CYBERCRIME INTERNATIONAL CONFERENCE 2002

Negli ultimi anni si è prospettata una nuova sfida alla Criminologia: il computer crime. I criminologi moderni stanno tentando di analizzare la modifica di forme criminali tradizionali indotta dal computer e l'avvento di forme criminali nuove. In particolare si sta cercando di analizzare la percezione del crimine informatico delineando nuovi profili di criminali. Alcuni esempi di ricerche sul computer crime condotte dall'U.A.C.I. della Polizia Postale, dal Centro di Neurologia e Psicologia Medica della Polizia di Stato, e, nel mondo universitario, dalla SIPTECH e dallo IURC[1]: differenze tra pedofili on-line e pedofili tradizionali; crimini informatici nelle aziende ad opera di insiders; utilizzo di internet da parte di organizzazioni criminali e terrorismo; diffusione di informazioni illegali on-line; caratteristiche psicologiche dei giovani hackers.

Le prime osservazioni della cybercriminologia, basate su tali ricerche, hanno mostrato come il crimine professionale si adatta a tutte le innovazioni che migliorano la sua efficienza, compreso quindi l'ICT. Alcune forme criminali tradizionali sono infatti rese più efficaci dalla telematica: comunicazione e organizzazione di terroristi; comunicazione, organizzazione e attività della criminalità organizzata (es. riciclaggio); pedofilia organizzata; spionaggio industriale.

L'ingresso dell'informatica nelle azioni criminali sembra poi in grado produrre nuovi profili di personalità dei delinquenti, rendendo "adatti al crimine" soggetti diversi dai criminali del passato. Alcuni studi condotti nell'ambito della Polizia di Stato italiana hanno permesso di cominciare a delineare alcuni "profili" tipici del cybercriminale:

- tendenzialmente non-violento
- capacità di pianificazione del comportamento per sfruttare le opportunità dell'informatica
- minori strumenti psicologici di contenimento dell'ansia per l'assenza di un contatto diretto con la scena criminis e la vittima
- tendenza ad operare in solitudine
- tendenza ad acquisire il know how criminale in ambiente informatico
- minore tendenza ad autopercepirsi come un soggetto criminale

L'information technology, infine, può generare, in alcuni individui, delle alterazioni della percezione del crimine, facilitando comportamenti criminali che difficilmente attuerebbero fuori dal cyberspazio[2], come ad esempio:

- pedofili che non avrebbero il coraggio di adescare un bambino per strada;
- terroristi psicologicamente non adatti ad azioni militari;
- truffatori che non reggerebbero l'impatto con la vittima face-to-face;
- donne che non avrebbero il coraggio di prostituirsi per strada;

- impiegati scontenti che non avrebbero il coraggio di compiere azioni di sabotaggio tradizionali nella propria azienda;

- ladri di informazioni che non avrebbero il coraggio di introdursi in uno spazio fisico (un ufficio) che contiene le informazioni da sottrarre;

- teppisti che non avrebbero il coraggio di tirare sassi ad una vetrina per strada e effettuano viceversa un defacement di siti web;

- ragazzi che non avrebbero il coraggio di frequentare il mondo della malavita per imparare tecniche utili a compiere azioni illegali;

- persone che non avrebbero il coraggio di insultare o molestare sessualmente nessuno senza la mediazione dell'email (o dell'SMS).

Lo scenario criminologico nel computer crime implica quindi l'utilizzo dell'informatica da parte di criminali professionisti determinati, la possibilità di azioni criminali eclatanti da parte di soggetti solitari e disorganizzati (es. i giovani hackers), nonché azioni illegali da parte di soggetti di basso profilo criminale (per ridotta percezione del crimine).

La diffusione delle tecnologie informatiche è relativamente recente e gli individui si stanno ancora adattando. In attesa di un adattamento completo il computer crime presenta ancora delle variabili diverse dal crimine convenzionale. Per la moderna Criminologia le azioni criminali vengono costruite, elaborate e spesso impedite da un processo di pensiero che molto si basa sull'anticipazione mentale degli effetti del comportamento e sulla percezione del crimine. Gli uomini, in pratica, orientano il proprio comportamento (anche quello criminale) in base ad una serie di informazioni che provengono dalla loro esperienza e dall'ambiente esterno: percepiscono, pensano e decidono. Nell'ambito del computer crime è interessante analizzare come l'avvento dell'informatica possa influenzare tali meccanismi di pensiero. Alcuni processi percettivi e di significazione sono modificati dal computer, come ad esempio: la percezione dell'illegalità del comportamento, la stima dei rischi di essere scoperto e denunciato, la percezione del danno procurato alla vittima, la paura della sanzione sociale e legale.

La cybercriminologia si occupa ora di computer crime cercando di evidenziare le variabili specifiche di tali crimini. In questa fase storico-scientifica vengono effettuate, ad esempio, ricerche comparative tra alcuni crimini commessi attraverso il computer e crimini simili commessi senza l'ausilio del computer. In un futuro più o meno prossimo, quando il processo di adattamento alle nuove tecnologie sarà completo, non avrà più senso studiare le variabili indotte dal computer nel comportamento criminale. Quando la telematica sarà entrata stabilmente nella struttura sociale, nelle organizzazioni, nell'antropologia e nella psicologia degli individui, non ci sarà più necessità di parlare di cybercriminologia o di computer crime. Un giorno i computer e la tecnologia digitale diverranno elemento imprescindibile di ogni comparto della vita umana. Gli individui in futuro diverranno quindi perfettamente consapevoli dei crimini commessi attraverso le reti telematiche. Il computer crime sarà allora definito
semplicemente crimine.

Marco Strano