

intervista di Federica Biolzi

Ci troviamo sempre in presenza di nuove forme di reati legati alla rete. il cittadino si scopre improvvisamente non protetto e insicuro e la maggior parte vittime, si ritrovano nelle fasce deboli e tradizionalmente più esposte della popolazione. Abbiamo fatto il punto su queste nuove realtà criminali con il professor Marcelo Aebi, Vice-direttore della School of Criminal Sciences di Losanna, intervistato in occasione del XXXI Congresso della Società Italiana di Criminologia.

Nuovi reati e cybercrime, come si definisce questa nuova galassia di crimini?

Ci sono tre modalità di reato, che possono essere fatti con internet, senza internet o con entrambi: gli offline, i reati ibridi e i reati online.

In quelli online, è per esempio oggi, molto semplice assumere l'identità di un'altra persona. Ma non solo il fatto di sostituirsi, oggi dobbiamo fare i conti con una serie di azioni che vengono poste in essere nel mondo virtuale. Ma in tutti i casi l'obiettivo è quello di minacciare l'intimità e la proprietà delle persone e delle istituzioni.

Reati commessi tramite un virus, un malware, prima non esistevano. La forma è cambiata ed il limite è rimasto lo stesso, la persona perde qualcosa nei suoi diritti fondamentali, come quelli espressi dalla Convenzione Europea dei Diritti dell'uomo. Ma per arrivare ad una tutela soddisfacente occorre tenere il codice penale al passo con i tempi e le tecnologie.

Ci sono crimini contro la persona e contro la proprietà, ma le fattispecie cambiano. Quando io mi approprio della tua identità virtuale su internet, è evidente che cambia la modalità in cui commetto il reato, la fattispecie e deve rientrare in norme che possano sanzionarlo o prevenirlo.

Poi bisogna tener conto degli ordinamenti dei singoli stati...

Al di là dei singoli ordinamenti, in tutti i Paesi si evidenzia come il risultato finale sia sempre una violazione al diritto della persona. Impossessarsi di un'identità virtuale comporta comunque, entrare in relazione con l'identità reale della stessa persona.

Un cambiamento che è visibile nella società attuale è il ruolo secondario assunto dallo Stato. Ad esempio, quando acquisto un computer, io acquisto l'antivirus da un'azienda privata, e quindi la sicurezza privata si rafforza. È un rapporto tra privati e solo successivamente può intervenire lo Stato. Lo Stato ha perso il controllo della sicurezza, questa è la realtà più preoccupante.

Vi sono poi tutte le banche dati che vengono create e alle quali le forze dell'ordine non hanno accesso, questo crea ancor più potere al privato.

Nel campo del cyber ci sono alcuni reati che si aggiungono ad altri reati. Ma vi sono alcuni reati che divengono più efficaci attraverso il cyber?

È difficile accedere ad un conto bancario in maniera tradizionale, se lo faccio via internet è più efficace, la connessione via web è velocissima. È più facile essere frodati e tutto avviene in tempo reale. Vi sono diverse

modalità che vengono utilizzate per entrare nelle banche dati o nei servizi online delle persone, proprio per riuscire velocemente a prenderne i beni patrimoniali, ma anche e soprattutto per appropriarsi dell'identità.

Con l'utilizzo della rete, le responsabilità del cittadino sono molto maggiori.

Si può prevenire il cybercrime, attraverso interventi più mirati?

E' necessario andare ad effettuare una prevenzione molto mirata mediante l'individuazione delle fasce più deboli, come gli anziani, i minori.

Questi crimini costituiscono limiti all'affermarsi della rete?

Martin Killias^[1], sostiene che se vi è una nuova tecnologia, ci sono sempre altre opportunità per la nascita di nuovi reati. Una nuova tecnologia comporta un momento di anomia. Tutta la nuova tecnologia crea un po' di devianza.

Noi non possiamo fare altro che lavorare sulla prevenzione. Internet continua a svilupparsi e non credo che ciò potrà cambiare. Siamo noi che dobbiamo adattare i nostri comportamenti, non sono solo le norme.

Mi sembra, però, che i crimini offline siano in diminuzione...

Sì, sono in diminuzione. Rubare in una casa comporta maggiori rischi (per l'introduzione di sistemi antifurto, telecamere, eccetera). Oggi non andiamo in giro con tanti soldi perché siamo in possesso delle carte di credito. Invece il crimine online si può commettere ovunque. Anche l'autore del reato di oggi, nel cyber, non è la stessa persona che prima faceva la rapina in modo tradizionale.

Attualmente, sui reati patrimoniali classici e sui crimini tradizionali, abbiamo più controllo e quindi per il reo, diviene più difficile e meno interessante. Nel reato online tutto è molto più semplice, veloce ed anche meno rischioso.

Da un punto di vista statistico, alcuni reati, quali l'omicidio, hanno avuto un calo, ciò è legato sia in Europa Occidentale, che negli Stati Uniti, a diversi fattori. Dopo la crisi del 2008, le condizioni generali di vita sono migliorate, le cure mediche sono più efficaci, vi sono meno armi che circolano, minori incidenti stradali, eccetera.

Anche se la raccolta dei dati in questo campo potrebbe essere migliorata...

Sì, sarebbe opportuno auspicare un'armonizzazione sia nella raccolta di questi dati, che nelle indagini di vittimizzazione da effettuarsi omogeneamente nei diversi territori, sia in ambito Europeo che Internazionale

Quindi occorre mettere in campo maggiori controlli, anche in campo internazionale.

Il controllo sul cybercrime è molto diverso da paese a paese, in alcuni stati è favorito e in altri no. L'unione europea è più avanti come normative a sostegno.

Quale sarà il futuro del cyber-crime?

A me preoccupa molto il ritorno del nazionalismo a livello europeo. Il cybercrime dovrà essere affrontato da

due punti di vista: *Geopolitico*, in quanto il Cybercrime può diventare uno strumento per dividere ulteriormente i paesi europei; *Individuale*, in quanto il cittadino avrà sempre di più una responsabilità ed un coinvolgimento personale.

I giovani sono particolarmente esposti al web, cosa si può fare per loro?

È fondamentale intervenire con campagne di prevenzione già all'interno del sistema scolastico, come ad esempio accade in Norvegia. Lo strumento prioritario diviene quello di educare e prevenire a scuola.

Sicuramente, non sappiamo come la tecnologia avanzerà nel tempo, in quanto, ha uno sviluppo che definirei atemporale. Ogni nuova tecnologia, avrà sempre un punto debole, per cui sarà attaccabile, ma necessiterà sempre di nuove strategie di sicurezza e di prevenzione.

[1] Killias Martin, Précise de Criminologie, Staempfli Editions SA Berne (2001)