Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia

Segreteria generale DFGP
Servizio d'informazione DFAE

Stato 18 agosto 2014

FAQ - Domande ricorrenti

Dalle statistiche del Servizio SCPT emerge che negli ultimi anni le sorveglianze ordinate dalle autorità inquirenti hanno registrato un netto aumento. Perché?

Il Servizio SCPT sorveglia la corrispondenza postale e il traffico delle telecomunicazioni su ordine delle autorità inquirenti svizzere. In effetti, negli ultimi anni il numero delle sorveglianze è in aumento. Stando alla statistica 2013, negli ultimi cinque anni le misure retroattive – vertenti sull'analisi dei dati del collegamento – sono aumentate di un quarto. Tale crescita è tuttavia inferiore a quella dell'utilizzo di mezzi di telecomunicazione in Svizzera. Tanto per fare un esempio, dal 2008 al 2012 la durata complessiva dei collegamenti è aumentata di un terzo (da ca. 8 000 mio. di minuti a ca. 10 500 mio. di minuti). Il volume dei dati trasmessi per telefonino si è moltiplicato di oltre il fattore venti (da ca. 700 a 16 600 terabyte). Infine il numero dei telefonini in uso è molto più elevato rispetto a pochi anni or sono: dal 2002 è infatti raddoppiato da 5,2 a 10,6 milioni (fonte: Statistica ufficiale sulle telecomunicazioni 2012; Statistica Svizzera; ComCom).

La decisione dell'8 aprile 2014 della Corte di giustizia delle Comunità europee (CGCE) concernente la conservazione dei dati è vincolante per la Svizzera?

No, la Svizzera non ha recepito, nel quadro degli accordi bilaterali con l'UE, la direttiva riguardante la conservazione di dati, che pertanto non è applicabile nel nostro Paese.

La conservazione di dati non riguarda i contenuti delle conversazioni, ma soltanto le informazioni su chi ha partecipato a una comunicazione, quando, dove, per quanto tempo e con quali mezzi tecnici. Queste informazioni possono aiutare a ricostruire in un secondo tempo comportamenti punibili o a individuare il luogo in cui si trovano persone disperse (ricerca di emergenza).

Con la sua decisione, la CGCE esige che la conservazione, l'impiego e l'accesso ai dati marginali siano disciplinati con rigore, senza pertanto vietarla. Queste norme aggiuntive mancano nella direttiva, ma sono previste dal diritto svizzero. Secondo una prima valutazione dell'Ufficio federale di giustizia, la decisione della CGCE non mette dunque neanche indirettamente in discussione la conservazione dei dati marginali. Ciò vale sia per il diritto vigente, sia per la modifica di legge proposta, tesa a prolungare il termine di conservazione da sei a dodici mesi.

Perche la conservazione di dati va ammessa in Svizzera?

In Svizzera, l'ingerenza nei diritti fondamentali costituita dalla conservazione dei dati marginali è limitata allo stretto necessario. Anche se i dati vengono conservati a titolo preventivo senza indizi di reato, la polizia e i ministeri pubblici non possono accedervi incondizionatamente poiché sono custoditi dal pertinente fornitore di servizi di telecomunicazione e non da un organo statale. La legge vincola inoltre l'accesso a numerose severe condizioni, che devono essere adempiute affinché le autorità inquirenti possano consultare i dati. Nelle procedure penali e di assistenza giudiziaria, la sorveglianza può in particolare essere ordinata soltanto in presenza di gravi indizi di delitto o crimine la cui gravità la legittimi. Infine, è necessario che le indagini svolte fino a quel momento non abbiano avuto successo, abbiano poche probabilità di successo o siano ostacolate in maniera sproporzionata. Ai fini della ricerca d'emergenza la sorveglianza è ammessa unicamente in presenza di importanti indizi di un grave pericolo per la salute o la vita della persona dispersa. L'adempimento di queste condizioni è verificato d'ufficio da un giudice in ogni singolo caso. La sorveglianza non è svolta in segreto, ma comunicata alla persona interessata assieme ai motivi, al tipo e alla durata, al più tardi al termine della procedura preliminare.

Quali ripercussioni avrebbe la rinuncia alla conservazione dei dati?

Rinunciare alla conservazione dei dati ostacolerebbe il perseguimento dei reati provocando quindi ripercussioni indesiderate sulla sicurezza pubblica. La polizia non potrebbe più analizzare le tracce telefoniche o elettroniche, che si tratti di cibercriminalità, di pedopornografia, di traffico di stupefacenti, di omicidio, di reati patrimoniali o di terrorismo. Senza la conservazione dei dati sarebbe pure più difficile cercare le persone disperse e condannate: sarebbe per esempio arduo ricostruire da dove una persona ha telefonato l'ultima volta.

In quali casi possono essere impiegati i cosiddetti cavalli di troia (GovWare o Government Ware) e da chi?

Il Consiglio federale ha deciso di creare una base legale univoca per l'impiego di GovWare, ammessi soltanto per un elenco di reati gravi più ristretto rispetto a quello della tradizionale sorveglianza postale e del traffico delle comunicazioni (art. 269 segg. CPP). Si tratta di reati che giustificano indagini sotto copertura («inchiesta mascherata», art. 286 cpv. 2 CPP). L'impiego sarà esplicitamente limitato alla sorveglianza del traffico delle telecomunicazioni. Ne restano pertanto escluse le perquisizioni online dei computer oppure ad esempio la sorveglianza di un locale mediante un microfono o la telecamera di un computer. L'impiego deve essere ordinato dal pubblico ministero e approvato dal giudice delle misure coercitive.

Perché i cavalli di troia o GovWare sono necessari?

I GovWare sono necessari affinché il perseguimento penale dei criminali possa tenere il passo con gli sviluppi tecnologici. Non si tratta di sorvegliare, né tantomeno di «ficcanasare» o perquisire un computer a titolo preventivo. Le autorità inquirenti devono però disporre dei mezzi necessari per perseguire i reati gravi. Altrimenti i criminali potrebbero servirsi delle moderne tecnologie di telecomunicazione, senza che le autorità possano competere: i narco-

trafficanti potrebbero, ad esempio, servirsi della telefonia Internet codificata per i loro affari, certi di non essere sorvegliati.

Quali misure adottano le autorità inquirenti per rendere l'impiego di GovWare il più sicuro possibile e per impedire gli abusi?
Per impedire un abuso di GovWare è necessaria una combinazione di provvedimenti tecnici e organizzativi. Le misure tecniche sono le seguenti: le autorità inquirenti definiscono le necessarie funzioni di sicurezza, mentre un organo indipendente verifica che tali funzioni siano complete e che siano state impiantate secondo gli standard riconosciuti. In ambito organizzativo, invece, le autorità descrivono una procedura dettagliata per l'impiego e l'esercizio di GovWare, definendo tra l'altro i diritti delle persone coinvolte o la gestione del sistema informatico. Infine, una verbalizzazione completa garantisce la tracciabilità, anche per i giudici, di tutte le fasi, dalla domanda alla conclusione della sorveglianza, passando per l'autorizzazione. Queste misure riducono fortemente le probabilità di un abuso di GovWare. Le informazioni derivanti da una sorveglianza telefonica sono ammesse come prove giudiziarie unicamente se la sorveglianza era stata ordinata e autorizzata correttamente anche per l'assunzione di tali prove.

Sembrerebbe che il Dipartimento federale di giustizia e polizia (DFGP) e il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) intendano acquisire e impiegare congiuntamente i programmi informatici di GovWare. Queste affermazioni sono corrette? Sono già in corso preparativi in tal senso?

Il DFGP e il DDPS non hanno alcuna intenzione di acquisire o impiegare GovWare congiunti e pertanto una tale collaborazione non è in fase di preparazione.

Le preoccupazioni per uno «Stato ficcanaso» e i timori di ingerenze nella sfera privata sono veramente ingiustificati?
Sì, poiché non è ammesso sorvegliare le conversazioni telefoniche e le attività in Internet a titolo preventivo, come un servizio segreto. La sorveglianza è possibile unicamente se è stato avviato un procedimento penale per un reato grave e va sempre autorizzata da un giudice. Dalle statistiche emerge che la sorveglianza è attivata nell'1,5 per cento dei casi di reato. Concretamente, nel 2013, a 725 678 reati hanno fatto fronte 10 860 sorveglianze; in questo contesto va osservato che sovente diverse sorveglianze riguardano un unico reato, ad esempio se devono essere sorvegliati la rete fissa e vari cellulari di uno spacciatore.

A che punto è l'introduzione del cosiddetto Interception System Svizzera (ISS)? Non andrebbe anzitutto portata a termine la revisione della legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT)?
Il Servizio Sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni gestisce un sistema d'informazione tramite il quale, se le condizioni legali sono adempiute, fornisce alle autorità inquirenti i dati dei fornitori di prestazioni di telecomunicazione. Questo sistema è ormai obsoleto e viene dunque sostituito con l'ISS, che soddisfa i requisiti legali vigenti e comprende funzionalità corrispondenti a quelle del sistema attuale. Quando la LSCPT riveduta entrerà in vigore sarà possibile adeguare il nuovo sistema informatico ai

nuovi requisiti. Secondo la pianificazione attuale, d’intesa con i fornitori di collegamenti di telefonia e Internet e le autorità inquirenti, l’ISS sarà operativo a partire dal primo semestre del 2015.