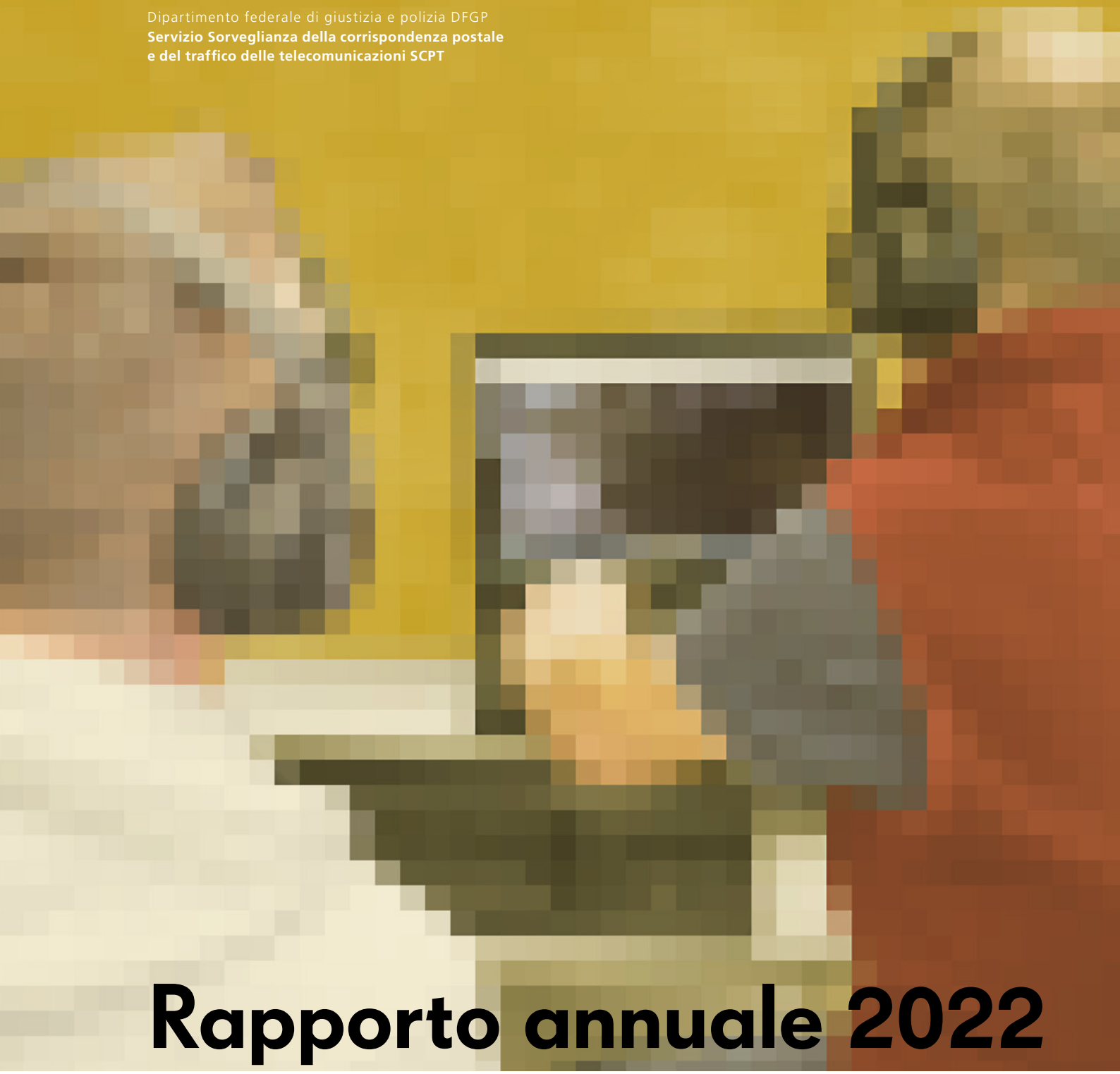
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni SCPT



Rapporto annuale 2022 Servizio SCPT

La sorveglianza del traffico delle telecomunicazioni va considerata in un contesto globale. La lingua utilizzata nelle conferenze internazionali, negli organismi multilaterali e nell'industria delle telecomunicazioni è l'inglese. Il termine inglese per la sorveglianza legale – Lawful Interception (LI) – si è pertanto affermato anche in Svizzera. Nel 2010 il Servizio SCPT ha tenuto conto di questa convenzione linguistica, creando il proprio sito Internet all'indirizzo:

www.li.admin.ch

Cara lettrice, caro lettore,

l'attuazione di ogni misura di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni costituisce una grave ingerenza nei diritti fondamentali della persona interessata. Le ingerenze in questi diritti costituzionali devono essere espressamente disciplinate in una legge. La concreta esecuzione delle misure è disciplinata da disposizioni dettagliate nelle ordinanze di attuazione. Ciascuna misura di sorveglianza deve essere approvata da un giudice.

Per dirlo con tutta la chiarezza necessaria: l'esecuzione di una misura da parte del Servizio SCPT deve rispettare severamente la sua base legale.

La tecnologia delle telecomunicazioni è in rapida evoluzione, offre sempre più servizi e possibilità di comunicazione. Per tenere il passo, occorre adeguare con una certa frequenza il quadro tecnico, organizzativo e amministrativo della sorveglianza del traffico delle telecomunicazioni. Tale adeguamento avviene sotto l'egida del Servizio SCPT, d'intesa con le autorità inquirenti e i fornitori di servizi di telecomunicazione.

Anche se la sorveglianza delle telecomunicazioni è in continua evoluzione, il nostro mandato legale resta lo stesso: garantire l'efficacia del perseguimento penale. Uno degli strumenti che abbiamo a disposizione a tal fine è il team Casi speciali.

«Anche se la sorveglianza delle telecomunicazioni è in continua evoluzione, il nostro mandato legale resta lo stesso: garantire l'efficacia del perseguimento penale.»

Questa unità mobile può, su ordine del giudice, eseguire misure di sorveglianza presso tutti i fornitori di servizi di telecomunicazione operanti in Svizzera. A pagina 15 del presente rapporto vi illustriamo come si svolge un tale intervento e come operano i nostri esperti per installare l'infrastruttura di sorveglianza in loco.

Personalmente questo contributo mi ricorda il mio arrivo al Servizio SCPT 15 anni fa. All'epoca, per i casi speciali il Servizio SCPT doveva ricorrere a partner esterni. Grazie alla mia formazione in tecnologia della telecomunicazione e ingegneria, per me era chiaro che in un'epoca di rapida evoluzione tecnologica questo modello sarebbe diventato obsoleto. È per questo che dal 2010 il Servizio SCPT si affida sempre più alle proprie competenze in tutti gli ambiti di attività. Lo sviluppo e l'ampliamento di tali competenze consente al Servizio SCPT di far fronte alle sfide in un ambiente complesso e altamente specializzato.

Vi auguro buona lettura.

René Koch
Capo Servizio SCPT (fino a fine maggio 2023)

01

PANORAMICA

■ Per fornitori di servizi di telecomunicazione si intendono in particolare i fornitori di servizi di telefonia mobile e fissa, di accesso a Internet ed e-mail, quali Swisscom, Sunrise e Salt.

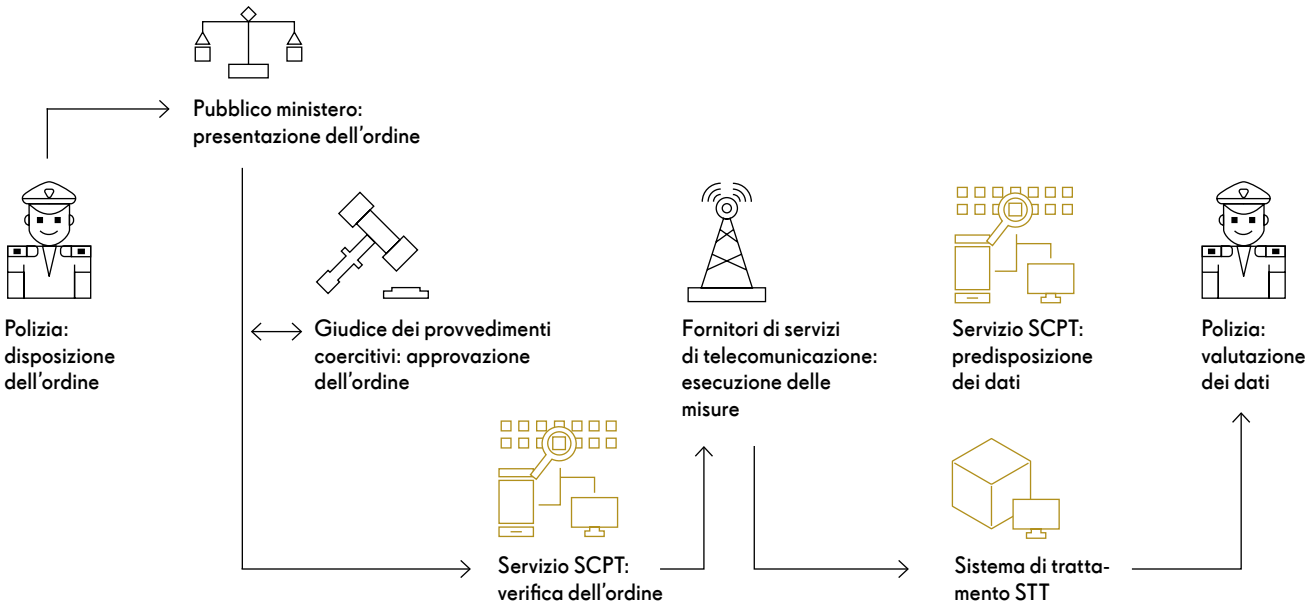
Il Servizio SCPT in breve

Per fare luce su reati gravi, le autorità di perseguimento penale della Confederazione e dei Cantoni hanno la possibilità di disporre misure di sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Dal 1° gennaio 1998 il Servizio SCPT è competente per l'attuazione di tali misure e al contempo garantisce il rispetto delle prescrizioni vigenti. Inoltre, raccoglie dai fornitori di servizi di telecomunicazione (FST) i dati richiesti dalle autorità di perseguimento penale o dal Servizio delle attività informative della Confederazione (SIC) e li trasmette agli inquirenti per la valutazione e l'analisi.

Né la criminalità né le moderne telecomunicazioni conoscono confini territoriali. La collaborazione internazionale assume quindi un valore importante nella lotta alla criminalità. A tal fine, il Servizio SCPT si impegna per garantire la standardizzazione internazionale e lo scambio di informazioni e conoscenze con le corrispondenti controparti straniere.

Il Servizio SCPT è responsabile per l'attuazione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni. Esegue i propri compiti autonomamente e non è vincolato da istruzioni. Dal punto di vista amministrativo, il Servizio SCPT è aggregato al Centro servizi informatici del Dipartimento federale di giustizia e polizia (CSI-DFGP) ed è suddiviso in quattro settori.

Il processo di sorveglianza



I quattro settori

La direzione del Servizio SCPT (da sinistra a destra): René Koch (capo del Servizio SCPT e del settore Procedimenti penali amministrativi), Jean-Louis Biberstein (capo del settore Diritto e controlling e capo supplente del Servizio SCPT, Alexandre Suter (capo del settore Provider Management) e Michael Galliker (capo del settore Gestione della sorveglianza)

Provider Management

I 22 collaboratori sono responsabili, tra le altre cose, per l'elaborazione e l'aggiornamento delle direttive tecniche che i FST devono rispettare nella procedura di scambio dei dati con il Servizio SCPT. Sono poi competenti per la cosiddetta procedura di conformità (*compliance*). In questo contesto il Servizio SCPT verifica se i fornitori di servizi di telecomunicazione sono in grado di eseguire la sorveglianza e trasmettere informazioni.

Secondo la legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT), i fornitori devono essere in grado di sorvegliare i servizi da loro offerti e fornire le relative informazioni in qualsiasi momento, a meno che non si siano fatti regolarmente esonerare dall'obbligo di effettuare la sorveglianza.

Il settore Provider Management sviluppa e gestisce soluzioni speciali ad hoc, i cosiddetti casi speciali, per eseguire misure di sorveglianza presso i fornitori che non sono obbligati ad effettuarla o che non sono in grado di farlo autonomamente. Questo compito spetta al team Casi speciali, che interviene, tra l'altro, quando un mandato di sorveglianza riguarda un piccolo fornitore – per esempio un gestore di una rete via cavo locale o un albergo. Maggiori dettagli nel rapporto sui casi speciali a pagina 15.

Inoltre, i collaboratori offrono consulenza a più di 900 fornitori per quanto riguarda questioni tecniche e giuridiche ed emanano, nel quadro delle loro competenze di vigilanza, pertinenti direttive e decisioni.

Un team di quattro persone è responsabile per il corretto funzionamento delle applicazioni del sistema di trattamento su cui sono trasmessi i dati intercettati.

Infine, gli esperti del settore Provider Management sostengono lo sviluppo di nuove applicazioni e sono attivi in diversi organismi di standardizzazione nazionali e internazionali. Si tratta, ad esempio, dello sviluppo e della predisposizione delle specifiche d'interfaccia nelle reti 4G e 5G.

Gestione della sorveglianza

Con i suoi 17 collaboratori, il settore Gestione della sorveglianza garantisce una collaborazione efficiente del Servizio SCPT con le autorità di perseguimento penale e il SIC.

Il team fornisce consulenza ai corpi di polizia, ai pubblici ministeri, ai giudici dei provvedimenti coercitivi e al SIC per quanto riguarda tutte le questioni giuridiche, tecniche, organizzative e amministrative nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

I collaboratori gestiscono i mandati di sorveglianza, li trasmettono ai fornitori dopo una verifica formale e garantiscono che le autorità ricevano i dati forniti. I loro compiti comprendono anche la fatturazione a carico delle autorità inquirenti e del SIC nonché il pagamento degli indennizzi ai FST.

Il team è l'interlocutore principale quando si tratta di risolvere problemi con il sistema di trattamento o altre difficoltà informatiche sollevate degli utenti. Segue anche lo sviluppo di nuove applicazioni.

Inoltre, il settore Gestione della sorveglianza gestisce la formazione degli utenti.

Al di fuori degli orari lavorativi, il settore fornisce un servizio operativo di picchetto, in particolare con il supporto tecnico garantito dal Provider Management. Il Servizio SCPT è pertanto reperibile 24 ore su 24.

Diritto e controlling

Le tecnologie dell'informazione e della comunicazione (TIC) sono uno dei rami più innovativi in assoluto. Implementano regolarmente nuovi standard e lanciano costantemente nuovi servizi per dispositivi finali sempre più performanti. Ciò si ripercuote sulla sorveglianza delle telecomunicazioni: l'interfaccia tecnica tra il sistema di trattamento del Servizio SCPT e le diverse centinaia di fornitori deve essere sottoposta a frequenti adeguamenti.

Insieme ai colleghi del settore Provider Management, gli esperti informatici del settore Diritto e controlling garantiscono che sia sempre possibile sorvegliare le telecomunicazioni anche

in un ambiente tecnologico estremamente dinamico. Con le loro conoscenze tecniche sostengono la pianificazione e la gestione di tutti i progetti informatici fondamentali per il Servizio.

Oltre che per lo svolgimento corretto dei progetti informatici, il team di 16 persone è responsabile per l'elaborazione delle basi legali necessarie per garantire la sorveglianza delle telecomunicazioni.

In molti casi si tratta di modificare le ordinanze in modo da tenere conto dei progressi della tecnica. L'ordinanza del DFGP sull'esecuzione della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OE-SCPT), ad esempio, viene verificata periodicamente e all'occorrenza adeguata.

Infine, rientrano nella competenza del settore Diritto e controlling la gestione finanziaria, la rendicontazione e l'informazione del pubblico. I collaboratori evadono le domande dei media e sono a disposizione dei cittadini per informazioni.

Procedimenti penali amministrativi

La LSCPT e le relative ordinanze d'esecuzione hanno attribuito al Servizio SCPT compiti aggiuntivi, tra cui l'esecuzione di procedimenti penali amministrativi. In questo caso la persona responsabile delle inchieste agisce in modo indipendente e dispone dei poteri di un pubblico ministero.

Dal marzo del 2018 il settore SCPT è autorizzato a procedere contro coloro che non adempiono i loro doveri legali nell'ambito della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni.

Un team di due persone del Settore Procedimenti penali amministrativi esamina le denunce, determina i fatti, effettua l'analisi giuridica e, se del caso, sanziona le violazioni. Chi dirige il procedimento può svolgere interrogatori e ordinare misure coercitive come perquisizioni e sequestri.

Al termine di un procedimento, il Servizio SCPT emana un decreto o una decisione penale o un decreto di abbandono.

Rassegna

Gennaio

Introduzione della tecnologia SLDT per gli utenti

La tecnologia SLDT (*secure large data transfer*) consente di trasmettere elettronicamente agli utenti maggiori quantità di dati in modo sicuro. In alcuni casi è quindi possibile rinunciare all'invio di supporti di dati per posta. Le prime organizzazioni di polizia hanno testato con successo la tecnologia SLDT assieme al Servizio SCPT e ora verrà progressivamente concesso agli utenti di accedervi.

Febbraio

Ripresa delle formazioni, anche se in forma ridotta

Dopo una lunga pausa dovuta alla pandemia, si sono potute svolgere le prime formazioni in presenza. Il materiale didattico online fornito durante tale periodo resta a disposizione e verrà ulteriormente sviluppato.

Marzo

Entrata in vigore della base legale necessaria per le funzioni di analisi

In data 11 marzo 2022, il Consiglio federale ha deciso di porre in vigore il 1° maggio 2022 la base legale necessaria per le funzioni di analisi. Con la modifica degli articoli 7 e 8 LSCPT è stata creata una base legale esplicita per poter analizzare i dati raccolti mediante la sorveglianza del traffico delle telecomunicazioni nel sistema di trattamento del Servizio SCPT.

Aprile

Serie web «La Suisse sous couverture»

Il 25 aprile 2022, la RTS ha annunciato l'uscita della seconda stagione della serie web «La Suisse sous couverture», incluso un reportage sul sistema di sorveglianza del Servizio SCPT. Questo documentario di 12 minuti è disponibile al seguente indirizzo: https://www.youtube.com/watch?v=kfJ2lQ1aok8.

Maggio

Proposta al Consiglio federale «Sorveglianza del traffico delle telecomunicazioni: maggiore fabbisogno finanziario e di personale presso il Servizio SCPT e CSI-DFGP»
Il programma per la sorveglianza delle telecomunicazioni (Programma STT)*, che ha lo scopo di sostituire e sviluppare il sistema di trattamento del Servizio SCPT, è stato avviato nel 2015 e si concluderà nel 2024. Il Servizio SCPT includerà nuove componenti nell'organizzazione di programma e si assumerà i relativi compiti. La proposta intende garantire che il Servizio SCPT disponga delle risorse necessarie. La proposta è stata discussa e approvata dal Consiglio federale il 4 maggio 2022.

Revisione delle ordinanze d'esecuzione (in particolare modifiche concernenti il 5G)
Il 23 maggio 2022 si è conclusa la procedura di consultazione sulla revisione parziale delle quattro ordinanze d'esecuzione della LSCPT. Al Servizio SCPT sono pervenuti 68 pareri, sulla base dei quali sono stati adeguati gli avamprogetti delle ordinanze.

Giugno

Legge federale sulle misure di polizia per la lotta al terrorismo
La legge federale sulle misure di polizia per la lotta al terrorismo (MPT), entrata in vigore il 1° giugno 2022, prevede diverse misure preventive di polizia. La MPT modifica anche la LSCPT. In particolare viene introdotto un nuovo tipo di sorveglianza per la localizzazione tramite telefonia mobile.

Luglio

Prima newsletter del Servizio SCPT per le autorità di perseguimento penale
Nel luglio 2022 è stata realizzata e pubblicata la prima newsletter per gli utenti del sistema di trattamento del Servizio SCPT, contenente informazioni pratiche sull'attività quotidiana nel quadro della sorveglianza delle telecomunicazioni. La newsletter verrà pubblicata a cadenza semestrale.

* Maggiori informazioni all'indirizzo www.li.admin.ch/it > Temi > Programma STT

Settembre

Preparazione della riorganizzazione del Servizio SCPT

Il Servizio SCPT è stato incaricato di effettuare una riorganizzazione con lo scopo di ottimizzare l'adempimento dei compiti nell'ambito dell'attuale quadro legale e organizzativo. Nella seconda metà del 2022 si è anche svolta una serie di workshop. La nuova organizzazione è attiva dal 1° maggio 2023.

Ottobre

Sondaggio sulla soddisfazione della clientela 2022

Ogni due anni il Servizio SCPT effettua un sondaggio sulla soddisfazione dei beneficiari di prestazioni. Secondo l'inchiesta, la soddisfazione rimane elevata. Su una scala da 1 (molto insoddisfatto) a 6 (molto soddisfatto) sono stati raggiunti i valori seguenti:

- soddisfazione delle autorità incaricate della valutazione: aumento da **4.7** a **4.9**,
- soddisfazione delle autorità competenti a ordinare una sorveglianza: aumento da **4.6** a **4.9**,
- soddisfazione delle autorità d'approvazione: calo da **5.7** a **5. 5**.

Dicembre

Ordinanza sul finanziamento della sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (OF-SCPT): termine della consultazione degli uffici

L'avamprogetto di ordinanza prevede l'introduzione di importi forfettari, con lo scopo di semplificare l'attuale sistema di finanziamento e fatturazione. Al contempo occorre incrementare il grado di copertura dei costi del Servizio SCPT. La consultazione degli uffici si è conclusa il 28 novembre 2022. Nella prima metà del 2023 si è svolta una seconda consultazione. L'entrata in vigore è prevista per il 1° gennaio 2024.

02

RETROSCENA

Mobile, flessibile e competente

Una squadra per interventi speciali

Piccoli fornitori di servizi di telecomunicazione, ad esempio i gestori locali di WLAN o di reti via cavo, possono farsi esentare dalla disponibilità a sorvegliare prescritta dalla legge. Se vi sono operazioni sospette nella loro rete e c'è una decisione di sorveglianza di un giudice, interviene il team Casi speciali del Servizio SCPT.

Eichenweg 3 a Zollikofen, il Campus dell'Amministrazione federale. Due membri del team Casi speciali riempiono una serie di scatole da trasporto con strumenti, cavi, spine e componenti elettroniche. Con l'ascensore merci portano il materiale alla consegna.

Il responsabile del team li sta già aspettando. Nel frattempo è arrivato un minivan. Dopo aver caricato il materiale, dalla portiera viene rimosso il logo della Confederazione svizzera «Nessuno deve rendersi conto da lontano che stiamo arrivando», dice l'autista.

Il suo capo prende posto sul sedile del passeggero. È uno specialista riconosciuto a livello internazionale nel settore della *lawful interception* (LI), la sorveglianza del traffico delle telecomunicazioni conforme alla legge. Laureato in informatica, ha lavorato per fornitori di servizi di telecomunicazione (FST) e gestori di reti operanti su scala internazionale. Dopo alcuni interventi in qualità di esperto di LI esterno, è entrato a far parte del Servizio SCPT nel 2012. Dal 2017 è responsabile del team Casi speciali.

È esperto nella conversione di dati, un elemento fondamentale degli interventi del team: si tratta di convertire i dati intercettati in loco nel formato previsto dall'Istituto europeo per gli standard delle telecomunicazioni (ETSI).

Negli scorsi anni in Svizzera sono state eseguite circa 10 000 misure di sorveglianza, la maggior parte nelle reti dei grandi FST. I principali attori sul mercato come Swisscom, Salt o Sunrise UPC devono essere per legge in grado di trasferire i dati dalle proprie reti al sistema di trattamento del Servizio SCPT nel formato richiesto.

Per le persone obbligate a collaborare, la LSCPT prevede obblighi attivi di sorveglianza o l'obbligo di meramente tollerare la sorveglianza. Si tratta sostanzialmente di proporzionalità. Le piccole e medie imprese che non sono interessate da molte misure di sorveglianza non devono nemmeno assumersi gli investimenti necessari a tal proposito. Non sono pertanto tenute a sviluppare internamente le competenze per la LI: devono solo tollerare le sorveglianze eseguite. «Il vero e proprio lavoro di sorveglianza è compito del nostro team Casi speciali», spiega Alexandre Suter, capo del settore Provider Management presso il Servizio SCPT.

Egli stima che in tutta la Svizzera possono essere coinvolte in casi speciali più di 1000 imprese. Si va dall'albergo che offre una WLAN gratuita ai propri ospiti, al fornitore di accesso a Internet, fino al fornitore di applicazioni per smartphone.

Dall'entrata in vigore della LSCPT nel marzo 2018, il settore Provider Management ha organizzato interventi del team Casi speciali presso circa 40 imprese. E ogni anno da cinque a

Una volta chiarita la situazione giuridica, inizia la discussione sull'attuazione tecnica.

dieci ulteriori fornitori, o meglio loro singoli clienti, entrano nel mirino delle autorità penali.

«Il nostro lavoro comincia con una telefonata al responsabile LI del fornitore», racconta il capo del team. Una volta stabilito il contatto, le persone coinvolte si scambiano, mediante e-mail criptate, le informazioni rilevanti sulle persone e gli apparecchi sorvegliati.

Dopo il chiarimento della situazione giuridica, il team Casi speciali discute l'attuazione tecnica. La discussione è breve se è già stata effettuata una sorveglianza, o lunga se un dato fornitore è coinvolto per la prima volta in un caso speciale.

Accertamenti sono necessari in particolare a causa della grande eterogeneità delle infrastrutture di telecomunicazione. Ciascun fornitore si affida a produttori di software e hardware diversi. Inoltre, spesso sono operative allo stesso tempo diverse generazioni dello stesso sistema. La squadra si trova di fronte a innumerevoli tipi di cavo, connettori elettronici e protocolli. Il responsabile del team si ricorda che «una volta, una componente della rete di cui avevamo assolutamente bisogno era ormai disponibile soltanto in Spagna».

Il minivan ha raggiunto la sua destinazione, un centro di dati nella regione di Zurigo. Un collaboratore del centro accoglie il team. Fuori splende il sole, dentro lampeggiano le luci dai rack dei server. Alcune plafoniere illuminano il locale. Si sente il ronzio dei server e il fruscio degli impianti di raffreddamento.

«Da alcuni anni, il traffico delle telecomunicazioni e dei dati si svolge in pratica esclusiva-

mente nel cloud», spiega il responsabile del team. Se gli elementi d'indirizzo della persona sospettata sono univoci, il team Casi speciali interviene soprattutto in centri di dati come questo. La squadra si reca in altri luoghi – ad esempio nei locali di un gestore locale di rete via cavo – soltanto se per ragioni tecniche è necessario avvicinarsi alla persona da sorvegliare.

Il team cerca un posto per installarsi tra gli armadi dei server. Porta sempre con sé l'attrezzatura di base per l'attività di sorveglianza vera e propria, acquisita presso produttori che riforniscono anche le autorità di perseguimento penale e i servizi delle attività informative di altri stati. A volte questi strumenti di base non sono sufficienti e l'operazione si svolge in due direzioni.

Mentre una parte del gruppo si occupa della sorveglianza in loco, i colleghi in ufficio sviluppano una soluzione software specifica per il caso. Non appena il server è online, partono

i cosiddetti test di connessione. Ciò permette di installare fino all'ultimo momento eventuali modifiche del software.

Nelle retrovie è a disposizione uno specialista del fornitore di servizi di telecomunicazione per rispondere alle domande che sorgono durante l'intervento. «Di norma la cooperazione è buona», afferma il responsabile del team. Le eccezioni confermano la regola: può ad esempio succedere che un fornitore opponga resistenza passiva e intenda lasciar lavorare i collaboratori del Servizio SCPT soltanto dopo l'intervento di un avvocato. In casi molto rari – ad esempio se il fornitore intende impedire l'accesso alla sua infrastruttura – il Provider Management del Servizio SCPT è costretto a far intervenire le forze di polizia.

Modifiche del software possono essere installate fino all'ultimo momento.

Spesso i motivi dei fornitori renitenti non sono chiari. I fornitori sospettati dalle autorità di perseguimento penale di agire d'intesa con le persone sospettate non vengono neanche contattati. «In questi casi», aggiunge il responsabile del team Casi speciali, «cerchiamo di raggiungere l'obiettivo attraverso una via alternativa». Egli non svela cosa succede concretamente se non è possibile accedere direttamente all'infrastruttura di un fornitore, ma aggiunge «Una cosa posso garantirla: non ci arrendiamo mai».

Gli interventi del team Casi speciali riguardano di norma la sorveglianza in tempo reale. Per il team questo significa che il lavoro è terminato soltanto quando i dati della comunicazione possono essere trasmessi immediatamente e senza intoppi al sistema di trattamento del Servizio SCPT.

Verso le ore 15.00 ci siamo. Il gruppo raccoglie i propri strumenti e li riporta nel minivan. Presso il fornitore lasciano una scatola poco appariscente: lo *special case server*, che registra il traffico dei dati e delle comunicazioni della persona sospettata.

Ora tocca intervenire agli inquirenti coinvolti e al pubblico ministero responsabile.

La grande ristrutturazione

La componente di sorveglianza in tempo reale del sistema di trattamento STT deve essere sostituita. Nell'estate 2021 sono iniziati i lavori per l'implementazione della Federal Lawful Interception Core Component (FLICC).

Quando il procuratore capo Urs Hubmann usa l'abbreviazione COI non intende il Comitato olimpico internazionale, bensì la criminalità organizzata italiana. «Al momento rappresenta una delle grandi minacce per la nostra sicurezza interna».

Dal 2011 il giurista 65enne è a capo della Procura II (Staatsanwaltschaft II; STA II) del Cantone di Zurigo e si occupa in particolar modo di quella che gli specialisti del settore chiamano «criminalità sommersa». Non indaga su denuncia bensì in presenza di un sospetto. L'obiettivo è raccogliere, mediante misure coercitive segrete, le prove che permettono di portare i sospettati in giudizio.

«La criminalità organizzata italiana rappresenta una delle più grandi minacce per la nostra sicurezza interna.»

Urs Hubmann, procuratore capo del Cantone di Zurigo

Rapina aggravata, traffico di droga e tratta di esseri umani

Le indagini si concentrano su casi di grave criminalità organizzata commessi in banda. I reati comprendono la rapina aggravata, il traffico qualificato di droga, la tratta di esseri umani, gravi casi di riciclaggio di denaro e la cibercriminalità qualificata.

Per indagare su questi reati, la STA II ha a disposizione tutta una serie di strumenti efficaci. Oltre agli agenti sotto copertura, all'analisi delle transazioni finanziarie, all'installazione di microfoni e telecamere, ne fa parte anche la cosiddetta *lawful interception* (LI), la sorveglianza del traffico delle telecomunicazioni conforme alla legge, sia in tempo reale che retroattiva.

La sorveglianza in tempo reale permette agli inquirenti di sapere dove si muove la persona sospettata e cosa sta discutendo con il suo interlocutore. Nel 2022 la STA II ha eseguito quasi 200 sorveglianze in tempo reale, il che corrisponde a circa il 20 per cento del totale di tali sorveglianze in Svizzera.

Tecnicamente le sorveglianze si svolgono mediante l'*Interception System Schweiz* (ISS), la componente di sorveglianza in tempo reale del sistema di trattamento STT del Servizio SCPT. «La piattaforma è stata introdotta nel 2013 ed è ormai sorpassata», spiega Ernesto Ruggiano, capoprogetto nel Servizio SCPT e responsabile per la sostituzione dell'ISS con la nuova *Federal Lawful Interception Core Component* (FLICC). Il progetto è stato avviato cinque anni fa. La fase di implementazione è iniziata nell'estate 2021.

La STA II vorrebbe disporre della FLICC il più presto possibile, principalmente per via dell'evoluzione tecnica nell'industria delle telecomunicazioni. Allo stato attuale della tecnica, si pensi alla tecnologia di rete mobile 5G, l'ISS non è più adatto alla sorveglianza del traffico delle telecomunicazioni. «L'analisi di un'unica attività di sorveglianza – ad esempio di una breve telefonata – è onerosa e dura parecchio tempo», spiega Urs Hubmann.

A questo si aggiunge un comportamento mutato nella comunicazione. Anche i criminali discutono di cose insignificanti e quindi gli inquirenti si trovano di fronte a un flusso di dati enorme.

La sorveglianza in tempo reale di comunicazioni orali e scritti dovrebbe essere disponibile a partire dalla metà del 2023. Successivamente sarà integrata la sorveglianza dei dati di Internet e delle e-mail e infine si passerà a quelle che si potrebbero chiamare le rifiniture interne: l'integrazione di nuove funzionalità avanzate.

«Provvediamo affinché la sorveglianza in tempo reale si affermi come strumento d'indagine moderno ed efficiente.»

Ernesto Ruggiano, capoprogetto FLICC, Servizio SCPT

Visualizzazione e trascrizione automatica

Di queste nuove funzionalità fanno ad esempio parte la visualizzazione chiara dei risultati della sorveglianza oppure la trascrizione automatica dei messaggi orali con l'opzione della traduzione, o ancora la localizzazione precisa delle apparecchiature sorvegliate. «Con la FLICC provvediamo affinché la sorveglianza in tempo reale si affermi come strumento d'indagine moderno, semplice da gestire ed efficiente», sostiene Ernesto Ruggiano.

Tra il 2016 e il 2022 il numero di sorveglianze in tempo reale in Svizzera è diminuito da 2800 a poco più di 1200. Tale riduzione è in parte dovuta al fatto che i procedimenti in cui la sorveglianza in tempo reale svolge un ruolo come mezzo di prova diventano sempre più complessi e richiedono sempre più conoscenze specialistiche. Con la FLICC s'intende migliorare la situazione.

Gli esperti concordano che un'alta pressione investigativa impedisce alla criminalità grave e organizzata di insediarsi nella società. Il perseguimento coerente dei corrispondenti reati impedisce in particolare che le bande criminali affrontino i loro conflitti interni in pubblico e che in caso di ricorso alla violenza siano danneggiati terzi.

«Eccessi di violenza in strada ci sono noti soprattutto dall'estero», afferma Hubmann, «dobbiamo assolutamente provvedere affinché non si diffondano anche in Svizzera».

«La Svizzera è un obiettivo interessante.»

Sulle tracce di spie, terroristi e cibercriminali: Jürg Bühler è vicedirettore del Servizio delle attività informative della Confederazione.*

Signor Bühler, Lei è un lettore assiduo di giornali?
Io personalmente non lo sono. Ma fondamentalmente tutti i contenuti pubblicati dai giornali svizzeri o esteri possono contenere informazioni rilevanti per un servizio come il nostro. Si tratta di cosiddette informazioni *open source*, che il Servizio delle attività informative della Confederazione (SIC) raccoglie e analizza sistematicamente. In tal modo dispongo di una buona panoramica delle notizie importanti.

Da quali altre fonti trae il SIC le sue informazioni?
Ce ne sono tante. Sostanzialmente abbiamo la possibilità di raccogliere informazioni rilevanti presso tutte le unità amministrative federali e cantonali. E, per mezzo della cooperazione con i Cantoni, anche presso i Comuni.

Non sembra un lavoro molto appassionante …
Lavoriamo anche con la cosiddetta *human intelligence*, ossia con fonti umane contattate dai nostri agenti responsabili. Questi intrattengono contatti con persone che hanno accesso a informazioni rilevanti per l'adempimento del mandato del SIC. Gli agenti responsabili delle fonti corrispondono all'idea che il pubblico ha di un «agente segreto». Altre fonti di informazione sono i servizi omologhi internazionali e quelli dei Cantoni.

Quanti agenti responsabili delle fonti impiega il SIC?
Forniamo questi dati soltanto ai nostri organi di vigilanza.

La controparte della human intelligence è la signal intellegence. Che cos'è?
Si tratta dell'individuazione di segnali tecnici, di regola segnali di strumenti di comunicazione. Ne fa ad esempio parte l'esplorazione di segnali radio dall'estero o di satelliti nello spazio. A ciò si aggiunge l'esplorazione di segnali via cavo: a determinate condizioni abbiamo la possibilità di intercettare flussi di dati transfrontalieri e di analizzarli secondo criteri di ricerca rientranti nel nostro mandato legale, ad esempio determinati nomi, progetti o elementi d'indirizzo della telecomunicazione quali i numeri di telefono.

* L'intervista con Jürg Bühler è stata condotta nel dicembre 2021 prima dello scoppio della guerra in Ucraina.

Questo ci porta al tema della cosiddetta lawful interception (LI) e al Servizio SCPT. Qual è l'importanza della sorveglianza del traffico delle telecomunicazioni per il lavoro del SIC?

La sorveglianza ci fornisce informazioni che non possiamo raccogliere in altro modo. Nel 2022 il SIC ha condotto due operazioni in cui ha fatto ricorso a questa misura soggetta ad autorizzazione: una nell'ambito della prevenzione del terrorismo, l'altra riguardante attività di spionaggio.

Nel 2022 sono state effettuate circa 10 250 sorveglianze del traffico delle telecomunicazioni, di cui 95 ordinate dal SIC. Come mai così poche?

Le condizioni legali per il ricorso a misure di sorveglianza sono molto severe per il SIC. Per una misura di LI dobbiamo presentare una domanda al Tribunale amministrativo federale. Se quest'ultimo approva la misura è necessario il nullaosta del capo del DDPS, che prima deve sentire i capi del DFAE e del DFGP. Solo dopo il nullaosta possiamo avviare la misura.

Uno dei padri fondatori del Servizio SCPT

Jürg Bühler è membro della direzione del Servizio delle attività informative della Confederazione (SIC) sin dalla sua creazione nel 2010 ed è al servizio della Confederazione nel settore della polizia e delle attività informative sin dagli anni Novanta. Ha assistito alla sorveglianza delle telecomunicazioni all'epoca del monopolio delle PTT, allora effettuata separatamente nei singoli circondari regionali della telecomunicazione: «Del compito si occupavano donne specializzate che ascoltavano in cuffia e mettevano a verbale i dialoghi rilevanti». In seguito, la liberalizzazione dei servizi di telecomunicazione pose il legislatore di fronte a una duplice sfida: in primo luogo doveva definire gli obblighi dei fornitori privati; in secondo luogo, andava creato un servizio indipendente dai fornitori cui conferire il compito sovrano della sorveglianza delle telecomunicazioni. Bühler, oggi 58enne, era all'epoca capo delle indagini di polizia giudiziaria della polizia federale: «in un gruppo di lavoro nazionale abbiamo elaborato, d'intesa con il servizio giuridico della Telecom PTT, proposte per un servizio di sorveglianza gestito dalla Confederazione». Il risultato fu il Servizio per compiti speciali (SCS) che iniziò la sua attività il 1° gennaio 1998. Esattamente dieci anni dopo, il SCS passò dal DATEC al DFGP e assunse il nome attuale di Servizio SCPT.

«I ciberattacchi qualificati sono quasi tutti transfrontalieri.»

Jürg Bühler, vicedirettore SIC

Anche se sussiste il sospetto che sia a rischio la sicurezza della Svizzera?
Questa è comunque una condizione che deve essere soddisfatta per applicare le suddette misure. In seguito all'analisi del cosiddetto scandalo delle schedature negli anni Novanta, il legislatore ha consapevolmente limitato il margine di manovra dell'ex Servizio informazioni in Svizzera. Fino all'entrata in vigore della legge federale sulle attività informative nel settembre 2017, in Svizzera ci era vietato sorvegliare il traffico delle telecomunicazioni. Da allora sfruttiamo questa possibilità, ma in misura molto minore di quanto temuto all'epoca dagli avversari della legge. Lo dimostrano le statistiche che pubblichiamo annualmente.

Uno dei compiti principali del SIC è il controspionaggio. Chi svolge attività di spionaggio contro la Svizzera?
Stimiamo che soggiornino durevolmente in Svizzera varie migliaia di collaboratori di servizi segreti esteri. Nelle rappresentanze diplomatiche di certi Paesi – non voglio fare nomi – circa un quarto dei collaboratori è incaricato di compiti legati all'attività informativa.

La Svizzera è così importante per i paesi esteri?
La Svizzera è un paese di alta tecnologia e in quanto tale un obiettivo interessante per lo spionaggio economico. Inoltre, Ginevra ospita molte istituzioni dell'ONU. In quanto Stato sede di organizzazioni internazionali abbiamo il dovere di impedire attività di spionaggio politico nei confronti di terzi che si trovano sul nostro territorio. Questo significa che il SIC raccoglie e analizza anche informazioni relative alle operazioni in Svizzera di un governo estero contro organizzazioni non governative, minoranze etniche o gruppi di opposizione.

Veniamo alla prevenzione del terrorismo: l'anno scorso tre misure di sorveglianza del traffico delle telecomunicazioni hanno riguardato questo ambito. Quali sono le priorità del SIC?
Al momento il cosiddetto «Stato islamico».

Quali gruppi di persone rappresentano un pericolo?
In Svizzera il pericolo è rappresentato, da una parte, da persone che si sono radicalizzate qui e che s'ispirano alla propaganda jihadista e a persone del loro ambiente; dall'altra, anche da persone la cui radicalizzazione e violenza è legata a crisi personali o problemi psichici. Entrambi i gruppi possono compiere attacchi, soprattutto su bersagli vulnerabili. I terroristi che entrano in Svizzera dall'estero con l'incarico di attacchi mirati sono più pericolosi. Osserviamo che in parte i due gruppi cooperano: i terroristi che arrivano dall'estero cercano di reclutare e istruire le persone residenti in Svizzera.

La forma di minaccia della sicurezza nazionale più presente nell'opinione pubblica è probabilmente quella dei ciberattacchi a istituzioni pubbliche quali ospedali o infrastrutture dell'approvvigionamento elettrico. Le vostre informazioni corrispondono a questa valutazione?
Il numero dei ciberattacchi contro obiettivi militari e civili è in progressivo aumento in tutto il mondo. Questi attacchi costituiscono una minaccia anche per la Svizzera, con il suo elevato grado di digitalizzazione dell'infrastruttura.

Il SIC è in grado di affrontare questa minaccia proveniente dal ciberspazio?
Il nostro settore «Ciber» ha il compito di riconoscere e prevenire tempestivamente gli attacchi ai sistemi informatici delle infrastrutture critiche. Bisogna però osservare che la base legale delle nostre attività è entrata in vigore più di cinque anni fa. Durante le deliberazioni parlamentari alla vigilia della votazione popolare dell'autunno 2016 i pericoli provenienti dal ciberspazio sembravano ancora limitati e il Parlamento e il Popolo hanno giudicato di elevata priorità la protezione della sfera privata. Pertanto, prima di poter sorvegliare attività sospette – sia mediante GovWare che mediante il Servizio SCPT – dobbiamo essere in grado di dimostrare che la sicurezza nazionale è minacciata in modo grave e imminente. Ma proprio questo ci causa difficoltà.

Come mai?
Perché gli attacchi qualificati sono quasi tutti transfrontalieri. L'ultimo obiettivo di un ciberattacco si trova quasi sempre al di là del confine nazionale. Questo significa che i ciberattacchi per i quali vengono usate in modo abusivo infrastrutture in Svizzera sono diretti contro istituzioni all'estero e quindi non rappresentano una minaccia diretta per la Svizzera ai sensi della legge. Ciononostante la loro individuazione è importante per poter proteggere la Svizzera da attacchi.

Come affrontano gli attacchi transfrontalieri i servizi delle attività informative dei nostri paesi limitrofi?
I nostri paesi limitrofi sono stati di diritto. Anche loro interpretano in modo relativamente restrittivo il concetto di «minaccia nazionale». Di conseguenza, anche a loro mancano in parte le basi legali per individuare e prevenire eventuali preparativi per attacchi su obiettivi in Svizzera. Poiché si tratta di un problema strutturale che gli autori degli attacchi sfruttano in modo mirato, esso va affrontato a livello sia nazionale che internazionale.

La Svizzera ha già intrapreso passi in questa direzione?
La legge federale sulle attività informative è attualmente in revisione. Si prevede di introdurre come motivo per l'impiego di misure di raccolta di informazioni soggette ad autorizzazione anche la minaccia di importanti interessi di sicurezza internazionali. Questo estenderebbe anche le possibilità nel settore dei ciberattacchi.

03

CIFRE E FATTI

Motivi della sorveglianza

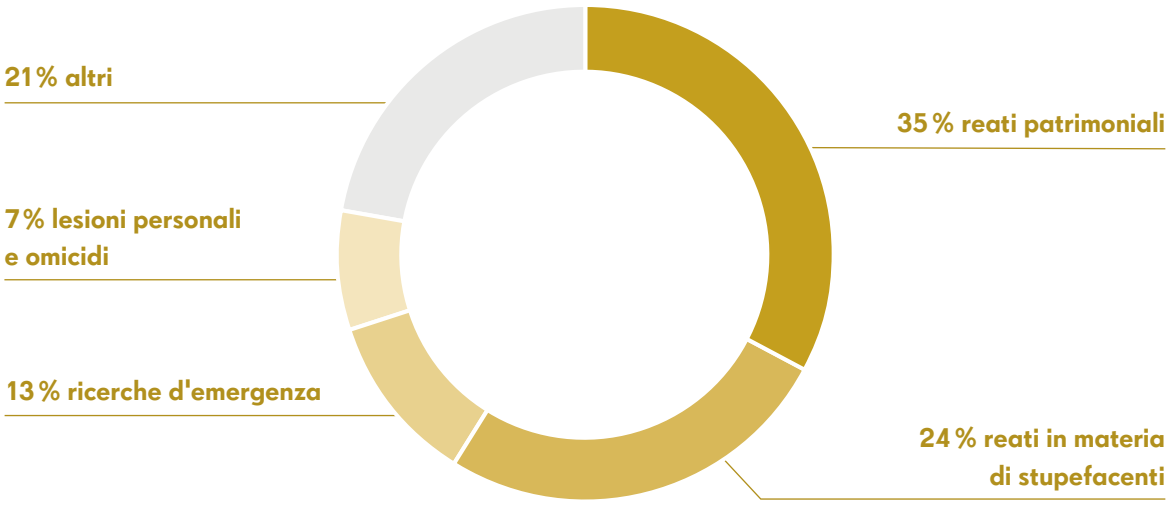
Secondo la Statistica criminale di polizia, nel 2022 in Svizzera sono stati notificati 549 404 reati. Ai fini del loro perseguimento in 10 253 casi, un numero relativamente esiguo, si è fatto ricorso alla misura investigativa della sorveglianza del traffico delle telecomunicazioni.

Va inoltre osservato che per un reato o una misura di acquisizione soggetta ad autorizzazione possono essere ordinate diverse sorveglianze, ad esempio perché possono essere sorvegliati sia il telefono fisso sia i cellulari del presunto autore. Spesso più persone obbligate a collaborare sono incaricate di sorvegliare gli stessi numeri di cellulare al fine di poter coprire tutti i casi di roaming. Il numero delle persone direttamente interessate da misure di sorveglianza è di conseguenza nettamente inferiore a quello delle misure di sorveglianza disposte.

Nella maggior parte dei casi la sorveglianza è stata disposta in relazione a reati patrimoniali (35%). Al secondo posto (24%) si trovano le violazioni della legge sugli stupefacenti e al quarto posto (7%) i reati contro la vita e l'integrità della persona.

La sorveglianza del traffico delle telecomunicazioni può essere disposta anche per cercare persone disperse. Le ricerche d'emergenza si trovano al terzo posto (13%).

Per ulteriori informazioni sulle statistiche si rimanda al sito
www.li.admin.ch / it / stats



Definizione e numero di misure di sorveglianza e tipi di informazione

Sorveglianza in tempo reale (1)
Nella sorveglianza in tempo reale i dati della corrispondenza postale e del traffico delle telecomunicazioni vengono trasmessi alle autorità di perseguimento penale simultaneamente, con un leggero ritardo o periodicamente mediante il sistema di trattamento.

Sorveglianza retroattiva (2)
Nella sorveglianza retroattiva si reperiscono soprattutto prove dei collegamenti per sapere, ad esempio, chi ha telefonato con chi, quando, dove e per quanto tempo.

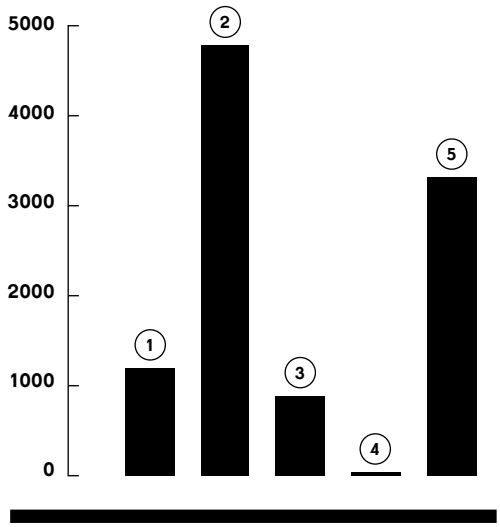
Ricerca d'emergenza (3)
La ricerca d'emergenza viene disposta, ad esempio, per localizzare e salvare escursionisti vittime di incidente o bambini scomparsi.

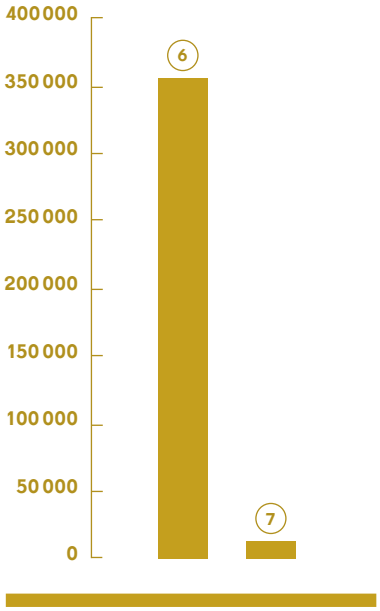
Ricerca di condannati (4)
Nel quadro della ricerca di condannati, le autorità inquirenti possono individuare persone condannate a una pena detentiva o nei cui confronti è stata disposta una misura privativa della libertà con una sentenza cresciuta in giudicato.

Ricerca per copertura delle antenne (5)
Nella ricerca per copertura delle antenne l'interesse si concentra su una cella radio o un punto d'accesso WLAN pubblico. Vengono registrate tutte le comunicazioni, i tentativi di comunicazione e gli accessi alla rete in un determinato periodo.

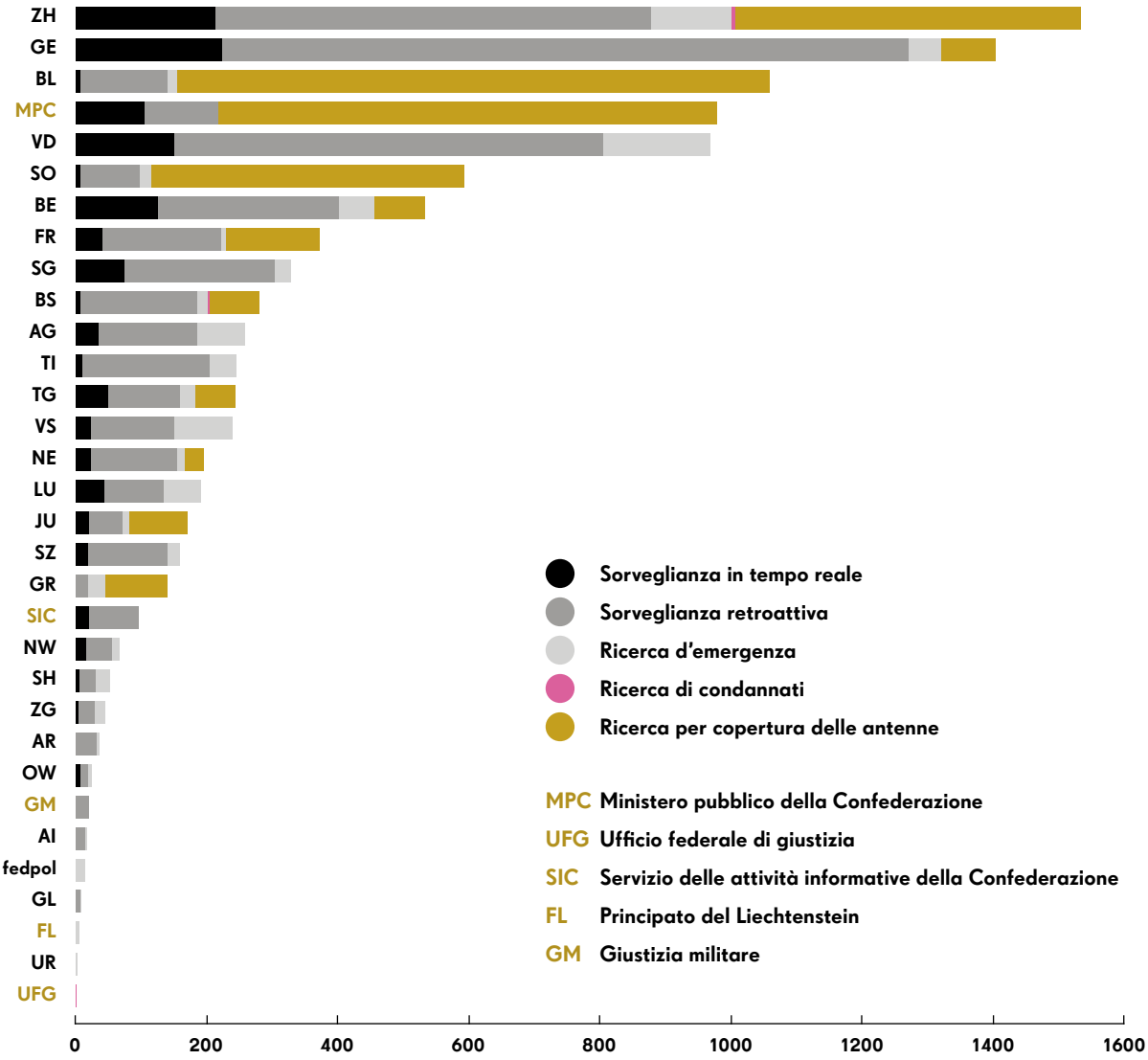
Informazioni semplici (6)
Le informazioni semplici forniscono informazioni di base sui collegamenti di telecomunicazione, in particolare a quale abbonato è attribuito un determinato numero di telefono o un indirizzo IP.

Informazioni complesse (7)
Le informazioni complesse forniscono informazioni più dettagliate sui collegamenti di telecomunicazione, come p.es. copie di contratti e documenti d'identità.





Mandati per Confederazione, Cantoni e Liechtenstein

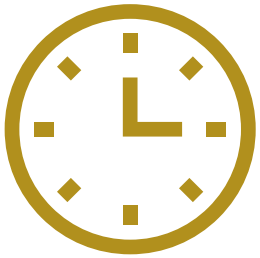


Ordini di sorveglianza dell'Ufficio federale di giustizia
La legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT) prevede la sorveglianza non solo per i procedimenti penali in corso in Svizzera. Le misure corrispondenti possono essere eseguite anche in esecuzione di una richiesta di assistenza giudiziaria presentata da autorità straniere. L'Ufficio federale di giustizia (UFG) è responsabile dei casi di assistenza giudiziaria.

Numero di domande dei cittadini

24

Servizi di pronto intervento effettuati



870

Utenti registrati sistema di trattamento

WMC 2400
Warrant Management Component (gestione dei mandati)

IRC 4300
Information Request Component (informazioni)

RDC 2200
Retained Data Component (sorveglianze retroattive)

ISS 2450
Interception System Schweiz (sorveglianze in tempo reale)

Numero di casi speciali

83

(cfr. pag. 8 / 9, parte Provider Management e p. 15 – 19, una squadra per interventi speciali)

Numero di domande dei media

2

Conto economico Servizio SCPT in CHF

Ricavi complessivi
12,4 mio.

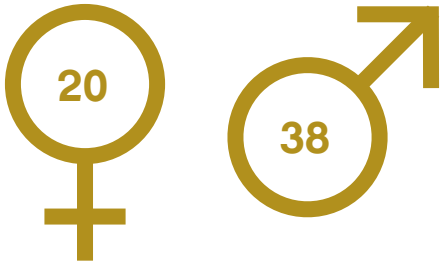
Costi complessivi
31,7 mio.

Contributo di copertura Confederazione
19,3 mio.

Numero di collaboratori

58

Quota di uomini e donne



Età media

46,5

Distribuzione linguistica

67 % Tedesco

6,4 % Italiano

24,5 % Francese

2,1 % Altro

Ripartizione per età

20 – 29 anni
10 %

30 – 39 anni
19 %

40 – 49 anni
26 %

50 – 59 anni
40 %

60 – 69 anni
5 %

«Il lavoro vero e proprio, la creazione della disponibilità a sorvegliare, è svolto dal nostro team Casi speciali.»

Alexandre Suter, capo del settore Provider Management

Colofone

Progetto: Servizio SCPT
Redazione: Servizio SCPT
Collaborazione: ufficio giornalisti JNB, Lucerna
Grafica e realizzazione: Schön & Berger, Zürich
Stampa: Druckerei Ruch, Ittigen
Foto: Lia Lüthi, Barbara Hesse, David Kelly
Font: Minion Pro, Drescher Grotesk
Carta: Z-Offset
Versioni linguistiche: tedesco, francese, italiano e inglese

■

Per una maggiore leggibilità e comprensibilità si è rinunciato a usare una terminologia tecnica e giuridica troppo specialistica. Quando possibile, sono state usate forme di genere neutre. Laddove sono stati usati termini esclusivamente maschili o femminili, essi si riferiscono a entrambi i generi.

Dipartimento federale di giustizia e polizia DFGP
Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni SCPT
3003 Berna