LINEAMENTI DI CYBERCRIMINOLOGIA

di Marco Strano (edizione 2011)

Premessa

L'avvento del terzo millennio rappresenta per gli studiosi del comportamento umano una fase di capillare diffusione di una modalità socio-comunicativa nuova, strettamente correlata alle tecnologie digitali. La cultura, le abitudini, la psicologia dei singoli individui e delle organizzazioni si trovano, a seguito di tale diffusione, "costrette" ad una sorta di ristrutturazione cognitiva che condurrà probabilmente entro breve tempo a vere e proprie modificazioni antropologiche stabili. Questa fase è caratterizzata dall'attività di alcuni 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.

L'adattamento al digitale

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. In questa fase storica la sua capacità adattiva deve far fronte ad una modifica rapida che incide profondamente sulle sue modalità percettive, cognitive e affettivo-relazionali, sottoponendolo probabilmente ad un impegno evolutivo mai sopportato prima d'ora. Mai come adesso le strutture del suo sistema nervoso devono sintonizzarsi e addomesticarsi a delle modalità nuove di interazione con gli altri esseri umani, con gli oggetti, con lo spazio fisico che lo circonda e addirittura con il proprio corpo (pensiamo alla realtà virtuale delle tute erotiche-stimolanti). L'individuo è immerso in una fitta rete di comunicazioni che spesso non è semplicemente "mediata" dalla tecnologia digitale ma che in particolari condizioni di complessità progettuale sembra assumere vita propria. L'uomo antico, analogico era abituato alla sola breve e temporanea esposizione alla virtualità, nella situazione di persistenza retinica delle immagini (ben conosciuta e sfruttata dall'inventore del cinema) in grado di ingannare la sua decodificazione per pochi istanti consentendo la ricostruzione visiva degli oggetti e del loro movimento. Al di là che per tale momento di asincronia tra il reale e la sua immagine ricostruita, la mente è progettata per affidare solo ai suoi strumenti di mediazione sensoriale l'acquisizione dell'ambiente fisico che la circonda. Le nuove modalità comunicative e di rappresentazione del reale introdotte dalla tecnologia digitale non possono quindi non comportare un

processo di adattamento dei sistemi di percezione e decodifica e, su un piano di maggior complessità, delle dinamiche emotive, affettive e relazionali offrendo intuitive opzioni e diversificazioni tra gli individui, nei casi estremi anche di tipo clinico. La diffusione di spazi virtuali nel cui ambito si snodano flussi di informazione e si costruiscono relazioni umane rappresenta del resto una modalità sociale in espansione costante. L'ambiente di lavoro ad esempio si trasforma da luogo fisico in luogo virtuale attraverso la diffusione delle reti L.A.N. e di INTRANET mentre l'ambiente sociale affida sempre più alla rete telematica la costruzione e il mantenimento delle interazioni tra gli individui. Tali condizioni necessitano dell'acquisizione di abilità nuove nello stile comunicativo ma soprattutto nei processi di pensiero a cui è chiesta sempre maggiore flessibilità e rapidità nel passaggio operativo tra dimensione reale e dimensione virtuale, tra una relazione mediata da uno spazio emotivo-fisico a una relazione mediata da uno spazio emotivo-artificiale. Molte delle categorie e dei sistemi che le persone si creano ed utilizzano per organizzare la propria immagine del mondo cominciano a essere infatti fortemente influenzati dalla logica digitale. Di conseguenza, le azioni che derivano dalle prospettive e dalle immagini costruite all'interno di un mondo digitalizzato necessitano a loro volta di nuove categorie analitiche dotate di diverse peculiarità.

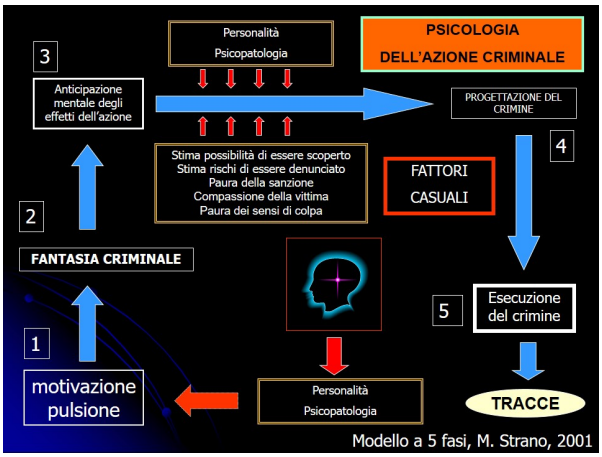
L'influenza del digitale sul crimine

Anche la valutazione criminologica di un comportamento criminale, il tentativo ovvero di definire in termini di responsabilità del soggetto i livelli di consapevolezza correlati all'azione criminale analizzata, implica quindi attualmente la necessità di una ricostruzione dell'influenza della dimensione digitale sulla modalità percettiva del soggetto nelle varie fasi dell'azione illegale. Gli utenti di tecnologia informatica e telematica sono infatti impegnati quotidianamente nella costruzione di una vasta porzione del loro "*costrutto personale della realtà*", usando un concetto di Kelly, attraverso la percezione e organizzazione di esperienze comunicative digitali trasferendolo in ambiti di vita sempre più ampi. Con queste premesse gli schemi cognitivi che hanno corresponsabilità nelle dinamiche criminali non possono non essere influenzati da tali dinamiche intervenendo anch'essi nell'attività di strutturazione dell'esperienza e nell'organizzazione e significazione delle azioni. Si rileva ad esempio, talvolta, in alcuni soggetti osservati, una certa difficoltà nell'identificare il limite che separa la realtà dal virtuale o nella capacità dinamica di tornare velocemente in una situazione di realtà dopo una certa permanenza in un fase di virtualità, e tale difficoltà assume rilevanza in Criminologia in special modo nello studio della fase di percezione, distinzione e valutazione, da parte dell'autore di un crimine, degli effetti provocati con il proprio comportamento. L'uomo "in fase di digitalizzazione relazionale" è ancora abituato ad un riscontro percettivo della sua operatività nella lettura delle modificazioni evidenti sugli oggetti tangibili, fisici, stabili nonché sull'emotività dell'interlocutore e tale riscontro sembra risultare meno efficace quando è mediato da un messaggio di ritorno digitale che pur se in continua raffinazione, costituisce ancora un simulacro imperfetto. Pensiamo ad esempio quanto la prova tangibile degli effetti negativi prodotti sulla vittima possa rappresentare un fattore di antagonismo al crimine in soggetti dotati di un quadro morale ben strutturato e come la mediazione di uno spazio virtuale tra l'autore del crimine e la sua vittima possa attenuare la percezione di tali effetti. Nella capacità dell'individuo di spostarsi rapidamente e con efficacia tra le interazioni digitali a quelle fisiche è quindi racchiusa, in quest'ottica, la chiave interpretativa di eventuali

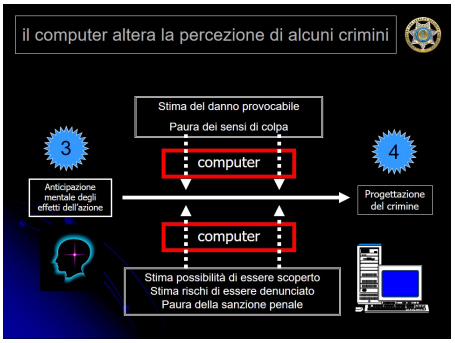
comportamenti disfunzionali, di interesse clinico (nelle modalità di fuga) o di interesse criminologico (nelle modalità di dispercezione delle conseguenze delle proprie azioni).

La spiegazione del crimine in ottica digitale

In questo inizio di secolo gli studiosi di Criminologia si stanno quindi confrontando con nuove modalità di comunicazione e di interazione, legate prevalentemente allo sviluppo e alla diffusione delle tecnologie informatiche e telematiche e con la nascita di nuove forme criminali definite genericamente computer crime. In tale confronto la dimensione cognitiva appare di evidente rilevanza essendo strettamente correlata alla dimensione simbolica connessa all'avvento del digitale. Le azioni criminali, così come documentato dalla letteratura specialistica risultano infatti essere frutto di dinamiche complesse, strettamente legate ai processi di interazione dell'autore con le norme penali e sociali, con l'ambiente esterno, con la vittima e, in definitiva con il proprio sé. I crimini vengono infatti costruiti, elaborati (e spesso impediti) da un processo di pensiero che molto si basa sull'anticipazione mentale degli effetti del proprio comportamento (effetti sociali e legali)[1[1]]. Gli uomini, ovvero, orientano il proprio comportamento in base a una serie di informazioni che provengono dalla sua esperienza e dall'ambiente esterno, soprattutto dall'interazione con gli altri individui e con le norme (giuridiche e sociali) attinenti a tale comportamento. Le sue azioni non possono quindi essere interpretate come il solo prodotto di pulsioni interne e immaginandole in un ambiente asettico ed ininfluente poiché esse risentono dell'attività del fitto "reticolo" socio-culturale che le circonda. Il contesto sociale e culturale riesce ad influenzare le azioni umane attraverso una dimensione intermedia costituita dalla percezione sociale che si "gioca" all'interno della mente dell'individuo. In tale ottica analizzare come le persone percepiscono e producono significato intorno ad un determinato comportamento criminale è assai importante poiché tale processo influenza in ultima analisi la progettazione e l'esecuzione di tale comportamento.[2[2]]



È possibile insomma definire il criminale, ma anche la persona comune, come *"social cognizer"* [3[3]], vale a dire una persona che seleziona, organizza le informazioni provenienti dal mondo esterno, costruendosi in questo modo rappresentazioni del contesto in cui vive. Il risultato finale di questi processi consiste in forme di attribuzione di significato a situazioni e a soggetti e, nell'ambito che ci interessa in particolar modo, a conseguenti costruzioni (o meno) di azioni criminali.

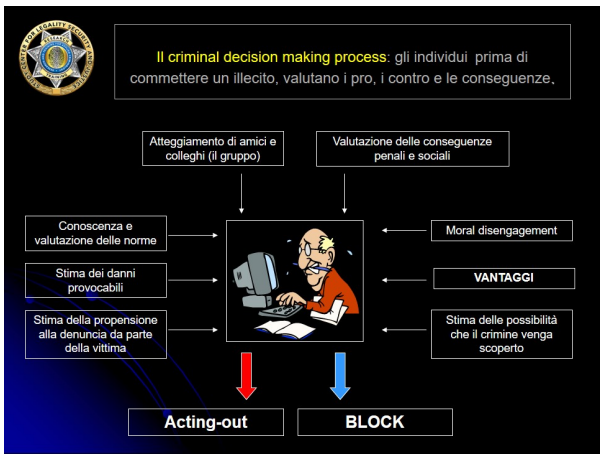


[1[1]] DE LEO G., PATRIZI P., *La spiegazione del crimine*, Il Mulino Bologna 1999:

[2[2]] A. BARATTA, *Problemi sociali e percezione della criminalità*, in Dei delitti e delle pene, 1, 1983.

[3[3]] M. HEWSTONE, W. STROEBE, 1991

Analizzando il crimine informatico in ottica sistemica e interazionista, proponiamo quindi 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*"4[4], 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.



Alcuni ambiti della cybercriminologia

In alcune ricerche condotte con tale approccio dall'autore è stato confermato dalle verifiche empiriche come la percezione del crimine, in ambiente digitale possa risultare notevolmente distorta. In alcuni casi di pedofilia on-line le modalità di approccio dei pedofili nelle chat line evidenziano una intuibile sottostima dei rischi di essere scoperti rispetto alle modalità di approccio classico del mondo reale. Tale circostanza potrebbe costituire un fattore disinibente per taluni soggetti e in un certo senso una facilitazione per il passaggio all'atto. Questa dinamica trova delle correlazioni, pur se in ambito non criminale, con l'evidente facilitazione che offre l'ambiente della chat rispetto all'esplicitazione di tematiche sessuali da parte di soggetti timidi ed introversi, mai capaci di eseguire la stessa performance nel corso di una interazione face-to-face. Uno studio pilota sulle truffe condotte con le carte di credito ha evidenziato una maggiore "disponibilità al crimine" da parte di soggetti completamente avulsi alle dinamiche criminali classiche nel momento in cui vengono proiettati in un contesto digitale laddove la scena criminis si trasferisce tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del monitor. Le esperienze di ricerca sugli hackers, infine, hanno spesso posto in evidenza la frequente percezione "ludica" delle intrusioni clandestine da parte dei giovani pirati informatici con l'evidente configurazione di atmosfere tipiche dei videogame. Gli studiosi contemporanei stanno sperimentando l'avvento e lo sviluppo di un nuovo mondo 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. La tendenza ad un agire comunicativo individuale e collettivo attraverso i collegamenti in rete implica l'insorgenza di problematiche percettive nuove che sembrano rappresentare variabili significative in ambito criminologico influenzando il processo di percezione, valutazione e attribuzione di significato che costituiscono la base del percorso che conduce gli individui dall'anticipazione mentale degli effetti del proprio comportamento alla decisione di porlo effettivamente in essere, violando le leggi.

Il criminologo moderno e il mondo digitale

Una delle funzioni primarie della Criminologia è il tentativo di spiegare il comportamento criminale. Il criminologo, per poter far questo, cerca in primo luogo di "entrare nella mente del criminale", tenta di delinearne la struttura di personalità, la sua sfera

4[4] Strano M., Computer crime, ed. Apogeo, Milano, 2000.

emozionale, la sua pericolosità. 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 però 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 dalla tecnologia digitale e dall'High Tech Crime (HTC). I criminologi contemporanei cercano infatti di applicare teorie interpretative classiche ai crimini informatici, adattando, o al massimo integrando tali teorie, spesso risultati modesti. 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).

High tech crime: le nuove frontiere del crimine

Lo scenario criminologico dell'high tech crime (HTC) si articola sostanzialmente attraverso tre fattori emergenti:

1. 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;
2. 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" del crimine assume un ruolo primario rispetto a quella pragmatico-utilitaristica;
3. 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[5]. 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. Ad esempio il *cyberstalking* eseguito da individui che non avrebbero mai il coraggio di molestare una persona nel corso di una relazione *face-to-face,* le minacce effettuate da timidi impiegati attraverso email, le truffe nell'e-commerce realizzate da informatici (non da truffatori professionisti), i pedofili che si aggregano sulla rete, rappresentano alcuni dei "sintomi" di tale situazione che suggerisce una certa alterazione della percezione, distinzione e valutazione degli effetti provocati con il proprio comportamento e della stima delle reali possibilità che il proprio crimine venga scoperto e sanzionato.

Tecnomediazione e cybercrime

La spiegazione del crimine tecnomediato e la definizione dei livelli di consapevolezza ad esso correlati implicano quindi la necessità di un'attenta analisi dell'influenza della dimensione digitale sulla modalità percettiva e cognitiva del soggetto nelle varie fasi dell'azione illegale.

La mediazione di uno spazio virtuale in un crimine sembra infatti 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

[5] Assenza di regole

- 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

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 che opera nell'ambito della Criminologia e della Sicurezza informatica.

LA RICERCA IN CYBERCRIMINOLOGIA

L'evoluzione rapida delle tecnologie comunicazionali ha indotto negli ultimi anni una altrettanto rapida modifica delle forme criminali connesse con tali tecnologie. I primi studi sulle azioni illegali condotte ai danni di mainframe da parte di esperti di informatica, hanno lasciato il campo, nel primo decennio del nuovo millennio, a ricerche sui comportamenti illegali connessi all'informatica distribuita e alla grande diffusione di internet. Sul piano prettamente psicotecnologico, la variabile maggiormente significativa per quanto attiene la percezione del crimine e di conseguenza i meccanismi di facilitazione dell'acting-out criminale, sembra essere legata all'avvento dei sistemi wireless che intervenendo sulla tecnomediazione, rendono ancor più impersonale e "distaccata" la connessione autore-vittima. L'assenza del cavo, che rende ancor più disancorata, sul piano simbolico, la scena del crimine digitale con il luogo fisico di abitazione o di lavoro del criminale informatico, rappresenta quindi probabilmente la variabile cybercriminologica emergente, su cui concentrare i nuovi protocolli di ricerca. Sul piano vittimologico, la diffusione dei social networks ha proposto nuovi rischi di vittimizzazione legati all'incremento del rilascio di informazioni sensibili già in fase di crescita attraverso i blogs e l'accesso a internet dei minori attraverso gli smartphone dell'ultima generazione ha inertizzato in larga parte le tecniche di prevenzione dei rischi attuate da genitori ed educatori attraverso la navigazione assistita e le tecnologie di parental-control. La costruzione del paradigma teorico della cybercriminologia, è ancora in prevalenza appannaggio di pochi gruppi di ricerca, prevalentemente di origine statunitense e britannica che negli anni hanno prodotto alcuni studi basati sulla raccolta tipologica dei crimini e sul tentativo di delineare dei tratti identificabili nei cybercriminali. Numerosi lavori sono stati realizzati nell'ambito della *cyberpedofilia* anche se raramente centrati sulla dimensione psicotecnologica e della *tecnomediazione*. Gli studi mirati sulle variabili indotte dalla *tecnomediazione* sul crimine in ottica sistemica e interazionistica appaiono ancora decisamente rari. I lavori che impiegano

strumenti per la valutazione della percezione del crimine (dalla parte quindi dell'autore) e della percezione del rischio (dalla parte della vittima) rimangono infatti ancora sporadici e poco sistematici. I filoni di ricerca moderni sulla cybercriminologia sono prevalentemente di due tipi: quelli tipologici e quelli basati sullo studio della *percezione del crimine*. I filoni di ricerca *tipologici* che partendo da soggetti già individuati come responsabili di azioni illegali cercano di delineare tratti comuni (biografici, personologici e psicopatologici) su base statistica, appaiono prevalenti nel panorama criminologico anglosassone e sono un valido supporto all'attività di *profiling* su base induttiva ma offrono scarsi contenuti conoscitivi di tipo applicativo sul versante della prevenzione. I filoni di ricerca basati sulla *percezione del crimine* il comportamento criminale viene costruito, elaborato (e spesso impedito) da un processo di pensiero del soggetto che molto si basa sull'anticipazione mentale degli effetti del proprio comportamento (effetti sociali e legali) e sull'aspettativa di reazione sociale. In questo approccio cybercriminologico (Strano M., 1995) quindi lo studio *percettivo* parte dall'assunto che il processo di digitalizzazione sociale abbia avuto una rapidità tale da non consentire un adeguamento antropologico da parte degli utenti con conseguenti ripercussioni sulle loro dimensioni percettive e cognitive e sulla correlata modalità di significazione dell'atto criminale. In particolare, come anzidetto, le dimensioni percettive e cognitive che entrano in gioco sembrano essere le seguenti:

- Stima dei rischi di essere individuato
- Stima dei rischi di essere catturato e denunciato (sanzione legale)
- Conoscenza della normativa
- Valutazione dei danni provocati alla vittima
- Paura della sanzione sociale

La ricerca cybercriminologica si focalizza quindi sulla capacità della tecnomediazione comunicazionale di alterare tali dimensioni influenzando la percezione individuale e sociale del crimine. L'individuazione precoce di modalità di atteggiamenti disfunzionali basati su errori cognitivi o su carenza di informazioni consente di attivare dei validi interventi di coscientizzazione (awareness) mediante percorsi di formazione-sensibilizzazione per gli utenti potenziali cybercriminali e attraverso l'adozione di soluzioni tecnologiche mirate.la cui efficacia è stata ampiamente documentata da ricerche specifiche (Strano M., 1995-2008)). Gli strumenti di ricerca utilizzabili in questo ambito sono generalmente assessment strutturati o interviste semistrutturate somministrate a gruppi delimitati che tendono a indagare i livelli di consapevolezza del rischio e le attribuzioni di significato rispetto a possibili azioni illegali attuate attraverso le tecnologie digitali comunicazionali.

I nativi digitali

La categoria emergente dei "nativi digitali", giovani nati intorno all'anno 2000 e cresciuti in un ambiente sociale fortemente permeato da tecnologie digitali comunicazionali suggerisce la possibilità in un futuro prossimo di una parziale messa in crisi degli assunti teorici basati interamente sul gap tecnologico-antropologico delle passate generazioni che ha considerato, a partire dal 1995, le variabili legate alla dispercezione da tecnomediazione in grado di interpretare una larga parte del comportamento criminale connesso all'uso di macro e microcomputer. La variabile adattiva rispetto alle tecnologie digitali (ad esempio sotto forma di significatività inversa della variabile biografica dell'età) dovrà probabilmente essere inserita nei nuovi strumenti di ricerca con una correlazione diretta rispetto ai livelli

di percezione e alla responsabilità legale del soggetto.

Download illegale di file

Il fenomeno dello scarico illegale di file musicali e cinematografici coperti da copyright costituisce ad esempio un problema enormemente diffuso. Tale contesto ha rappresentato motivo di progressivo inasprimento delle sanzioni in numerose Nazioni ad alto tasso di digitalizzazione sociale. Dal punto di vista criminologico sembra però manifestarsi un aumento della diffusione del fenomeno legato ancora a una ridotta percezione della gravità di tali azioni. I dati quantitativi che emergono ciclicamente da una ricerca iniziata nel 2004 e tuttora in corso di svolgimento in Italia indicano un livello di percezione del comportamento illegale on-line relativo alle violazioni di copyright (lo scarico e la diffusione di file musicali e cinematografici coperti da diritti d'autore) estremamente basso.

Sviluppo delle tecnologie e variabili criminologiche

La cybercriminologia di "scuola percettiva" ha mostrato in questi anni una progressiva modifica delle tipologie di criminali informatici del loro modus operandi e delle vittime. Tale evoluzione è legata in parte allo sviluppo delle tecnologie comunicazionali digitali, alla loro maggiore portabilità, alla maggiore diffusione delle tecnologie wireless e all'incremento della loro caratteristica userfriendly che ha ridotto alcune esigenze di manualità nell'impiego.

Mainframe e computer crime

All'inizio era computer crime. Giovani studenti di college americani che attaccavano i primi mainframe per sfida tecnologica, all'interno di spazi dedicati a queste macchine. L'accesso alla scena del crimine necessitava ancora di un contatto fisico con la macchina e l'introduzione dell'attaccante all'interno dello spazio vitale dell'apparato. Ambienti asettici con pavimenti flottanti, spazi refrigerati e i rumori tipici del funzionamento delle grandi macchine di calcolo rappresentavano la cornice percettiva di queste azioni criminali.

L.A.N. crime

Poi l'avvento dell'informatica distribuita, dei server e dei desktop nelle postazioni di lavoro apre la strada a forme di illegalità a tecnici e impiegati che accedono al sistema aziendale senza muoversi dalla loro postazione di lavoro. La scena del crimine digitale è ancora all'interno del perimetro aziendale ma la dimensione percettiva trova delle notevoli modifiche.

Internet crime

L'avvento di internet e l'interconnessione tra organizzazioni digitalizzate (tra reti di computer) propone nuove azioni criminali. Dal proprio spazio vitale l'individuo esce e si inserisce in un altro gruppo interconnesso. Il tipico suono del modem che attiva l'accesso all'infosfera digitalizzata segna anche percettivamente il passaggio a una possibilità di azione. La scena del crimine (il sistema attaccato) si può collocare anche a migliaia di chilometri dall'attaccante e la distanza geografica influisce sui livelli di percezione del crimine.

Home computer crime

La diffusione dell'informatica home e dei desktop sposta dal gruppo di computer aziendali all'abitazione dell'individuo il punto di partenza del net-surfing, e dell'invio di messaggi attraverso i programmi di e-mail. L'accogliente e rassicurante ambiente domestico influisce sulle dimensioni percettive del crimine.

ADSL connection crime

La connessione perenne, silenziosa e latente dei sistemi ISDN e ADSL porta lo strumento (desktop e Laptop) ad "appartenere alla rete". Scompare il suono di connecting del modem. La connessione agisce anche mentre l'utente utilizza la macchina in remoto e il passaggio da l'impiego di software office a software comunicazionale può divenire impercettibile per l'utente.

Wireless crime

La nascita dei sistemi wireless di connessione (gprs-umts) riduce ancora la percezione di localizzazione dell'utente. Il cavo, ultimo cordone ombelicale tra la dimensione fisica del soggetto e l'infosfera digitalizzata lascia il posto a uno spazio elettromagnetico. Si diffonde la tecnica del wardriving che consiste nel girare in automobile con un computer portatile per trovare qualche connessione wireless non protetta. Accedere alla rete attraverso la connessione di un altro soggetto ignaro abbatte la percezione del rischio da parte del computer criminal di essere individuato. Gli adattamenti percettivi e cognitivi in ottica criminologia legati alle tecnologie wireless riguardano quindi la difficoltà di comprendere cognitivamente l'esistenza e l'inviolabilità di uno spazio virtuale definito all'interno di una impalpabile rete di onde elettromagnetiche.

Palmtop crime

La riduzione delle dimensioni dello strumento di connessione alla rete porta alla nascita dei palmtop e a una modalità di connessione inframmezzata alle attività quotidiane. Il comando di connessione è agito con un semplice pressione di un pulsante o toccando una parte dello schermo con una piccola penna. L'utente è connesso e comunica mentre si muove e la percezione della sua rintracciabilità si affievolisce.

Smartphone & Blackberry crime

La diffusione di smartphone e blackberry propone una modalità nuova di connessione alla rete. L'accesso è perenne e i servizi web ed email si mischiano con i servizi voice e sms. L'attivazione delle connessioni è automatica all'atto dell'accensione dell'apparato. L'utente percepisce sempre meno la sua collocazione all'interno di una rete di scambio comunicazionale pervasivo.

Studi vittimologici sulla percezione del rischio

Gli studi vittimologici in ottica cybercriminologica sono centrati sulla percezione del rischio delle potenziali vittime e su comportamenti che possano agevolare l'azione da parte dell'autore del crimine.

Riferimenti bibliografici

1. Caretti V., La Barbera D., (a cura di) *Psicopatologia delle realtà virtuali*, Masson editore, Milano, 2001.
2. De Leo G., Patrizi P., *La spiegazione del crimine*, Il Mulino, Bologna, 1999.
3. De Leo G., Strano M., De Lisi C., Pezzuto G., *Evoluzione mafiosa e tecnologia criminale*, Giuffrè editore, Milano,1995.
4. Di Maria F., Cannizzaro S., (a cura di), *Reti telematiche e trame psicologiche* editore Franco Angeli, Milano, 2001.
5. Formenti C., *Not Economy*, Rizzoli, Milano, 2004
6. Galdieri P., Giustozzi C. Strano M, *Sicurezza e privacy in azienda*, Apogeo editore, Milano, 2001.
7. Rogers, M.A. *Modern-day Robin Hood or Moral Disengagement, Understanding the Justification for Criminal Computer Activity* Daily Mail & Guardian 10 February 1999
8. Strano M. Bodei A. Florio V *"Juvenile hacking criminological analysis" - 29th International Congress on Law and Mental Health* 2-9 Luglio 2005, Paris (France).

9. Strano M., "*HCP: hacking criminal profiling*" ICT security, Roma, luglio 2007;
10. Strano M., "*psicocriminologia delle truffe on-line*" ICT security, Roma, luglio 2007;
11. Strano M., "*Psicologia degli hacker*" ICT Security, Roma, Maggio 2003;
12. Strano M., "*un progetto di ricerca sulla percezione del rischio phishing*" ICT security, Roma, luglio 2007;
13. Strano M., *Computer crime*, Edizioni Apogeo, Milano, 2000
14. Strano M., *Dalle subculture devianti alle dimensioni dissociali dell'infosfera: le nuove modalità di aggregazione tecnomediata dei gruppi delinquenziali nel cyberspazio*., in Ricerche sui Gruppi, n° 11/12, (Gruppi e Internet), 2001;
15. Strano M., ed altri, Responsabilità penale e processo di digitalizzazione sociale, atti del convegno: Giovani, responsabilità e giustizia, Torino, 1998;
16. Strano M., Giustozzi C., I criminologi della rete: la ricerca universitaria sulla criminalità informatica in: BYTE, Giugno 1998;
17. Strano M., *Hackers: sviluppi e prospettive della cybercriminologia* in: *Psicopatologia delle realtà virtuali*, (Caretti V., La Barbera D.) Masson editore, Milano, 2001.
18. Strano M., Il computer crime nelle aziende, in BYTE, gennaio 1999
19. Strano M., Il furto di tempo macchina, in Byte, Luglio 1999
20. Strano M., *Manuale di Criminologia Clinica*, See Edizioni, Firenze, 2003
21. Strano M., Neigre B., Galdieri P., *Cyberterrorismo*, Yackson Libri, Milano, 2002
22. Strano M., Nuove tecnologie e nuove forme criminali. Atti della *Cybercrime International Conference*, Palermo, 3, 4, 5 ottobre 2002;
23. Strano M., *Relazioni digitali e comportamenti devianti*, Atti del convegno "Psichiatria, informatica e telemedicina. Realtà e prospettive nel campo dell'assistenza e della formazione". Velletri, Sala Micara, 29 marzo 2001.
24. Strano M., Telematica e cyberpedofilia in: Cantelmi T. et altri, La mente in internet, Piccin, Padova, 1999;
25. Strano M., *Nuovi media e violazioni al copyright: aspetti psicocriminologici,* Relazione al Convegno Proprietà intellettuali e nuove tecnologie in biblioteca, Milano, 7 maggio 2004, Centre Culturel Francais de Milan.
26. Turkle S., Vita sullo schermo, nuove identità e relazioni sociali nell'epoca di internet. Edizioni Apogeo.