MOZIONE

Aggiunta di normative riguardanti lo spazio cibernetico e creazione di un corpo per la lotta alla cibercriminalità (online e offline)

del 19 giugno 2017

Premessa

Lo sviluppo di Internet caratterizza la nostra era. È attraverso lo spazio cibernetico che sempre più si realizzano le fondamentali libertà di informazione, di espressione e di associazione del cittadino, viene perseguita la trasparenza della politica e l'efficienza dei servizi della Pubblica Amministrazione, si promuove la crescita e l'innovazione delle nostre aziende. Lo spazio virtuale rappresenta un'arena in cui ogni giorno si stabiliscono attraverso le frontiere geografiche miliardi di interconnessioni e si scambia conoscenza a livello globale, ridisegnando il mondo ad una velocità senza precedenti.

Il risiedere all'interno delle reti di una mole ogni giorno maggiore di saperi essenziali ai fini della sicurezza e della prosperità del sistema-Paese rende sempre più pressante l'esigenza di garantire, anche nello spazio cibernetico, il **rispetto dei diritti e dei doveri**, che già vigono nella società civile, nel tessuto economico e nella comunità internazionale.

L'arena digitale non è uno spazio al di fuori delle leggi, ed è nostra responsabilità lavorare affinché vi si affermino compiutamente i valori ed i princìpi democratici, oltre che le norme di rispetto dell'individuo, di eguaglianza e di libertà nelle quali crediamo. È peraltro solo in un ambiente contrassegnato da fiducia e rispetto reciproco che sarà possibile cogliere appieno le opportunità di crescita offerte dalle piattaforme digitali, assicurando lo sviluppo di uno **spazio cibernetico aperto, affidabile e sicuro per il sistema finanziario, per le aziende e per i consumatori.**

La crescente dipendenza delle società moderne dallo spazio cibernetico rende sempre più grave il danno che può giungere dalla compromissione delle reti o da mirati attacchi attraverso di esse. Le minacce possono originare da qualsiasi punto della rete globale e spesso colpiscono gli anelli più deboli della catena, ossia i soggetti più fragili, o i sistemi meno protetti. Attraverso le reti possono compiersi crimini odiosi come lo scambio online di materiale pedopornografico, o realizzarsi furti e truffe che, oltre a danneggiare gravemente gli interessi privati, impediscono che si affermi il necessario livello di fiducia nella comunità digitale.

Le Problematiche

Le forme di criminalità segnalate allo **SCOCI Servizio di coordinazione per la lotta contro la criminalità su Internet** possono essere suddivise in due ambiti interconnessi. Per criminalità su Internet in senso stretto s'intendono:

- i reati perpetrati utilizzando le tecnologie di Internet o sfruttando i punti deboli di esse. Ne fanno parte ad esempio i fenomeni quali l'hacking, i Distributed Denial of Service (gli attacchi DDoS) o la creazione e la diffusione di software nocivi (malware). Tali reati sono diventati possibili soltanto con l'avvento di Internet e sono diretti contro le sue tecnologie.
- La criminalità su Internet in senso lato sfrutta invece le possibilità offerte da Internet, quali la posta elettronica o i server per lo scambio di dati, per commettere reati. Rientrano ad esempio in tale categoria i metodi di truffa utilizzati su piattaforme di piccoli annunci o la diffusione di materiale pornografico illegale.

Nel dettaglio:

Furto d'Identità

Internet è una vera fonte di informazioni personali. Molte società o istituzioni conservano informazioni circa i loro clienti in database installati in sistemi connessi a Internet non protetti adeguatamente. Sono molteplici i casi in cui dei malintenzionati sono riusciti a procurarsi l'accesso a database contenenti dati considerati sensibili, quali ad esempio i numeri delle carte di credito. Internet è anche il luogo più usato per vendere o scambiare informazioni di qualsiasi tipo, rendendo sempre più difficile per le istituzioni preposte il riconoscimento dei colpevoli.

Stalking

Il diritto svizzero non prevede il reato di stalking, quando per questo termine si intende una serie di atteggiamenti tenuti da un individuo, detto *stalker*, che affliggono un'altra persona, perseguitandola, generandole stati di paura e ansia, arrivando persino a compromettere lo svolgimento della normale vita quotidiana. In altri Stati europei gli atti persecutori sono puniti penalmente.

Grooming

Grooming significa costruire un legame emotivo con un bambino per guadagnare la sua fiducia a fini di abuso sessuale o di sfruttamento. I bambini e i giovani possono essere presi di mira in Internet o nel mondo reale, da un estraneo o da qualcuno che conoscono - ad esempio, un familiare, un amico - o in ambito professionale. I molestatori possono essere sia maschio che femmina. Potrebbero essere di qualsiasi età. Molti bambini e giovani non capiscono di essere stati molestati, o in che modo è successo è l'abuso. Al momento, in Svizzera **non esiste una legge sul "grooming"**.

Furti d'identità, stalking e grooming devono perciò diventare **reati penali**. I pedofili che adescano minorenni in rete vanno puniti severamente e la pedocriminalità in Internet va combattuta in modo sistematico.

Polizia e cybercriminalità

Risale al 2001 l'approvazione del Consiglio federale riguardante la Convenzione del Consiglio d'Europa sulla cybercriminalità, che voleva adeguare il diritto e la procedura penale nonché la collaborazione internazionale all'evoluzione in atto nell'ambito delle tecnologie informatiche e con la quale il Consiglio federale s'impegnava a lottare in modo più incisivo a livello internazionale contro la criminalità ad alta tecnologia che opera a mezzo computer e Internet.
Nel 2012 il SCOCI dell'Ufficio federale di polizia (fedpol) ha ricevuto un numero nettamente maggiore di segnalazioni di sospetto da parte della popolazione. Infatti, le 8241 comunicazioni pervenute nel 2012 corrispondono a un aumento del 55 per cento rispetto all'anno precedente. Per la prima volta le comunicazioni concernenti i reati economici hanno superato quelle relative alla pornografia vietata.
Le comunicazioni inviate a SCOCI tramite l'apposito modulo online sono di varia natura e presentano di norma una buona qualità. Oltre l'80% delle comunicazioni pervenute nel 2012 (6639 segnalazioni) presentano una **rilevanza penale**. Tra i reati più frequentemente segnalati vi sono la pornografia con fanciulli, la truffa, il phishing, lo spamming e il danneggiamento di dati.

Lotta attiva contro la pedocriminalità

Anche nel 2012 il lavoro di SCOCI non si è limitato soltanto alla ricezione e al trattamento di comunicazioni inoltrate dalla popolazione. SCOCI effettua ricerche in rete anche indipendentemente dalla presenza di indizi ed è quindi presente su Internet anche in settori

meno accessibili. Le ricerche attive svolte nel 2012 hanno generato 450 dossier su casi sospetti, ovvero quasi il doppio rispetto all'anno precedente.

La maggioranza dei dossier su casi sospetti è scaturita dal monitoraggio delle reti peer to peer che ha permesso di identificare 417 persone coinvolte nello scambio attivo di file dai contenuti pedopornografici su tali reti. Nel 98% dei casi le indagini hanno dato luogo a perquisizioni domiciliari eseguite dalle autorità cantonali di perseguimento penale.
Sulla base dell'ordinanza del Cantone di Svitto sulla polizia, nel 2012 i collaboratori di SCOCI in 33 casi hanno svolto indagini preliminari sotto copertura nei confronti di pedocriminali in chatroom, su siti Internet o in reti private di condivisione di dati peer to peer.

Rapporto SCOCI 2014

Lo SCOCI coopera in modo proattivo con Interpol, Europol, FBI, HSI e molte altre autorità estere. Quale rappresentante della Svizzera, lo SCOCI partecipa a gruppi di lavoro internazionali insieme ai seguenti partner: i pubblici ministeri svizzeri, le polizie cantonali, i rappresentanti del settore finanziario, i fornitori di servizi Internet oppure la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, SWITCH Internet Domains e diverse ONG. Altri partecipanti sono la Prevenzione svizzera della criminalità, il Servizio delle attività informative della Confederazione, il DFAE nonché altri servizi federali e cantonali. Affinché la Svizzera possa contare sul sostegno necessario anche in tempi difficili, occorre - come sosteneva già l'ex Consigliere federale Ogi - curare personalmente i contatti e le amicizie a livello internazionale.
La cooperazione internazionale consiste anche nello smantellare reti bot illegali costituite da computer infetti collegati tra loro per compiere atti fraudolenti, come pure nel **coordinare operazioni nazionali** che conducono all'arresto di hacker. Anche l'adesione a comitati o alleanze internazionali che intendono **combattere la pedocriminalità** su Internet come la *Global Alliance against Child Sexual Abuse Online*[1] è altrettanto importante. Ad essere fondamentale è tuttavia la fiducia che lo SCOCI è in grado di suscitare grazie all'elevata qualità del suo lavoro. Questa fiducia gli permette infatti di continuare ad essere un partner apprezzato e affermato nella lotta alla cibercriminalità.
Nemmeno in futuro lo SCOCI dovrà temere di non avere sufficiente lavoro o di svolgere un'attività ordinaria priva di sfide. Le cyber-rapine in banche con un bottino miliardario, il sequestro di **quantità record di materiale pedopornografico** o i danni milionari causati alle piccole e medie imprese svizzere da attacchi di ingegneria sociale sono solo alcuni esempi che mostrano il carico di lavoro che lo SCOCI - **finanziato per due terzi dai Cantoni e per un terzo dalla Confederazione** - è chiamato ad affrontare insieme ai suoi dieci collaboratori e ai sei collaboratori di fedpol assegnatigli a titolo di sostegno.
Alla fine del 2016 lo SCOCI inoltre ha sottoposto al Consiglio federale il piano di attuazione della misura 6 della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi. In tale contesto proseguono i lavori per la gestione di una panoramica svizzera dei casi e il coordinamento di affari di portata intercantonale. Lo SCOCI è ambito, non passa quasi giorno senza che si parli di un caso nuovo, sempre più eclatante, di cibercriminalità. Chissà, forse la sfida più grande per lo SCOCI è quella di trasmettere agli organi decisionali una cognizione generale ed estesa della portata della criminalità informatica. In ogni caso **servono buone condizioni quadro e investimenti nel settore della sicurezza**, anche se questo può comportare costi aggiuntivi.

A tal proposito invito a leggere l'accurato rapporto del SCOCI 2014:
https://www.cybercrime.admin.ch/dam/data/kobik/Berichte/2015-03-26/jb-kobik-i.pdf

[1] *https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_switzerland_en.pdf*

Al momento il Cantone Ticino non dispone di un servizio preposto alla lotta contro la criminalità su Internet, e pare che al momento anche le forze spiegate a questo scopo a livello nazionale siano insufficienti.

Per le facoltà concesse dalla legge, chiedo al Consiglio di Stato:

- di aggiungere delle normative riguardanti il Cyberspazio al fine di combattere:
  - **furti d'identità;**
  - **stalking;**
  - **grooming,**

  e **creare un corpo di Polizia formato e preposto alla lotta contro questi crimini.**

Sara Beretta Piccoli
Per il Gruppo PPD+GG