono costantemente essere in grado di fornire le copie dei documenti d'identità dei propri clienti. VD chiede inoltre di menzionare esplicitamente le carte wireless prepagate.

Otto partecipanti[96] propongono la seguente nuova formulazione: «I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge devono essere in grado di fornire per almeno due anni dopo l'avvio di un rapporto commerciale nel settore della telefonia mobile con clienti *che hanno effettuato la prima registrazione* e che non hanno sottoscritto un abbonamento, le informazioni di cui al capoverso 1 relative a tale rapporto». L'aggiunta «e di Internet» va cancellata poiché l'obbligo di registrazione, p.es. per carte WLAN prepagate, non è praticabile.

UNIZH propone di adeguare il termine di conservazione proposto di due anni alla durata di conservazione generale di 12 mesi (cfr. art. 19 cpv. 2 AP-LSCPT e art. 23 AP--LSCPT), poiché in caso contrario è necessaria un'onerosa procedura di selezione per separare i dati a cui si applicano termini diversi.

---

95 ZH, LU, GL, GR, TG, VS, JU, CCDGP, CCPCS.

96 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

5.1.3 Capoverso 3

SO ritiene che l'estensione dell'obbligo di fornire informazioni che consentano di identificare l'autore di un reato agevola notevolmente il compito della polizia.

UCS chiede una precisazione in merito alle informazioni sui collegamenti di telecomunicazione, dato che non è chiaro quali dati devono raccogliere e conservare i fornitori di collegamenti pubblici «Wi-Fi».

Otto partecipanti[97] propongono la seguente riformulazione: «Se un reato è commesso mediante Internet, i soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge forniscono al Servizio qualsiasi indicazione *disponibile sui collegamenti di telecomunicazione che possa contribuire all'identificazione dell'autore*». Motivano la modifica proposta adducendo che dovrebbero essere fornite soltanto informazioni sui collegamenti e non sui dati della comunicazione. Inoltre, i dati che vanno al di là di quelli previsti dal capoverso 1 dovrebbero poter essere richiesti soltanto se disponibili. L'identificazione dell'utente può costituire l'obiettivo, ma non può essere compito dei fornitori. Infine, Cablecom osserva che nella maggior parte dei casi è possibile identificare l'apparecchio per mezzo del quale è stato commesso il reato, ma non se l'apparecchio è collegato attraverso un «router» privato. In tal caso è possibile identificare il «router», ma non l'apparecchio finale utilizzato. In tale contesto UNIZH osserva che occorre distinguere tra la persona abbonata e la persona da sorvegliare. È possibile fornire informazioni soltanto sull'abbonamento di un collegamento via cavo o sulla persona per la quale è riservato un elemento d'indirizzo. È un compito quasi impossibile individuare chi ha effettivamente usato il computer, lo smartphone, ecc. UNIZH propone pertanto la seguente formulazione: «…che consenta di identificarne l'autore, *a condizione che riguardi un collegamento di telecomunicazione*».

Secondo switch e switchplus il capoverso 3 non sembra più limitarsi soltanto ai collegamenti di telecomunicazione. Chiede pertanto di precisare che il capoverso è applicabile esclusivamente ai collegamenti di telecomunicazione e non concerne i nomi di dominio.

ISSS propone di adattare e precisare l'oggetto e la portata dell'identificazione degli utenti alle forme odierne e a future dell'uso della comunicazione digitale e di Internet. L'introduzione dell'obbligo dei fornitori di servizi di telecomunicazione di identificare ogni singolo utente del traffico digitale delle telecomunicazioni e di Internet pone gli aventi obbligo di fronte a un compito quasi insormontabile.

Per KFG la disposizione è un passo verso la totale sorveglianza di Internet. Ogni utente è costretto a identificarsi. Propone pertanto di adattare la disposizione in modo tale che debbano essere identificati solo gli utenti di Internet con un collegamento registrato, oppure di stralciare la disposizione.

ifpi e safe osservano che per i reati in materia di diritti d'autore il bene giuridico protetto è costituito da diritti privati. Internet si sottrae all'ordinamento giuridico, se agli aventi diritto è tolta la possibilità di rivolgersi direttamente a chi viola il diritto. Ne consegue un perseguimento penale che consente di intervenire contro chi viola il diritto. Questa criminalizzazione indesiderata di chi viola diritti privati non è necessaria se gli aventi diritto conoscono gli autori della violazione e possono agire in sede civile contro questi ultimi. ifpi e safe propongono pertanto di modificare l'AP-LSCPT in modo tale che, se è resa verosimile una violazione del diritto mediante l'uso di un determinato indirizzo IP, le informazioni di cui al capoverso 3 debbano,

---

[97] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

su richiesta, essere fornite anche al danneggiato oppure che il danneggiato possa ottenere le informazioni direttamente dagli ISP.

5.1.4 Capoverso 4

Alcuni partecipanti[98] criticano la forma potestativa della disposizione rinviando alla Convenzione sulla cibercriminalità[99]. Propongono di prevedere nella legge un obbligo di comunicazione gratuito 24 ore su 24.

SZ, NW, SG e CAIS chiedono un «accesso online» per le autorità di perseguimento penale. A seconda del fornitore oggi bisogna attendere varie ore per sapere a chi appartiene un determinato numero telefonico, il che è inaccettabile in caso di ricerche urgenti e dopo la commissione di reati gravi. I fornitori si rifiutano di mettere a disposizione questi dati per via elettronica perché temono che possa utilizzarli la concorrenza. Questo problema è tuttavia tecnicamente di facile soluzione.

Alcuni partecipanti appartenenti al ramo dei servizi di telecomunicazione[100] osservano per contro che non si possono esigere sempre maggiori prestazioni da parte dei fornitori di servizi di telecomunicazione e propongono di stralciare l'ultimo periodo del capoverso 4.

Per Cablecom non è chiaro cosa s'intenda con la consultazione online menzionata al capoverso 4.

UNISG e UNIZH ritengono problematica la possibilità delle autorità di accedere a elenchi non pubblici.

switch e switchplus chiedono di limitare esplicitamente gli elenchi non pubblici menzionati a quelli riguardanti i collegamenti di telecomunicazione.

5.2. Articolo 21 Obblighi connessi all'esecuzione della sorveglianza

[1] I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge forniscono al Servizio, su sua richiesta, le comunicazioni della persona sorvegliata, i dati che permettono di individuare quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione. È fatto salvo l'articolo 16 lettera d. Forniscono parimenti le informazioni necessarie per attuare la sorveglianza.

[2] I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge trasmettono nel più breve tempo possibile i dati che permettono di individuare quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione, nonché, laddove possibile in tempo reale, le comunicazioni della persona sorvegliata. Eliminano le codificazioni da loro introdotte.

[3] I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge trasmettono al Servizio tutto il flusso di dati relativo alla persona sorvegliata. Tuttavia, su richiesta del Servizio, trasmettono soltanto il tipo o i tipi designati di dati del flusso in questione.

[4] I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge prestano al Servizio l'aiuto necessario per attuare qualsiasi misura di sorveglianza che richieda l'impiego di programmi informatici che permettono di intercettare e leggere i dati (art. 270 CPP e art. 70a^{bis} Procedura penale militare).

[5] Tutti i soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge e che partecipano alla fornitura del servizio di telecomunicazione da sorvegliare forniscono al soggetto incaricato della sorveglianza i dati di cui dispongono.

---

98 ZH, LU, GL, GR, TG, VS, JU, CCPCS, CCDGP.
99 FF **2010** 4119
100 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.

Numerosi partecipanti[101] ritengono che gli obblighi concreti siano disciplinati in modo troppo poco chiaro. Per creare maggiore certezza giuridica propongono pertanto di definire un chiaro elenco degli obblighi, presentando in parte proposte concrete di formulazione. Swissconm chiede inoltre d non obbligare i fornitori di servizi di telecomunicazione ad assolvere compiti di coordinamento per tutti i servizi offerti da terzi. I terzi devono essere obbligati direttamente dal Servizio.

5.2.1 Capoverso 1

La CCPCS chiede di estendere l'obbligo d'informazione al caso in cui la persona sorvegliata ha solo tentato di stabilire un collegamento.

Vari partecipanti appartenenti al ramo dei servizi di telecomunicazione[102] chiedono, con proposte concrete di formulazione, di precisare che l'obbligo di sorvegliare il traffico delle telecomunicazioni riguarda il traffico di un determinato collegamento messo a disposizione da un fornitore di servizi di telecomunicazione. Propongono inoltre la creazione di un articolo a sé stante sul rilevamento dei dati di collegamento. Per Cablecom non è chiaro cosa s'intenda con «informazioni necessarie».

5.2.2 Capoverso 2

Gli stessi partecipanti[103] chiedono di limitare anche nel capoverso 2 l'obbligo di sorveglianza a un determinato collegamento messo a disposizione da un determinato fornitore di servizi di telecomunicazione. Chiedono inoltre di chiarire che la leggibilità dei dati non può essere garantita.

Un numero notevole di partecipanti[104] chiede di cancellare le espressioni «nel più breve tempo possibile» e «laddove possibile in tempo reale», poiché sono imprecise e, visti i costi prevedibili per l'infrastruttura, inaccettabili. Anche la CCPCS ritiene imprecisa la formulazione «nel più breve tempo possibile», chiede tuttavia di inserire nella legge un rinvio alle direttive tecniche, in cui occorre definire il termine entro cui fornire i dati.

UNISG e UNIZH dubitano che sia tecnicamente possibile la prevista eliminazione della codificazione. IT(19), SWICO, hp e COG chiedono una disposizione secondo cui i fornitori di servizi di telecomunicazione devono informare, ancora prima dell'adozione di una misura di sorveglianza, il loro cliente «sorvegliato» del fatto che la codificazione utilizzata viene eliminata in vista di una misura di sorveglianza secondo la LSCPT e che egli sarà oggetto di una sorveglianza. Anche ISSS ritiene che in virtù del loro obbligo legale di fedeltà e di diligenza i fornitori di servizi di telecomunicazione debbano informare i loro clienti della possibilità di eliminare la codificazione. Chiede che l'eliminazione della codificazione da parte dei fornitori di servizi di telecomunicazione sia limitata a casi chiaramente definiti nella legge e che sia prevista una procedura in cui i fornitori di servizi di telecomunicazione possano far valere l'interesse dei loro clienti a una comunicazione protetta e chiedere la decisione di un giudice.

HR rileva il tenore impreciso della disposizione e chiede di chiarire che le codificazioni non sono di principio vietate. Una crittografia «end-2-end» è un'importante condizione in partico-

---

101 PPD, PLR, UDC, VERDI, SKS, economiesuisse, ICT, ePower, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SIUG, SPICT.
102 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
103 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
104 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom, IT(19), ISSS, PPS.

lare per il lavoro di ONG[105] quali il CICR o Amnesty International.

5.2.3 Capoverso 3

Undici partecipanti[106] ritengono che la selezione di determinati dati dal flusso di dati da fornire non sia tecnicamente possibile e pertanto vada stralciata (cfr. cap. III n. 3.3.6 ad art. 16 lett. f AP-LSCPT). UNIZH mette perlomeno in questione la fattibilità sotto il profilo tecnico. Alcuni partecipanti[107] chiedono che la selezione dei dati debba competere al Servizio.

privatim ritiene la formulazione troppo aperta e propone la seguente limitazione: «… tutto il flusso dei dati *nell'ambito dell'ordine di sorveglianza* …". In caso contrario non sono rispettati il principio di determinatezza, nonché il principio del vincolo allo scopo e della proporzionalità.

CP osserva che la selezione dei dati comporta anche la consultazione di dati personali sensibili e il rischio di perdere dei dati. La disposizione dovrebbe quindi essere rielaborata. Secondo SIMSA il termine «flusso di dati» non è appropriato per limitare la portata della sorveglianza e viola quindi il principio del trattamento confidenziale dei dati personali. Dovrebbero essere di rilievo per la sorveglianza soltanto i dati della comunicazione individuale della persona sorvegliata. IT(19), SWICO, hp e COG paragonano la sorveglianza dell'intero flusso di dati a una perquisizione domiciliare. Secondo loro una siffatta misura di sorveglianza può essere eseguita soltanto previa approvazione del giudice, che va prima presentata ai fornitori di servizi di telecomunicazione e all'ISP. Inoltre chiedono di rimborsare il lavoro della selezione dei dati.

ISSS avverte che lo sviluppo di sistemi di filtraggio e selezione può purtroppo anche avere la conseguenza di facilitare l'individuazione di raccolte e di flussi di dati da parte di terzi non autorizzati, intaccando così il livello della sicurezza informatica nel nostro Paese. ISSS propone pertanto che l'impiego di programmi di analisi e filtraggio sia imposto soltanto in singoli casi specifici su ordine di un giudice.

5.2.4 Capoverso 4

Le osservazioni di carattere generale in merito al previsto impiego di programmi informatici si trovano al capitolo III numero 11.1.2 ad articolo 270bis CPP. Qui di seguito sono riassunte le osservazioni che riguardano in senso lato l'obbligo di sostegno previsto dal capoverso 4.

Vari partecipanti[108] ritengono poco chiaro chi sia concretamente responsabile per lo sviluppo, l'acquisto e l'impiego dei programmi. Di conseguenza privatim, SIMSA e ISSS chiedono di precisare l'espressione «l'aiuto necessario».

Secondo altri partecipanti[109] l'impiego di tali programmi non può essere delegato a imprese private, bensì deve essere compito dell'autorità competente. Nel sistema giuridico svizzero non è auspicabile il coinvolgimento obbligatorio di privati in operazioni di polizia. Secondo il PPS ciò dovrebbe valere anche per la produzione e manutenzione del sistema d'infiltrazione.

Alcuni partecipanti[110] ritengono in generale che non si possa pretendere l'introduzione, su i-

---

105 Organizzazioni non governative.
106 UDC, VERDI, SKS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
107 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.
108 ZH, BL, ZG LU, PS, privatim, ISSS.
109 UDC, PPD, PLR, PPS, economiesuisse, Swisscable.
110 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG.

struzione del Servizio, di «Government Software» (spesso chiamati «cavalli di troia federali») nei sistemi dei clienti. Un siffatto coinvolgimento vincolante di privati in operazioni di polizia è unico nel suo genere e intacca il rapporto di fiducia tra i fornitori e la loro clientela, poiché l'impiego di tali programmi è totalmente contrario agli interessi dei clienti. I partecipanti in questione rifiutano i pertinenti obblighi di esecuzione e partecipazione e, insieme a IT(19) e Cablecom, chiedono di stralciare la disposizione.

RD osserva che questi programmi sono di per sé problematici e discutibili. A suo parere non è proponibile e neppure necessario costringere i fornitori ad aiutare in qualsiasi forma ipotizzabile le autorità a introdursi nei sistemi dei clienti e di terzi senza che la legge preveda direttive chiare. Ciò intacca la fiducia in un intero settore industriale e crea rischi di sicurezza che in ultimo danneggiano l'economia intera.

switch rileva che in quanto gestore di reti informatiche mette in atto ampie misure per combattere programmi dannosi o di spionaggio. In caso di sorveglianza non può distinguere tra software dannosi indesiderati e programmi di spionaggio. La cooperazione con il Servizio è quindi indispensabile. Inoltre, se è eseguita una misura di sorveglianza mediante programmi informatici, occorre bloccare tutte le misure tese a evitare software dannosi. Alla luce di queste considerazioni, switch chiede di precisare la disposizione in modo da evitare il conflitto menzionato.

5.2.5 Capoverso 5

VD chiede di chiarire la disposizione. Altri partecipanti chiedono di stralciarla[111].

5.3. Articolo 22 Identificazione degli utenti Internet

I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge adottano le misure tecniche necessarie per identificare gli utenti che accedono a Internet per loro tramite.

Un numero ragguardevole di partecipanti[112] accoglie esplicitamente con favore la disposizione. Secondo ZH l'identificazione degli utenti Internet è in grado di fornire indicazioni importanti o decisive per il perseguimento penale. D'altro canto la possibilità di identificare gli utenti può produrre anche un effetto preventivo. SZ e CAIS rimandano ai Paesi confinanti, in cui non è più possibile avere accesso a Internet senza identificarsi. Il conseguente onere amministrativo dei fornitori di accessi temporanei a Internet (alberghi, Internet caffé ecc.) è ritenuto sostenibile.

Numerosi rappresentanti[113] chiedono invece di stralciare o adeguare la disposizione. Per VD, ISSS e Verdi l'obbligo previsto dall'articolo 22 è sproporzionato, soprattutto per quando riguarda gli accessi senza cavo mediante «Wi-Fi» (stazioni ferroviarie, scuole, alberghi, ecc.). Ne potrebbe conseguire che molti collegamenti attualmente messi a disposizione del pubblico vengano eliminati. Chiedono di stralciare questo obbligo unico nel suo genere in Europa o di modificarlo notevolmente. L'UDC fa notare l'onere sproporzionato e chiede anch'essa di stralciare la disposizione. Anche UCS e privatim respingono la disposizione, osservando tra l'altro che è facile eluderla («proxie»; occultamento dell'indirizzo IP, annuncio con carta SIM di seconda mano) e che si tratta di un'ingerenza sproporzionata nella libertà personale di tutti

[111] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon.
[112] ZH, LU, SZ, NW, SO, GL, GR, TG, VS, JU, CCDGP, CCPCS, CAIS.
[113] VD, VERDI, UDC, PLR, ISSS, UCS, privatim, GDS, gr.ch, RD, IT(19), Cablecom, switch und switchplus, CP, FSA, KFG, PPS, ETH, UNISG, UNIZH.

gli utenti di Internet. Per GDS e gr.ch la disposizione è assurda e mette in risalto la tendenza totalitaria di tutto il progetto. È come se chi intende telefonare da una cabina telefonica pubblica dovesse prima dimostrare la sua identità. Secondo la disposizione, una persona che metta a disposizione di un conoscente il proprio computer o smartphone per navigare in rete, dovrebbe prima permettere al proprio provider di identificare il conoscente. Inoltre, la disposizione significa che i provider devono vietare ai propri utenti di gestire reti non protette da una parola chiave. La proposta registrazione per mezzo del numero del cellulare esclude inoltre alcune persone ed è facile da eludere. Anche RD ritiene la disposizione insensata e adduce l'assenza dell'obbligo d'identificazione nell'ambito della telefonia. Secondo parecchi partecipanti[114] un fornitore di servizi di telecomunicazione può riconoscere i clienti abbonati, ossia i suoi partner contrattuali, ma non ogni singolo utente che accede a Internet mediante il collegamento di un abbonato. La disposizione andrebbe stralciata oppure, secondo IT(19), occorrerebbe chiarire e delimitare l'onere necessario per l'identificazione, che va rimborsato. Anche Cablecom, switch e switchplus si esprimono a favore dello stralcio o della modifica della disposizione e osservano che è ipotizzabile al massimo l'identificazione dell'apparecchio utilizzato. Anche tale identificazione è tuttavia possibile soltanto se tutti gli apparecchi intermedi («router», «wireless AP», ecc.) si trovano nella sfera di responsabilità e sotto il controllo tecnico dell'avente obbligo. L'identificazione per mezzo del numero di cellulare non è praticabile: se l'utente usa un cellulare estero, i dati d'utente devono essere ordinati presso il fornitore estero, che in tal caso non è tuttavia soggetto al diritto svizzero. PLR, CP e FSA dubitano che siano state sufficientemente ponderate l'applicabilità e le conseguenze della disposizione. KFG e PPS chiedono di limitare l'obbligo d'identificazione o di stralciare la disposizione. Secondo ETH, UNISG e UNIZH il Legislatore sembra partire dal presupposto che le scuole, gli alberghi, ecc. accedano a Internet per il tramite di un access-provider tradizionale. Le università assegnano indirizzi IP propri, ma non offrono i propri servizi al pubblico. Si tratta quindi di access-provider, ma non fornitori di accesso a Internet ai sensi dell'articolo 2 lettera a OSCPT e pertanto a loro non si applica l'articolo 22 LSCPT. Secondo le suddette università l'articolo 22 rende possibile una sorveglianza totale e occorre pertanto riesaminarlo attentamente e precisarlo nell'ottica del principio della proporzionalità.

5.4. Articolo 23 Conservazione dei dati

I soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge conservano per dodici mesi i dati che permettono di individuare quando e con quali collegamenti di telecomunicazione la persona sorvegliata è stata o è in contatto e i dati relativi alle comunicazioni e alla fatturazione.

Numerosi partecipanti[115] accolgono in linea di massima con favore la durata più lunga di conservazione. FR ritiene tuttavia necessario stimare dapprima i compiti supplementari che i Cantoni devono assolvere in seguito al prolungamento. SO fa notare la necessità di un termine più lungo in particolare in occasione di lunghe procedure di assistenza giudiziaria. BS chiede inoltre di disciplinare il trattamento di reperti casuali. AR, SZ e VD propongono di completare la disposizione con regole in merito alla sicurezza dei dati, alla protezione dall'uso abusivo e alla trasparenza della trasmissione dei dati.

Un gruppo ragguardevole di partecipanti[116] propone di prolungare a dieci anni il termine di conservazione, di modo che elementi d'indagine decisivi siano a disposizione anche parec-

---

[114] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG, IT(19).
[115] OW, ZH, LU, SZ, NW, BL, GL, GR, TG, VS, JU, FR, SO, BS, AR, AG, TI, VD, GE, PPD, PLR CCDGP CCPCS, FSFP, CAIS, SPICT.
[116] ZH, LU, SZ, NW, BL, GL, GR, TG, VS, JU, PLR, CCDGP, CAIS.

chi anni dopo. Si osserva che i fornitori di servizi di telecomunicazione conservano i dati di propria iniziativa per dieci anni. Nove partecipanti[117] propongono di limitare il termine *per consultare* i dati a sei o dodici mesi, indipendentemente dalla durata di conservazione di dieci anni. Anche BE chiede di estendere la durata di conservazione dei dati secondari a oltre dodici mesi.

Un notevole numero di partecipanti[118] rifiuta la disposizione. GDS, gr.ch, Verdi e SKS fanno notare che essa permette di registrare preventivamente e in modo sistematico dati di persone non sospette. Verdi e SKS la ritengono tanto più incomprensibile in quanto a fine giugno 2010 la Delegazione delle Commissioni della gestione ha espresso i propri dubbi in merito alla correttezza e all'importanza dei dati contenuti nella banca dati ISIS. Vari partecipanti[119] fanno inoltre notare i costi maggiori connessi al prolungamento della durata di conservazione e la prevista abolizione di qualsiasi tipo d'indennità.

Secondo SIUG la disposizione non menziona in alcun modo la determinazione della posizione dell'antenna di telefonia mobile, attualmente prevista dall'OSCPT. Se tale determinazione sarà prevista anche in futuro, propone di sancirla nella legge. La sorveglianza retroattiva, completa e indipendente da un sospetto riguarda tutti gli abitanti della Svizzera e pertanto non è appropriata. La registrazione dei dati secondari per dodici mesi consente di allestire una mappa dettagliata delle comunicazioni e dei movimenti di tutti gli abitanti della Svizzera. Inoltre, non è dimostrata la necessità di raddoppiare la durata di conservazione. L'avamprogetto non definisce in modo sufficiente i tipi di sorveglianza, i dati da registrare e i termini usati. Anche ISSS respinge la disposizione, proponendo tuttavia di adattare eventualmente la legge in modo tale che il Servizio possa, nel singolo caso, esortare il fornitore a conservare più a lungo, ossia fino a 12 mesi, i dati relativi alla comunicazione.

BL, PS, 3D4X e privatim chiedono una disposizione riveduta che corrisponda ai criteri sviluppati dalla Corte costituzionale tedesca nel contesto della sua decisione in merito alla conservazione di dati[120]. 3D4X si chiede come una piccola impresa IT possa essere in grado di pagare gli strumenti di sorveglianza se non riceve alcuna indennità. Anche IT(19) fanno notare l'aumento dei costi in seguito al prolungamento della durata di conservazione.

Cablecom si chiede come i provider possano mettere al sicuro i dati se non ne hanno, visto

---

[117] NW, GL, GR, TG, VS, JU, PLR, CAIS, CCDGP.

[118] BL, VERDI, PS, SKS, USS, GDS, gr.ch, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SIUG, ISSS, SWICO, hp, privatim, COG, 3D4X, PPS.

[119] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SWICO, hp, COG, PPS.

[120] BVerfG, 1 BvR 256/08 del 2.3.2010, capoverso n. (1 - 345); dal regesto: una conservazione preventiva di sei mesi senza un motivo specifico di dati del traffico delle telecomunicazioni da parte di fornitori privati, come quella prevista dalla direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 (GU L 105 del 13 aprile 2006, pag. 54; qui appresso: Direttiva 2006/24/CE) non è del tutto incompatibile con l'articolo 10 del Grundgesetz (GG). Il principio della proporzionalità esige che la base legale di una siffatta conservazione di dati tenga debitamente conto dell'importanza specifica dell'ingerenza nei diritti fondamentali connessa alla conservazione. Secondo i principi della sentenza è necessario un disciplinamento chiaro ed esigente in merito alla sicurezza dei dati, alla loro utilizzazione, alla trasparenza e alla protezione giuridica. […] La consultazione e l'utilizzazione diretta dei dati sono proporzionali soltanto se servono a eseguire compiti della massima importanza nell'ambito della protezione di beni giuridici. Nel settore del perseguimento penale ciò presuppone un sospetto di reato grave, fondato su fatti concreti […]. L'uso indiretto dei dati per il rilascio di informazioni da parte dei fornitori di servizi di telecomunicazione sugli utenti di indirizzi IP è ammesso per il perseguimento penale, la prevenzione di pericoli e l'esecuzione di compiti di intelligence, indipendentemente da cataloghi restrittivi di reati o beni giuridici. Per il perseguimento di infrazioni disciplinari tali informazioni sono ammesse soltanto nei casi esplicitamente menzionati dalla legge […] (trad.).

che gli apparecchi non rientrano nella loro sfera d'influenza.

All'UCS non è chiaro quali dati debbano rilevare e conservare i fornitori di collegamenti «Wi-Fi» pubblici.

Rimandando al tenore della disposizione, ETH, UNISG e UNIZH constatano che non sussiste un obbligo di conservazione per i gestori di reti di comunicazione e centralini interni.

FSA deplora l'assenza di un motivo per il prolungamento della durata di conservazione.

switch e switchplus chiedono di precisare il tenore dell'articolo 23 AP-LSCPT, affinché sia chiaro che anche i soggetti di cui all'articolo 2 capoverso 2 AP-LSCPT devono conservare i dati della comunicazione.

safe propone che sia inclusa nella disposizione anche la ricerca di una persona *sconosciuta* all'origine di un determinato processo di comunicazione di dati in Internet. Secondo safe il tenore dell'articolo è troppo restrittivo, poiché non contempla il caso fondamentale in cui non si tentano di individuare i collegamenti di una persona nota o sorvegliata, ma si cerca una persona sconosciuta all'origine di un determinato traffico di dati in Internet.

5.5. Articolo 24 Certificazione

Le osservazioni sulla certificazione si trovano al capitolo III numero 3.5 ad articolo 18 AP-LSCPT.

5.6. Articolo 25 Informazioni relative alle tecnologie e ai servizi

Su richiesta, i soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù della presente legge informano in qualsiasi momento e in modo dettagliato il Servizio sulla natura e le caratteristiche delle tecnologie e dei servizi che hanno immesso o intendono immettere sul mercato.

Per nove partecipanti[121] l'informazione sui servizi e le tecnologie future rientra nel segreto d'affari e pertanto rifiutano un pertinente disciplinamento nella legge. In ogni caso informazioni così specifiche dovrebbero essere indennizzate. ISSS fa notare che, oltre a intaccare il segreto d'affari e quello aziendale, la disposizione si riferisce a tecnologie che sono in gran parte in possesso di imprese straniere. La disposizione potrebbe quindi creare notevoli problemi alla piazza economica svizzera e provocare misure di ritorsione o indurre i proprietari delle tecnologie a non impiegare più in Svizzera i propri sistemi e processi più nuovi, a causa del pericolo di essere svelati. In tal modo si rende un cattivo servizio alla società dell'informazione in Svizzera. ISSS chiede pertanto di prendere in considerazione un accordo internazionale.

SIMSA rende inoltre attenta al pericolo per la protezione delle innovazioni. IT(19), SWICO, hp e COG chiedono di completare la disposizione con un'aggiunta secondo cui i fornitori non devono rendere noti i segreti d'affari o professionali.

switch e switchplus chiedono di chiarire se l'obbligo d'informazione riguardi anche i soggetti di cui all'articolo 2 capoverso 2 AP-LSCPT. Inoltre, ritengono un tale obbligo un'attività formativa a favore di impiegati federali, che va pertanto indennizzata.

---

[121] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, ISSS, Cablecom.

5.7. Articolo 26 Gestori di reti di telecomunicazione interne e di centralini privati e soggetti di cui all'articolo 2 capoverso 1 che non esercitano la loro attività nell'ambito del traffico delle telecomunicazioni a titolo professionale

Osservazioni sull'obbligo di sorveglianza dei soggetti menzionati nel titolo dell'articolo si trovano al capitolo III numero 1.2.3 ad articolo 2 capoverso 2 AP-LSCPT

6. Sorveglianza al di fuori di un procedimento penale

6.1. Articolo 27 Ricerca in casi urgenti

[1] Al di fuori di un procedimento penale, l'autorità competente può ordinare la sorveglianza del traffico delle telecomunicazioni limitata all'identificazione degli utenti, ai dati relativi alle comunicazioni e alla localizzazione per ritrovare una persona dispersa. Se necessario, può consultare i dati relativi a terzi non implicati.

[2] Una persona è considerata dispersa quando:

a. la polizia constata che è impossibile rintracciarla; e

b. seri indizi lasciano supporre che la sua salute o la sua vita siano in grave pericolo.

6.1.1 Capoverso 1

Un gruppo notevole di partecipanti[122] chiede di completare la disposizione in modo tale che in certi casi, oltre ai dati relativi al collegamento, si possa rilevare anche il contenuto dei colloqui, per verificare che sia stata effettivamente la persona smarrita a usare l'apparecchio sorvegliato. La prevista procedura d'autorizzazione permette in ogni caso di tenere debitamente conto dell'esigenza di protezione dell'interessato. VD ritiene necessaria una procedura più semplice, affinché si possa procedere alla sorveglianza ancora prima dell'autorizzazione da parte del giudice.

Vari partecipanti appartenenti al ramo dei servizi di telecomunicazione[123] chiedono di limitare la sorveglianza alla localizzazione e sono contrari alla possibilità di consultare dati relativi a terzi non implicati. Inoltre, Cablecom ritiene che la disposizione riguardi soltanto la telefonia mobile, poiché in caso di servizi Internet la localizzazione non è attualmente possibile.

FSA non comprende perché sia stato stralciato l'attuale articolo 8 capoverso 5 LSCPT e chiede pertanto di reintegrarlo.

Secondo SIMSA i fornitori di servizi di telecomunicazione non sono in grado di prevedere le conseguenze di questa norma, soprattutto in riferimento ai «dati relativi a terzi non implicati». Anche SZ chiede di precisare quali dati di terzi non implicati possano essere consultati. In tale contesto KFG teme che venga sorvegliato un maggior numero di terzi non implicati soltanto perché si muovono nell'ambiente della persona sorvegliata. Chiede pertanto di stralciare la disposizione.

6.1.2 Capoverso 2

Nessuna osservazione.

---

[122] ZH, LU, SZ, SH, SG, AG, GL, GR, TG, VS, JU, CCDGP, CCPCS, CAIS, SSDP.

[123] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

6.2. Articolo 28 Ricerca di persone condannate

Al di fuori di un procedimento penale, l'autorità competente può ordinare la sorveglianza della corrispondenza postale o del traffico delle telecomunicazioni per ritrovare una persona condannata a una pena detentiva o soggetta a una misura privativa della libertà in base a una sentenza passata in giudicato, se le misure già adottate a tal fine non hanno avuto esito positivo o se altrimenti le indagini risulterebbero vane o eccessivamente difficili.

Molti partecipanti[124] accolgono con favore la nuova possibilità di sorveglianza nell'ambito della ricerca di persone condannate. OW e SO approvano inoltre il fatto che la sorveglianza non sia limitata ai dati secondari e sia possibile registrare anche i colloqui che forniscono indizi sul luogo di permanenza del ricercato.

Per motivi di sicurezza pubblica (pericolo per sé stessi e per terzi), ZG chiede se non vada menzionata anche la privazione della libertà a scopo d'assistenza (art. 397a segg. CC).

privatim ritiene la disposizione una clausola troppo generale dal punto di vista della protezione dei dati. Non è chiaro chi debba essere sorvegliato come, dove e quando, nonostante si tratti di una grave ingerenza nei diritti fondamentali, soprattutto per persone che si muovono nell'ambiente dei condannati. Si propone pertanto di disciplinare i particolari di questa possibilità di sorveglianza nel CPP o nell'OSCPT. USS ritiene un'ingerenza sproporzionata nella sfera privata il fatto che sia in futuro possibile sorvegliare anche le persone che sono state presumibilmente in contatto con la persona condannata.

Otto partecipanti[125] chiedono di precisare la disposizione indicando che la persona condannata deve essere *fuggitiva*. Cablecom chiede inoltre di precisare le espressioni «vane» e «eccessivamente difficili».

FSA osserva che chi si sottrae all'esecuzione di una pena detentiva o di una misura privativa della libertà non commette ancora un reato. Per tali ingerenze nei diritti fondamentali è quindi importante rispettare il principio della proporzionalità, tenendo conto della gravità del reato o della pena inflitta. Nel primo caso ci si può riferire al catalogo di reati dell'articolo 269 capoverso 2 CPP. Se si sceglie come parametro la pena inflitta, occorre fissare un limite a partire dal quale è ammessa la sorveglianza (p.es. un anno). VD e CP chiedono di limitare la sorveglianza a reati per cui sono state pronunciate pene detentive di almeno sei mesi.

SIMSA osserva che prima di una misura di sorveglianza nessuno può prevedere quali colloqui contengano indizi e quali no. Da ciò consegue che o non si procede alla sorveglianza oppure la disposizione conduce a una sorveglianza generale dei colloqui. SIMSA rileva inoltre che la nuova possibilità di ricerca di persone condannate comporta oneri supplementari notevoli per gli aventi obbligo di sorveglianza.

AG propone di sostituire il termine «Untersuchungshandlungen (indagini)» con «Fahndungsmassnahmen (misure di ricerca)», poiché dopo la condanna passata in giudicato non vengono più effettuate indagini.

6.3. Articolo 29 Procedura

[1] La procedura è retta per analogia dagli articoli 271-279 CPP. La sorveglianza deve essere autorizzata da un'au-

[124] ZH, LU, SZ, VD, GE, UR, OW, NW, FR, SO, AR, TI, CCDGP, CCPCS, CAIS, FSFP, SSDP.
[125] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom.

torità giudiziaria.
[2] I Cantoni designano l'autorità che ordina la sorveglianza, l'autorità d'approvazione e l'autorità di ricorso.

6.3.1 Capoverso 1

SZ ritiene immotivato e non condivisibile il rinvio all'applicazione per analogia degli articoli 271-279 CPP, anziché, come finora, agli articoli 274-279 CPP. Occorre chiarire nella legge che mediante l'applicazione per analogia della CPP la procedura della ricerca in casi urgenti e di quella di persone condannate non sono trasformate in un procedimento penale, bensì che rimangono procedimenti amministrativi o di polizia. In riferimento a una ricerca in casi urgenti, una cernita giudiziaria di dati specifici per proteggere un segreto professionale non entra in linea di conto. Le informazioni ottenute in occasione di una ricerca in casi urgenti da una sorveglianza limitata all'identificazione dell'utente e ai dati relativi al traffico delle telecomunicazioni, possono essere utilizzate soltanto per salvare la persona smarrita e vanno distrutti non appena è venuto a cadere il motivo della sorveglianza. L'obbligo di autorizzazione è inoltre retto dall'articolo 29 capoverso 1 secondo periodo AP-LSCPT. Il rinvio per analogia all'obbligo d'approvazione dell'articolo 272 CPP è superfluo e crea confusione. Anche nel caso dell'articolo 273 CPP si tratta di ordini nell'ambito di un procedimento penale aperto. Anche il rinvio all'applicazione per analogia dell'obbligo di comunicazione dell'articolo 279 CPP in riferimento alla conclusione di una ricerca urgente ha ripetutamente dato adito a discussioni e non è adatta allo scopo. L'obbligo di comunicazione risulta dal diritto cantonale in materia di protezione dei dati e di polizia e non dal CPP. Non vi è alcuna necessità di disciplinare il differimento della comunicazione autorizzato dal giudice dei provvedimenti coercitivi, poiché ciò porta a confondere il procedimento penale e quello amministrativo. La comunicazione, da parte della polizia, alla persona ritrovata o ai suoi congiunti della ricerca urgente effettuata, eventualmente connessa all'assunzione delle spese, continua a essere una decisione amministrativa soggetta alla giurisdizione amministrativa e non al reclamo di cui agli articoli 393-397 CPP.

UCS ritiene contrario al sistema il rinvio globale al CPP, poiché la ricerca in casi urgenti non è uno strumento del diritto processuale penale bensì della politica di sicurezza. Inoltre UCS ritiene in generale problematico l'obbligo d'approvazione da parte del giudice, poiché vi è regolarmente «pericolo nel ritardo». La polizia dovrebbe avere la competenza di ordinare autonomamente la ricerca in casi urgenti, poiché è necessario agire senza indugio. La rinuncia all'approvazione da parte del giudice può essere successivamente compensata con rimedi giuridici. Nell'interesse di una ripartizione il più possibilmente chiara delle competenze, la valutazione giudiziaria dovrebbe inoltre essere effettuata dal giudice (dell'arresto).

6.3.2 Capoverso 2

Nessuna osservazione.

7. Spese ed emolumenti

ICT ed ePower chiedono in generale di ridurre le spese per le misure di sorveglianza e di adattare l'ordinanza sulle tasse. Ciò presuppone che nelle direttive tecniche del Servizio sia riprodotto un «processo End to End» digitalizzato. Certezza del diritto significa che tutti i partecipanti di un sistema sappiano che cosa si esige da loro. ICT ed ePower chiedono che questo punto sia disciplinato prima del dibattito parlamentare.

7.1. Articolo 30

[1] Le spese delle installazioni necessarie per attuare la sorveglianza e le spese di sorveglianza sono a carico dei soggetti che effettuano la sorveglianza in virtù della presente legge.

[2] L'autorità che ha ordinato la sorveglianza corrisponde un emolumento al Servizio. Il Consiglio federale determina gli emolumenti per le prestazioni del Servizio.

7.1.1 Capoverso 1

Numerosi partecipanti[126] approvano l'abolizione dell'indennità per i fornitori, rinviando soprattutto all'obbligo di pubblicazione di banche, fiduciari, assicurazioni ecc., senza che sia loro corrisposta un'indennità. Ritengono che il versamento di un'indennità sia contrario al sistema. ZH osserva inoltre che le banche devono assumersi costi notevoli anche per impedire il riciclaggio di denaro. NW, SO, CAIS e SSDP rilevano infine che in passato i fornitori di una certa dimensione e ben organizzati hanno realizzato guadagni notevoli grazie alla sorveglianza.

Per diversi motivi illustrati qui appresso, un notevole numero di partecipanti[127] è invece fondamentalmente contrario all'abolizione dell'indennità per l'esecuzione di misure di sorveglianza.

La maggioranza di questi partecipanti[128] osserva che il perseguimento penale è un compito statale i cui costi vanno assunti dalla comunità. Secondo alcuni partecipanti[129] non convince soprattutto l'argomento secondo cui, in considerazione dell'obbligo di pubblicazione di banche, fiduciari, assicurazioni, ecc., il versamento di un'indennità sarebbe contraria al sistema. Il PS osserva che ciò che si chiede ai provider va ben oltre la pubblicazione di dati o atti già disponibili. GDS e gr.ch ritengono fuorviante il confronto con il menzionato obbligo di pubblicazione, per il solo fatto che non dovrebbero essere postulati obblighi di conservazione e altri obblighi di collaborazione nell'ambito della LSCPT, se fossero a disposizione richieste di pubblicazione in virtù del CPP. Secondo ISSS e MS la disposizione è contraria ai principi riconosciuti della partecipazione di privati a un procedimento penale contro terzi, quali ad esempio l'indennizzo di testimoni e periti. MS rinvia inoltre all'articolo 434 CPP, che prevede esplicitamente che i terzi danneggiati nel prestare assistenza alle autorità penali hanno diritto a un adeguato risarcimento del danno non coperto in altro modo. Secondo gli articoli 422 segg. CPP tali spese fanno infatti parte delle spese procedurali, che alla fine sono a carico del condannato.

Per un gran numero di partecipanti[130] il versamento di un'indennità per i fornitori di servizi di telecomunicazione ha anche un effetto disciplinante o di limitazione dei costi, poiché l'obbligo di versare un'indennità evita una sovrabbondanza di ordini di sorveglianza.

---

126 ZH, LU, UR, OW, NW, SO, BL, SG, AG, NE, VD, GL, GR, TG, VS, JU, CCDGP, CCPCS, CAIS, SSDP.

127 PS, PPD, PLR, UDC, Verdi, PPS, GDS, gr.ch, RD, ISSS, MS, SIUG, SIMSA, INT, asut, Finecom, Orange, Swisscom, Sunrise, Colt, Verizon, Cablecom, FSA, SKS, Swisscable, CP, CCC, Sitrox, economiesuisse, IT(19), SWICO, hp, COG.

128 PPD, PLR UDC, Verdi, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, FSA, SKS Swisscable, SIUG, CP, CCC, Sitrox, PPS.

129 PS, GDS, gr.ch, Colt, Cablecom, RD.

130 UDC, Verdi, asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, FSA, SKS, Swisscable, SIUG, CP, CCC, Sitrox, PPS, economiesuisse.

Alcuni partecipanti[131] osservano che per soddisfare le esigenze della legge ed essere in grado di adottare per tempo le misure tecniche in caso di incarico da parte del Servizio, sono necessarie un'infrastruttura costosa e notevoli conoscenze specifiche. Per le imprese di piccole dimensioni costituiscono già un problema grave o, secondo i Verdi, sono insostenibili le spese d'investimento necessarie per la sorveglianza, poiché è presumibile che tali spese aumenterebbero notevolmente. Colt ritiene inoltre che venga violato il principio di proporzionalità nel caso in cui si debba acquistare un'apparecchiatura costosa poi raramente o mai utilizzata. Nel caso in cui gli investimenti andassero lo stesso a carico dei fornitori di servizi di telecomunicazione, secondo Colt questi ultimi non dovrebbero essere costretti ad acquistare l'apparecchiatura necessaria prima che debba essere messa in atto una sorveglianza. Inoltre, in caso di sorveglianza ripetuta, i fornitori di servizi di telecomunicazione dovrebbero essere liberi di decidere se ricorrere a un'apparecchiatura esterna, assumendone eventualmente i costi. Il PS osserva che le condizioni richieste distorcono il mercato a favore dei grossi fornitori, che già ora godono di una posizione quasi monopolistica. Chiede pertanto una soluzione differenziata per il rimborso dei fornitori, che tenga conto della sostenibilità economica della misura a dipendenza delle dimensioni del fornitore.

Un numero cospicuo di partecipanti[132] propone pertanto una formulazione secondo cui l'autorità che ha ordinato la sorveglianza corrisponde al Servizio un emolumento che contiene l'indennità a favore dei fornitori.

Proponendo una pertinente formulazione, economiesuisse chiede che le spese d'investimento siano assunte dai fornitori di servizi di telecomunicazione, ma che l'utilizzazione possa essere fatturata. Il PPD chiede che siano rimborsate le spese dei provider per l'upgrade dei loro sistemi, necessario per poter eseguire la sorveglianza ordinata.

ZG teme che in caso di abolizione dell'indennità per i fornitori, la Confederazione debba in qualche modo garantire che i fornitori continuino a mettere a disposizione i dati in modo rapido e affidabile.

7.1.2 Capoverso 2

ZH, LU e ZG osservano che anche se formalmente i costi possono essere addebitati come spese ai condannati o alle persone obbligate a pagarli, in molti casi essi non possono essere addossati alle parti (ricerca in casi urgenti, ricerca di persone condannate, assoluzioni, procedure di assistenza giudiziaria) o non sono rimborsati perché le persone obbligate ad assumerli non sono in grado di pagarli, e quindi i costi vanno a carico dell'autorità che ha ordinato la sorveglianza. Vari partecipanti[133] chiedono di fissare in modo adeguato o abbassare le tariffe dell'ordinanza del 7 aprile 2004[134] sulle tasse e indennità nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. SZ osserva che in tale contesto il Servizio non dovrebbe assumere funzioni inutili come ad esempio il controllo della durata di conservazione e il rilascio di informazioni in merito a collegamenti di telecomunicazione. LU e ZG chiedono di potersi esprimere a tempo debito in merito all'ordinanza sulle tasse. FR chiede di esaminare, in base a una valutazione ancora da effettuare, la questione degli emolumenti che i Cantoni devono corrispondere al Servizio. VD ritiene che il mantenimento degli emolumenti per il Servizio conduca a un'eccedenza dei costi. NE chiede

---

131 PS, Colt, SIUG, SIMSA, INT, ISSS, PPS, Verdi.
132 asut, Finecom, Orange, Swisscom, Sunrise, Verizon, Cablecom, Swisscable, IT(19), SWICO, hp, COG.
133 ZH, LU, ZG, BL, AG, TI, GL, GR, TG, VS, JU, SZ, OW, CCDGP, CCPCS
134 RS **780.115.1**

di verificare se non si possano abolire del tutto gli emolumenti a carico dell'autorità che ordina la sorveglianza. Secondo il PS occorre garantire che per le autorità di perseguimento penale gli emolumenti non siano troppo elevati, affinché indagini importanti non siano ostacolate a causa dei costi troppo alti.

8. Disposizioni penali

8.1. Articolo 31 Contravvenzioni

[1] È punito con una multa fino a 100 000 franchi chi intenzionalmente non osserva:

a. gli ordini del Servizio;

b. l'obbligo di conservare i dati di cui agli articoli 19 capoverso 2 e 23.

[2] Sono punibili il tentativo e la complicità.

[3] Se l'autore agisce per negligenza, è punito con una multa fino a 40 000 franchi.

[4] Gli articoli 102 capoversi 1, 3 e 4 CP e 112 CPP sono applicabili per analogia. La multa ammonta al massimo a un milione di franchi.

SO e CP sono in linea di massima d'accordo con la disposizione penale. Per CP, tuttavia, ciò presuppone che la legge preveda un'indennità e una certificazione gratuita a favore degli aventi obbligo.

Verdi e SKS ritengono la disposizione penale decisamente troppo severa, in particolare perché chi esegue la sorveglianza non dispone praticamente di nessun mezzo per opporvisi. Di conseguenza, e a causa della tendenza ad eseguire sempre più sorveglianze, la disposizione penale fa sì che i fornitori di servizi di telecomunicazione siano soggetti arbitrariamente agli ordini di sorveglianza. Inoltre, la pena commisurata mette in questione la sopravvivenza dei provider di piccole dimensioni. Chiedono pertanto una disposizione penale notevolmente meno severa.

In tale contesto diversi partecipanti[135] rinviano al disciplinamento poco chiaro degli obblighi. Alla luce di questa situazione, il PLR ritiene perlomeno delicata la disposizione penale. Secondo SIMSA mancano elementi univoci delle figure di reato, che permettano una sanzione penale. Alcuni partecipanti[136] ritengono pertanto che oltre a violare l'obbligo di determinatezza, la disposizione costituisca una pretesa inaccettabile poiché in base all'articolo 15 lettera a AP-LSCPT il Servizio deve emanare istruzioni e decisioni anche se le ritiene errate.

Orange e Colt ritengono inadeguato che siano soggette alla disposizione anche le persone fisiche. Chiedono pertanto che la cerchia dei destinatari della LSCPT e quindi anche delle sue disposizioni penali sia circoscritta alle persone giuridiche.

8.1.1 Capoverso 1

Vari partecipanti[137] chiedono di inasprire la disposizione. OW dubita che la disposizione sia efficace. Per NW e CAIS, la valutazione del reato come infrazione è inappropriata e inefficace in considerazione del rapporto tra i profitti realizzati nel traffico delle telecomunicazione e le spese della sorveglianza, poiché in certi casi la multa prevista per la violazione dell'obbligo (CHF 100 000.-) è più che compensata dal risparmio delle spese. Alcuni partecipanti[138] chie-

[135] PLR, SIMSA, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
[136] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
[137] ZH, LU, AG, GL, GR, TG, VS, JU, NW, CCDGP, CAIS.
[138] ZH, AG, LU, GL, GR, TG, VS, JU, CCDGP.

dono pertanto di aumentare l'importo di CHF 100 000. Una maggioranza[139] propone un aumento a 1 milione di franchi.

Lettera a

Rinviando all'obbligo di determinatezza dell'articolo 1 CP, otto partecipanti[140] ritengono dubbia sotto il profilo dello Stato di diritto la formulazione «chi intenzionalmente non osserva gli ordini del Servizio».

Lettera b

VD, BL e AG chiedono di applicare la disposizione anche alle violazioni dell'articolo 20 AP-LSCPT; AG anche a quelle dell'articolo 22 AP-LSCPT.

8.1.2 Capoverso 2

UNIZH ritiene contraria al sistema la punibilità del tentativo e della complicità, poiché si tratta di contravvenzioni e non di delitti o crimini.

8.1.3 Capoversi 3 e 4

Nessuna osservazione

8.2. Articolo 32 Giurisdizione

Il perseguimento e il giudizio dei reati ai sensi dell'articolo 31 competono ai Cantoni.

CCPCS approva esplicitamente la competenza dei Cantoni, poiché è conforme al principio secondo cui il perseguimento e il giudizio dei reati competono ai Cantoni.

Per definire la competenza territoriale alcuni partecipanti[141] intendono introdurre un disciplinamento che si basi sul luogo in cui il fornitore imputato offre il suo servizio. Se tale fornitore offre i suoi servizi in diversi Cantoni, occorre prevedere la giurisdizione federale.

Secondo BL e CAIS non è comprensibile perché il perseguimento e il giudizio debba competere ai Cantoni. Chiedono pertanto di prevedere la competenza generale della Confederazione. BL osserva che l'articolo 31 AP-LSCPT contiene contravvenzioni in ambiti di competenza del Servizio e quindi in linea di massima della Confederazione. A questo si aggiunge che le contravvenzioni dei fornitori riguardano di regola più Cantoni. CAIS ritiene che contro le decisioni del Servizio sia ammissibile il ricorso secondo le regole della procedura federale e quindi le regole sul diritto penale amministrativo dovrebbero essere applicabili anche ai procedimenti penali.

---

139 AG, LU, GL, GR, TG, VS, JU, CCDGP.
140 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
141 ZH, LU, SG, GL, GR, TG, VS, JU, CCDGP.

9. Vigilanza e rimedi giuridici

9.1. Articolo 33 Vigilanza

[1] Il Servizio vigila sul rispetto della legislazione in materia di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

[2] Se constata una violazione del diritto può adottare, per analogia, i provvedimenti di cui all'articolo 58 capoverso 2 lettera a della legge del 30 aprile 1997 sulle telecomunicazioni. Può disporre provvedimenti cautelari.

Secondo vari partecipanti[142] la formulazione del capoverso 1 «Il Servizio vigila sul rispetto della legislazione» contraddice l'articolo 15 lettera a AP-LSCPT secondo cui il Servizio non può controllare la correttezza legale di un ordine di sorveglianza. L'articolo 33 AP-LSCPT va quindi interpretato in modo tale che il Servizio non deve garantire il rispetto della legislazione in generale, bensì soltanto unilateralmente il rispetto delle disposizioni legali da parte dei fornitori di servizi di telecomunicazione. Tale interpretazione è confermata anche dal tenore del capoverso 2. Il Servizio dovrebbe assumere il ruolo di unità amministrativa tra le autorità di perseguimento penale e i fornitori di servizi di telecomunicazione, applicare la legge e decidere in casi controversi, cosa che attualmente però non può fare. Tuttavia, il Servizio non si vede in questo ruolo, ma agisce progressivamente come se fosse un'autorità di vigilanza. Nelle direttive tecniche e nelle prescrizioni organizzative e amministrative che dovrebbe emanare come mere istruzioni amministrative, il Servizio non si limita a disciplinare il modo in cui i fornitori di servizi di telecomunicazione devono mettere a disposizioni determinati dati, bensì emana sempre più regole che disciplinano le prestazioni che i fornitori devono svolgere. Inoltre, si deplora che a volte in un eccesso di zelo vengono preventivamente richieste prestazioni che vanno oltre le richieste delle autorità inquirenti. Quest'evoluzione verso un Servizio che si rende progressivamente autonomo e non controllabile mediante rimedi giuridici o un'autorità di vigilanza è ritenuta preoccupante. I partecipanti che si esprimono in merito all'articolo 33 AP-LSCPT concludono che, alla luce della legge in complesso poco chiara e insoddisfacente, l'articolo 33 vada riesaminato, poiché il Servizio stesso non si vede nel ruolo di guardiano del diritto, ma piuttosto come autorità che cerca di garantire il maggior numero di sorveglianze possibili. Alla luce di questa situazione non è idoneo come autorità di vigilanza.

Cablecom critica che con la formulazione attuale il Servizio deve vigilare sulla propria attività Propone di affidare la vigilanza all'Ufficio federale delle comunicazioni (UFCOM).

Rinviando all'affare delle schedature, KFG chiede di garantire il controllo del Servizio. Propone l'istituzione di un ufficio di controllo che verifichi regolarmente le spese del Servizio come pure l'appropriatezza e la liceità delle misure ordinate.

9.2. Articolo 34 Rimedi giuridici

[1] I ricorsi contro le decisioni adottate dal Servizio sono retti dalle disposizioni generali concernenti l'organizzazione giudiziaria federale.

[2] Il ricorrente non può presentare ricorso contro una decisione del Servizio che gli ingiunga di eseguire un incarico di sorveglianza, invocando l'illegalità dell'ordine di sorveglianza sul quale si fonda tale decisione. Contro le decisioni del Servizio può invece far valere eccezioni di ordine tecnico o organizzativo connesse all'esecuzione della misura di sorveglianza ordinata.

9.2.1 Capoverso 1

Nessuna osservazione.

---

[142] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable, SWICO, hp, COG.

9.2.2 Capoverso 2

Nove partecipanti[143] rilevano che la disposizione proposta corrisponde a un'esigenza pratica. Secondo CAIS l'esclusione generale del controllo della liceità è tuttavia troppo estesa. I fornitori di servizi di telecomunicazione dovrebbero avere la possibilità di contestare il fatto che una misura ordinata non sia prevista dalla legge, poiché l'autorità che autorizza la misura non dispone delle conoscenze tecniche necessarie.

Numerosi partecipanti[144] chiedono che, a differenza di quanto proposto nel capoverso 2, sia in generale prevista la possibilità di far verificare la liceità di un ordine di sorveglianza.

Alcuni partecipanti[145] osservano che un ordine di sorveglianza illegale, ossia il perseguimento di un reato non compreso nel catalogo dell'articolo 269 capoverso 2 lettera a CPP o una misura di sorveglianza che non è prevista dalla legge, non intacca soltanto i diritti dell'interessato, bensì che, in considerazione della portata dell'ingerenza nei diritti fondamentali, esiste anche un interesse pubblico di poter contestare un ordine erroneo. Inoltre, osservano che in casi urgenti, durante la procedura di ricorso, le autorità di perseguimento penale possono chiedere una misura preventiva oppure può essere revocato l'effetto sospensivo di un eventuale ricorso.

BE ritiene urtante che i soggetti obbligati erroneamente dal Servizio ad eseguire una sorveglianza non possano opporsi.

Otto partecipanti[146] osservano che secondo le regole generali l'autorità di ricorso non può avere cognizioni più estese di quelle dell'autorità di prima istanza. Poiché il Servizio, in qualità di autorità di prima istanza, non ha competenze materiali di controllo e riprende semplicemente gli ordini di sorveglianza, anche l'autorità di ricorso non può eseguire tale controllo. Ciò significa che in definitiva le decisioni del Servizio non sono impugnabili. Chiedono pertanto che al Servizio sia conferita la competenza per i pertinenti controlli (cfr. anche le spiegazioni al cap. III n. 3.2.1 ad art. 15 lett. a AP-LSCPT).

Secondo Cablecom il capoverso 2 è contrario alle disposizioni della procedura penale federale e va quindi stralciato. Swisscable osserva che un capitolato d'oneri è inutile se non esiste la possibilità di esigere, se del caso, i diritti e gli ordini ivi previsti. Per garantire la certezza del diritto, occorre quindi prevedere in futuro rimedi giuridici contro gli ordini travalicanti delle autorità. Tali rimedi giuridici non sono previsti né nella legge in vigore, né nell'avamprogetto posto in consultazione, il che comporta una mancanza di certezza giuridica.

Un notevole numero di partecipanti[147] propone la seguente nuova formulazione: «Il ricorrente non può presentare ricorso contro una decisione del Servizio, invocando, nel caso concreto, che l'ordine di sorveglianza è sproporzionato o che l'autorità che ha ordinato la sorveglianza non ha esercitato correttamente il proprio potere discrezionale».

---

143 LU, NW, GL, GR, TG, VS, JU, CCDGP, CAIS.
144 ZG, BE, BL, AR, PLR, PS, economiesuisse, UCS, privatim, UCS, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Cablecom, Swisscable, SKS, SIUG, VSPF, SWICO, hp, COG, IT(19), ISSS.
145 ZG, privatim, PS, PLR, economiesuisse, UCS.
146 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, SKS.
147 economiesuisse, SWICO, hp, COG, asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, IT(19).

BL osserva inoltre che se, come previsto dal capoverso 2, possono essere fatte valere eccezioni di ordine tecnico o organizzativo, l'eseguibilità dal punto di vista tecnico e organizzativo andrebbe prima accertata. Occorre quindi completare in tal senso l'articolo 15 lettera a AP-LSCPT. (cfr. sopra cap. III n. 3.2.1 ad art. 15 lett. a AP-LSCPT).

Se i fornitori non possono invocare l'illegalità di una musura di sorveglianza, AG propone di prevedere un'altra possibilità di controllo. Secondo OW occorre prevedere la possibilità di verificare se il Servizio abbia assolto i compiti ci cui all'articolo 15 AP-LSCPT. Non è chiaro se ciò sia già previsto.

10. Disposizioni finali

10.1. Articolo 35 Esecuzione

Il Consiglio federale e, nella misura in cui sono competenti, i Cantoni emanano le disposizioni necessarie all'esecuzione della presente legge.

Nessuna osservazione.

10.2. Articolo 36 Abrogazione e modifica del diritto vigente

L'abrogazione e la modifica del diritto vigente sono disciplinate nell'allegato.

Le osservazioni in merito alle modifiche del diritto vigente sono riassunte qui di seguito al numero 11.

10.3. Articolo 37 Disposizioni transitorie

Le sorveglianze ordinate prima dell'entrata in vigore della presente legge sono rette dal nuovo diritto.

Vari partecipanti[148] appartenenti al ramo dei servizi di telecomunicazione chiedono termini transitori adeguati per l'attuazione tecnica. Propongono la seguente formulazione: «Le sorveglianze ordinate prima dell'entrata in vigore della presente legge sono rette dal diritto *previgente*. *All'entrata in vigore della presente legge, le sorveglianze ordinate sotto la legge previgente possono essere proseguite soltanto se sono lecite anche secondo il nuovo diritto*». Poiché vengono estesi sia il campo d'applicazione materiale che quello personale, switch e switchplus chiedono termini transitori adeguati per i nuovi soggetti obbligati a eseguire le misure di sorveglianza. Propongono quindi un nuovo capoverso 2: «*I nuovi soggetti che, in seguito all'estensione del campo d'applicazione materiale e personale, sottostanno all'obbligo di eseguire le misure di sorveglianza, sono tenuti ad eseguirle entro un anno dall'entrata in vigore della presente legge*.»

Secondo BL la disposizione è formulata in modo ambiguo. Suppone che all'entrata in vigore della nuova legge il nuovo diritto si applichi alle sorveglianze *in corso* ordinate prima dell'entrata in vigore e non retroattivamente a tutte le sorveglianze ordinate prima dell'entrata in vigore della legge.

In tale contesto SZ chiede se, nel caso in cui il nuovo diritto si applichi anche alle sorveglian-

[148] asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

ze già concluse, la comunicazione secondo l'articolo 11 AP-LSCPT debba essere effettua successivamente.

Cablecom ritiene problematica l'applicazione del nuovo diritto alle sorveglianza ordinate prima della sua entrata in vigore, poiché ad esempio i dati retroattivi non saranno eventualmente ancora a disposizione da 12 mesi. Propone la seguente formulazione: «Le sorveglianze ordinate prima dell'entrata in vigore della presente legge sono rette dal diritto *previgente. Le sorveglianze ordinate dopo l'entrata in vigore della presente legge sono rette per un periodo transitorio di sei mesi dal diritto previgente»*.

Secondo MS la disposizione non rispetta il principio di determinatezza secondo cui il cittadino deve conoscere le conseguenze di un suo comportamento. La nuova LSCPT deve pertanto essere applicata soltanto alle sorveglianze nuove.

Altri partecipanti[149] ritengono che vi sia una svista: probabilmente il Legislatore intendeva dire che le sorvegliante in corso *ordinate* prima dell'entrata in vigore sono rette dal nuovo diritto. In tal caso tuttavia ritengono la disposizione inutile, rinviando al rapporto esplicativo.

10.4. Articolo 38 Referendum ed entrata in vigore

[1] La presente legge sottostà a referendum facoltativo.
[2] Il Consiglio federale ne determina l'entrata in vigore.

Nessuna osservazione.

11. Abrogazione e modifica del diritto vigente (allegato; art. 36 AP-LSCPT)

11.1. Codice di diritto processuale penale svizzero del 5 ottobre 2007 (CPP)[150]

11.1.1 Articolo 269 capoverso 2 lettera a CPP Condizioni

[2] La sorveglianza può essere ordinata per perseguire i reati di cui alle disposizioni seguenti:

a. CP: articoli 111-113; 115; 118 numero 2, 122; 127, 129; 135; 138-140; 143; 144 capoverso 3; 144bis numero 1 capoverso 2 e numero 2 capoverso 2; 146-148; 156; 157 numero 2; 158 numero 1 capoverso 2, e numero 3, 160; 161; 163 numero 1; 180; 181-185; 187; 188 numero 1; 189-191; 192 capoverso 1; 195; 197; 220; 221 capoversi 1 e 2; 223 numero 1; 224 capoverso 1; 226; 227 numero 1 capoverso 1; 228 numero 1 capoversi 1-4; 230bis; 231 numero 1; 232 numero 1; 233 numero 1; 234 capoverso 1; 237 numero 1; 238 capoverso 1; 240 capoverso 1; 242; 244; 251 numero 1; 258; 259 capoverso 1; 260bis-260^{quinquies}; 261bis; 264-267; 271; 272 numero 2; 273; 274 numero 1 capoverso 2; 285; 301; 303 numero 1; 305; 305bis numero 2; 310; 312; 314; 317 numero 1; 319; 322ter; 322^{quater}; 322^{septies};

Dodici partecipanti[151] approvano esplicitamente l'estensione del catalogo di reati all'articolo 220 CP (sottrazione di minorenne).

Secondo USS, l'AP-LSCPT è eccessivo. Il catalogo dei reati è troppo esteso. L'installazione di «Government Software» (spesso chiamati «cavalli di troia federali») in caso di reati quali danneggiamento con danno considerevole o perturbamento del servizio ferroviario non è ad esempio giustificato.

---

149 GL, GR, TG, VS, JU, CCDGP, CAIS.
150 RU **2010** 1881; in vigore dal 1° gennaio 2011.
151 LU, ZH, OW, NW, GL, GR, TG, VS, JU, CCPCS, CCDGP, CAIS.

SIUG e VSPF osservano che già oggi il catalogo esaustivo di reati non si applica se il reato è stato commesso per mezzo di Internet. Secondo l'articolo 20 capoverso 3 AP-LSCPT, se un reato è commesso mediante Internet, i soggetti che effettuano la sorveglianza del traffico delle telecomunicazioni in virtù di tale legge forniscono al Servizio qualsiasi indicazione che consenta di identificarne l'autore. Chiedono che l'estensione a ulteriori reati sia esaminata in modo critico. Inoltre, il catalogo di reati deve essere applicato anche all'accesso alle informazioni risultanti dalla conservazione dei dati della telecomunicazione.

KFG ritiene ingiustificata l'estensione del catalogo di reati all'articolo 220 CP. La fattispecie non costituisce un «reato grave» e va pertanto stralciata.

CFCG intende completare il catalogo di reati con l'articolo 55 capoverso 1 della legge del 18 dicembre 1998[152] sul gioco d'azzardo e sulle case da gioco (LCG), poiché un numero sempre maggiore di case da gioco illegali sono gestite mediante Internet. Per perseguire in modo efficace queste case da gioco, sono necessari nuovi strumenti d'indagine. Per assicurare gli elementi di prova necessari è indispensabile entrare nella rete virtuale di queste case da gioco illegali in maniera analoga a una perquisizione domiciliare nel mondo reale. Quest'ultima è possibile in virtù dell'articolo 56 LCG. Nel mondo virtuale invece la perquisizione non è possibile, a causa della mancanza di misure di sorveglianza ai sensi della LSCPT. Tali misure sarebbero tuttavia indispensabili per perseguire penalmente le case da gioco illegali gestite mediante Internet. CFCG ritiene che l'articolo 55 capoverso 1 LCG soddisfi i criteri necessari per essere incluso nel catalogo dell'articolo 269 capoverso 2 CPP, poiché si tratta di un reato di particolare gravità, commesso sempre più spesso mediante Internet.

11.1.2 Articolo 270bis CPP Intercettazione e decodificazione di dati (*nuovo*)

[1] Se nell'ambito della sorveglianza del traffico delle telecomunicazioni le misure di sorveglianza già adottate non hanno avuto esito positivo o se altre misure di sorveglianza sarebbero vane o renderebbero la sorveglianza eccessivamente difficile, il pubblico ministero può disporre, anche all'insaputa della persona sorvegliata, l'installazione in un sistema informatico di programmi informatici che permettano di intercettare e leggere i dati. Nell'ordine di sorveglianza il pubblico ministero indica il tipo di dati che desidera ottenere.

[2] L'ordine di sorveglianza sottostà all'autorizzazione del giudice dei provvedimenti coercitivi.

Quattordici partecipanti[153] approvano la nuova disposizione. Alcuni di loro[154] fanno notare la diffusione sempre maggiore del problema della codificazione. UCS è inoltre contraria all'ulteriore condizione della cosiddetta «doppia sussidiarietà», che è troppo severa e poco praticabile. L'installazione di «Government Software» (spesso chiamati «cavalli di troia federali») non è una misura più severa rispetto ad altre misure di sorveglianza, in particolare quelle previste dall'articolo 280 CPP. Secondo UCS non convince il fatto che in base a detta sussidiarietà, prima di sorvegliare la telefonia mediante Internet di un imputato, debbano essere sorvegliate la telefonia fissa e quella mobile. È sufficiente l'esame della proporzionalità ai sensi dell'articolo 269 CPP.

Dieci partecipanti[155] respingono del tutto l'installazione di programmi informatici all'insaputa della persona sorvegliata, altri partecipanti[156] esprimono delle riserve.

---

152 RS **935.52**

153 ZH SZ, NW, OW, GL, GR, TG, VS, JU, CCDGP, CCPCS, CAIS, SPICT, UCS.

154 ZH, GL, GR, TG, VS, JU, CCDGP, CCPCS.

155 Verdi, GDS, gr.ch, Cablecom, CCC, SKS, SIUG, KFG, PPS, ISSS.

156 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, ZH, BL, AR, LU, PS, SIUG, privatim, economiesuisse, Swisscable.

Verdi, GDS, gr.ch, SKS e SIUG osservano innanzitutto che l'installazione di programmi informatici all'insaputa della persona sorvegliata non significa altro che installare un software dannoso nei computer di privati. Ne consegue una grave ingerenza nella sfera privata dell'interessato, poiché con questa misura di sorveglianza si può accedere all'intero sistema di elaborazione dei dati (fotografie, lettere, parole chiave, microfono, ecc.). Reputano incomprensibile o forse addirittura significativo che non vi sia alcun rinvio alla sentenza di fondo della Corte costituzionale federale tedesca di febbraio 2008[157], secondo cui tale metodo viola il diritto fondamentale, risultante dai diritti della personalità, alla garanzia della confidenzialità e dell'integrità dei sistemi informatici. La Corte costituzionale federale tedesca ammette questa perquisizione «online» soltanto per proteggere «beni giuridici della massima importanza». Ne fanno parte l'integrità fisica, la vita e la libertà delle persone oppure beni della comunità la cui minaccia mette in pericolo le basi o l'esistenza dello Stato o le basi esistenziali dei cittadini. Secondo i partecipanti menzionati un siffatto diritto fondamentale risulta dall'articolo 10 Cost.

SIUG rinvia alla Corte federale di giustizia tedesca che ritiene illecita una misura di questo tipo ai fini del perseguimento penale. La Corte motiva la sua decisione[158] anche col fatto che la misura è eseguita all'insaputa dell'interessato, mentre per la perquisizione domiciliare la legge prevede la presenza di testimoni o del titolare dell'oggetto perquisito. Secondo SIUG l'articolo 245 CPP (esecuzione della perquisizione domiciliare) costituisce una disposizione in tal senso.

Verdi, GDS, gr.ch e SKS criticano inoltre che la perquisizione del computer non è limitata a determinati programmi – come ad esempio programmi di posta elettronica. Una siffatta limitazione presuppone infatti la perquisizione dell'intero disco duro allo scopo di trovare i dati rilevanti. Anche l'argomento della «doppia sussidiarietà» non riesce a convincere, poiché già la sorveglianza ordinaria del traffico delle telecomunicazioni è legata alla condizione che altri metodi non abbiano avuto esiti positivi o siano vani. In pratica ciò significa che, in caso di insuccesso della sorveglianza ordinaria del traffico delle telecomunicazioni, le autorità inquirenti e il tribunale cui compete l'approvazione dispongono automaticamente delle basi per installare sistemi informatici nel computer dell'interessato. Non è inoltre previsto un catalogo specifico di reati, perché secondo il rapporto esplicativo tutti i reati per i quali è ammessa la sorveglianza telefonica «normale» «possono, in un caso concreto, presentare una gravità che giustifica il ricorso a tale metodo di sorveglianza». Il rapporto esplicativo tuttavia non chiarisce in cosa consista la particolare gravità del reato. Secondo i suddetti partecipanti, alla luce di questa situazione è evidente che si tratta di creare una base legale possibilmente facile da gestire per un metodo di sorveglianza tecnicamente possibile. Oltre alla questione della protezione giuridica, occorre valutare anche l'efficienza di questo metodo di sorveglianza. È probabile che chi viene sorvegliato con un siffatto metodo, lo eluda adottando misure precauzionali o utilizzando canali di comunicazione diversi dal computer sorvegliato.

Verdi, SKS, KFG e PPS esprimono il timore che l'installazione di sistemi informatici all'insaputa delle persone sorvegliate crei una lacuna nel sistema di sicurezza che prima o poi potrebbe essere sfruttata anche da criminali. È ad esempio possibile che il software alla base del «cavallo di troia federale» appaia in rete e possa essere usato abusivamente dai criminali.

Secondo KFG qualsiasi software installato in un sistema informatico modifica il sistema stes-

---

[157] BVerfG, 1 BvR 370/07 del 27.2.2008, capoverso n. (1-333).
[158] BGH, decisione del 31.1.2007 – StB 18/06.

so e può pregiudicare la sicurezza del computer e dell'intera rete informatica. In tale contesto occorre chiedersi come un'autorità possa provare che il mezzo di prova individuato non sia stato caricato o inviato dal «cavallo di troia federale» stesso. Infatti oltre a poter essere letti, i dati possono anche essere creati o cambiati. Ciò rende impossibile l'assunzione delle prove.

PPS osserva che l'interazione tra il «cavallo di troia federale» e gli altri elementi del sistema informatico non può essere prevista con esattezza. Occorre quindi chiedersi chi debba coprire gli eventuali danni causati dal «cavallo di troia federale».

Il CCC ritiene imprudente che lo Stato intenda impiegare software simili a cavalli di troia che non possono essere messi in circolazione in Svizzera. È inoltre possibile che vengano danneggiati anche computer di terzi, poiché a seconda della rete informatica sono coinvolti anche terzi. L'impiego di «cavalli di troia» da parte dello Stato è arrogante e la probabilità che vengano sorvegliati anche terzi (innocenti) è alta.

Anche SIUG indica in modo dettagliato diversi pericoli e difficoltà tecniche legati all'installazione di siffatti software sul computer da sorvegliare. Inoltre, ritiene che il rischio della diffusione da parte delle autorità svizzere di un software dannoso a una cerchia notevole di persone, anche all'estero, non possa essere corso.

Sette partecipanti[159] deplorano la mancanza di un disciplinamento delle modalità di cancellazione dei programmi dai sistemi informatici interessati. Secondo ZH, BL, ZG e PS non sono neppure chiariti i requisiti relativi alla sicurezza applicabili sia ai programmi da installare sia a coloro che li forniscono.

Secondo il PLR, economiesuisse e Swisscable le ripercussioni dei «cavalli di troia federali» sono difficilmente prevedibili. economiesuisse e Swisscable chiedono che siano impiegati soltanto programmi che si limitano alla sorveglianza degli ambiti autorizzati e che non intacchino la funzionalità di altri programmi di software. Inoltre, la Confederazione dovrebbe rispondere di eventuali danni. Entrambi propongono formulazioni concrete.

Per l'UDC tali ingerenze nella sfera privata delle persone devono essere attuate soltanto come ultima ratio. I requisiti e i criteri devono pertanto essere severi; una condizione che la disposizione non soddisfa. L'UDC propone di fissare esplicitamente nella legge le figure di reato che permettono l'impiego di siffatti strumenti. Il PPD esprime certe riserve nei confronti dell'impiego di metodi con cui si accede anche a dati non pertinenti e che costituiscono un rischio elevato anche per terzi non coinvolti.

Anche privatim fa notare la gravità dell'ingerenza. In virtù della Costituzione federale lo Stato non può in linea di massima introdursi nei sistemi informatici dei soggetti del diritto. Una base legale che permette l'introduzione di un programma informatico in sistemi informatici privati, all'insaputa dell'interessato, deve pertanto soddisfare i massimi requisiti in riferimento alla determinatezza; una condizione che la presente disposizione non soddisfa del tutto. Riferendosi alla Corte costituzionale federale tedesca[160], privatim e il PS chiedono che il catalogo dei reati dell'articolo 269 capoverso 2 lettera a CPP si limiti ad alcuni reati molto gravi contro la vita e l'integrità fisica oppure contro lo Stato. Anche BS e FR chiedono in generale la restrizione del catalogo di reati per i quali è ammesso l'impiego di «cavalli di troia federali». FR chiede inoltre che siffatti impieghi siano permessi soltanto a condizioni molto severe, vale a dire in caso di indizi concreti di pericoli imminenti per un bene giuridico fondamentale, e non in caso di mero grave sospetto ai sensi dell'articolo 269 capoverso 1 lettera a CPP. Secondo

[159] ZH, BL, AR, ZG, PS, SIUG, privatim.
[160] BVerfG, 1 BvR 370/07 del 27.2.2008, capoverso n. (1-333).

FR le autorità federali devono infine valutare la portata di tali misure in rapporto alla totalità delle misure di sorveglianza.

BE propone di chiarire nella legge se con i «cavalli di troia federali» è permessa una «perquisizione domiciliare virtuale» o se si può sorvegliare soltanto il traffico delle telecomunicazioni.

MS constata che la disposizione permette di rilevare qualsiasi tipo di dati e chiede pertanto di integrarla all'articolo 280 CPP. Inoltre, dal tenore non si evince chiaramente che la disposizione si limita al catalogo di reati dell'articolo 269 capoverso 2 lettera a CPP.

UNISG e UNIZH esprimono riserve di fondo in merito a questo tipo di sorveglianza e ne rilevano la particolare complessità dal punto di vista organizzativo e del personale.

ISSS ci tiene a osservare che l'impiego di siffatti programmi informatici è suscettibile di pregiudicare il livello di protezione dei dati e di sicurezza informatica raggiunto in Svizzera.

11.1.3 Articolo 270ter CPP Impiego di dispositivi di localizzazione *(nuovo)*

[1] Il pubblico ministero può disporre l'impiego da parte della polizia di dispositivi volti a individuare i dati d'identificazione specifici degli apparecchi di telefonia mobile e a localizzare tali apparecchi. I dispositivi utilizzati devono prima essere stati debitamente autorizzati.

[2] L'ordine di sorveglianza sottostà all'autorizzazione del giudice dei provvedimenti coercitivi.

Un notevole numero di partecipanti[161] approva in linea di massima la nuova disposizione.

Alcuni di questi partecipanti[162] chiedono di sostituire l'espressione «apparecchi di telefonia mobile» con «mezzi di comunicazione mobili», in modo da tenere conto dei nuovi sviluppi tecnologici (p.es. notebook con carta SIM). CCPCS propone un nuovo capoverso 3 che preveda l'impiego di dispositivi di localizzazione per la ricerca in casi urgenti. Altri[163] osservano che i dispositivi di localizzazione sono apparecchi tecnici di sorveglianza impiegati dalla polizia e non dal Servizio. Propongono pertanto di inserire la disposizione nell'articolo 280 CPP e di prevedere una procedura d'autorizzazione.

Verdi, GDS, gr.ch, SKS e SIUG rifiutano la disposizione e osservano che l'impiego dei cosidetti «IMSI[164]-Catcher» non riguarda soltanto un singolo utente di telefonia mobile. Tali dispositivi infatti deviano o disturbano, all'insaputa degli interessati, il traffico di telefonia mobile di tutte le persone, sospette o meno, che si trovano nei dintorni dei dispositivi. Inoltre, le esperienze raccolte all'estero con gli «IMSI-Catcher» mostrano che in certe situazioni questi dispositivi permettono soprattutto di scoprire «spontaneamente» chi si trova in un determinato luogo oppure di disturbare in modo mirato il traffico telefonico. Verdi, GDS e gr.ch si chiedono inoltre se l'impiego di questi dispositivi appartenga all'ambito del diritto processuale penale. Secondo il rapporto esplicativo la polizia può impiegare i dispositivi su ordine del pubblico ministero, ma al fine di «garantire la sicurezza pubblica». I suddetti partecipanti ritengono tuttavia che tale garanzia sia un compito della polizia, il cui disciplinamento non compete alla Confederazione. Inoltre, l'articolo 270ter CPP non indica criteri che indichino quando è giustificato l'impiego dei dispositivi, né menziona condizioni che vadano oltre l'autorizzazione da parte del giudice delle misure coercitive. Tale giudice non dispone pertanto di parametri per autorizzare o vietare l'impiego dei dispositivi.

---

161 ZH, LU, SZ, OW, NW, SG, BL, GL, GR, TG, VS, JU, CCDGP, CCPCS, CAIS.
162 ZH, LU, CCDGP, GL, GR, TG, VS, JU, CCPCS.
163 LU, NW, BL, SG, GL, GR, TG, VS, JU, CCDGP, CAIS.
164 International Mobile Subscriber Identity.

Secondo TI la legge dovrebbe precisare che l'autorizzazione di tali dispositivi compete all'UFCOM, in modo da evitare confusioni con l'autorità di approvazione dell'ordine di sorveglianza menzionata nel capoverso 2. Occorre inoltre precisare se l'autorizzazione dell'UFCOM riguardi il tipo di dispositivo («una tantum») o se debba essere ottenuta per ogni utilizzazione, nel singolo caso, del dispositivo in questione. Anche NW chiede di disciplinare la procedura d'autorizzazione nella legge.

Vari partecipanti appartenenti al ramo dei servizi di telecomunicazione[165] osservano che in caso di impiego di «IMSI-Catcher», ai fornitori di servizi di telecomunicazione saranno automaticamente richiesti «IMSI» o addirittura «TIMSI»[166]. Il rilascio di «IMSI» è tuttavia problematico poiché costituisce un elemento di sicurezza della rete di telecomunicazione. I suddetti partecipanti possono accettare che gli organi di polizia tentino autonomamente di localizzare gli apparecchi, ma non appena è necessario il sostegno in forma di carte speciali, la cosa diventa molto costosa, poiché tale sostegno può essere fornito soltanto da pochissimi specialisti.

MS osserva che l'«IMSI-Catcher» consente anche di accedere al contenuto dei colloqui. Ciò deve essere assolutamente menzionato, anche nel titolo marginale, per evitare che siano raccolti dati ai sensi dell'articolo 269 CPP.

11.1.4 Articolo 271 capoversi 1 e 2 CPP Salvaguardia del segreto professionale

1 In caso di sorveglianza di una persona appartenente a una delle categorie professionali di cui agli articoli 170-173, è escluso l'accesso diretto da parte delle autorità di perseguimento penale alle informazioni raccolte nell'ambito della sorveglianza. Le informazioni estranee all'oggetto delle indagini e al motivo per cui tale persona è posta sotto sorveglianza vengono filtrate sotto la direzione di un giudice. La cernita è effettuata in modo che l'autorità di perseguimento penale non venga a conoscenza di informazioni coperte dal segreto professionale.

2 La cernita non ha luogo se:

a. sussiste un grave sospetto nei confronti della persona vincolata dal segreto professionale;

b. ragioni particolari lo esigono..

OW ritiene la modifica appropriata e giusta.

NW, BL, SG e CAIS deplorano che non sia disciplinato il caso in cui il titolare del segreto professionale è l'interlocutore della persona sorvegliata e chiedono di completare la disposizione in tal senso. Se il titolare del segreto professionale è sorvegliato in qualità di terzo, secondo SG e CAIS la sorveglianza dovrebbe limitarsi ai colloqui con l'imputato (o a colloqui dell'imputato effettuati con il collegamento del titolare del segreto professionale). Oltre che attraverso il filtraggio sotto la direzione di un giudice, ciò è eventualmente possibile anche mediante un filtraggio tecnico. Questa possibilità dovrebbe essere prevista nella legge (p.es. registrare esclusivamente le connessioni tra il collegamento sorvegliato e la persona sospetta). Al contrario di quanto previsto dalla disposizione, non si può tuttavia esigere che il giudice non deleghi la valutazione della sorveglianza a un'autorità di perseguimento penale, poiché solo tale autorità dispone delle conoscenze specifiche necessarie per la valutazione. I suddetti partecipanti chiedono pertanto di completare il capoverso 1 come segue: «[…] è escluso l'accesso diretto da parte dell'autorità di perseguimento penale *che si occupa dell'indagine preliminare* […]».

Secondo FSA l'articolo proposto contiene elementi privi di qualsiasi logica. Non si capisce ad

---

165 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

166 Temporary International Mobile Subscriber Identity.

esempio perché i segreti professionali siano protetti mediante la cernita delle informazioni degli atti se non sono connessi all'oggetto delle indagini e il titolare del segreto professionale è sorvegliato soltanto in quanto mero titolare del collegamento, mentre non sono protetti nel caso in cui la sorveglianza è effettuata in base a un sospetto fondato di reato nei confronti del titolare del segreto professionale. L'interesse alla protezione del segreto sussiste in entrambi i casi e non vi è alcun motivo di lasciare negli atti delle informazioni che non sono connesse all'oggetto delle indagini e che sono soggette al segreto professionale.

Secondo FSA, in caso di misure di sorveglianza, ogni Stato civile protegge il segreto professionale in base ai seguenti tre principi: la sorveglianza di apparecchi di telecomunicazione di titolari del segreto professionale deve restare un'eccezione; la sorveglianza deve essere eseguita in modo tale che siano raccolte solo le informazioni connesse all'oggetto dell'indagine; infine, la valutazione delle informazioni così ottenute deve essere effettuata da un giudice che non si occupa del caso. Ciò significa che la sorveglianza può essere eseguita soltanto in casi eccezionali. Le informazioni protette dal segreto professionale ottenute in occasione della sorveglianza di terzi vanno eliminate dagli atti e non sono utilizzabili. In virtù di questi principi la FSA chiede di riformulare la disposizione.

11.1.5 Articolo 273 capovers 3 CPP Dati relativi alle comunicazioni e alla fatturazione, identificazione degli utenti

3 Le informazioni di cui al capoverso 1 possono essere richieste con effetto retroattivo fino a dodici mesi, indipendentemente dalla durata della sorveglianza.

LU, NW, CAIS e CCDGP rinviano alle loro osservazioni all'articolo 23 AP-LSCPT (cap. III n. 5.4). OW ritiene la modifica appropriata.

11.1.6 Articolo 274 capoverso 4 lettere c e d CPP Procedura di approvazione *(nuove)*

4 L'autorizzazione indica espressamente:

c. se è ammessa l'installazione di programmi informatici in un sistema informatico per intercettare e leggere i dati criptati;

d. se è ammesso l'impiego da parte della polizia di dispositivi volti a individuare i dati d'identificazione specifici degli apparecchi di telefonia mobile e a localizzare tali apparecchi.

OW ritiene appropriata la modifica della disposizione.

Lettera c

BL e AG chiedono di disciplinare nella lettera c le modalità della cancellazione dei programmi informatici dal sistema informatico in cui sono stati installati. NW chiede di disciplinare la procedura d'approvazione per l'installazione di tali programmi.

Lettera d

Vari partecipanti[167] chiedono di sostituire l'espressione «apparecchi di telefonia mobile» con «mezzi di comunicazione mobili», in modo da garantire la sorveglianza anche in vista dei futuri sviluppi tecnologici (p.es. notebook con carta SIM).

CAIS e CCDGP rinviano alla loro proposta di inserire l'impiego di tali dispositivi nell'articolo 280 CPP (cfr. le osservazioni nel cap. III n. 11.1.3 ad art. 270ter CPP) e, insieme

[167] ZH, LU, AG, GL, GR, TG, VS, JU, CCPCS, CCDGP.

a NW, chiedono di disciplinare la pertinente procedura d'approvazione nell'articolo 274 CPP.

11.1.7 Articolo 278 capoverso 1bis CPP Reperti casuali

1bis Se nell'ambito della sorveglianza di cui agli articoli 27 e 28 della legge federale del ... sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni vengono scoperti reati, le informazioni raccolte possono essere utilizzate alle condizioni di cui ai capoversi 2 e 3.

OW ritiene appropriata la modifica della disposizione.

11.2. Procedura penale militare del 23 marzo 1979 (PPM)[168]

OW ritiene appropriate e giuste le modifiche e le integrazioni del PPM proposte.

11.2.1 Articolo 70a^{bis} PPM Intercettazione e decodificazione di dati *(nuovo)*

1 Se nell'ambito della sorveglianza del traffico delle telecomunicazioni le misure di sorveglianza già adottate non hanno avuto esito positivo o se altre misure di sorveglianza sarebbero vane o renderebbero la sorveglianza eccessivamente difficile, il giudice istruttore può disporre, anche all'insaputa della persona sorvegliata, l'installazione in un sistema informatico di programmi informatici che permettano di intercettare e leggere i dati. Nell'ordine di sorveglianza il giudice istruttore indica il tipo di dati che desidera ottenere.

2 L'ordine di sorveglianza sottostà all'autorizzazione del presidente del tribunale militare di cassazione.

Alcuni partecipanti[169] rinviano alle osservazioni in merito all'articolo 270bis CPP (cfr. cap. III. n. 11.1.2).

11.2.2 Articolo 70a^{ter} PPM Impiego di dispositivi di localizzazione *(nuovo)*

1 Il giudice istruttore può disporre l'impiego da parte della polizia di dispositivi volti a individuare i dati d'identificazione specifici degli apparecchi di telefonia mobile e a localizzare tali apparecchi. I dispositivi utilizzati devono prima essere stati debitamente autorizzati.

2 L'ordine di sorveglianza sottostà all'autorizzazione del presidente del tribunale militare di cassazione.

Vari partecipanti[170] chiedono di sostituire l'espressione «apparecchi di telefonia mobile» con «mezzi di comunicazione mobili», in modo da garantire la sorveglianza anche in vista dei futuri sviluppi tecnologici (p.es. notebook con carta SIM).

Alcuni partecipanti[171] rinviano alle osservazioni in merito all'articolo 270ter CPP (cfr. cap. III. n. 11.1.3).

11.2.3 Articolo 70b PPM Salvaguardia del segreto professionale

1 In caso di sorveglianza di una persona appartenente a una delle categorie professionali di cui all'articolo 75 lettera b, è escluso l'accesso diretto da parte delle autorità di perseguimento penale alle informazioni raccolte nell'ambito della sorveglianza. Le informazioni estranee all'oggetto delle indagini e al motivo per cui tale persona è posta sotto sorveglianza vengono filtrate sotto la direzione del presidente del tribunale militare. La cernita è effettuata in modo che l'autorità di perseguimento penale non venga a conoscenza di informazioni coperte dal segreto professionale

2 La cernita non ha luogo se:

a. sussiste un grave sospetto nei confronti della persona vincolata dal segreto professionale;

b. ragioni particolari lo esigono.

---

168 RS **322.1**

169 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

170 ZH, LU, AG, GL, GR, TG, VS, JU, CCPCS, CCDGP.

171 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.

[3] Le informazioni raccolte nell'ambito della sorveglianza di altre persone e in merito alle quali una persona menzionata nell'articolo 75 lettera b potrebbe rifiutarsi di deporre devono essere rimosse dagli atti del procedimento penale e distrutte immediatamente; non possono essere utilizzate nell'ambito di detto procedimento.

Nessuna osservazione

11.2.4 Articolo 70d capoverso 3 PPM

[3] Le informazioni di cui al capoverso 1 possono essere richieste con effetto retroattivo fino a dodici mesi, indipendentemente dalla durata della sorveglianza.

Alcuni partecipanti[172] rinviano alle loro osservazioni in merito al prolungamento del termine di conservazione dell'articolo 19 capoverso 2 AP-LSCPT (cfr. cap. III. n. 4.1.2) e dell'articolo 23 AP-LSCPT (cfr. cap. III. n. 5.4).

11.2.5 Articolo 70e capoverso 4 lettere c e d PPM *(nuove)*

[4] L'autorizzazione indica espressamente:

c. se è ammessa l'installazione di programmi informatici in un sistema informatico per intercettare e leggere i dati criptati;

d. se è ammesso l'impiego da parte della polizia di dispositivi volti a individuare i dati d'identificazione specifici degli apparecchi di telefonia mobile e a localizzare tali apparecchi.

In riferimento alla lettera c alcuni partecipanti[173] rinviano alle loro osservazioni nel capitolo III numero 11.1.2 ad articolo 270bis CPP e in riferimento alla lettera d al capitolo III numero 11.1.3 ad articolo 270ter CPP.

11.3. Legge del 30 aprile 1997[174] sulle telecomunicazioni (LTC)

11.3.1 Articolo 6a LTC Blocco dell'accesso ai servizi di telecomunicazione (*nuovo*)

I fornitori di servizi di telecomunicazione bloccano l'accesso alla telefonia mobile e a Internet dei clienti che non hanno sottoscritto un abbonamento, se questi ultimi, in occasione dell'avvio del rapporto commerciale, hanno utilizzato l'identità di una persona inesistente o che non ha acconsentito all'avvio di tale rapporto.

Dieci partecipanti[175] approvano esplicitamente che il blocco dell'accesso in caso di abusi sia sancito dalla legge. La prassi attuale mostra che i delinquenti che sfruttano la telefonia mobile usano spesso apparecchi rubati oppure apparecchi il cui abbonamento è intestato a un'altra persona o a una persona inesistente. L'esperienza insegna che la qualità del controllo dell'identità dei clienti in occasione della conclusione di un contratto con un fornitore di servizi di telefonia mobile lascia a desiderare.

OW ritiene che il previsto adattamento della LTC sia insufficiente. L'uso abusivo di carte SIM prepagate riscontrato nella prassi può essere impedito soltanto con una registrazione coerente delle relazioni con i clienti. Per le autorità di perseguimento penale la situazione attuale è insoddisfacente. AG chiede di completare la disposizione in modo tale che su autorizzazione delle autorità di perseguimento penale, ed eventualmente con l'approvazione del giudice delle misure coercitive, si possa chiedere il blocco dell'accesso a «carte SIM prepagate e carte wireless prepagate», se con queste carte sono stati commessi o continuano a essere

---

172 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
173 asut, Finecom, Orange, Swisscom, Colt, Sunrise, Verizon, Swisscable.
174 RS 784.10
175 ZH, NW, CCDGP, GL, GR, TG, VS, JU, CCPCS, CAIS.

commessi reati.

Orange chiede di stralciare la formulazione „[…] e a Internet […]“.