Dipartimento della Gioventù – POAT Per la Gioventù - CUP J71I09000020007

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

Michele Crudele - 2011-10-10

B.3.a) Linee guida sulla sensibilizzazione degli utenti giovani ai problemi di legalità informatica - Guida operativa

Premessa

La trattazione giuridica di questo tema è stata sviluppata nel documento *A.1.a) Relazione sulla situazione legislativa riguardante i delitti che coinvolgono i giovani su Internet* e nel documento *A.2.a) Relazione sulla situazione legislativa riguardante il diritto d'autore e Internet*.

Il tema del rispetto della *privacy* è declinato in diversi argomenti connessi e in particolare nel documento *B.1.a) Linee guida sulla tutela dell'identità digitale*.

Introduzione

L'obiettivo di questa guida è fornire agli utenti dei portali destinati ai giovani un'informativa semplice e sintetica dei diversi ambiti connessi alla legalità informatica.

I rischi della navigazione su Internet si sommano alla facilità di commettere azioni illegali. Le sanzioni non sono sempre facili da comminare e spesso non sono conosciute. Non è formativo partire dal regime sanzionatorio per insegnare a rispettare le norme vigenti. È necessario far comprendere la *ratio* legislativa ed educare a una cultura del rispetto dei beni "digitali", divenuti ormai tanto importanti quanto quelli "materiali".

I capitoli seguenti affrontano gli argomenti principali di legalità informatica, in ordine di frequenza e gravità in relazione alla capacità di azione dei giovani. In alcuni casi i giovani sono contemporaneamente attori e vittime.

La redazione della guida risponde a necessità di rapidità di consultazione, considerata la scarsa propensione dei giovani a leggere le "istruzioni per l'uso".

Ogni portale valuterà quali capitoli sono necessari o in che modo evidenziarne uno piuttosto che un altro, anche in relazione ai servizi prestati agli utenti.

Poiché, soprattutto nelle regioni meridionali, il tema dell'educazione alla legalità è particolarmente sentito e oggetto di numerose iniziative formative, conviene inserire in quegli ambiti un riferimento alla legalità informatica, intesa come rispetto dei diritti altrui in ambito digitale e di telecomunicazioni, parte ormai importante dell'educazione civica.

Tutela del diritto d'autore

È un dato di fatto che la maggior parte dei giovani scarica liberamente da Internet musica e film senza pagare, anche quando questi contenuti sono protetti da diritto d'autore. L'esperienza insegna che spesso la qualità del materiale scaricato non è quella attesa. A volte il contenuto previsto dal titolo è molto diverso e si può arrivare a scoprire che, dopo pochi minuti di un film commerciale, ci sono immagini pedopornografiche. Ma la frustrazione non è un ostacolo per i giovani, che continuano a provare a scaricare da fonti diverse fino a che ottengono quanto cercano. Oppure utilizzano programmi speciali per rimuovere le protezioni contro la duplicazione o il riutilizzo di materiale protetto da diritto d'autore.

Ci sono casi compulsivi, più frequenti di quanto sembri, di giovani e adulti che scaricano per il gusto di farlo, riempiendo i propri dischi di materiale audiovisivo in quantità tali che non basterebbe tutta la vita per ascoltarlo o vederlo. Non si accorgono dei costi "nascosti" di questa attività, apparentemente gratuita: il proprio tempo, l'energia elettrica del computer acceso, i dispositivi di memorizzazione. Certamente si tratta di cifre più basse rispetto a quelle dell'acquisto legale degli stessi contenuti, ma è opportuno chiedersi quanto sarebbe l'investimento se si comprasse solamente quello che si vuole utilizzare al momento, senza "accaparrare". Per contrastare questo modello di comportamento, stanno nascendo servizi legali di fruizione di film e musica senza scaricamento, in *streaming*, con sistemi di pagamento forfettari oppure a durata.

Si nota che alcuni ragazzi smettono di scaricare illegalmente musica quando iniziano a suonare o cantare in forma professionale. Capiscono che devono guadagnarci e che il sistema di diffusione totalmente gratuita delle canzoni non può funzionare. Solamente i cantanti che possono permettersi di guadagnare molto dai concerti dal vivo hanno la possibilità di sottovalutare l'impatto della mancata vendita di CD o di musica *on line*.

Il modello iTunes Store con facilità di acquisto a basso costo di musica di alta qualità con un'offerta amplissima ha dimostrato negli USA che è possibile un'alternativa allo scaricamento illegale. In Italia iTunes Store è meno utilizzato, ma ha un suo pubblico che preferisce non perdere tempo e, per pochi euro, avere subito quello che cerca, con certezza di qualità.

Non sembra che le minacce della SIAE, che negli ultimi tempi cerca però un approccio con i giovani più basato sull'educazione, siano un deterrente. I ragazzi e le ragazze non conoscono con precisione la legislazione sul diritto d'autore e non sanno che, scaricando dal P2P, mettono involontariamente contenuti protetti a disposizione di altri (ogni pezzo scaricato è immediatamente rimesso in gioco nei grandi sistemi di condivisione tipo eMule): possono quindi incorrere nelle sanzioni penali previste dall'art. 171 e successivi della legge 633 del 1941 che è stata modificata più volte negli ultimi anni proprio in relazione a questa fattispecie anche per renderla più ragionevole (la sostituzione nell'art 171ter di "a fini di lucro" al posto di "per trarne profitto" è un esempio). La realtà dimostra che di fatto non corrono praticamente alcun rischio, neppure pecuniario, se scaricano qualche canzone o film e non ne organizzano una rivendita o ridistribuzione organizzata.

Quindi la difesa del diritto d'autore è lasciata all'intelligenza dei giovani. Se tutti scaricano illegalmente, chi ci guadagna? Chi continuerà a produrre film e musica se non riesce a trarne profitto economico? La risposta abituale è: "Non è un problema mio. Lo risolvano gli altri. Intanto io prendo ciò che trovo". Ma forse fra un po' non troverà più nulla.

Pornografia e pedofilia on line

In Italia la pedopornografia è punita gravemente. Consiste nella detenzione, diffusione o produzione di immagini di minori di 18 anni in pose erotiche, anche se si tratta di costruzioni artificiali ("bambini virtuali").

È quindi un reato scambiarsi foto e video pornografici di compagni minorenni, anche se questi sono consenzienti.

Mentre, di fatto, la Polizia di Stato non agisce nei confronti della diffusione generica di pornografia (che pure, per l'art. 21 della Costituzione e a norma dell'art. 528 del Codice Penale, dovrebbe essere perseguita quando si tratta di diffusione pubblica), nel caso di quella minorile è particolarmente attiva e severa.

I pedofili iniziano la fase principale del loro adescamento inviando immagini erotiche di altri bambini, chiedendo alla loro vittima di fotografarsi in situazioni simili. La ridotta sensibilità dei bambini attuali, ormai abituati a vedere scene di sesso dappertutto, fa sì che non si meraviglino della richiesta e non vadano a chiedere spiegazioni ai genitori. Invece acconsentono al "gioco" con il pedofilo, che è sempre molto affettuoso, magari in cambio di ricariche di cellulare o altri regali. Da quel momento nasce un rapporto di complicità che il pedofilo sfrutta chiedendo sempre di più, con la minaccia di rivelare tutto ai genitori in caso di rifiuto. Poiché nel bambino c'è la consapevolezza di star facendo qualcosa di proibito, il timore dei genitori lo spinge ad aderire alle richieste che arrivano, alla fine, a un rapporto personale, con violenze sessuali.

Quello che comincia come un gioco diventa un dramma, del quale ci si porta il peso per tutta la vita.

Non è meno grave il danno personale dell'adolescente che distribuisce, in cambio di soldi, proprie immagini erotiche ad amici o sconosciuti. Non ne può controllare la diffusione e può scoprire che sono pubblicate su Internet, anche a distanza di tempo, con una chiara identificazione. Non basta fotografarsi avendo la mascherina o usare altri trucchi per celare la propria identità. L'esperienza insegna che c'è gente in grado di scoprirla e farne un uso criminale. Come reagirebbe una giovane che si sta sposando se qualcuno la minacciasse di far vedere al futuro marito le sue immagini porno di ragazzina? E cosa direbbe un datore di lavoro scoprendole in rete prima di assumere una neo laureata?

Non ci sono quindi solamente considerazioni morali, che pure sono importanti, in questo campo della pornografia. Perdere il controllo (e il rispetto) del proprio corpo, sia pure "virtualmente" o "digitalmente", può avere conseguenze molto negative. Allo stesso modo, rispettare gli altri, non guardandoli esclusivamente dal lato sessuale, porta benefici nella relazione interpersonale, utile per la propria crescita professionale.

Scommesse e giochi *on line*

In Italia i giochi con premi su Internet sono regolamentati in modo piuttosto accurato con una legislazione continuamente aggiornata. In particolare quelli con vincite monetarie sono tutti controllati dall'AAMS – Amministrazione Autonoma Monopoli dello Stato che registra ogni singola giocata e ne verifica i meccanismi a tutela del giocatore. Per giocare bisogna essere maggiorenni e fornire il codice fiscale e gli estremi di un documento. L'AAMS effettua controlli sulla validità dei codici fiscali e quindi non è possibile inventarne uno per spacciarsi come maggiorenne.

L'AAMS ha lanciato la campagna "Gioco legale e responsabile" in modo che i gestori dei siti possano manifestare la propria adesione ai regolamenti nazionali, tutelando in questo modo gli utenti dalle truffe.

I siti esteri di scommesse sono normalmente bloccati a livello nazionale in forza di una regolamentazione che vuole tutelare gli italiani da truffe straniere ma anche garantire che chi scommette dall'Italia paghi le tasse previste (le paga il gestore, non il giocatore). Tuttavia la loro proliferazione è tale che è sempre possibile trovarne uno accessibile, oppure aggirare il blocco con metodi non molto complessi. È una pratica pericolosa, perché eccetto il caso di famose agenzie di scommesse come quelle storiche inglesi, non c'è nessuna garanzia di equità nella gestione delle probabilità di vincita.

Si può quindi in teoria giocare anche essendo minorenni, dichiarando il falso su un sito estero, ma si rischia di perdere molti soldi: dopo una fase iniziale di vincite facili, ben congegnate per attirare l'attenzione, si inizia a scommettere senza speranza.

La Polizia Postale e delle Comunicazioni segnala che il fenomeno dell'eccesso di gioco d'azzardo *on line* da parte dei minorenni è in crescita, anche con situazioni di *Internet & gambling addiction*, cioè dipendenza morbosa. Un problema connesso sono i reati per procurarsi i soldi per giocare: è una spirale negativa, analoga a quella della dipendenza dalla droga.

Cyberbullismo

Tutti i giovani sanno cosa è il bullismo. Negli ultimi anni se ne parla più spesso, a volte esagerando e spacciando come bullismo un evento singolo di prevaricazione di uno studente su un altro. I bulli sono quelli che continuamente vessano ragazzi più piccoli o deboli, mostrando un atteggiamento di superiorità fisica che denuncia una loro debolezza mentale.

Il cyberbullo è colui che usa il cellulare, Internet e altri mezzi di comunicazione per molestare un altro, insultandolo, calunniandolo, infastidendolo. Mentre negli atti di bullismo si sa subito chi è il colpevole, il cyberbullo può essere sconosciuto alla vittima. Normalmente però si vanta delle sue azioni con gli amici per dimostrare la sua "forza" e quindi la sua identità è presto svelata.

Le azioni di cyberbullismo possono degenerare in reati, anche se non c'è nessuna violenza fisica. Per esempio, se si divulgano in rete informazioni false denigratorie della vittima oppure se ne sottrae l'identità digitale e si commettono illeciti al posto del malcapitato. Ma anche la diffusione non autorizzata di dati personali riservati o di fotografie private ha un risvolto legale.

La reazione migliore dal cyberbullismo, sia quando si è coinvolti, sia quando si vedono altre vittime, è parlarne immediatamente con le persone intorno, sin dalle prime avvisaglie: compagni, professori, genitori, amici, per stabilire una rete di difesa.

I docenti e i dirigenti scolastici conoscono le procedure per queste situazioni e possono agire di conseguenza. In particolare la direttiva 104 del Ministero della Pubblica Istruzione del 30 novembre 2007 affronta diverse situazioni connesse all'uso improprio di videotelefoni nelle scuole.

Non conviene rispondere all'aggressore ed è utile impostare un blocco delle chiamate o dei messaggi da quella provenienza. Conviene conservarsi tutti i messaggi offensivi perché, in caso di degenerazione della situazione, diventano importanti a fini legali. Le misure estreme di cambiare numero di telefono o indirizzo di posta elettronica sono riservate a casi gravi.

Frode informatica

La frode informatica è l'alterazione del funzionamento normale di un computer per trarne profitto a danno di altri ignari. È un reato punito dall'art. 640 ter del Codice Penale.

Un esempio tipico è l'alterazione delle macchinette mangiasoldi o di videopoker, in modo che le vincite siano estremamente rare e non basate sul caso.

Fino a quando si utilizzavano i *modem*, una frode frequente era il *dialer*, cioè un programma che, senza avvisare l'utente, cambiava il numero telefonico del fornitore di connettività Internet, sostituendolo con un numero a pagamento (i famigerati 899 e simili). In questo modo il malcapitato trovava in bolletta telefonica cifre altissime per aver usato Internet con tariffazione esosa al minuto. L'installazione inconsapevole del *dialer* avveniva spesso in concomitanza alla fruizione di materiale pornografico e di scaricamento di visualizzatori di film pirata.

Può essere considerata frode anche l'installazione di un *keylogger*, dispositivo *hardware* o *software* che permette di registrare tutte ciò che l'utente digita sulla tastiera, compresi codici di accesso privati o altri dati personali.

Accesso abusivo a sistema informatico, diffusione abusiva dei codici, danneggiamento

La nozione di accesso abusivo a sistema informatico non si applica solamente ai casi clamorosi di violazione di siti istituzionali per danneggiarli o all'intromissione nella rete di un'azienda per carpirne segreti industriali. È abusivo anche l'accesso di uno studente negli archivi digitali della segreteria della scuola, per gioco o, peggio ancora, per alterare i dati (per esempio, cambiare i propri voti).

L'accesso abusivo è un reato punito dall'art. 615 ter del Codice Penale che prevede alcune aggravanti, per esempio quando si tratta di sistemi informatici sanitari. È quindi particolarmente grave un'intromissione di uno studente di una Facoltà di Medicina nei sistemi universitari quando questi sono connessi anche alla gestione del Policlinico. Il danneggiamento è proibito dai diversi articoli 635 del Codice Penale.

Non è una scusante il fatto che alcuni sistemi informatici siano poco protetti, magari con *password* banali. Basta che ci sia un accorgimento, per quanto debole, di sicurezza, a far scattare il reato di accesso abusivo in caso di violazione.

La detenzione e diffusione abusiva dei codici è reato per l'art. 615 quater. Comunemente si realizza attraverso le pratiche di *phishing*, cioè l'inganno dell'utente che crede di introdurre i suoi codici nel sistema della banca o del fornitore di servizi, mentre li sta invece passando al criminale che ha costruito una copia apparentemente identica all'originale della pagina di accesso.

Gli inganni in questo modo sono a volte molto sofisticati e contano sulla superficialità o fretta dell'utente che si trova ad esempio un messaggio di posta elettronica con un collegamento alla propria banca per controllare l'estratto conto. Invece di aprire il sito della banca con la solita procedura, magari dai propri segnalibri, l'utente malcapitato fa clic sul *link* ed entra in un sito *clone* dal quale, subito dopo aver immesso le credenziali, viene rimandato a quello legittimo con un avviso del tipo "errore di *password*, ritentare". Nel frattempo il criminale utilizza i dati di accesso che ha catturato nella prima immissione.

Diffusione di virus informatici e apparecchiature per danneggiare

Accanto alla diffusione deliberata di virus, l'art 615 quinquies del Codice Penale considera reato anche la produzione o l'acquisto di strumenti che siano usati per danneggiare sistemi informatici o telematici. Non è quindi necessario che questi strumenti vengano effettivamente usati o causino danni: è sufficiente che siano predisposti a farlo e che ci sia l'intenzione di usarli a questo scopo.

Anche per questo motivo è illegale usare un *jammer* (proibito soprattutto dagli articoli 617 e seguenti), un dispositivo che impedisce le telefonate cellulari nel suo raggio di azione, che è consentito solamente ai militari e in situazioni particolari.

Non è colpevole chi involontariamente infetta altri computer con il proprio che è stato compromesso da un virus o altro programma maligno (si chiama *malware* tutto ciò che può creare danni), ma certamente è buona norma difendersi da queste infezioni con opportuni programmi di protezione, cosiddetti antivirus. È importante aggiornarli spesso, meglio se automaticamente, perché a volte le nuove minacce arrivano quotidianamente.

Il rischio attuale maggiore per un utente in rete è essere vittima di una *botnet*. Esistono criminali che infettano migliaia di computer con programmi che rispondono al loro controllo: possono comandarli da lontano per eseguire determinate azioni, come attaccare un sito istituzionale, lanciare *spam*, cercare di violare un portale, diffondere materiale pedopornografico, ecc. L'infezione è silente e l'utente non si accorge di nulla, tranne qualche rallentamento e un traffico insolito anche quando non sta lavorando. Non è particolarmente esaltante sapere a posteriori di essere stato protagonista inconsapevole di un'azione criminale. Per difendersi, vale il criterio di aggiornare continuamente il sistema operativo e l'antivirus.

Truffa nel commercio elettronico

Vendere su un sito di commercio elettronico o di aste qualcosa che non corrisponde alle caratteristiche descritte è una truffa. È abbastanza frequente ed è un reato nel quale il raggiro è lo strumento per indurre il compratore a pagare per ciò che crede di poter ottenere. Nel caso peggiore, l'oggetto non viene neppure consegnato.

Si verifica anche la situazione opposta in cui il compratore non paga.

Sempre più frequentemente compriamo e vendiamo in rete, per cui è necessario mantenere un livello di affidabilità del sistema, rispettando le regole contrattuali. La fiducia è una leva molto forte per lo sviluppo di un'economia e la somma dei piccoli ruoli di giovani che fanno transazioni elettroniche in modo legale può causare un effetto benefico per il Paese.

Abuso di carte di credito e debito

Apparentemente l'illecito utilizzo di carte di debito e credito su Internet sembra un esempio di frode informatica. Per il legislatore ci sono delle differenze, è questo reato è stato definito specificamente dalla legge 197/1991. È condannato chi usa indebitamente carte non proprie oppure le falsifica o duplica. Usare quindi la carta di credito dei genitori a loro insaputa è un reato.

Siccome molti siti consentono l'acquisto di beni digitali con la semplice comunicazione del numero di carta di credito, se il gestore del portale di vendita ne memorizza i dati, può illecitamente farne uso per proprio tornaconto.

Per questo motivo è importante rivolgersi a siti di vendita con buona reputazione e preferire quelli che fanno realizzare la transazione della carta di credito direttamente sul sito protetto della banca o del circuito di emissione della carta stessa.

Coloro che non usano mai su Internet carte di credito non sono immuni dall'abuso perché quando la consegnano al ristorante o al negozio stanno comunicando a un altro tutti i dati sufficienti per fare transazioni elettroniche.

In caso di utilizzo indebito della mia carta di credito, ho lo svantaggio del rischio di sottrazione di una cifra elevata, pari al *plafond* massimo concordato con la mia banca, ma ho il vantaggio del rimborso per questo tipo di furti, se contestati opportunamente. Se uso invece una carta prepagata, rischio meno perché normalmente la carico con cifre ridotte, ma non ho sempre la garanzia di un'assicurazione.

Spamming

Spam è quell'insieme di messaggi non richiesti con finalità promozionale o pubblicitaria, normalmente inviati per posta elettronica o SMS. Non è consentito dalla legge che esige il consenso del destinatario.

La facilità di invio di milioni di messaggi in poco tempo a indirizzi di posta elettronica raccolti a caso sul *web* fa sì che il fenomeno sia dilagante, soprattutto da Paesi esteri dove la legislazione è meno protettiva dell'utente oppure da sistemi nascosti e distribuiti tra ignari possessori di computer infetti.

Per difendersi esistono antispam che hanno un'efficacia parziale anche perché gli autori dello *spamming* aggiornano le loro tecniche di invio per aggirare le protezioni.

Una forma di *spam* diffusa tra i giovani è l'invio a gruppi di conoscenti (o semplicemente di contatti) di messaggi di qualsiasi natura a scopo ludico o informativo. Oltre a non aver ottenuto il consenso, neppure implicito, dei destinatari, spesso l'errore grave è di mettere in copia tutti gli indirizzi dei destinatari stessi, divulgandoli quindi a tutto il gruppo. Nel caso di invio a più persone che tra loro non si conoscono, è necessario usare la copia carbone nascosta (*ccn* o *bcc*) nel programma di posta elettronica, in modo che nessuno riceva l'elenco degli indirizzi dei destinatari.

Michele Crudele - 2011-10-10