Dal cyberfuturismo al cybercrime: la spiegazione del comportamento criminale connesso alla tecnologia digitale

di Marco Strano

Intervento al Convegno Internazionale FUTURNET, Roma, 4-5-6 dicembre 2003

Premessa: la nuova frontiera della Criminologia

Una delle funzioni primarie della Criminologia è la spiegazione del comportamento criminale. Il criminologo, per poter far questo, cerca di "entrare nella mente del criminale", tenta di delinearne la struttura di personalità, la sua sfera emozionale. In altre parole cerca di pensare come lui e cerca di sentire cosa ha sentito e provato lui al momento della commissione del crimine. Per poter comprendere il comportamento criminale è anche indispensabile isolare ed analizzare gli elementi che hanno influito sull'individuo, sia di tipo psicologico che di tipo sociale e culturale.

Gli approcci criminologici moderni, propongono infatti una spiegazione del crimine dove gli influssi provenienti dal mondo esterno, le pulsioni e le esperienze provenienti dal mondo interno dell'individuo vengono mediati, significati e rappresentati dalla mente dell'attore sociale che orienta di conseguenza la sua azione.

In questo inizio di millennio il paradigma della Scienza criminologica sembra essere stato messo in crisi proprio dal cybercrime. I criminologi tradizionali in attività cercano di applicare teorie classiche ai crimini informatici, adattando, o al massimo integrando tali teorie, con fortune incerte. Solo in rari casi si assiste ad una ricerca empirica sistematica ed a una produzione teorica specifica, centrata sulle variabili indotte dal mezzo informatico sul comportamento criminale (la cybercriminologia).

Lo scenario criminologico del computer crime si articola sostanzialmente attraverso tre fattori emergenti:

Un utilizzo dell'informatica da parte di criminali professionisti determinati (mafiosi, terroristi, spie industriali, trafficanti vari ecc.) che sono stati pronti a cogliere le nuove opportunità offerte dalla tecnologia per incrementare i loro guadagni e per eludere con più facilità le strategie di contrasto da parte delle agenzie istituzionali;

Alcune azioni eclatanti condotte da parte di soggetti solitari e disorganizzati (es. i giovani hackers)che riescono, grazie al funzionamento delle reti, ad "attaccare" i gangli vitali della società moderna. Si tratta spesso di comportamenti criminali dove la dimensione "espressiva" assume un ruolo primario rispetto a quella pragmatico-utilitaristica;

Azioni illegali svolte da soggetti di basso profilo criminale o completamente avulsi dal mondo del crimine che confondono, sottostimano o addirittura ignorano la dimensione dissociale e antigiuridica di comportamenti eseguiti interamente in ambiente digitale.

L'avvento della tecnologia digitale e la sua influenza sul crimine

L'uomo, come tutte le altre specie del resto, si adatta continuamente alle modifiche dell'ambiente, fornendo delle risposte adattive che dopo un certo tempo si stabilizzano in caratteristiche strutturali. La capillare diffusione delle nuove modalità socio-comunicative correlata alle tecnologie digitali sta però imponendo una ristrutturazione della cultura, delle abitudini, e della psicologia dei singoli individui e delle organizzazioni forse troppo rapida per non presentare momenti di anomia.
L'individuo si è trovato immerso nel giro di pochi anni in una fitta rete di comunicazioni digitali (l'infosfera digitalizzata) che offre nuove forme di rappresentazione del reale e necessita di un processo di adattamento dei sistemi di percezione e decodifica oltre che delle dinamiche di relazione con le norme sociali e penali. Talvolta le azioni che derivano dalle prospettive e dalle immagini costruite all'interno di un mondo digitalizzato tendono a svincolarsi dal metro di giudizio morale e legale convenzionale.
Di fatto molte persone che utilizzano forme di comunicazione tecnomediata attuano taluni comportamenti (alcun illegali) che difficilmente porrebbero in essere in ambiente fisico convenzionale. Il potere disinibente del *cybersex* nelle chat line, il *cyberstalking* eseguito da individui che non avrebbero mai il coraggio di molestare una persona nel corso di una relazione *face-to-face*, rappresentano alcuni dei "sintomi" di tale situazione.

Tecnomediazione e cybercrime

Con un approccio criminologico costruzionistico, proponiamo una definizione di computer crime come tutti quei casi in cui "*il computer si interpone tra l'autore del crimine e la vittima o comunque rappresenta lo strumento principale per eseguire una determinata azione criminale*"1, sottolineando la sua capacità di alterare ad esempio la percezione di gravità dell'azione criminale, la percezione della vittima, la stima dei rischi di essere scoperto e catturato.
La spiegazione del crimine tecnomediato e la definizione della responsabilità e dei livelli di consapevolezza ad esso correlati implicano quindi la necessità di una ricostruzione dell'influenza della dimensione digitale sulla modalità percettiva e valutativa del soggetto nelle varie fasi dell'azione illegale.
Si rileva ad esempio, in alcuni casi di cybercrime, una certa alterazione da parte dei soggetti della fase di percezione, distinzione e valutazione degli effetti

1 Strano M., Computer crime, ed. Apogeo, Milano, 2000.

provocati con il proprio comportamento e della stima delle reali possibilità che il proprio crimine venga scoperto e sanzionato. La mediazione di uno spazio virtuale in un crimine sembra quindi poter:

1. attenuare la percezione da parte del delinquente degli effetti negativi prodotti sulla vittima;
2. allargare la base dei possibili autori di reato rendendo adatti al crimine molti individui avulsi al mondo dell'illegalità;
3. creare un fenomeno di illegalità distribuita in larghe aree sociali (ad esempio nell'ambito della violazione dei diritti d'autore);
4. diffondere atteggiamenti di impunità su determinati crimini (spesso basati su errori cognitivi e logici);
5. mantenere una scarsa conoscenza delle leggi civili e penali in materia.

Il profilo del cybercriminale

Le indagini di polizia nell'ambito del computer crime e le ricerche criminologiche accademiche hanno consentito di isolare alcune variabili ricorrenti nella struttura di personalità e nelle caratteristiche socio-biografiche degli individui che si sono resi responsabili di azioni criminali tecnomediate. Fatte salve le ovvie atipicità, proponiamo un possibile profilo del cybercriminale tipico, riassumibile nelle seguenti peculiarità:

- livello sociale e culturale medio-alto
- tendenzialmente non-violento e lontano dallo stereotipo del criminale di strada (street-crime)
- parziali contiguità con le teorizzazioni sui white collar crime
- dimostra ridotta percezione del crimine
- ha buona capacità di pianificazione del comportamento per sfruttare le opportunità dell'informatica
- possiede minori strumenti psicologici di contenimento dell'ansia per l'assenza di un contatto diretto con la scena criminis e la vittima rispetto ai criminali di strada
- ha la tendenza ad operare in solitudine e ha scarsi contatti con gli ambienti delinquenziali tradizionali
- ha la tendenza ad acquisire il know how criminale in ambiente informatico (es. gli hackers)
- presenta scarse rispondenze diagnostiche con il Disturbo Antisociale di Personalità (ADP)
- dimostra minore tendenza ad autopercepirsi come un soggetto criminale

Prospettive future della Cybercriminologia

Alcune ricerche su come la percezione del crimine, in ambiente digitale possa risultare notevolmente distorta sono attualmente condotte in Italia dall'UACI

(Unità di Analisi sul Crimine Informatico)[2] della Polizia di Stato, dall'ICAA (International Crime Analysis Association) e dalla SIPTECH (Società Italiana di Psicotecnologie e Clinica dei Nuovi Media). Tali ricerche stanno fornendo interessanti spunti conoscitivi sull'influenza delle tecnologie digitali sul crimine.
Le indagini condotte dalla Polizia Postale e delle Comunicazioni sul fronte della pedofilia on-line hanno ad esempio evidenziato nel comportamento dei cyberpedofili nelle chat una significativa sottostima dei rischi di essere scoperti.
Uno studio pilota condotto dall'ICAA sul fenomeno degli *insiders* (impiegati che commettono reati informatici all'interno della loro azienda) ha rilevato una notevole "dispercezione" dei rischi di scoperta e una certa sottostima dei danni provocabili.
Nelle moderne compagini terroristiche trovano sempre più spesso posto individui ben lontani dallo stereotipo "militaresco" dei cosiddetti anni di piombo e deputati al funzionamento on-line dell'organizzazione.
Le esperienze di ricerca sugli hackers dell'ICAA e della SIPTECH hanno posto in evidenza la prevalente percezione "ludica" delle intrusioni clandestine da parte dei giovani pirati informatici con l'evidente configurazione di una sorta di Sé ideale proiettato nel cyberspazio.

Conclusioni

Gli studiosi contemporanei stanno sperimentando l'avvento e lo sviluppo di un nuovo mondo comunicazionale e relazionale elettronico, che rappresenta uno dei terreni di confronto culturale maggiormente vivo in questo inizio di secolo essendo portatore di modificazioni in grado di incidere sulle principali dinamiche psicologiche e sociali.
Questa fase è ancora caratterizzata dall'attività di una elìte di studiosi (psicologi, psichiatri, sociologi, criminologi, antropologi) che prima degli altri hanno acquisito le competenze digitali e la capacità di correlarle teoricamente all'azione umana e alla devianza e che costituiscono una vera e propria avanguardia nel panorama scientifico mondiale.
In un futuro prossimo queste teorizzazioni e la dimestichezza operativa con le interazioni digitali, dovranno essere inserite in pianta stabile nel bagaglio formativo di ogni figura professionale vicina alle Scienze dell'Uomo.

Riferimenti bibliografici

Caretti V., La Barbera D., (a cura di) *Psicopatologia delle realtà virtuali*, Masson editore, Milano, 2001.
De Leo G., Patrizi P., *La spiegazione del crimine*, Il Mulino, Bologna, 1999.

[2] L'U.A.C.I. della Polizia di Stato è una sezione della Polizia Postale e delle Comunicazioni. E' diretta da uno Psicologo (Marco Strano, autore di questo articolo) ed è composta da personale investigativo e tecnico della Polizia. Si occupa di sperimentare e sviluppare nuove tecniche investigative nell'ambito dei crimini ad alta tecnologia e collabora a tal fine con Università e aziende del settore sicurezza informatica.

De Leo G., Strano M., De Lisi C., Pezzuto G., *Evoluzione mafiosa e tecnologia criminale*, Giuffrè editore, Milano,1995.
Di Maria F., Cannizzaro S., (a cura di), *Reti telematiche e trame psicologiche* editore Franco Angeli, Milano, 2001.
Galdieri P., Giustozzi C. Strano M, *Sicurezza e privacy in azienda*, Apogeo editore, Milano, 2001.
Rogers, M.A. *Modern-day Robin Hood or Moral Disengagement, Understanding the Justification for Criminal Computer Activity* Daily Mail & Guardian 10 February 1999
Strano M., *Computer crime*, Edizioni Apogeo, Milano, 2000
Strano M., *Hackers: sviluppi e prospettive della cybercriminologia* in: *Psicopatologia delle realtà virtuali*, (Caretti V., La Barbera D.) Masson editore, Milano, 2001.
Strano M., *Manuale di Criminologia Clinica*, See Edizioni, Firenza, 2003
Strano M., Neigre B., Galdieri P., *Cyberterrorismo*, Yackson Libri, Milano, 2002
Strano M., Telematica e cyberpedofilia in: Cantelmi T. et altri, La mente in internet, Piccin, Padova, 1999;
Turkle S., Vita sullo schermo, nuove identità e relazioni sociali nell'epoca di internet. Edizioni Apogeo.