KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI

Rapporto annuale 2012

PREFAZIONE

del consigliere di Stato Neuhaus, presidente del comitato direttivo dello SCOCI

Dove c'è molta luce, c'è anche molta ombra. Queste ombre si addensano anche nelle aree difficilmente accessibili della rete, in cui si aggirano senza scrupoli i cibercriminali. È proprio in queste zone d'ombra che il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI) è chiamato a far luce, intervenendo direttamente per smascherare i criminali e contribuire ad assicurarli alla giustizia. In veste di centro di contatto nazionale per le persone che intendono segnalare la presenza di contenuti sospetti su Internet, lo SCOCI sta purtroppo registrando un vero e proprio record di segnalazioni. Nel 2012 il numero di comunicazioni pervenute è cresciuto del 55 per cento rispetto all'anno precedente. Per la prima volta le comunicazioni concernenti i reati economici (37 %) hanno superato le comunicazioni relative a casi di pornografia illegale (33 %).

Lo SCOCI continua ad assolvere i propri compiti principali in modo competente, senza tuttavia rinunciare a esplorare nuove strade. Nel 2012 si è tenuto il primo forum sulla collaborazione tra i pubblici ministeri e lo SCOCI in materia di cibercriminalità. L'evento era inteso tra l'altro a eliminare le eventuali incertezze dei pubblici ministeri riguardo alla criminalità su Internet e all'utilizzo delle risorse tecnologiche.

Inoltre, lo SCOCI non si limita soltanto a ricevere e a trattare le segnalazioni inviate dalla popolazione, ma opera anche nelle aree meno accessibili della rete, contribuendo alla prevenzione dei reati. Ogni anno il comitato direttivo dello SCOCI stabilisce un nuovo settore su cui incentrare le ricerche attive. Analogamente agli anni precedenti, anche nel 2012 la priorità è stata data alla lotta alla pedocriminalità su Internet. Tuttavia, nel quadro della definizione di tali priorità, il comitato direttivo ha dichiarato espressamente che lo SCOCI non deve escludere dalle proprie ricerche i reati economici e la criminalità su Internet in senso stretto. Questa strategia trova conferma nei dati rilevati nel 2012. Infatti, lo SCOCI e le sue attività sono diventati un elemento imprescindibile per la lotta alla cibercriminalità.

Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI)
Nussbaumstrasse 29
3003 Berna
www.scoci.ch
www.cybercrime.ch

Pubblicato il: 23 aprile 2013

Indice

1. L’essenziale in breve

- Nel 2012 sono pervenute allo SCOCI complessivamente 8242 comunicazioni tramite l’apposito modulo online, ovvero il 55 per cento in più rispetto all’anno precedente.

- Il 39 per cento delle comunicazioni pervenute ha riguardato reati contro il patrimonio. Per la prima volta la percentuale di comunicazioni concernenti i reati economici ha superato pertanto quella delle segnalazioni relative alla pornografia vietata (33 %), il cui numero è cresciuto comunque sensibilmente rispetto all’anno precedente.

- 383 comunicazioni sono scaturite in dossier su casi sospetti che sono stati direttamente trasmessi, in virtù della loro rilevanza penale, alle autorità e organizzazioni nazionali o estere.

- Le ricerche attive nelle reti *peer to peer* hanno permesso allo SCOCI di identificare 417 persone coinvolte nello scambio attivo di file dai contenuti pedopornografici.

- Le indagini preliminari sotto copertura condotte dallo SCOCI, in 33 casi sono scaturite in denunce penali trasmesse ai Cantoni competenti.

- La raccolta nazionale di file e valori hash (RNFVH) è entrata in funzione nell’ottobre 2012 a seguito della conclusione positiva degli ultimi test e delle modifiche di sistema necessarie.

- Il 27 giugno 2012 il Consiglio federale ha approvato la «Strategia nazionale per la protezione della Svizzera contro i rischi informatici», cui lo SCOCI ha collaborato attivamente. Con la Strategia il Consiglio federale, in collaborazione con le autorità, il mondo dell’economia e i gestori di infrastrutture critiche, intende minimizzare i rischi informatici ai quali sono esposti quotidianamente.

2. Lo SCOCI, il centro di contatto nazionale

Lo SCOCI funge da centro di contatto nazionale per le persone che intendono segnalare la presenza di contenuti sospetti su Internet. Dopo un primo esame e dopo aver messo al sicuro i dati, lo SCOCI trasmette le segnalazioni di rilevanza penale pervenute tramite l'apposito modulo online alle competenti autorità di perseguimento penali nazionali o estere.

2.1 Comunicazioni pervenute

Nel 2012 sono pervenute allo SCOCI **8242 comunicazioni** tramite l'apposito modulo online. Si tratta di un aumento considerevole pari al 55 per cento rispetto all'anno precedente (5330 segnalazioni). L'evoluzione del numero di segnalazioni pervenute non consente di trarre conclusioni in merito allo sviluppo effettivo della criminalità su Internet o ai contenuti illegali diffusi in rete. Le statistiche forniscono piuttosto delle indicazioni sulla propensione della popolazione a segnalare eventuali casi di cibercriminalità e su come vengono percepiti dalla società.

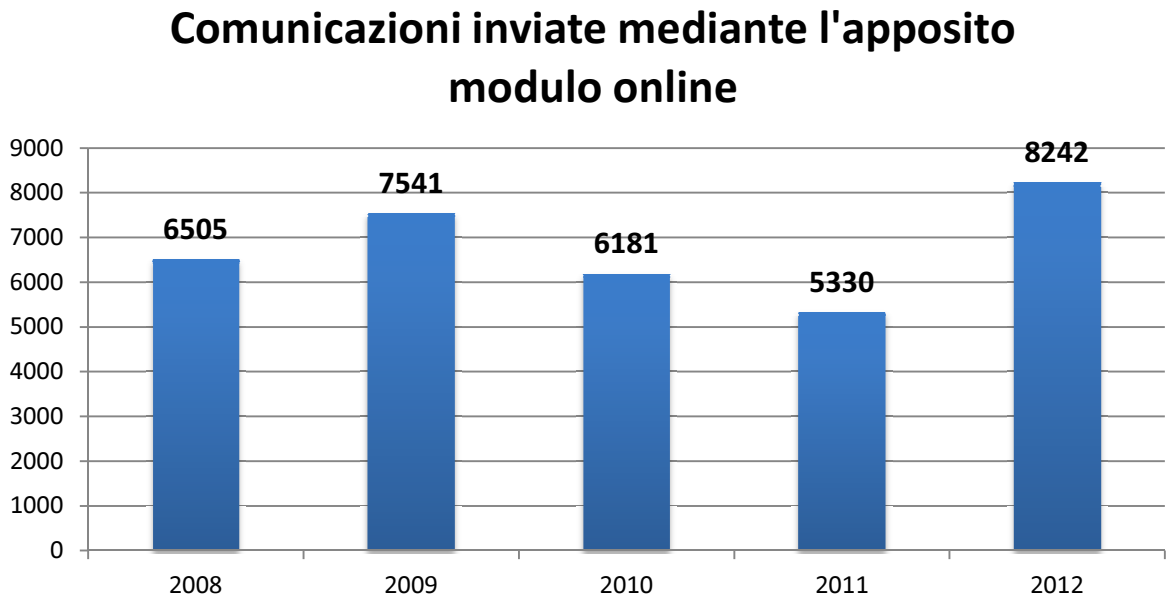


Grafico 1: Comunicazioni pervenute tramite www.scoci.ch – dati annuali

È ipotizzabile che l'aumento delle comunicazioni inviate tramite il modulo online sia dovuto in parte dal risalto dato dai media ad alcune vicende come pure dalla continua diffusione da parte dello SCOCI di avvisi rivolti alla popolazione.

Il numero di comunicazioni pervenute è rimasto costante nei primi mesi del 2012. Per contro, nei mesi estivi e autunnali una serie di casi concreti e limitati nel tempo hanno interessato diversi cittadini, contribuendo all'aumento del numero complessivo di segnalazioni (cfr. grafico 2).

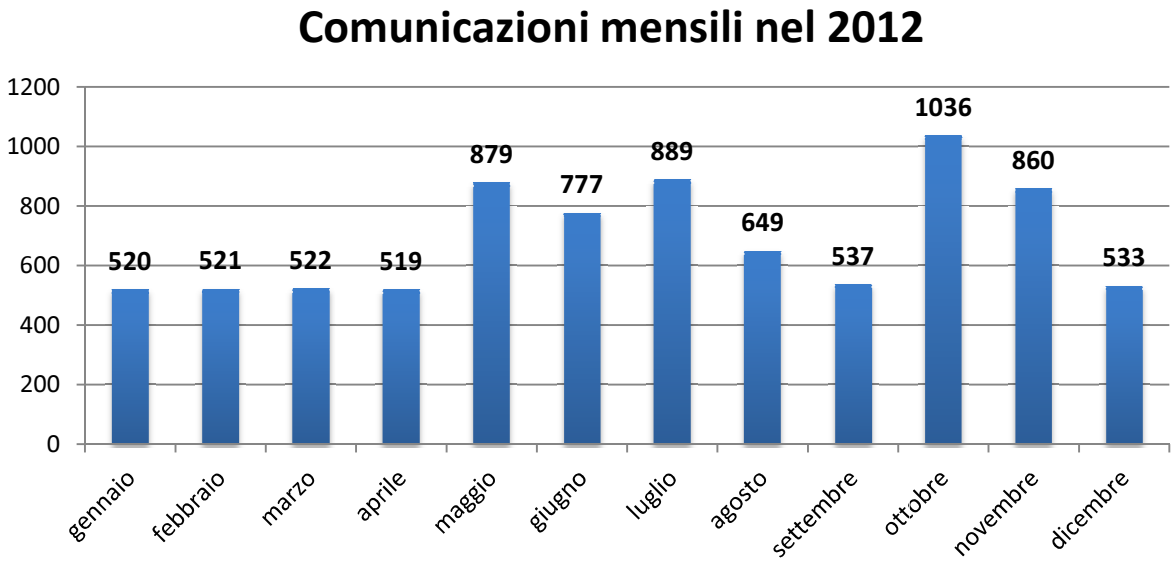


Grafico 2 : Comunicazioni pervenute tramite il modulo online – dati mensili (totale: 8242)

2.2 Contenuto delle comunicazioni

Le comunicazioni inviate allo SCOCI tramite l'apposito modulo online sono di varia natura e presentano di norma una buona qualità. Oltre l'80 per cento delle comunicazioni pervenute nel 2012 (6639 segnalazioni) presentavano una rilevanza penale. Tra i reati più frequentemente segnalati vi sono la pornografia illegale, le rappresentazioni di atti di cruda violenza, il razzismo, l'estremismo, i delitti contro l'onore, le minacce, il *phishing*, le truffe, l'accesso indebito a sistemi informatici, il danneggiamento di dati e l'abuso di un impianto per l'elaborazione di dati. Un numero elevato di segnalazioni ha riguardato reati punibili a querela di parte, che richiedono una denuncia da parte della persona interessata. In tali casi, lo SCOCI invita a rivolgersi all'autorità di polizia localmente competente.

Per la prima volta dall'istituzione dello SCOCI nel 2003, la maggior parte delle comunicazioni ha riguardato reati contro il patrimonio (art. 137–172ter CP). Questo dato conferma la tendenza di crescita registrata negli ultimi anni. È rimasto stabile invece l'elevato numero di segnalazioni concernenti reati contro l'integrità sessuale (art. 187–212 CP).

Percentuali delle comunicazioni pervenute suddivise per categoria

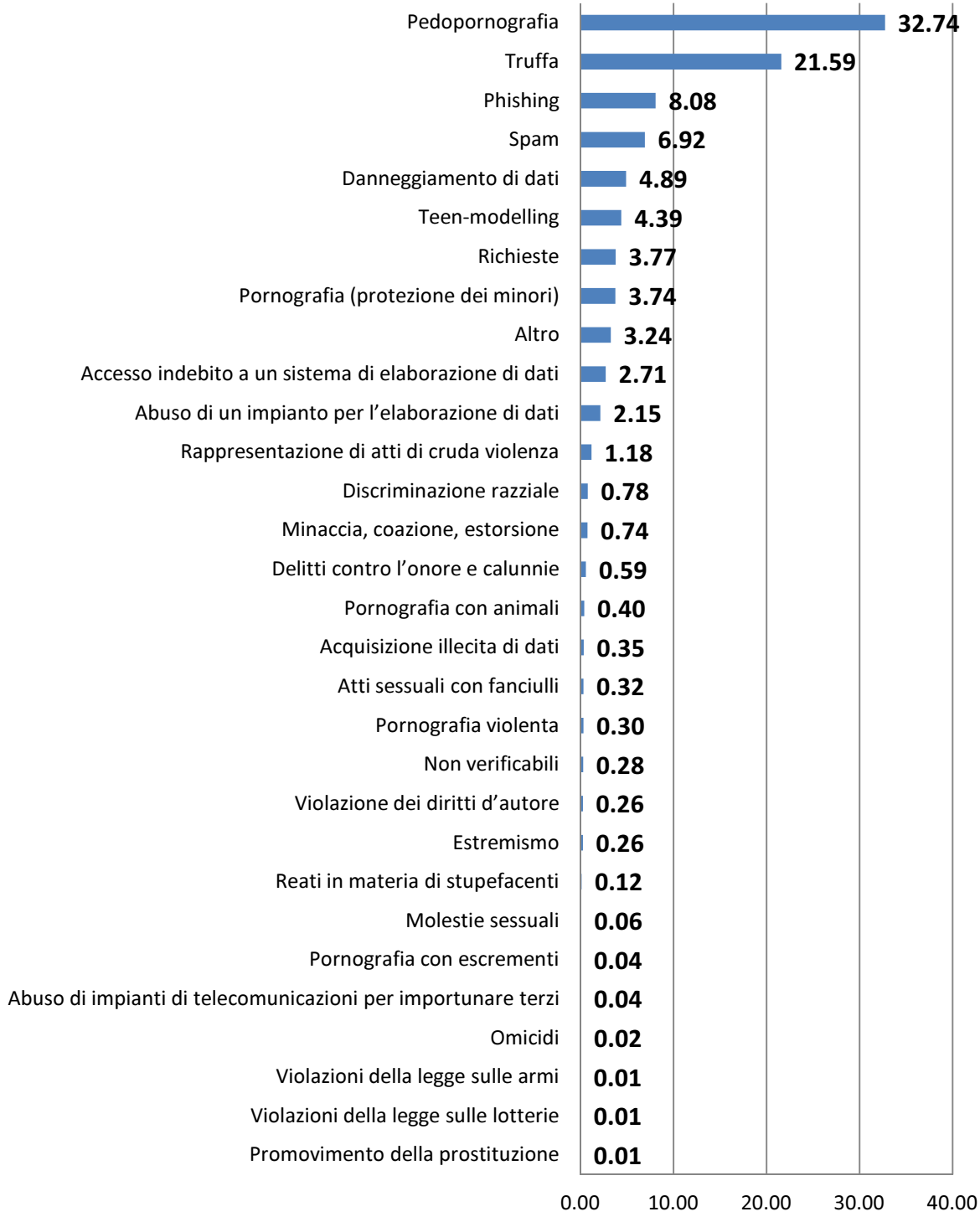


Grafico 3 : Percentuali delle comunicazioni pervenute nel 2012 suddivise per categoria

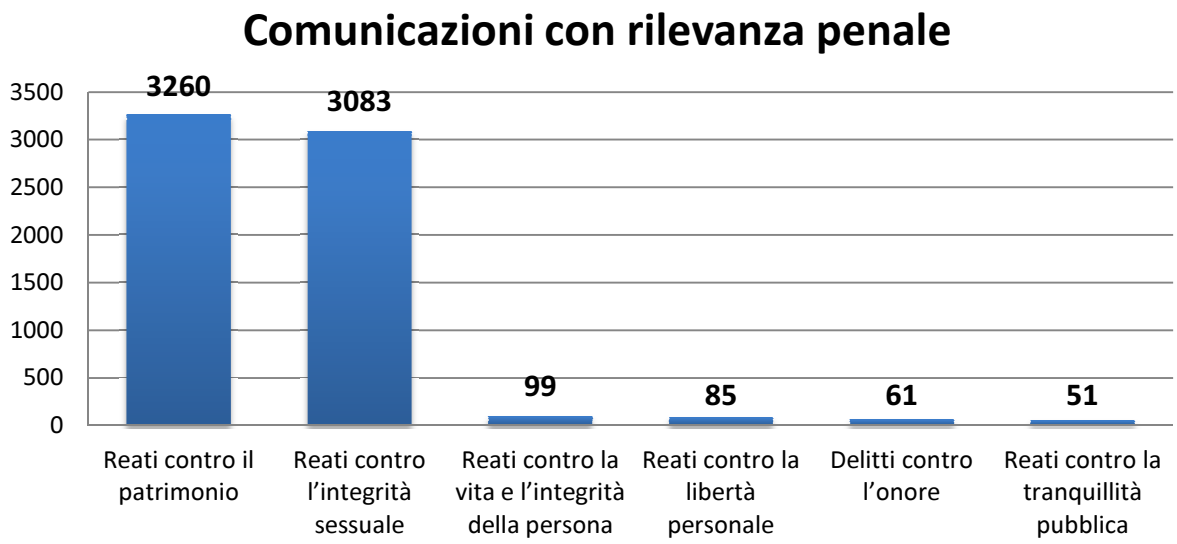


Grafico 4: Numero delle comunicazioni con rilevanza penale pervenute nel 2012 (totale: 6639)

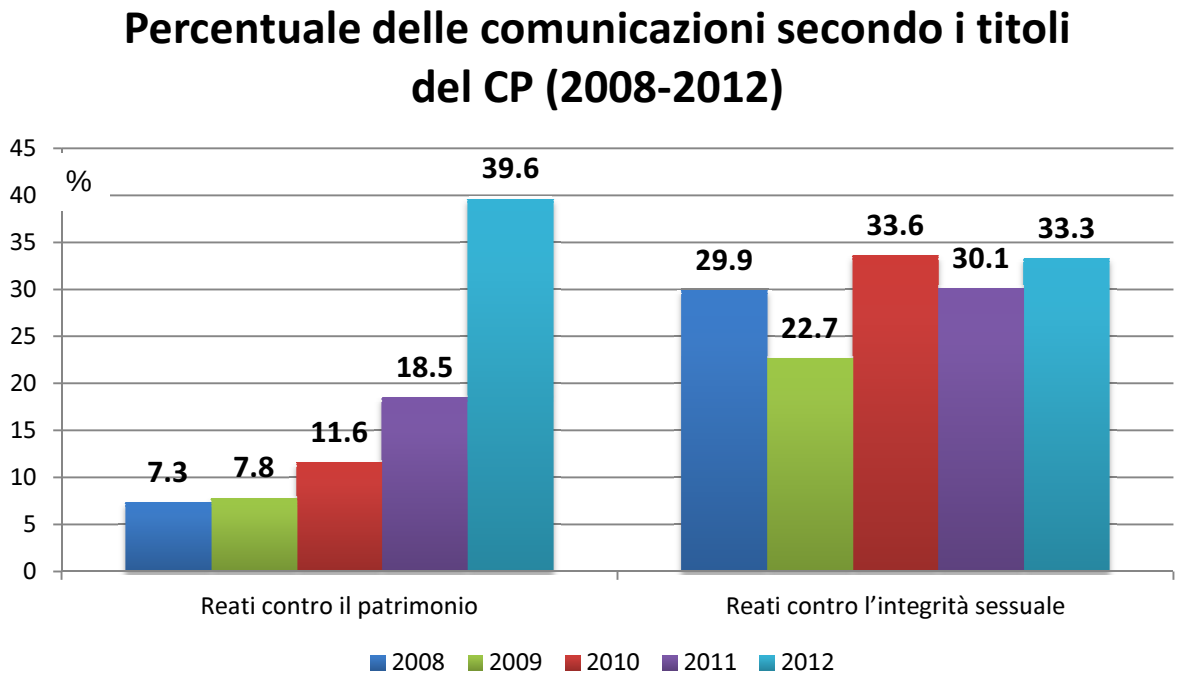


Grafico 5: Percentuale delle comunicazioni, 2008-2012

a) Reati contro il patrimonio

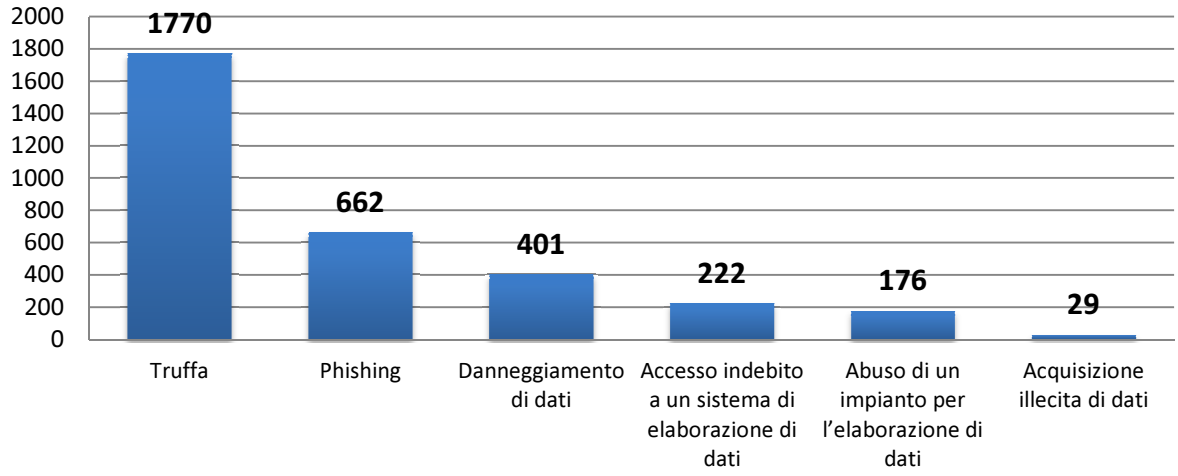


Grafico 6: Numero delle comunicazioni concernenti i reati contro il patrimonio pervenute nel 2012 (totale: 3260)

Con 1770 segnalazioni, la truffa guida la classifica delle comunicazioni concernenti i reati contro il patrimonio. Gran parte delle comunicazioni per truffa pervenute riguarda offerte fraudolente pubblicate su siti di aste online o di piccoli annunci, con cui gli impostori inducono le potenziali vittime ad anticipare loro una somma, astenendosi tuttavia dal fornire successivamente la merce / i servizi pattuiti. Aumentano inoltre i casi segnalati in cui dei truffatori rispondono a un annuncio, sovente di natura immobiliare, affermando di risiedere momentaneamente all'estero. Per concludere l'affare, chiedono alle vittime il versamento di finte tasse doganali o di somme per uno spostamento fittizio. Riscosse tali somme, i truffatori fanno perdere le proprie tracce senza tuttavia corrispondere quanto concordato. Questo tipo di truffa ha colpito svariati siti di annunci immobiliari.

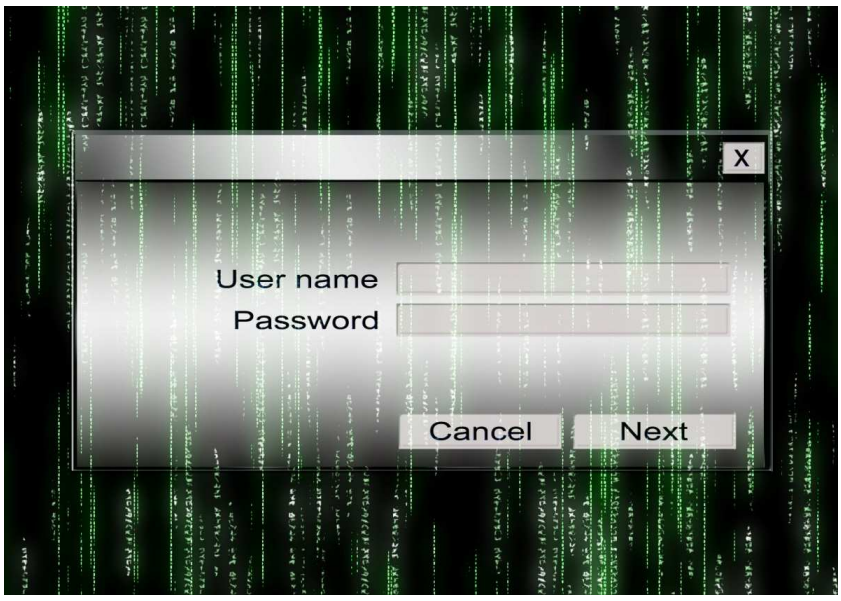
Anche nel 2012 sono pervenute numerose segnalazioni riguardanti i casi di truffa dell'anticipo. Tale stratagemma consiste nel convincere le potenziali vittime, spesso tramite l'invio massiccio di e-mail (spam), a versare un piccolo anticipo promettendo loro lauti guadagni.

Nel 2012, i casi di «***phishing***», ovvero i tentativi di accedere attraverso e-mail false o telefonate ai dati sensibili degli utenti, sono stati registrati per la prima volta in una categoria a parte. Pertanto, essi non sono più riportati sotto la categoria «***spam***» in senso stretto, ossia l'invio di e-mail pubblicitarie indesiderate. Tale scelta è stata dettata dal fatto che le comunicazioni riguardanti gli attacchi di *phishing*, con l'8 per cento delle segnalazioni complessive hanno superato numericamente le segnalazioni concernenti i casi di *spam* in senso stretto (7 % del totale). Gli attacchi di *phishing* erano per lo più volti a carpire i numeri di carte di credito o di conti bancari, i dati di accesso alle caselle di posta elettronica o i dati relativi ai conti di e-banking. La somma di entrambe le categorie ammonta 15 per cento, ovvero la stessa quota raggiunta nel 2011 dalla categoria «*spam*» che, come illustrato in precedenza, comprendeva allora anche i tentativi di *phishing*. Il calo registrato nel 2012 dalla categoria «*spam*» non implica tuttavia necessariamente una diminuzione del volume di e-mail indesiderate in circolazione. Esso potrebbe testimoniare piuttosto la rassegnazione degli utenti nei confronti a questo fenomeno e la maggiore efficacia dei filtri *anti-spam*.

La quota di segnalazioni concernenti **la criminalità su Internet in senso stretto** ha fatto registrare un nuovo aumento rispetto all'anno precedente. Tale categoria comprende i reati di «accesso indebito a un sistema di elaborazione di dati», «danneggiamento di dati» e «abuso di un impianto per l'elaborazione di dati » (cfr. grafico 3).

In relazione al reato di «accesso indebito a un sistema di elaborazione di dati», diversi cittadini hanno segnalato che persone estranee si erano introdotte illecitamente nelle loro caselle di posta elettronica, inviando a tutti i contatti registrati nella rubrica un'e-mail con cui, spacciandosi per il titolare dell'indirizzo e-mail e affermando di trovarsi in vacanza e in difficoltà finanziarie, chiedevano ai destinatari d'inviarle delle somme di denaro.

Un ulteriore esempio del reato di **«accesso indebito a un sistema di elaborazione di dati»** consiste nell'accedere illecitamente a pagine Internet di aziende o associazioni per ottenere dati sensibili dell'azienda o dell'associazione stessa o riguardanti i gli utenti del loro sito. I truffatori s'impossessano di tali dati (indirizzi e-mail, password di conti bancari online, numeri di carte di credito ecc.) per rivenderli successivamente sul mercato nero. Oltre al furto di dati, spesso i criminali riescono a danneggiare i siti web e addirittura a cancellare intere banche dati o il contenuto dei siti colpiti.



Fonte: Gerd Altmann /Pixelio

Lo SCOCI ha ricevuto inoltre segnalazioni su attacchi o minacce d'attacchi DDoS (***Distributed-Denial-of-Service*)** ai danni di gestori di negozi online. Tale tecnica consiste nel chiedere a quest'ultimi una forma di «riscatto», minacciando, in caso di mancato pagamento, di sovraccaricare i server che ospitano il sito web del loro negozio con un numero esorbitante di richieste fino a renderlo inaccessibile per diverse ore.

Nel 2012 i cibercriminali hanno inoltre compiuto alcuni attacchi di *malware* ai danni di cittadini privati, spacciandosi per l'Ufficio federale di polizia o la Società svizzera per i diritti degli autori di opere musicali SUISA. I criminali hanno bloccato il computer delle vittime, affermando che si tratta di una misura temporanea adottata in seguito al presunto *download* di contenuti illegali. Infine, hanno esortato quest'ultime a pagare una multa pari a 100 franchi per sbloccare il computer ed evitare sanzioni penali.

b) Reati contro l'integrità sessuale

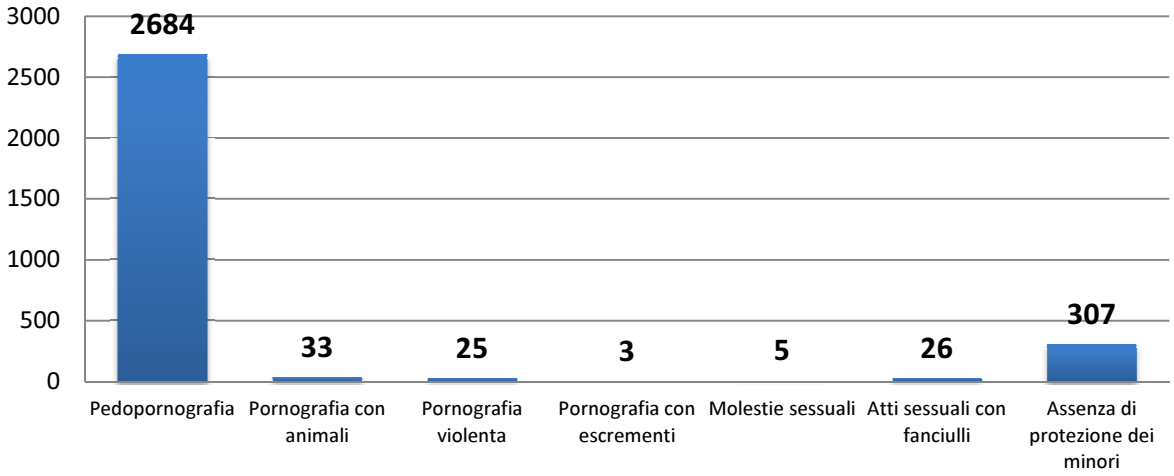


Grafico 7: Numero delle comunicazioni concernenti i reati contro l'integrità sessuale pervenute nel 2012 (totale: 3083)

Nel 2012 si è registrato un lieve aumento della percentuale di comunicazioni concernenti i «**reati contro l'integrità sessuale**». La maggior parte di tali segnalazioni ha riguardato la distribuzione su siti Internet di pornografia inscenante bambini. Inoltre, 307 annunci provenivano da persone che reputavano che alcuni siti pornografici non precludevano sufficientemente l'accesso ai minori.

Fonte: S. Hofschlaeger /Pixelio

c) Ulteriori reati

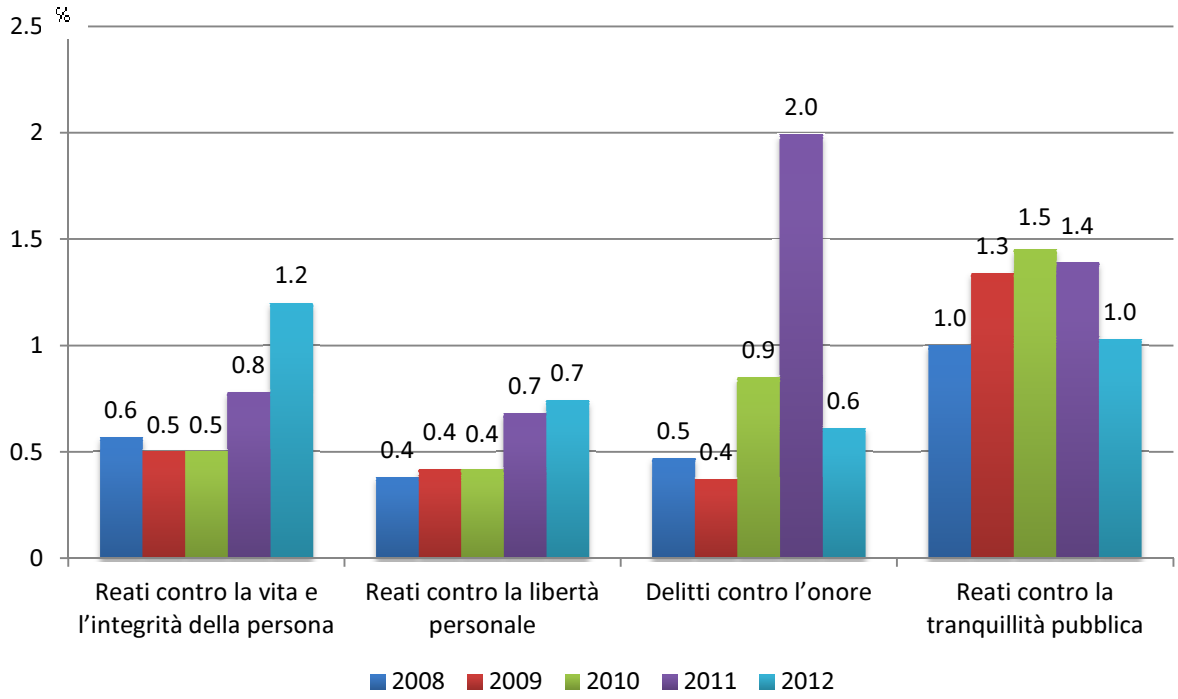


Grafico 8: Percentuale delle comunicazioni concernenti altre categorie di reato elencate nei titoli del CP (2008-2012)

Analogamente agli anni precedenti, anche nel 2012 lo SCOCI ha ricevuto tramite l'apposito modulo online delle segnalazioni concernenti altre categorie di reati. Dopo l'aumento significativo nel 2011, il numero di segnalazioni concernenti i «delitti contro l'onore» è calato notevolmente, interrompendo dunque l'aumento registrato nei due anni precedenti. Tale dato è dovuto alla maggiore attenzione consacrata dai media ai **casi di ciberbullismo** e alla conseguente sensibilizzazione dei cittadini a un uso maggiormente consapevole dei *social media*.

d) Conclusioni

Si osservano due tendenze:

In primo luogo, il numero di comunicazioni concernenti i **reati contro il patrimonio**, **ovvero i cosiddetti reati economici** (soprattutto truffe e attacchi di *phishing*), è cresciuto costantemente negli ultimi anni. Sono aumentati anche gli abusi indebiti di un sistema di elaborazione di dati finalizzati a ottenere dati sensibili o a estorcere denaro alle vittime.

In secondo luogo, la categoria dei **reati contro l'integrità sessuale**, nonostante il numero elevato di comunicazioni pervenute anche nel 2012 (3083 comunicazioni a fronte delle 2150 segnalazioni del 2011), è stata superata in termini percentuali dai reati contro il patrimonio (cfr. grafico 5).

2.3 Sviluppi

Sulla base delle segnalazioni, lo SCOCI ha svolto diverse operazioni e adottato una serie di misure. Qui di seguito sono riportati i dati e le informazioni più significative:

- tutte le 8242 comunicazioni pervenute sono state analizzate tempestivamente sotto il profilo della loro rilevanza penale e della competenza territoriale;
- lo SCOCI ha risposto individualmente a oltre 2200 segnalazioni;
- 38 segnalazioni sono state direttamente trasmesse, in virtù della loro rilevanza penale, al Cantone o all'autorità competente;
- 345 comunicazioni concernenti pagine Internet dai contenuti penalmente rilevanti sono state trasmesse alle autorità estere di perseguimento penale (tramite Interpol/Europol) o a organizzazioni attive nel settore della criminalità su Internet (p. es. l'associazione «In Hope»);
- centinaia di segnalazioni sono state inviate direttamente a fornitori di servizi Internet svizzeri o esteri (p. es. richieste di cancellazione di contenuti penalmente rilevanti o richieste concernenti degli indirizzi IP);
- numerosi casi sono stati segnalati all'interno di fedpol ai commissariati Criminalità generale, organizzata e finanziaria, Pedocriminalità / pornografia e Protezione dello Stato della Polizia giudiziaria federale (PGF).

2.4 Descrizione di un caso significativo registrato nel 2012

Nel 2012 lo SCOCI ha ricevuto diverse segnalazioni concernenti persone che avevano annunciato sul web la propria intenzione di suicidarsi. Una comunicazione di questo tipo è giunta ad esempio da un'azienda informatica francese, il cui team competente per la segnalazione di abusi era venuto a conoscenza di alcune affermazioni che lasciavano presagire intenzioni suicide fatte da un utente nella chat room di un popolare gioco online. Poiché l'indirizzo IP dell'utente risultava registrato in Svizzera, il team ha deciso di segnalare il caso allo SCOCI. Grazie agli accertamenti eseguiti, lo SCOCI è riuscito in breve tempo a individuare l'indirizzo della connessione Internet e ad allertare la polizia cantonale competente. Quest'ultima ha potuto, nell'arco di poche ore, individuare e interrogare la ragazza che aveva esternato le proprie intenzioni suicide nonché i rispettivi genitori. Dal colloquio è emerso che i sospetti risultavano fondati, motivo per cui alla ragazza è stata fornita l'assistenza psicologica necessaria. Questo caso dimostra l'importanza di una cooperazione coordinata e gestita a livello centrale tra le autorità di perseguimento penale e il settore privato.

3. Ricerche attive da parte dello SCOCI (*monitoring*)

Lo SCOCI, oltre a ricevere segnalazioni inviate dalla popolazione, effettua anche ricerche su Internet in assenza di sospetti. In tal modo, lo SCOCI opera anche nelle aree meno accessibili della rete, contribuendo alla prevenzione dei reati. Ogni anno il comitato direttivo dello SCOCI fissa un nuovo settore su cui incentrare le ricerche attive. Come negli anni precedenti, nel 2012 tali ricerche erano focalizzate sulla lotta alla pedocriminalità su Internet. Il comitato direttivo ha tuttavia dichiarato espressamente che lo SCOCI non deve escludere dalle proprie ricerche i reati economici e la criminalità su Internet in senso stretto.

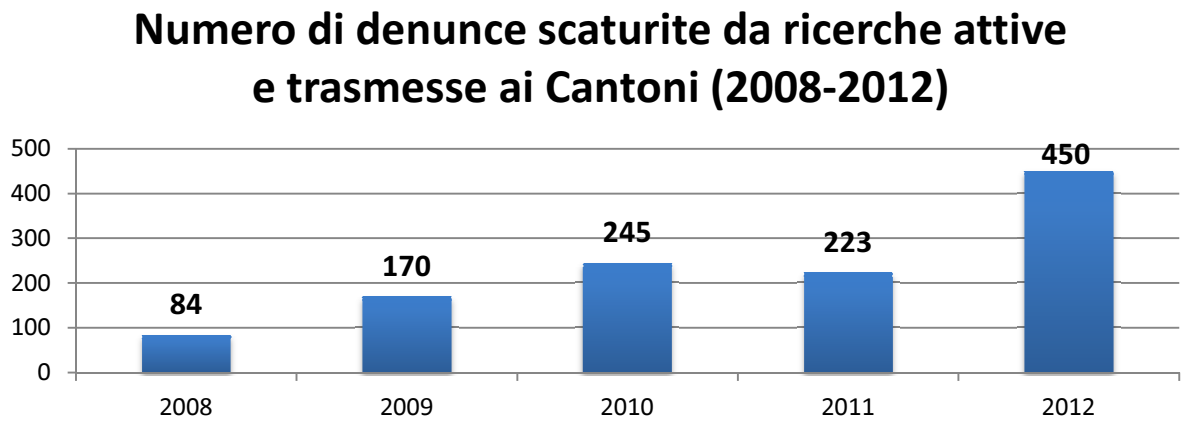


Grafico 9: Numero di procedimenti penali avviati nell'ambito di ricerche attive (2008-2012)

Grazie alle ricerche attive, nel 2012 sono stati allestiti complessivamente 450 dossier su casi in cui si sospetta la commissione di reato, ovvero quasi il doppio rispetto all'anno precedente.

Grafico 10: Denunce suddivise in base al tipo di monitoraggio effettuato (totale: 450)

3.1 Ricerche attive nelle reti *peer to peer* (P2P)

Dei 450 dossier su casi in cui si sospetta la commissione di reato allestiti, ben 417 sono scaturiti dal monitoraggio delle reti *peer to peer* (P2P), volto a individuare gli utenti di Internet che in Svizzera partecipano attivamente allo scambio di file con contenuti pedopornografici. Nel 2012 sono stati allestiti 214 dossier in più rispetto all'anno precedente, pari a un incremento del 95 per cento. Le reti P2P sono tuttora uno degli strumenti preferiti per scambiare dati illegali su Internet in modo relativamente anonimo. L'aumento marcato del numero di dossier è attribuibile, in primo luogo, al costante sviluppo di nuovi software e in secondo luogo all'ottimizzazione delle procedure interne da parte dello SCOCI.

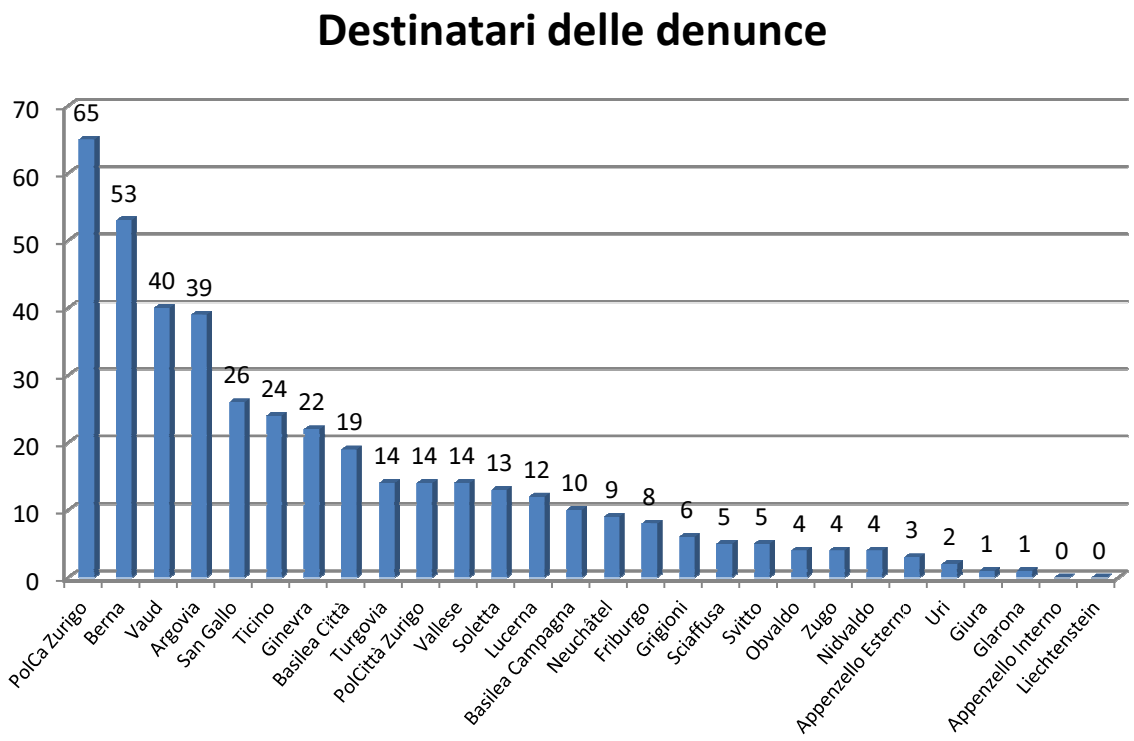


Grafico 11: Ripartizione delle denunce in base alla competenza cantonale (totale: 417)

Come in passato, lo SCOCI ha trasmesso la maggior parte dei casi alle autorità dei Cantoni più popolosi, quali Zurigo, Berna e Vaud (cfr. grafico 11).

Nonostante lo SCOCI cerchi specificatamente utenti domiciliati in Svizzera, nell'anno in esame sono stati riscontrati alcuni reati compiuti da nove persone domiciliate all'estero. Lo SCOCI ha trasmesso tali informazioni via Interpol ai Paesi competenti.

3.2 Indagini preliminari sotto copertura svolte in assenza di sospetti

Fonte: Alexander Klaus /Pixelio

L'accordo sulla collaborazione in materia di indagini preliminari di polizia svolte su Internet al fine di combattere la pedocriminalità (monitoraggio di chat) concluso tra lo SCOCI, il Dipartimento di sicurezza del Cantone di Svitto e fedpol, disciplina le modalità secondo cui i collaboratori dello SCOCI possono svolgere indagini preliminari sotto copertura per combattere la pedocriminalità in rete[1]. In virtù dell'accordo i collaboratori dello SCOCI eseguono indagini preliminari mascherate esclusivamente su incarico e sotto il controllo della polizia cantonale di Svitto. In questo modo si garantisce che nel settore della pedocriminalità su Internet le ricerche attive possano continuare a essere svolte a livello centrale (ovvero federale) sotto forma d'inchieste sotto copertura preventive.

Le indagini preliminari svolte sotto copertura dallo SCOCI hanno condotto nel 2012 all'allestimento e alla trasmissione di 33 dossier ai Cantoni competenti. 13 di queste denunce erano scaturite da indagini condotte in alcune chat elvetiche frequentate da minori e riguardavano tentati atti sessuali con fanciulli e/o l'invio di materiale pornografico a minori.

Nei restanti 20 casi, le indagini preliminari sotto copertura erano state invece condotte su reti private di condivisione P2P dei dati. Questi tipi di reti si differenziano dalle reti P2P classiche, in quanto i dati sono scambiati direttamente tra due computer tramite una rete privata. In questo ambito vigono le disposizioni concernenti le inchieste sotto copertura. Finora è stato possibile condurre indagini su tali reti soltanto in misura limitata, dato l'ingente dispendio di tempo e di personale richiesto. Se si considera tuttavia che gran parte delle 20 persone indiziate era già nota alle forze di polizia come autori recidivi di reati in materia di pornografia vietata o, addirittura, di reati sessuali, la decisione dello SCOCI di estendere le indagini preliminari sotto copertura anche alle reti private di condivisione P2P dei dati si è rivelata giustificata.

[1] Intervento ai sensi del § 9d dell'ordinanza del 22 marzo 2000 del Cantone di Svitto sulla polizia cantonale (PolV – SRSZ 520.110).

3.3 Riscontri dei Cantoni

Fonte: Thorben Wengert /Pixelio

lo SCOCI trasmette ai Cantoni competenti tutti casi nei quali sussistono dei sospetti fondati di reato (cfr. grafico 11). Per disporre di una panoramica generale delle attività intraprese dai Cantoni, lo SCOCI è grato a quest'ultimi per ogni loro resoconto sugli sviluppi del caso che (misure di polizia adottate e/o esito dei procedimenti giudiziari) gli inviano.

L'analisi di questi riscontri costituisce un mezzo essenziale per valutare l'efficacia dell'attività dello SCOCI e la qualità delle denunce e dei casi inoltrati ai Cantoni. La stragrande maggioranza dei casi trasmessi (417) scaturisce dalle ricerche attive nelle reti P2P e riguarda pertanto persone che partecipano attivamente allo scambio di contenuti illeciti di carattere pedopornografico.

a) Riscontri delle autorità cantonali di polizia

Grafico 12: Perquisizioni domiciliari 2012

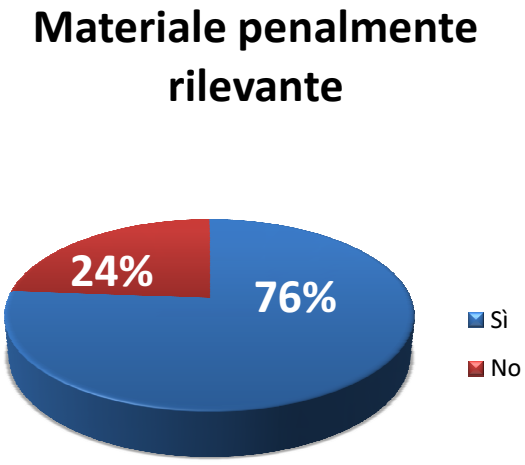


Grafico 13: Materiale penalmente rilevante 2012

Come si evince dal grafico 12, nel 98 per cento di tutti i casi trasmessi dallo SCOCI le autorità cantonali di polizia hanno eseguito perquisizioni domiciliari.

Nel 76 per cento delle perquisizioni domiciliari effettuate in seguito a delle segnalazioni di sospetto è stato sequestrato del materiale illegale. Per quanto concerne i restanti casi, non è sempre facile individuare le cause del mancato ritrovamento di materiale. In alcuni casi esso è riconducibile al fatto che le reti wireless aperte e non protette o il trasferimento dei dati su dei servizi di *cloud computing* complicano il sequestro delle prove e impediscono un'identificazione precisa delle persone indiziate.

Un intervento tempestivo (perquisizione domiciliare) della polizia, immediatamente dopo la trasmissione dei dossier, permetterebbe di evitare che gli autori dei reati possano sostituire i computer e/o cancellare i supporti di dati in questione.

Nel 97 per cento dei casi il materiale sequestrato era di carattere pedopornografico. Tale dato non è sorprendente, se si considera che le ricerche attive nelle reti P2P sono incentrate su reati di questo genere e che la maggior parte dei casi scaturiscono da questo tipo di ricerche. Occorre inoltre sottolineare che in più del 50 per cento dei casi sono stati riscontrati anche altri reati correlati alla pornografia vietata (art. 197 CP; cfr. grafico 14). Nella metà delle perquisizioni domiciliari effettuate sono stati ad esempio sequestrati anche contenuti di pornografia con animali.

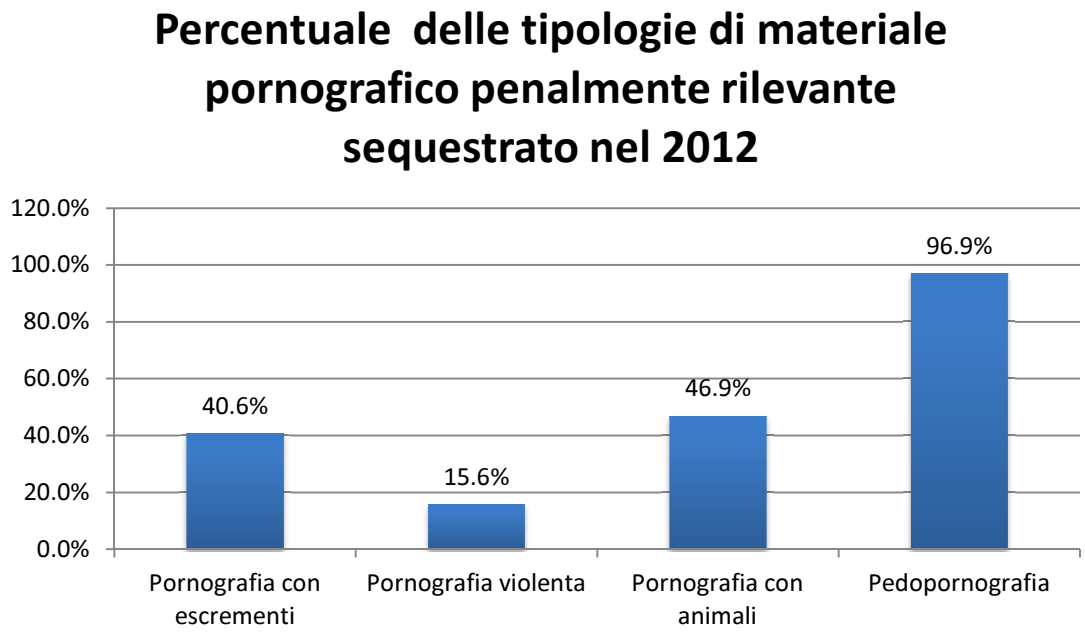
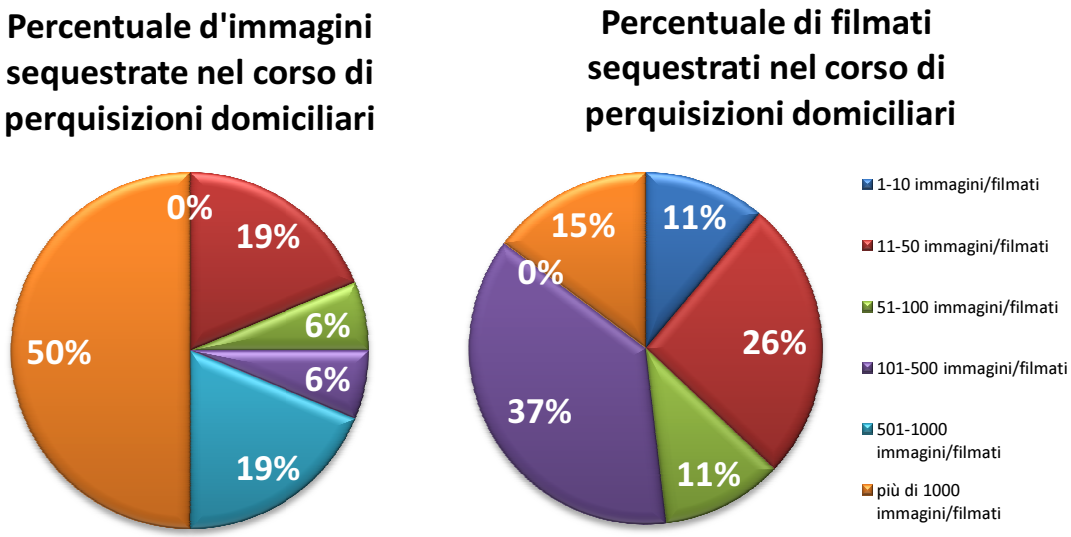


Grafico 14: Tipologia di materiale pornografico penalmente rilevante sequestrato nel 2012

Dai riscontri forniti dalle autorità cantonali di polizia emerge che le perquisizioni domiciliari effettuate con successo hanno condotto nel 94 per cento dei casi al sequestro di filmati e nel 66 per cento dei casi al sequestro di immagini. In molti casi è stato trovato e sequestrato materiale probatorio di entrambe le categorie. Nel complesso, le perquisizioni domiciliari hanno consentito di sequestrare diversi milioni di filmati e immagini penalmente rilevanti.



Grafici 15 e 16: Percentuale di immagini e filmati sequestrati

b) Riscontri delle autorità giudiziarie cantonali

Nel 90 per cento dei casi in cui le autorità giudiziarie cantonali hanno fornito un riscontro allo SCOCI, i procedimenti penali si sono conclusi con una condanna.

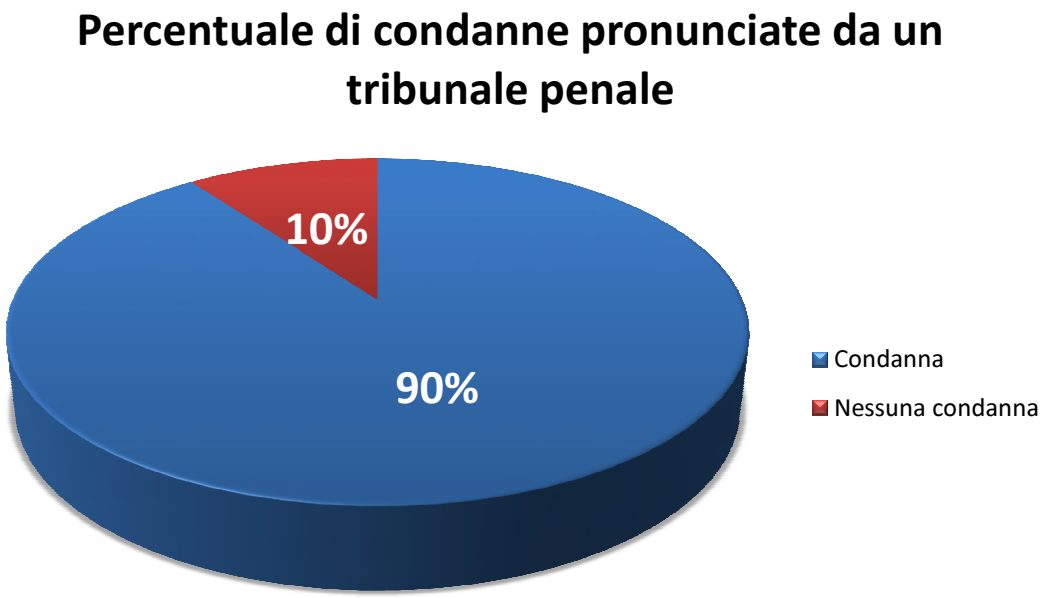


Grafico 17: Condanne penali pronunciate nel 2012

La maggior parte delle condanne è stata pronunciata per possesso di pornografia dura, reato represso all'art. 197 CP e nella fattispecie all'art. 197 numero 3 e 3bis CP.

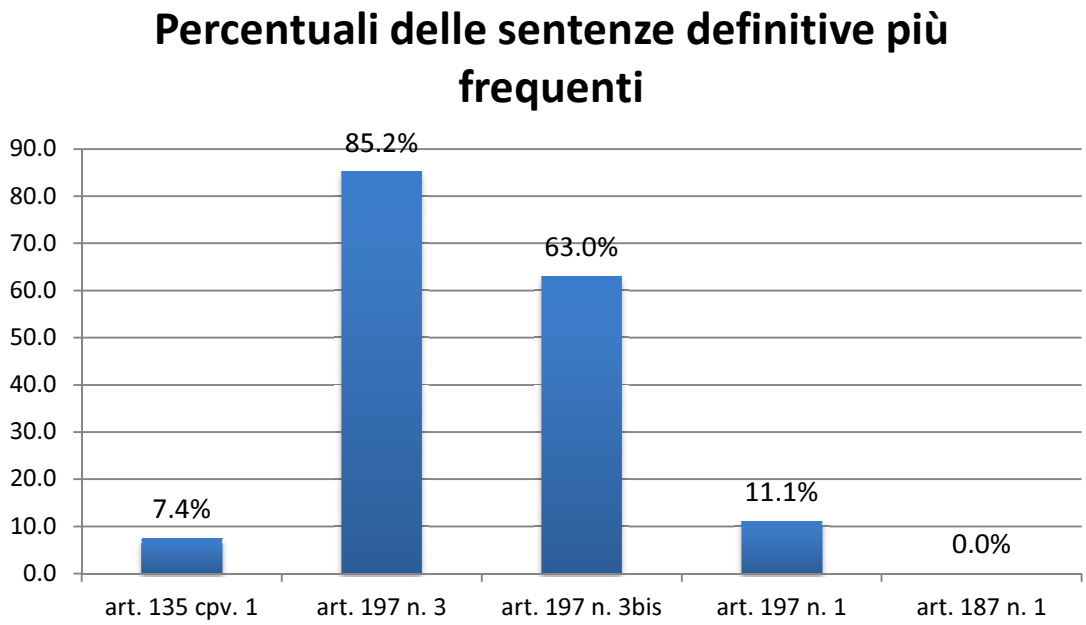
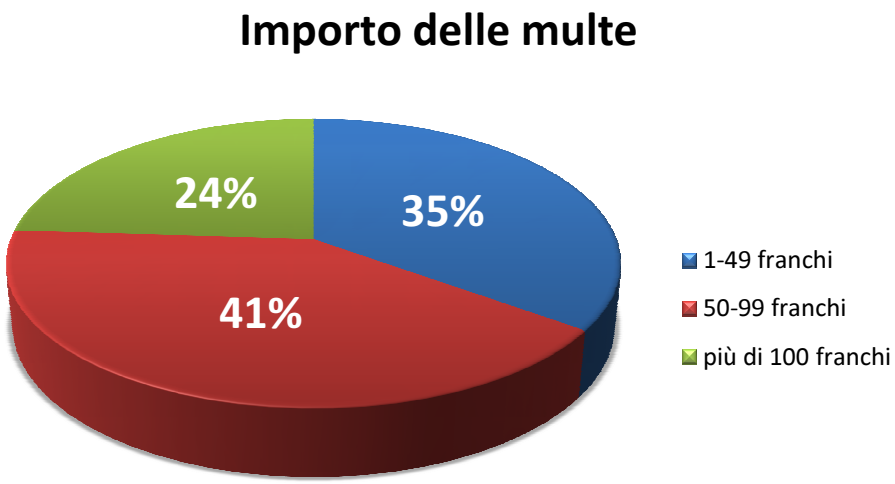


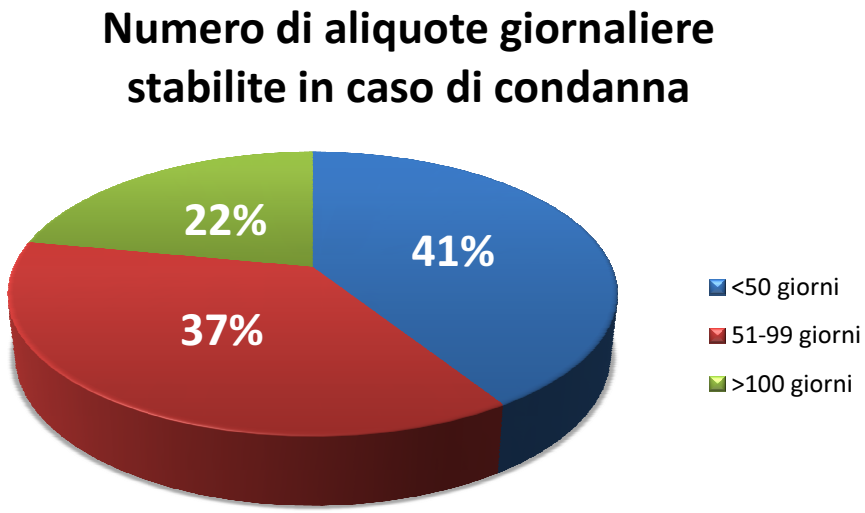
Grafico 18: Percentuali delle sentenze definitive più frequenti nel 2012

In tutte le condanne comunicate allo SCOCI nel 2012, è stata comminata una **pena pecuniaria (in aliquote giornaliere)**. Nel 63 per cento di questi casi il condannato ha ricevuto anche una **multa**. Nel **96 per cento dei casi** è stata pronunciata una **pena pecuniaria con la condizionale**. Infine, in linea con la tendenza degli ultimi anni, nessuna delle condanne ha riguardato provvedimenti quali il lavoro di pubblica utilità, la privazione della libertà (carcere), pene pecuniarie senza condizionale o misure terapeutiche.

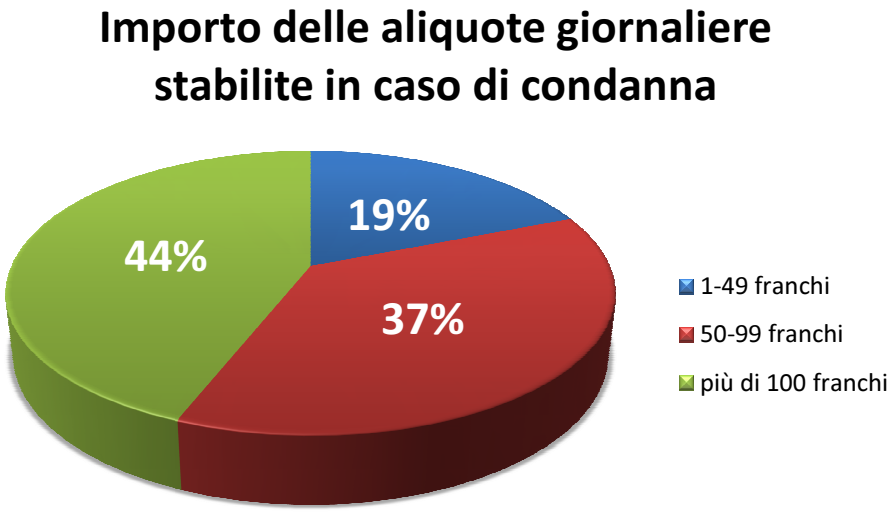


In circa il 35 per cento dei casi l'importo delle multe era inferiore ai 1000 franchi. Nel 41 per cento dei casi la loro entità era invece compresa tra i 1000 e i 2000 franchi. Soltanto il 24 per cento delle multe ha superato i 2000 franchi.

Il 41 per cento delle pene pecuniarie ammontava a meno di 50 aliquote giornaliere, mentre nel 37 per cento dei casi il loro numero era compreso tra 51 e 100. Soltanto nel 22 per cento dei casi sono state comminate più di 100 aliquote giornaliere.



Per quanto concerne, infine, l'importo delle aliquote giornaliere, il 19 per cento oscillava tra 1 e 50 franchi, il 37 per cento tra i 51 e i 100 franchi e il restante 44 per cento superava i 100 franchi.



Di regola, i condannati di regola sono inoltre tenuti ad assumere le spese procedurali che in molti casi superano ampiamente l'importo della multa.

3.4 Esempio di un’indagine preliminare svolta in assenza di sospetti nelle reti P2P

Le indagini condotte da una polizia cantonale nelle reti P2P sulla base di un dossier trasmesso dallo SCOCI, hanno permesso di accertare che una persona indiziata si era recata due volte all’estero per compiere abusi su diversi minori. Il pedocriminale aveva filmato e successivamente diffuso sul web le scene di tali abusi. Dalle indagini è emerso inoltre che l’indiziato abusava sessualmente anche del proprio figlio di tre anni.

Fino al momento della trasmissione del caso da parte dello SCOCI, la persona in questione non risultava registrata in alcun registro di polizia. Grazie alla collaborazione professionale tra lo SCOCI e la competente polizia cantonale nonché all’intensa attività investigativa, è stato possibile assicurare alla giustizia l’autore degli abusi, impedendogli dunque di sottoporre il proprio figlio o altri minori ad ulteriori violenze.

Questo caso dimostra l’importanza di un trattamento sistematico dei casi concernenti le reti P2P da parte delle autorità cantonali. A tale proposito, occorre tuttavia sottolineare le enormi sfide che alcuni Cantoni sono chiamati ad affrontare, a causa delle risorse limitate di cui dispongono e dell’aumento considerevole dei dossier trasmessi dallo SCOCI, nel trattare in tempo utile questi casi.

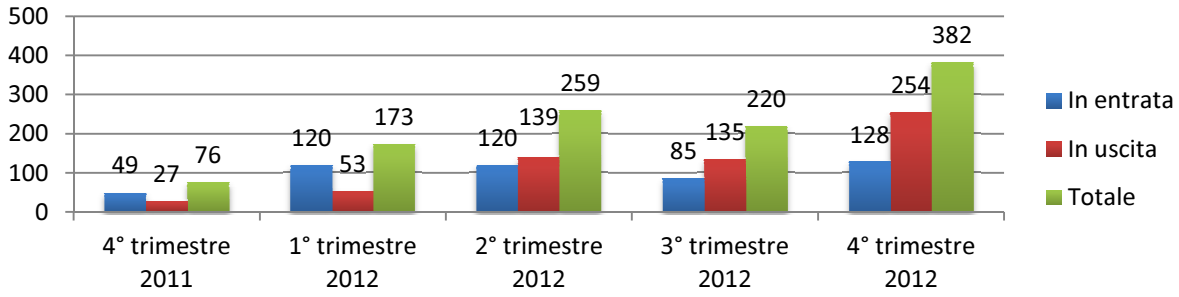
4. Scambio d’informazioni di polizia giudiziaria

Con l’entrata in vigore della Convenzione del Consiglio d’Europa sulla cibercriminalità, avvenuta il 1° gennaio 2012, a livello internaz ionale la Svizzera viene considerata sempre di più come partner attivo nella lotta contro la criminalità su Internet. Lo dimostra l’aumento considerevole dello scambio d’informazioni di polizia giudiziaria con le autorità estere in merito a casi che rientrano nel campo d’applicazione della Convenzione. A tale proposito assume un ruolo fondamentale anche la decisione del comitato direttivo dello SCOCI secondo cui lo SCOCI non deve escludere dalle ricerche i reati economici e la criminalità su Internet in senso stretto. Ciò si spiega anche alla luce del trasferimento dello SCOCI nel settore di polizia di fedpol. Con la subordinazione amministrativa dello SCOCI alla Polizia giudiziaria federale, avvenuta nel 2009, lo scambio d’informazioni in materia di polizia giudiziaria e l’attività di coordinamento hanno acquisito maggiore importanza. Le cifre seguenti lo mostrano chiaramente.

Nel 2012 lo SCOCI ha ricevito complessivamente 483 comunicazioni concernenti il campo d’applicazione della Convenzione. Solamente nel quarto trimestre del 2012 lo SCOCI ha ricevuto 128 segnalazioni provenienti dall’estero, ovvero un aumento pari al 161 per cento rispetto all’anno precedente (quarto trimestre 2011: 49 comunicazioni). Tale tendenza si evidenzia anche per quanto concerne le comunicazioni in uscita inviate dallo SCOCI alle autorità estere di perseguimento penale e che sono strettamente legate all’aumento delle segnalazioni in entrata. Nell’anno in esame, lo SCOCI ha inoltrato complessivamente 561 comunicazioni all’estero (Interpol ed Europol). Confrontando il numero delle segnalazioni trasmesse nel quarto trimestre del 2012 (254 comunicazioni) con quelle dell’anno precedente (27 comunicazioni), è possibile dunque constatare un netto aumento.

Scambio d'informazioni di polizia giudiziaria con le autorità estere nel 2012

Sviluppo delle comunicazioni in entrata/in uscita 2011-2012



4.1 Alcuni esempi

I due casi seguenti dimostrano che lo scambio d'informazioni in materia di polizia giudiziaria sulla base della Convenzione del Consiglio d'Europa sulla cibercriminalità si è rilevato rapido ed efficace.

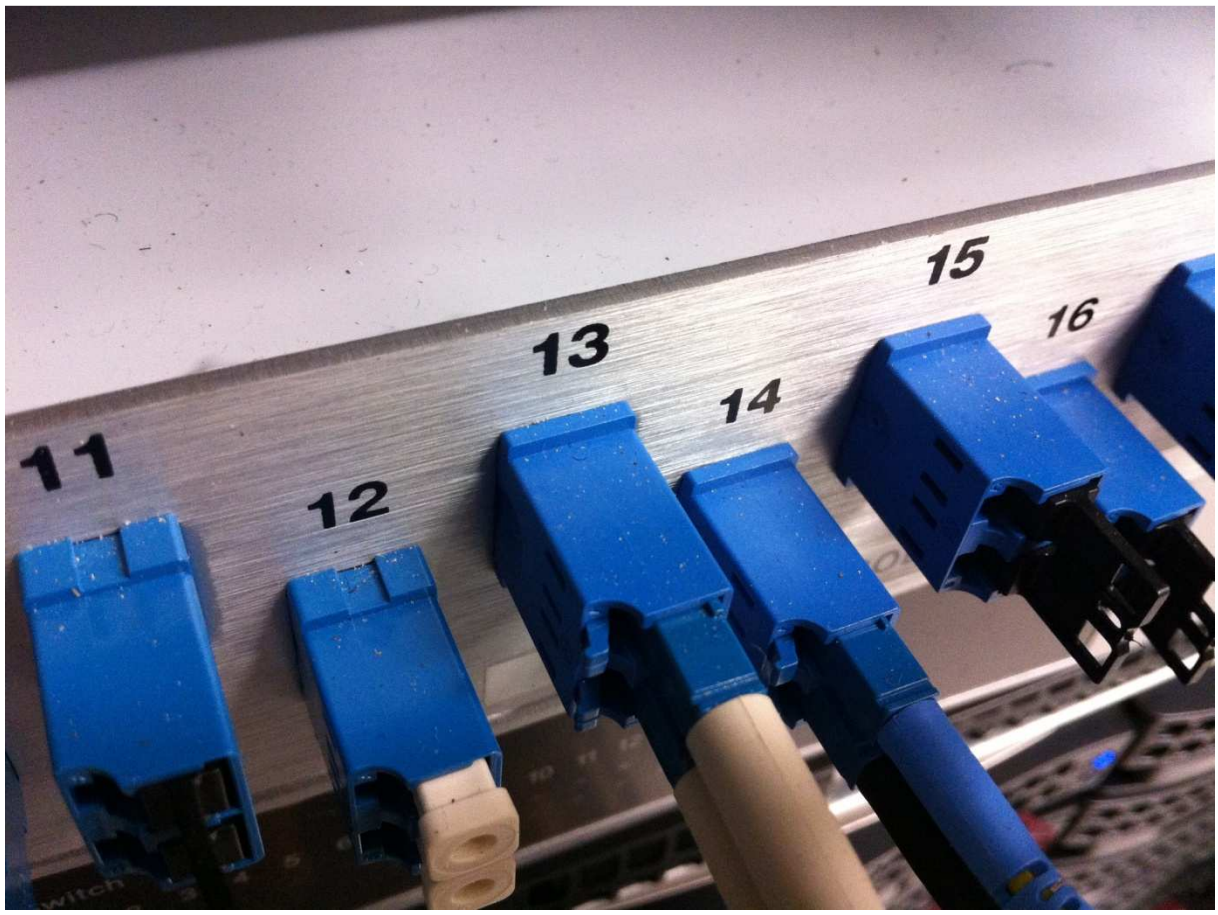
Interpol ha trasmesso allo SCOCI una comunicazione secondo cui alcuni membri di partiti politici del Paese richiedente avevano ricevuto delle e-mail in cui veniva minacciata la loro vita e integrità fisica. Lo SCOCI ha ricevuto questa comunicazione poiché i dati relativi al mittente delle e-mail presentavano un legame con la Svizzera. Grazie alle procedure già elaborate tra lo SCOCI e il provider in questione, nell'arco di 24 ore è stato possibile salvaguardare preventivamente tutti i dati, ottenere le informazioni necessarie all'identificazione del meittente e informare la polizia cantonale competente. Interpol ha ricevuto quindi immediatamente tutte le informazioni che potevano essere rilevanti ai fini di una domanda di assistenza giudiziaria.

In un altro caso lo SCOCI è stato informato da Interpol in merito a e-mail ricattatorie con contenuto e mittente identici. Gli autori del messaggio chiedevano una cospicua somma di denaro e, in caso di rifiuto, minacciavano un grossista internazionale di perpetrare attacchi dinamitardi contro le sue filiali. Una delle e-mail proveniva da un account di posta elettronica svizzero ed era rivolta personalmente al direttore di una delle filiali del grossista. In collaborazione con il comando di polizia competente, lo SCOCI ha subito avviato la procedura di salvaguardia dei dati rilevanti presso il provider svizzero. In tal modo è stato possibile contribuire in maniera sostanziale e tempestiva alle indagini d'Interpol volte a identificare i presunti autori delle e-mail.

5. Progetti

5.1 Raccolta nazionale di file e valori hash (RNFVH)

Il progetto prevede che le autorità cantonali trasmettano allo SCOCI i file (immagini, video) sequestrati nell'ambito di indagini sulla pedopornografia dopo averli preclassificati. Lo SCOCI calcola per ogni file un valore hash[2] e lo registra nella Raccolta nazionale di file e valori hash. In seguito la lista con i valori hash viene messa a disposizione dei Cantoni. In questo modo, quando le autorità cantonali sequestrano dei nuovi file, esse possono verificare se sono già presenti nella RNFVH senza doverli visualizzare ad uno ad uno. Questo confronto, operato in maniera automatica, permette di analizzare grandi quantità di file accelerando in questo modo il lavoro degli inquirenti. La RNFVH, riducendo il numero di file da visualizzare singolarmente, ha il pregio di alleggerire marcatamente il carico di stress psicologico degli inquirenti legato alla visualizzazione di materiale pedopornografico.



[2] Valore attribuibile in modo univoco a un'immagine (impronta digitale).

La RNFVH è stata concepita ed elaborata sotto la direzione dello SCOCI e con il contributo delle autorità di polizia cantonali. Per la prima volta sono stati definiti requisiti universalmente validi per una tale raccolta (p. es. un metodo di classificazione unitario). La sfida colta dalla RNFVH è stata quindi lo sviluppo tecnico di una soluzione efficiente per efficiente per l'elaborazione e il confronto di grandi quantità di file all'interno di sistemi di banche dati.

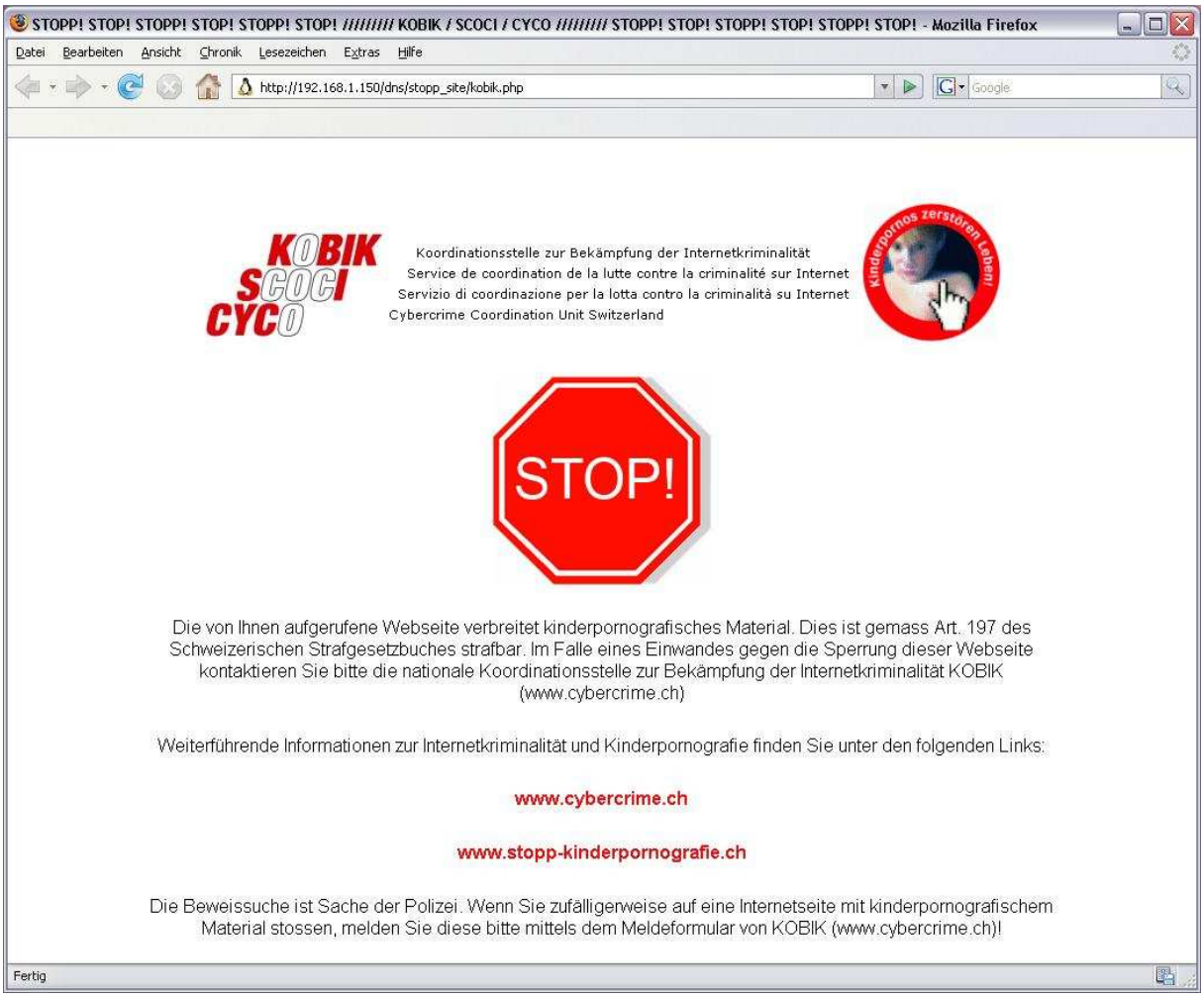
Il 2012 è stato un anno cruciale per la realizzazione del progetto pilota della RNFVH. Nel febbraio 2012 è stato predisposto l'hardware necessario alla sua entrata in funzione. Tra aprile e luglio, lo SCOCI ha installato il software sviluppato appositamente e ha effettuato i primi test. A ottobre sono stati ultimati con successo i test ancora necessari, così come alcune modifiche del sistema, rendendo così pienamente operativa la RNFVH. I servizi cantonali e comunali specializzati possono dunque inviare allo SCOCI il loro materiale visivo preclassificato. Lo SCOCI provvederà alla classificazione definitiva seguendo il sistema di duplice controllo e alla sua immissione nella RNFVH.

5.2 Progetto per il monitoraggio delle reti *peer to peer*

Negli ultimi anni lo SCOCI ha sviluppato, in collaborazione con l'organizzazione non governativa Action Innocence Genève, il programma di sorveglianza P2P-Scan nell'ambito del monitoraggio effettuato in assenza di sospetti. Questo software permette di contrastare lo scambio di materiale pedopornografico attraverso le reti peer to peer in Internet. Il programma è costantemente aggiornato in stretta collaborazione con Action Innocence Genève, che assume il pieno finanziamento del progetto, e messo a disposizione di altre autorità di perseguimento penale.

Grazie al monitoraggio effettuato su Internet anche in assenza di sospetti è stato possibile individuare e arrestare in Svizzera non solo i meri «consumatori», che con il loro comportamento favoriscono la produzione di sempre nuovo materiale, ma anche i pedocriminali che abusavano loro stessi di bambini realizzando materiale visivo.

5.3 Collaborazione con i provider svizzeri di accesso a Internet



Dal 2007 lo SCOCI appoggia i principali provider Internet svizzeri Internet nel bloccare l'accesso ai siti pedopornografici esteri. Nell'ambito di questa collaborazione, lo SCOCI mette a disposizione dei provider una lista costantemente aggiornata di siti a carattere pedopornografico (ca. 200-300 siti). In virtù della loro etica aziendale così come delle condizioni generali di contratto, i provider bloccano l'accesso a questi siti tramite una cosiddetta *stop page*.

Nell'ambito della lotta contro la pedopornografia su Internet, lo SCOCI collabora strettamente con Interpol. La lista che lo SCOCI trasmette ai provider è aggiornata grazie a una lista simile gestita da Interpol (*worst of* list). Inoltre, lo SCOCI segnala quotidianamente a Interpol i siti contenti immagini e filmati pedopornografici in cui si imbatte nel corso delle sue attività. Grazie a questo scambio reciproco, la worst of list e la lista inviata ai provider sono sempre attuali e permettono un blocco rapido dei siti con contenuti pedopornografici.

6. Gruppi di lavoro, cooperazione e contatti

6.1 Gruppi di lavoro nazionali

Nell'anno in esame, lo SCOCI ha partecipato a diversi gruppi di lavoro nazionali.

Lo SCOCI ha proseguito la sua collaborazione attiva al gruppo di lavoro nazionale «*Kindsmissbrauch*» (abusi sui fanciulli), assieme al commissariato Pedocriminalità / pornografia della Polizia giudiziaria federale, a organizzazioni di utilità pubblica, ai Cantoni e alla Prevenzione svizzera della criminalità.

Anche nel 2012, come nell'anno precedente, lo SCOCI ha partecipato ai lavori del programma nazionale «Protezione della gioventù dai rischi dei media e competenze mediali», sia in seno al comitato direttivo, incaricato dell'elaborazione del programma, sia nel gruppo esecutivo di accompagnamento. Il programma intende aiutare bambini e giovani a utilizzare i media moderni in modo sicuro, responsabile e adeguato alla loro età.

Dal 2011 lo SCOCI rappresenta fedpol anche in seno alla commissione speciale della «Prevenzione svizzera della criminalità (PSC)». La commissione sviluppa il materiale informativo e i progetti per la prevenzione della criminalità nei Cantoni, valutandone l'attuazione.

Infine, partecipando ai gruppi di lavoro «*IT Ermittler*» (Inquirenti IT) e «*Telekommunikationsüberwachung*» (Sorveglianza delle telecomunicazioni), lo SCOCI si è occupato e ha approfondito, anche nel 2012, le tematiche legate allo sviluppo tecnico e all'efficienza nel perseguimento penale.

Lo SCOCI ha contribuito altresì ad attuare il piano denominato «Sicurezza e fiducia», diretto dall'Ufficio federale delle comunicazioni (UFCOM). Il piano illustra le misure volte a promuovere la sicurezza e la fiducia della popolazione nei confronti delle moderne tecnologie dell'informazione e della comunicazione (TIC).

Fonte: Gerd Altmann /Pixelio

6.2 Collaborazione con i servizi della Confederazione

Anche nell'anno in esame, lo SCOCI ha lavorato a stretto contatto con altri servizi della Confederazione nel settore della lotta alla criminalità su Internet. In seno a fedpol, lo SCOCI ha collaborato intensamente con i commissariati Pedocriminalità / pornografia, Indagini Tecnologie dell'informazione, Protezione dello Stato e Inchieste mascherate della Polizia giudiziaria federale nonché con la divisione principale Cooperazione internazionale di polizia (CIP). Considerata la convergenza degli ambiti di attività si è sviluppata una collaborazione particolarmente intensa tra lo SCOCI e il commissariato Pedocriminalità / pornografia. Inoltre lo SCOCI ha sviluppato e approfondito vari contatti e intensificato la collaborazione con diversi servizi collocati in altri dipartimenti federali, tra cui la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), l'ambito direzionale Assistenza giudiziaria internazionale dell'Ufficio federale di giustizia (UFG), l'Ufficio federale dell'informatica e della telecomunicazione (UFIT), l'Ufficio federale della comunicazione (UFCOM), l'Ufficio federale delle assicurazioni sociali (UFAS) e la Commissione federale contro il razzismo (CFR).

Diverse sedute con Ministero pubblico della Confederazione hanno permesso l'analisi di azioni comuni e l'affinamento della collaborazione. Un risultato concreto di queste nuove sinergie è la decisione della Polizia giudiziaria federale di fornire allo SCOCI in maniera tempestiva tutte le informazioni relative a inchieste della Confederazione con riferimenti alla cibercriminalità in senso stretto. In questo modo lo SCOCI è in grado di svolgere i suoi compiti in maniera più efficace nell'elaborazione di una panoramica dei casi come pure nell'analisi della situazione della criminalità su Internet in Svizzera o nell'ambito della sua funzione di punto di contatto tra le autorità di polizia e il Servizio delle attività informative tramite MELANI.

6.3 Scambio di esperienze con i Cantoni

Nell'anno in esame, lo SCOCI ha intrattenuto diversi contatti con vari corpi di polizia e pubblici ministeri cantonali. Oltre al normale scambio di esperienze, sono state organizzate diverse riunioni di lavoro nel quadro del progetto RNFVH e delle indagini preliminari sotto copertura.

Nel 2012 si è tenuto il primo «*Forum Cybercrime Staatsanwaltschaften - KOBIK*» (forum sulla collaborazione tra i pubblici ministeri e lo SCOCI in materia di cibercriminalità). L'obiettivo del forum era di eliminare le eventuali incertezze dei pubblici ministeri riguardo alla criminalità su Internet e all'utilizzo delle risorse tecnologiche. In occasione del forum sono intervenuti diversi esperti che hanno spiegato concretamente come gestire la lotta alla cibercriminalità in funzione delle proprie esigenze specifiche. Il vivo interesse dimostrato dai pubblici ministeri ha confermato che l'iniziativa partita dal pubblico ministero di Zurigo era giustificata e che l'estensione del forum a livello intercantonale è stata opportuna.

Fonte: Gerd Altmann /Pixelio

6.4 Collaborazione con Action Innocence Genève

Da diversi anni lo SCOCI collabora strettamente con l'organizzazione non governativa Action Innocence (AIG) nella lotta contro la pedopornografia. Grazie al sostegno attivo offerto di AIG, negli ultimi anni è stato possibile proseguire e approfondire ulteriormente il progetto per il monitoraggio delle reti *peer to peer*. La collaborazione con AIG assume un'importanza ancora maggiore, se si considera che la maggior parte delle ricerche attive condotte dallo SCOCI sono rese possibili dal software messo a disposizione da AIG. Quest'ultima sostiene inoltre lo SCOCI, sviluppando ulteriori progetti nell'ambito della lotta alla pedocriminalità.

6.5 Collaborazione con il settore privato (partenariato pubblico-privato)

La collaborazione dello SCOCI con il settore privato assume un ruolo sempre più determinante nella lotta alla criminalità in rete. Nell'anno in esame hanno avuto luogo diversi incontri e visite con i rappresentanti delle imprese che operano su Internet. Particolarmente positivi si sono rivelati i contatti stabiliti con diversi fornitori di servizi Internet. Tale collaborazione è decisiva per lo svolgimento di accertamenti sulle connessioni di persone sospette (indirizzi IP) nel quadro di indagini (preliminari) di polizia. Per combattere la cibercriminalità tutti gli attori coinvolti devono agire rapidamente e in modo sinergico. A causa della criminalità economica su Internet attualmente in espansione, nel 2012 sono stati avviati incontri con i rappresentanti delle piattaforme di vendita online.

6.6 Cooperazione internazionale

Dal 2011 lo SCOCI è membro del *Focal Point* (FP) «*Cyborg*» di Europol, il cui obiettivo è contrastare la criminalità transfrontaliera su Internet, in particolare i fenomeni di *phishing*, reti bot e *hacking*. Nel 2012 lo SCOCI ha inoltre aderito al FP «*Twins*» incentrato sulla lotta alla pedocriminalità. Entrambi i *Focal Point* sono integrati nell'*European Cybercrime Center* (EC3), operativo dal 1° gennaio 2013.

Il centro per la lotta contro la criminalità su Internet EC3, che ha sede presso Europol all'Aia, fornisce sostegno operativo agli Stati dell'UE e le proprie conoscenze specialistiche nelle indagini comuni a livello europeo. Gli agenti focalizzano la propria attenzione sulle forme di cibercriminalità organizzata, in particolare sulla lotta contro lo sfruttamento sessuale dei bambini su Internet e sull'accertamento di reati finanziari. Gli inquirenti IT dell'UE si occupano inoltre di attacchi alle infrastrutture critiche e ai sistemi d'informazione. Le loro mansioni comprendono l'analisi e la stesura di valutazioni con lo scopo di individuare tempestivamente e contrastare delle eventuali situazioni di minaccia.

Lo SCOCI collabora inoltre a «CIRCAMP», progetto avviato dall'*European Chief of Police Task Force* (EPCTF) al fine di combattere la diffusione di materiale pedopornografico su Internet. Come negli anni precedenti, nel 2012 lo SCOCI ha inoltre preso parte all'*European Financial Coalition* (EFC), cofinanziata dall'UE e composta dai principali attori operanti nel perseguimento penale e nel settore privato il cui obiettivo comune è di contrastare lo sfruttamento sessuale commerciale di minori su Internet.

Nell'anno in esame lo SCOCI ha curato attivamente i contatti con diversi partner esteri. Tale scambio serve in primo luogo a sviluppare delle procedure congiunte volte a migliorare la cooperazione tra le parti che, ormai, non si concentra più soltanto sulla lotta alla pedocriminalità. Infatti, gli sforzi internazionali si focalizzano sempre più sulla lotta alla criminalità su Internet in senso stretto e alla criminalità economica. Lo scambio diretto con le autorità di perseguimento penale estere si rivela proficuo soprattutto nell'ambito degli interventi operativi (p. es. inchieste sotto copertura). Anche in tale ambito lo SCOCI ha instaurato un intenso ed efficace rapporto di cooperazione con diverse autorità.

7. Presenza nei mass media, attività didattica e conferenze

7.1 Presenza nei mass media

Nel 2012, i media hanno dato ampia risonanza allo SCOCI e alle sue attività. Particolare importanza è stata data alle indagini preliminari effettuate sotto copertura di carattere preventivo condotte dallo SCOCI, a singoli attacchi spettacolari ai danni di sistemi informativi (attacchi DDoS[3]) e alle infezioni causate da *malware* che hanno colpito numerosi computer.

7.2 Attività didattica e conferenze

Nell'anno in esame i collaboratori dello SCOCI hanno partecipato a numerose conferenze, convegni internazionali e corsi di formazione e colto l'occasione per rinsaldare i contatti con partner ed esperti.

[3] Distributed Denial of Service

8. Interventi politici a livello federale

8.1 Selezione degli interventi parlamentari presentati nel 2012

- Interrogazione 12.5264: Sollicitation d'enfants à des fins sexuelles sur Internet - Amherd Viola; Groupe PDC-PEV
- Interrogazione 12.5198: Assurer la neutralité du réseau en Suisse également - Glättli Balthasar
- Interrogazione 12.5185: DFAE. Trois attaques informatiques en cinq ans - Killer Hans; Groupe de l'Union démocratique du centre
- Interrogazione 12.5005: Investigations secrètes. Etat des travaux - Schmid-Federer Barbara; Groupe PDC-PEV
- Postulato 12.4238: Utilisation d'offres illégales sur Internet. Impact sur l'économie - Fluri Kurt; Groupe libéral-radical
- Mozione 12.4212: Inscrire la neutralité du réseau dans la loi sur les télécommunications - Glättli Balthasar; Groupe des Verts
- Mozione 12.4161: Pour une stratégie nationale contre le cyberharcèlement - Schmid-Federer Barbara; Groupe PDC-PEV
- Interpellanza 12.4086: Mesures techniques de surveillance et nouveaux outils de communication - Janiak Claude; Groupe socialiste
- Interpellanza 12.3902: La Suisse, paradis du téléchargement illégal - Fluri Kurt; Groupe libéral-radical
- Interpellanza 12.3898: Plus de sécurité juridique dans le commerce électronique - Amarelle Cesla; Groupe socialiste
- Mozione 12.3834: Protection du droit d'auteur - Freysinger Oskar; Groupe de l'Union démocratique du centre
- Postulato 12.3545: Accès des enfants à Facebook - Amherd Viola; Groupe PDC-PEV
- Mozione 12.3476: Harcèlement sexuel des mineurs. Adapter les éléments constitutifs de l'infraction - Schmid-Federer Barbara; Groupe PDC-PEV
- Postulato 12.3326: Vers un droit d'auteur équitable et compatible avec la liberté des internautes - Recordon Luc; Groupe des Verts
- Postulato 12.3289 : Atteintes à la personnalité sur Internet - Malama Peter; Groupe libéral-radical
- Postulato 12.3152 : Droit à l'oubli numérique - Schwaab Jean Christophe; Groupe socialiste

8.2 Sviluppi giuridici e politici

La lotta contro la cibercriminalità pone anche la giurisprudenza e la legislazione dinanzi a nuove sfide. La presente sezione si sofferma sui particolari sviluppi giuridici a livello nazionale e internazionale.

Fonte: Gerd Altmann /Pixerio

a) Convenzione sulla cibercriminalità

Con la ratifica della Convenzione del Consiglio d'Europa sulla cibercriminalità, la Svizzera intensifica la sua partecipazione alla lotta contro la criminalità informatica e su Internet. La Convenzione e le modifiche di diritto interno che ha comportato sono entrate in vigore in Svizzera il 1° gennaio 2012.

La Convenzione costituisce il primo trattato internazionale per la lotta contro la criminalità informatica e su Internet. Essa obbliga gli Stati contraenti a sanzionare in particolare la frode informatica, il furto di dati, la falsificazione di documenti mediante computer, l'accesso a sistemi informatici protetti come pure la pedopornografia e la violazione di diritti d'autore su Internet.

La Convenzione disciplina inoltre le modalità di raccolta e conservazione, nelle inchieste penali, delle prove costituite da dati elettronici. Intende in particolare garantire che le autorità inquirenti possano accedere rapidamente ai dati trattati elettronicamente, affinché questi ultimi non possano essere falsificati o eliminati nel corso della procedura. Infine, la Convenzione intende garantire una cooperazione ampia, rapida ed efficace tra gli Stati contraenti.

Per attuare la Convenzione è stato necessario adeguare il Codice penale e la legge sull'assistenza in maniera penale:

- per quanto concerne la fattispecie penale dell'accesso indebito a un sistema per l'elaborazione di dati (*hacking*; art. 143bis CP), la punibilità è stata anticipata: ora è perseguibile anche chi rende accessibili o diffonde password, programmi e altri dati, sapendo o presumendo che essi saranno usati per accedere illegalmente a un sistema informatico protetto;

- la legge sull'assistenza in materia penale conferisce alla competente autorità svizzera la facoltà di trasmettere, in determinati casi e a fini investigativi, i dati relativi al traffico informatico all'autorità richiedente prima della conclusione della procedura di assistenza giudiziaria (cfr. art. 18*b* AIMP). Tuttavia, tali dati, che forniscono informazioni sul mittente, il destinatario, l'orario, la durata, la dimensione e il percorso di un messaggio, possono essere utilizzati come mezzi di prova soltanto dopo che la decisione finale sulla concessione e sulla portata dell'assistenza giudiziaria è passata in giudicato;

- è stato inoltre deciso di affidare alla Centrale operativa fedpol (SPOC, CO fedpol), la funzione di punto di contatto operativo 24 ore su 24, prevista dall'articolo 35 della Convenzione. Lo SCOCI offre sostegno allo SPOC nell'ambito del trattamento delle richieste ai sensi della Convenzione.

b) Strategia nazionale per la protezione della Svizzera contro i rischi informatici

Il 27 giugno 2012 il Consiglio federale ha approvato la «Strategia nazionale per la protezione della Svizzera contro i rischi informatici»[4]. Con la Strategia il Consiglio federale, in collaborazione con le autorità, il mondo dell'economia e i gestori di infrastrutture critiche, intende minimizzare i rischi informatici ai quali sono esposti quotidianamente.

La Strategia considera i rischi informatici come fenomeno direttamente collegato ai processi esistenti e alle responsabilità degli attori coinvolti. Tali rischi informatici devono pertanto trovare riscontro anche all'interno dei processi di gestione dei rischi già in uso. Occorre in primo luogo che i responsabili acquisiscano una conoscenza di base e sviluppino una certa sensibilità nei confronti dei rischi informatici.

A tale scopo il Consiglio federale ha incaricato i Dipartimenti di avviare al loro interno l'attuazione delle 16 misure e di estenderle alle autorità cantonali e al mondo dell'economia. Le misure previste spaziano dall'analisi dei rischi delle infrastrutture TIC critiche alla maggiore considerazione degli interessi della Svizzera in tale settore a livello internazionale.

La misura 6 prevede la gestione di una panoramica a livello nazionale dei casi penali e la garanzia del coordinamento dei casi di portata intercantonale. Le informazioni ricavate dovranno confluire in una rappresentazione globale della situazione. Il DFGP dovrà, in collaborazione con i Cantoni, sottoporre entro la fine del 2016 il documento programmatico che chiarirà le questioni relative ai punti di contatto con altri attori coinvolti nell'ambito della minimizzazione dei rischi informatici, al coordinamento con i lavori per la rappresentazione della situazione nonché alle risorse e agli adeguamenti giuridici necessari a livello federale e cantonale. Sulla base della decisione del comitato direttivo dello SCOCI e della direzione di fedpol, lo SCOCI garantirà per conto di fedpol il coordinamento e l'adempimento del mandato in relazione ai lavori di attuazione della Strategia.

[4] http://www.admin.ch/ch/i/ff/2013/499.pdf

9. Glossario

Adult check	Sistema per limitare l'accesso a un sito web esclusivamente agli utenti maggiorenni.
Chat	Comunicazione elettronica in tempo reale, solitamente via Internet.
Cloud Computing	Utilizzo della memoria, delle capacità di calcolo dei computer e di server sparsi in tutto il mondo, connessi tra loro attraverso una rete (Internet). Le applicazioni e i dati non si trovano più sul computer locale, ma in una cosiddetta nuvola (*cloud*) composta da un numero determinato di server distanti fra loro e interconnessi grazie a dei collegamenti a banda larga di eccellente qualità, indispensabili per la fluidità del sistema.
Cyberbullying	Si parla di ciberbullismo quando sono utilizzati mezzi di comunicazione moderni quali cellulari, chat, reti sociali informatiche quali Netlog o Facebook, portali video, forum o blog per pubblicare testi, immagini o filmati diffamatori con cui denigrare, offendere o molestare una determinata persona. Le aggressioni in genere si ripetono nel tempo o persistono durante un periodo prolungato e le vittime risultano particolarmente vulnerabili.
One-Click-hosting	Servizi web che offrono agli utenti spazio per salvare i propri file (soprattutto video o audio). Tali servizi forniscono inoltre un URL che permette d'accedere ai file per poterli scaricare.
Peer-to-Peer	Modello di rete informatica per la condivisione di file tra utenti di stesso livello (*peer*).
Phishing	Metodo utilizzato per ottenere in modo fraudolento i dati personali dell'utente (password, nome utente ecc.), soprattutto imitando nella grafica e nel contenuto siti Internet autentici.
Pornografia dura	Rappresentazione di atti sessuali con fanciulli (pedofilia, pedopornografia), animali, escrementi umani o atti violenti. (art. 197 n. 3 CP).
Proxy	Un *proxy* è un server che funge da tramite tra un client (l'utente) e un server (il sito web che s'intende consultare).
Redirect Service	Un *redirect service* permette di beneficiare di un URL semplificato per accedere a un contenuto (URL più semplice da ricordare o comunque più breve rispetto a quello del contenuto verso cui si viene deviati).
Spam	Invio di enormi quantità di e-mail indesiderate per fini pubblicitari, e talvolta anche per installare *malware* sul computer dell'ignaro destinatario.
Streaming	Modalità di trasmissione in diretta di dati audio e video che non necessita il *download* sul disco rigido dei contenuti visionati.
URL	(*Uniform Resource Locator*) sequenza di caratteri utilizzata per indirizzare gli utenti verso le risorse del web (indirizzo web).
Valore hash	Valore attribuibile in modo univoco a un'immagine (impronta digitale).

10. Possibili sviluppi e minacce del 2013

Il numero di segnalazioni pervenute allo SCOCI permette solo in minima parte di trarre conclusioni in merito allo sviluppo effettivo della criminalità su Internet o dei contenuti illegali diffusi in rete. Tutt'al più consente di rilevare le tendenze relative alla disponibilità della popolazione a segnalare eventuali casi di cibercriminalità e al modo in cui la società percepisce la criminalità su Internet.

***Trojan* bancari:** non è possibile escludere l'eventualità che l'operazione annunciata da alcuni gruppi di *hacker* russi denominata «*Blitzkrieg Project*» ai danni delle banche statunitensi possa costituire una minaccia anche per le banche svizzere. Gli attacchi informatici dovrebbero consistere soprattutto nel furto di dati di login per mezzo di *trojan*. Tuttavia, considerando che la maggior parte delle banche svizzere utilizza meccanismi di autenticazione a più livelli, il rischio di danni finanziari diretti causati da transazioni effettuate erroneamente dovrebbe essere minimo ma non del tutto inesistente.

***Malware* sugli apparecchi di telefonia mobile:** nel 2012 il numero delle varianti di software dannosi che infettano soprattutto gli *smartphone android* è aumentato in maniera esponenziale e gli esperti prevedono che possa incrementare ulteriormente. Le vittime di questi attacchi si trovano così a dover sostenere costi aggiuntivi generati dall'utilizzo di Internet a banda larga, dato che gli apparecchi infettati vengono impiegati con lo scopo di lanciare attacchi DDoS, oppure a ricevere SMS di spam indesiderati. Inoltre è possibile che i dati personali quali i contatti registrati nella rubrica o le password vengano carpiti e venduti ad altri criminali.

Malware: anche il numero dei casi di infezioni da *malware* dovrebbe far registrare un ulteriore aumento. Questi programmi continuano ad avere come obiettivo principale il furto di dati bancari, dei numeri delle carte di credito e delle password. I cibercriminali mirano inoltre a carpire i dati contenuti nelle rubriche per creare false identità ai fini di truffa o a costituire reti bot per compiere attacchi DDoS. È presumibile inoltre che possano nascere nuovi metodi d'infezione, come ad esempio gli *add-on* per i browser o le applicazioni web per i siti di *social media*. È inoltre possibile che vengano sfruttate le falle presenti nei sistemi di sicurezza dei servizi di *cloud computing* per installare software dannosi sui computer oggetto dell'attacco.

Furto di dati: come dimostrano diversi casi, neanche i siti web più piccoli vengono risparmiati dagli attacchi informatici. I dati dei clienti, ad esempio gli indirizzi, sono un bene prezioso per gli *hacker*, in quanto facilitano enormemente il ricorso alle tecniche d'ingegneria sociale e possono essere quindi sfruttati anche per compiere altri tipi di truffe. Gli *hacker* hanno inoltre la possibilità di vendere su determinati forum gli indirizzi e-mail ottenuti abusivamente. Proprio perché i criminali informatici si specializzano in determinati ambiti, come ad esempio il furto e la vendita di dati, è presumibile che in futuro anche gli obiettivi più piccoli possano rivelarsi interessanti e dunque essere presi di mira.

***Scam*:** con la diffusione di Internet in Africa e con l'espansione del ceto medio in Paesi quali la Nigeria, il Sud Africa o il Marocco (seppur meno abbiente rispetto a quello dei Paesi occidentali), gli esperti temono che nei prossimi anni le offerte fraudolente presenti su annunci privati o su siti di aste online possano tornare ad aumentare no-

tevolmente. Si prevede che il volume di questo tipo di annunci raddoppierà entro il 2015.

Attacchi DDoS: nel 2012 sono stati lanciati diversi attacchi DDoS a scopo ricattatorio oppure a sfondo politico. Anche nel 2013 si prevedono attacchi di questo tipo. Le grandi potenze stanno nel frattempo allestendo unità di riserva, militari e di intelligence, destinate alla difesa delle infrastrutture critiche dagli attacchi DDoS o di *hacking*. Questo dimostra che gli attacchi DDoS perpetrati su larga scala sono considerati come una minaccia quanto mai realistica.

Per contrastare tutte le forme di cibercriminalità, è indispensabile la collaborazione di tutte le parti coinvolte (governi, autorità di perseguimento penale, provider e autorità regolatrici). Lo SCOCI partecipa già a diversi gruppi di lavoro nazionali e internazionali incentrati sulla lotta a reati specifici. Si presume infine che la collaborazione tra le istituzioni pubbliche e private (partenariato pubblico-privato) finalizzata a contrastare la criminalità su Internet assumerà un ruolo sempre più decisivo.