

Supporto allo sviluppo della sicurezza e legalità informatica nell'ambito delle iniziative rivolte ai giovani

Michele Crudele - 2011-07-24

A.1.b) Relazione sulle politiche di prevenzione della Polizia delle comunicazioni

Premessa

La presente relazione è frutto dei seguenti approfonditi colloqui:

- 13 maggio – Antonio Apruzzese, direttore della Polizia delle comunicazioni
- 1 giugno – Nunzia Ciardi, vicedirettore della Polizia delle comunicazioni
- 13 giugno – Marco Valerio Cervellini, Responsabile della Polizia delle comunicazioni per i progetti educativi sulla navigazione sicura dei minori
- 12 luglio – Caterina Feroletto e Paola Turi, incaricate della Polizia delle comunicazioni per la divulgazione nelle scuole, e alcuni incaricati del Centro nazionale per il contrasto alla pedopornografia sulla rete

Le opinioni espresse in questa relazione sono dell'autore, anche quando sono frutto delle conversazioni con i protagonisti della difesa dei diritti del cittadino.

La Polizia delle comunicazioni, è un Servizio centrale della Polizia di Stato abitualmente chiamato, per motivi storici, Polizia Postale e delle comunicazioni, oppure Polizia Postale.

La Polizia delle comunicazioni è organizzata nelle seguenti aree di intervento:

- Pedopornografia: attraverso il Centro Nazionale per il contrasto della pedopornografia su Internet raccoglie segnalazioni, coordina le indagini sulla diffusione, in Internet o tramite altre reti di comunicazione, delle immagini di violenza sessuale sui minori e stila le *black list* dei siti web pedofili.
- Cyberterrorismo: una qualificata squadra di investigatori monitora costantemente la rete Internet e conduce indagini specialistiche sul sempre più diffuso utilizzo delle nuove tecnologie di comunicazione da parte dei gruppi antagonisti ed eversivi nazionali e stranieri.
- Copyright: i circuiti di condivisione di file (*file sharing*) e i numerosi altri servizi Internet che consentono la circolazione di opere dell'ingegno hanno contribuito alla diffusione illegale di file e hanno imposto un'attenzione operativa costante al fenomeno.
- Hacking: tutti coloro che utilizzano la Rete Internet per danneggiare o per colpire, tramite la stessa, obiettivi a essa correlati sono oggetto di attenzione da parte degli investigatori.
- Protezione delle Infrastrutture Critiche del Paese: le aziende e gli enti che sostengono e garantiscono il funzionamento del Paese mediante reti e servizi informatici o telematici vengono monitorati e protetti da attacchi informatici attraverso l'azione di una equipe di investigatori specializzati.
- E -banking: le nuove frontiere del commercio e della circolazione di denaro impongono un puntuale monitoraggio delle risorse tecnologiche correlate con la finalità di garantirne la sicurezza.
- Analisi criminologica dei fenomeni emergenti: una qualificata equipe di psicologi e investigatori analizza ed elabora dati relativi alle nuove frontiere del crimine informatico, ponendo il sapere clinico e criminologico delle scienze sociali al servizio di una più efficace azione di prevenzione e repressione dei reati informatici.

- Giochi e scommesse *online*: attraverso il monitoraggio della Rete e un'attenta analisi dei siti dedicati si individuano le attività non autorizzate dal Ministero delle Finanze - Amministrazione autonoma monopoli di Stato.

Senza pretesa di esaustività, in calce alla presente relazione, sono riportate alcune pagine del sito istituzionale della Polizia di Stato, sull'azione della Polizia delle comunicazioni in relazione ad attività criminose connesse con i minori.

Interventi formativi

Il progetto "In strada come in rete" realizzato in collaborazione con Provincia di Roma, Polizia Provinciale, Unicef, Microsoft e Google, per contrastare i pericoli della strada e le minacce del web, soprattutto pedopornografia e bullismo in rete, è rivolto agli studenti delle scuole secondarie di I grado e ai loro genitori e insegnanti. Nell'anno scolastico 2010-11 si è svolta la seconda edizione, con una forte richiesta da parte degli istituti scolastici per ospitare gli incontri formativi. Ne sono stati oggetto di intervento 70 in un anno a Roma, ma esistono iniziative analoghe al nord, anche da più anni come "Web in cattedra", promosso da Microsoft, alla quale collabora la Polizia delle comunicazioni con l'Osservatorio Nazionale Abusi Psicologici (O.N.A.P.) e gli Uffici scolastici regionali. È interessante notare che il materiale informativo diffuso nell'ambito di questi progetti di formazione attinge anche dal portale www.ilFiltro.it creato dall'autore di questo documento nel 2001 e divenuto molto presto un punto di riferimento per la conoscenza e la valutazione dei sistemi di protezione della navigazione su Internet. Questa constatazione rafforza la tesi dell'importanza della pubblicazione in rete di contenuti di qualità, perché possano essere liberamente riprodotti e costituire un patrimonio culturale comune: nello specifico si tratta di contribuire alla difesa dei minori.

Nel progetto "In strada come in rete" è particolarmente interessante l'accostamento dell'educazione stradale con quella della navigazione in rete. È vero infatti che "attraversare" la rete richiede una formazione specifica, analoga a quella che i genitori trasmettono ai figli piccoli per attraversare la strada o a quelli più grandi per imparare i comportamenti corretti come pedoni e automobilisti. Purtroppo gli stessi genitori non hanno, nella maggior parte dei casi, le conoscenze e l'esperienza necessarie per segnalare ai propri figli i veri rischi di Internet o per indirizzarli a un uso consapevole e positivo delle risorse in rete. Disgraziatamente questa evidente carenza formativa non trova riscontro nella partecipazione agli incontri organizzati dalla Polizia delle comunicazioni, ai quali sono presenti nella maggior parte dei casi pochi genitori fino a un minimo, in una situazione peraltro sostenuta da una intensa promozione, di 6 su 400 invitati. Di contro, l'interesse degli insegnanti è quasi sempre alto.

Un ambito nel quale l'intervento formativo della Polizia delle comunicazioni è meno frequente è quello delle scuole primarie, dove i maestri (o meglio le maestre, che ormai sono la quasi totalità) non hanno competenze sufficienti per affrontare la responsabilità di condurre i bambini nella navigazione in rete. La diffusione dei laboratori di informatica e dei computer in quelle scuole non è stata equilibrata da un incremento della formazione specifica per i docenti. La minore varietà di professionalità dei maestri rispetto ai professori delle scuole secondarie rende anche più raro nelle scuole primarie il caso di "volontariato" di docenti che si accollano il compito della gestione delle attrezzature informatiche scolastiche.

Alcuni poliziotti sottolineano che non si tratta solamente di un problema tecnico o di saper installare i sistemi di protezione della navigazione, ma di una carenza culturale che non permette ai formatori di dialogare con gli studenti più giovani in un linguaggio comune, per invitarli a coltivare le caratteristiche positive e utili di Internet conoscendone i pericoli e le criticità.

La Polizia delle comunicazioni interviene anche in manifestazioni destinate al grande pubblico, come ad esempio i campionati mondiali di Beach Volley al Foro Italico, dove nel giugno 2011 è stata presente nello stand del Dipartimento della Gioventù della Presidenza del Consiglio dei Ministri. In quella circostanza, i bambini e ragazzi presenti nelle diverse aree di gioco sono stati invitati a partecipare ad alcune sessioni formative a carico del personale presente della Polizia delle comunicazioni.

Analisi dei comportamenti

Tra i comportamenti giovanili legati all'uso di Internet, oggetto di denuncia alla Polizia, il cyberbullismo occupa un posto costante. Il fenomeno è esploso mediaticamente con le vessazioni filmate e pubblicate nel 2006 su YouTube da parte di alcuni studenti nei confronti di un compagno di scuola disabile mentale. A fine 2010 è stata condannata anche la docente che appare nel filmato, per non essere intervenuta. Se tali comportamenti violenti sono sempre stati presenti nelle scuole, sia pure in misura limitata, la novità degli ultimi anni sta nella loro spettacolarizzazione: i ragazzi se ne vantano pubblicando immagini e video delle "bravate" senza rendersi conto che diventano così anche loro vittime, perché la traccia dei loro comportamenti scorretti resterà per lungo tempo e inquina la loro reputazione da adulti.

Ma il cyberbullismo in senso stretto non è la occasionale pubblicazione di un evento di aggressione o violenza, ma la reiterata vessazione nei confronti di un minore, fatta attraverso mezzi informatici e di telecomunicazione: invio continuo di SMS, denigrazione su *social network*, furto di identità per diffondere calunnie, e-mail di insulto, con comportamenti anche analoghi a quello che per gli adulti si chiama *stalking*.

Un problema che registra un aumento delle segnalazioni e denunce è il gioco *online* illegale di minorenni. In Italia non è possibile accedere in situazioni normali a siti esteri di scommesse, a causa della legislazione che impone un regime di autorizzazione e tassazione a chi esercita l'attività di gestore di scommesse. Tuttavia il sistema di blocco dei siti stranieri è aggirabile senza particolari difficoltà e lo stratagemma è alla portata degli adolescenti che, non potendo giocare legalmente sui siti italiani dove è richiesta la maggiore età, accedono a quelli esteri, impegnando cifre personali o sottratte a genitori e parenti, avendone carpito i codici delle carte di credito.

Questa abilità dei minori di superare barriere tecnologiche e la consueta definizione di "nativi digitali" per indicare la loro capacità di affrontare le apparecchiature informatiche e di telecomunicazioni senza nessun timore, non vuol dire necessariamente che siano "esperti" delle reti e quindi capaci di capire i rischi e adottare le misure difensive opportune. Anzi, a volte, l'eccessiva familiarità con Internet li porta a sottovalutarne le minacce, oppure a "cavalcare" situazioni pericolose per ottenerne un vantaggio.

L'esempio più clamoroso è la vendita di proprie immagini oscene in cambio di ricariche telefoniche o di altri regali in moneta o in oggetti. Il ragionamento delle ragazzine (ma a volte sono anche maschi) è apparentemente logico: non mi fa nessun danno fisico cedere una mia immagine, anzi ci guadagno. Senza entrare in analisi psico-pedagogiche, è un dato di fatto che alcune di queste situazioni iniziano con trasferimento di fotografie e poi degenerano in contatti personali, causati dal ricatto del pedofilo di "mostrare le foto ai genitori della vittima", oppure per curiosità morbosa della minorenne. Non sono rari i casi opposti, nei quali la ragazza ricatta il pedofilo, avendone scoperto l'identità, minacciando di denunciarlo per ottenere più soldi. Si sviluppa così una relazione digitale (termine più consono di "virtuale" che fa pensare erroneamente ad assenza di conseguenze reali) o materiale che svilisce il rispetto di se stesse e introduce a potenziali situazioni più gravi di depravazione.

L'ostentazione di sé è anche frequente su Facebook, dove molti minorenni, persino quelli che hanno meno di 13 anni (età limite per i gestori del *social network*), aprono un profilo alterando le informazioni personali, ma lasciando involontariamente sufficienti elementi agli adescatori per essere riconosciuti e rintracciati.

La finta dichiarazione di età genera anche situazioni impreviste: una dodicenne, spacciata per una ventenne, ha ricevuto proposte "audaci" da un ventiduenne convinto di aver a che fare con una maggiorenne. La bambina, non abituata a un linguaggio sessuale adulto, ha subito un trauma psicologico.

Equivoci simili nascono dal comportamento di alcuni genitori che lasciano usare ai loro figli il proprio profilo Facebook: capita quindi che il bambino o la bambina dialoghi in rete con l'identità di un quarantenne, con tutti i rischi connessi.

Si è anche dato il caso di un diciassettenne che vessava a lungo, anche con proposte oscene, bambini di dieci anni, che non avevano avuto il coraggio di raccontare a nessuno quanto subivano, ma davanti alla poliziotta in occasione di un intervento formativo a scuola, riconoscendo nei racconti di quest'ultima situazioni analoghe alla propria, hanno finalmente trovato la forza di denunciare il colpevole. Siamo quindi in presenza di minorenni che sono sia vittime che colpevoli.

Sono segnalati anche casi di minori che compiono azioni illegali di vandalismo o altri crimini informatici, credendo di poter passare inosservati perché adottano misure di camuffamento. È invece molto frequente che la loro presunta abilità sia solamente una conoscenza superficiale del funzionamento dei protocolli di Internet per cui non è difficile alla Polizia delle comunicazioni rintracciare i colpevoli. D'altra parte, i ragazzi non sanno difendersi efficacemente, sia dal punto di vista tecnico che comportamentale: il *social engineering* funziona anche con i giovani e non solo con gli anziani. Le ormai tradizionali truffe e le frodi nate da messaggi di posta elettronica falsificati o confezionati ad arte, si affiancano ad altri sistemi più sofisticati che partono da *social network*.

Proprio Facebook è diventata in Italia la piazza migliore per gli adescatori, sostituendosi a MSN come canale di comunicazione iniziale.

Riferimenti

È utile riportare alcuni testi dal sito *web* della Polizia di Stato che ne illustrano l'attività e le metodologie.

Centro nazionale per il contrasto alla pedopornografia sulla rete

La legge 6 febbraio 2006 n. 38 affida al "Centro Nazionale per il contrasto della pedopornografia sulla rete Internet" la lotta a questo odioso crimine.

Il Centro è la risposta della Polizia di Stato ai criminali che usano la rete per delinquere senza frontiere nei confronti dei minori.

E' istituito presso il Servizio Polizia postale e delle comunicazioni del Dipartimento della Pubblica Sicurezza, e si occupa di prevenzione e repressione di questi reati.

L'obiettivo primario è la difesa dei ragazzi in Internet, attraverso servizi di monitoraggio per la ricerca di spazi virtuali clandestini dove si offrono immagini e filmati di minori abusati per un turpe commercio online. Più in generale il monitoraggio continuo focalizza l'attenzione sulla scoperta di siti e dinamiche che possano rappresentare fonte di pericolo nella navigazione dei più giovani.

Per ciò che concerne i siti pedopornografici, la legge istitutiva individua nel Centro il punto di raccordo per la trattazione delle segnalazioni, provenienti sia da altre Forze di Polizia anche straniere, sia da cittadini, da Associazioni di volontariato e da Provider.

Da tutta questa attività il Centro provvede a ricavare l'elenco dei siti pedopornografici della Rete, la c.d. "black list", che viene fornito agli "Internet Service Provider" perché ne venga inibita la navigazione, attraverso sistemi tecnici di filtraggio.

Se navigando ci si imbatte, anche involontariamente, in uno di questi siti interdetti appare un'apposita "stop page", pagina di blocco, contenente l'avviso di interdizione.

Contribuiscono al contrasto di questi crimini anche i sistemi nazionali bancario e finanziario, tramite la mediazione della Banca d'Italia, che consente di acquisire informazioni relative alle transazioni ed alle spendite illecite sul mercato online volte all'acquisto di foto e filmati di abusi nei confronti di minori.

La stessa legge 6 febbraio n. 38 istituisce l' "Osservatorio per il contrasto della pedofilia e della pornografia minorile", presso la Presidenza del Consiglio dei Ministri, con compiti di monitoraggio del fenomeno per il raccordo di tutte le Istituzioni interessate alle tematiche minorili, inclusi gli organi giudiziari ed i Servizi sociali.

Il Centro, quale organo di raccordo operativo, dialoga costantemente con l'Osservatorio, organo di raccordo istituzionale, al quale fornisce propri dati per l'analisi e la prevenzione dell'abuso minorile.

Una coalizione mondiale sotto la guida di Interpol, con la partecipazione di Europol, attua quotidianamente collaborazioni internazionali di Polizia per l'identificazione delle vittime della pedopornografia, dovunque esse risiedano.

Nuove frontiere nell'adescamento online dei bambini

La rete internet ha cancellato i confini geografici aprendo per tutti enormi potenzialità di comunicazione, scambio e contatto tra le persone. Tale meravigliosa opportunità ha purtroppo un suo rovescio della medaglia: dietro nickname di fantasia, attraverso falsi profili su community e social network veri e propri pedofili navigano la rete in cerca di contatti con bambini e ragazzi, si scambiano informazioni sui luoghi virtuali dove reperire materiale di abuso sessuale sui minori, argomentano scambiandosi opinioni sulla liceità della pedofilia.

Il pedofilo è in generale un criminale piuttosto lucido e con una scarsa percezione della gravità delle sue inclinazioni: spesso quindi la manipolazione è una modalità che ben sanno utilizzare e che mettono al servizio di una buona capacità di intrattenere rapporti "epistolari" e conversazioni scritte, le forme tipiche della comunicazione on-line. I pedofili inoltre sono sempre dei profondi conoscitori del mondo infantile e adolescenziale e sanno quindi come e dove concentrare le loro energie per aumentare al massimo la probabilità di ottenere confidenze da utenti minori della rete.

L'iter che conduce un contatto casuale tra un adulto e un minore a divenire un tentativo di adescamento è assai variegato in ragione di molti elementi tra cui spicca decisamente l'estrema variabilità tra personalità e comportamenti tipici dei pedofili.

Nella casistica arrivata all'attenzione dell'unità di Analisi dei Crimini Informatici e del Centro Nazionale per il contrasto alla pedofilia on-line ci sono soggetti con caratteristiche tipiche del criminale lucido, caratterizzato da complesse abilità relazionali che ne fanno un interlocutore attraente e competente nei contatti con minori e altri invece particolarmente diretti e aggressivi nell'interazione on-line, incapaci di attendere i tempi e le difficoltà dei minori più inibiti, con evidenti modalità di interazione e controllo delle emozioni particolarmente immature.

Il pedofilo tuttavia in genere inizia una conversazione su tematiche banali e tipiche della vita di un bambino/ragazzo cercando nelle chat (anche telefoniche), nei forum, nei siti di giochi di ruolo, nei social network proprio quei profili che corrispondono alla sua fascia di età preferita. Talvolta mente sulla sua età anagrafica, salvo poi rivelarla quando la relazione si approfondisce. Le richieste di confidenze sessuali arrivano a volte subito, a volte sono precedute da dichiarazioni di trasporto

sentimentale. La richiesta di immagini osè è il passo successivo a cui segue, qualora ci sia la disponibilità del minore, la richiesta di un incontro reale.

Più recentemente è emerso come sempre più spesso minori in età preadolescenziale (età compresa tra gli 11 e i 14 anni) utilizzino pagine di social network per proporsi in modo provocante e allusivo di una disponibilità sentimentale e d erotica a coetanei ed adulti. Tale fenomeno costituisce una nuova frontiera di impegno delle azioni di prevenzione e repressione dello sfruttamento sessuale di minori a mezzo internet perché, comprendendo come l'inesperienza e l'im maturità di soggetti in fase evolutiva possa ingenerare comportamenti imprudenti, si ravvede in tali comportamenti elementi di grande pericolosità e di estrema preoccupazione. Soggetti pedofili ancora indecisi nel mettere in atto comportamenti di molestia on-line potrebbero interpretare i messaggi allusivi delle potenziali vittime come profferte di disponibilità autentica e consapevole, utilizzando di fronte a se stessi e alla propria coscienza deviata, argomentazioni che conducono ad un pericoloso passaggio all'atto.

Come la Postale smaschera i pedofili online

Hanno competenze informatiche aggiornatissime, passano molte ore del loro lavoro on-line, usano il computer e la tecnologia con grande dimestichezza: sono gli investigatori della Polizia Postale e delle Comunicazioni che, sempre pronte nel cassetto manette e pistola, usano l'ingegno e il click del mouse per "ripulire" la rete da chi ne fa un uso distorto, un uso riprovevole, lo sfruttamento sessuale dei minori.

Con lo studio delle nuove tecnologie, grazie al coordinamento degli uffici periferici e in accordo con le altre forze di polizia straniera, la lotta alla pedofilia on-line individua, indaga, perquisisce e assicura alla giustizia circa 3000 persone negli 11 anni di attività di contrasto.

E' un lavoro complesso e articolato quello degli investigatori, che quando conducono in un'indagine sottocopertura devono, non solo impegnare la loro mente, ma mettere in campo anche tutte le loro risorse psicologiche ed emotive per essere credibili nel fingersi pedofili e per non lasciarsi travolgere dal disgusto e dalla rabbia.

Lo sanno bene anche gli psicologi del Centro Nazionale per il Contrasto alla Pedofilia on-line, che proprio recentemente stanno portando avanti un progetto di formazione assistita che ha come suo obiettivo primario quello di dare voce alle difficoltà del personale e di trasformarle in uno spunto di formazione per tutti i futuri investigatori del web e di valorizzazione della professionalità fino ad oggi espressa dagli operatori.

Cyberbullismo

Un'età compresa tra i 10 e i 16 anni, un'immagine di bravi studenti, una competenza informatica superiore alla media, incapacità a valutare la gravità delle azioni compiute on-line: questo l'identikit del cyber bullo, che usa internet per realizzare quello che magari non riesce a vendicare nella vita reale, quello che non ha il coraggio di fare nel cortile della scuola.

Si conoscono tra i banchi di scuola o nella palestra del pomeriggio. Tramite il click del mouse, si sostituiscono ai compagni di classe più timidi sui social network, a nome di altri diffondono immagini e informazioni riservate tramite mms sui telefonini, raccontano particolari personali o dichiarano disponibilità sessuali a nome delle compagne: questi i comportamenti devianti più spesso arrivati all'attenzione degli agenti della Polizia delle Comunicazioni.

Quando dopo una denuncia intervengono gli agenti per fermare azioni di bullismo spesso si hanno delle reazioni di stupore di vergogna e lacrime da parte dei cyber bulli più giovani che ovviamente non si sono resi conto di quanto fosse stato feroce il loro modo di prendere in giro qualcuno.

Il quadro cambia notevolmente con l'avanzare dell'età dei cyber bulli, i comportanti diventano più articolati, più vessatori, più simili ai maltrattamenti ripetuti, agli insulti davanti agli amici tipici del bullismo "reale".

Numerosi i casi negli ultimi anni, ma nulla vieta di ritenere che i giovani tengano sotto silenzio molte delle prepotenze on-line perché non sanno che esistono leggi per tutelarli e perché in fondo la sofferenza di "leggersi" insultato sul web è motivo di vergogna, è testimonianza di debolezza che non si vuole confessare, nemmeno alla Polizia.

La Polizia delle Comunicazioni promuove progetti per sensibilizzare i giovani nei confronti di questo cattivo uso della rete perché solo una buona informazione può aiutare a tutelare i minori e non solo.

Conclusioni

L'azione della Polizia delle comunicazioni si concentra sul far capire ai giovani il parallelo tra vita reale e "virtuale" che, come detto sopra, sarebbe preferibile definire "digitale". Per esempio, insegnano a non usare una sola *password* per tutte le utenze in rete, così come non hanno una sola chiave per casa, automobile e cassetta di sicurezza.

I poliziotti ricordano ai genitori che il computer non è l'unico strumento di accesso a Internet e che la diffusione di *smartphone* connessi in rete apre uno scenario preoccupante: si è sempre disponibili a contatti anche con sconosciuti e non ci sono ancora efficaci sistemi di protezione.

Per incrementare il dialogo con i cittadini, il Commissariato *online*, portale dedicato ai servizi di Polizia, introdurrà forum per accogliere richieste e dare risposte alle situazioni più diverse.

La Polizia delle comunicazioni ritiene opportuno indirizzare in futuro la formazione ai bambini più piccoli, per prevenire in tempo comportamenti lesivi della loro dignità. Questa necessità si affianca a quella, già menzionata, dell'importanza dell'azione formativa nelle scuole primarie.

I messaggi principali che la Polizia delle comunicazioni vuole trasmettere ai cittadini anche attraverso le campagne di sensibilizzazione e formazione sono:

- Incrementare il dialogo tra genitori e figli
- Avere fiducia nelle istituzioni e ricorrere alla Polizia tutte le volte che è necessario
- Salvaguardare i dati personali, evitando di mettere in rete dati sensibili
- Insegnare a verificare le fonti di Internet, filtrando ciò che è necessario
- Tenere il computer in casa in zone condivise, di passaggio, così che per i bambini la navigazione sia un fatto familiare e non individuale

È significativo che, ancor prima degli accorgimenti tecnici, la Polizia dia consigli di buon senso per una conduzione familiare serena, come migliore prevenzione del crimine e per favorire la tutela dei minori.

Michele Crudele - 2011-07-24