

***Il Computer crime:  
"L'evoluzione del crimine Attraverso  
Le nuove tecnologie"***

[Pulcrano Luigi](#) & [Puglia Alessandra](#)

*INDICE: Introduzione 1 - Il fenomeno del computer crime 6, Tipologie di autore 9 - La formazione di subculture devianti 11 - Aspetti criminali della Rete Internet 13 - Internet e pedofilia 15, il caso Wonderland 22 - Omicidi e Internet 25 - Aspetti normativi 27 - Bibliografia 30.*

**INTRODUZIONE**

Intendendo con questa breve tesina approfondire quelle che sono le tematiche affrontate dallo studio e dalle ricerche nel campo dei crimini informatici, riteniamo opportuno introdurre l'argomento partendo da un più ampio spettro.

Possiamo considerare la Psicologia Forense quel settore della psicologia applicata che si occupa di tutte le problematiche psicologiche che insorgono nella pratica giudiziaria e in particolare dei casi in cui risulta indispensabile l'accertamento dell'integrità psichica del reo. In tutte le sue articolazioni (giudiziaria, criminale e carceraria), il lavoro dello psicologo forense si è espresso in due direzioni, diagnostica e terapeutica.

Interessando a noi l'ambito della psicologia criminale, ne diamo una più specifica definizione sottolineandone gli aspetti più salienti.

Con questo termine s'intende lo studio dei motivi, della personalità e delle scelte dei trasgressori. I motivi di molte trasgressioni, siano essi di approvazione, violente, sessuali o relative al traffico, sono normali, nel senso che esse vengono attuate di tanto in tanto da adulti normali: l'attività, la rabbia, la libidine, l'impazienza, il desiderio di eccitazione.

Quello che ha interessato gli psicologi clinici, gli psichiatri e gli psicanalisti è il motivo, che è anormale o per la sua intensità, tale che il trasgressore trova difficile esistervi anche quando è manifestamente pericoloso abbandonarvisi, o per la sua natura, come nel caso del sadismo o della pedofilia.

Alcune forme di disturbo mentale sembrano associate con certi tipi di comportamento riprovevole, benché non ci siano prove sufficienti del fatto che il disturbo mentale aumenti in generale la probabilità di avere problemi con la legge. Non di rado si riscontra che le persone che hanno commesso gravi violenze sulla persona sono depresse, schizofreniche o psicopatici aggressivi. Si ritiene che alcuni truffatori cronici abbiano una personalità isterica. Alcuni trasgressori in campo sessuale, soprattutto contro i bambini sono handicappati mentali.

L'incendio doloso se commesso in stato di esaltazione più che per desiderio di vendetta o di guadagno, sembra spesso un comportamento compulsivo.

In che misura la predisposizione a forme antisociali di comportamento sia congenita è stato a lungo oggetto di ricerca e di controversia. Quella che è certa è la trasmissione genetica di alcuni disturbi diagnosticabili, che a volte causano a chi ne soffre problemi antisociali (Es.: Corea di Huntington). Ci sono anche anomalie cromosomiche indiscutibili, non necessariamente ereditarie, come la sindrome XYY, associata con statura sopra la media, intelligenza inferiore alla media ed una probabilità poco più alta del normale di essere implicati in atti violenti, compresi quelli di natura sessuale. La maggior parte dei trasgressori, non presenta queste anomalie. I loro atti spesso derivano dalle circostanze e spesso è il comportamento della vittima che richiede una spiegazione. La trasgressione premeditata o comunque ripetuta, ha bisogno di una spiegazione approfondita. La causa può risiedere nell'imprudenza del trasgressore o in una deliberata assunzione di rischi, o nella mancanza di coscienza o di senso della vergogna o nell'attrazione per la vita criminale. Le spiegazioni correnti insistono sui metodi educativi o sui

valori di una cultura, su una scarsa intelligenza o su una ridotta capacità di apprendimento sociale.

Una delle nuove forme di criminalità che, alle porte del terzo millennio, appare emergente è: la criminalità tecnologica.

Tale forma criminale, che sembra progredire e svilupparsi di pari passo col progresso tecnologico della società postindustriale e con la sua informatizzazione, costituisce per molti aspetti un'area tematica ancora oscura. Il motivo di tale situazione è probabilmente riconducibile, oltre che alla giovane fenomenologia, anche alla notevole presenza, in questo ambito di studi, di variabili ad alto contenuto tecnologico che, per certi versi, sembrano scoraggiare gli studiosi di criminologia provenienti da percorsi accademici di tipo tradizionale.

La fine di questo secolo evidenzia una crescente diffusione di tecnologie informatica e telematica in ogni ambito della struttura sociale destinata ad un notevole incremento anche in base alla riduzione dei prezzi d'acquisto attuata quasi in tutto il mondo e all'aumento dei servizi offerti "on-line".

Secondo Negrotti il computer è "uno strumento, per giunta sempre definito stupido in sé che si è trasformato in una sorta di fonte primaria le cui conseguenze negative possono essere:

disumanizzazione del lavoro, distruzione della privacy, dipendenza eccessiva dalla macchina”.

Oggetto d’interesse criminologico sembra essere anche la definizione di forme criminali nuove, fortemente connotate dalla vasta area del computer-crime.

Nel 1982 uno scrittore di fantascienza inventò il termine di “ciberspazio” usato per indicare uno spazio virtuale nel cui ambito vengono consumati, i crimini legati al settore informatico e telematico. Secondo alcuni studiosi, la costruzione dell’ambiente virtuale relativo alla comunicazione telematica (il ciberspazio) possiede delle prerogative in grado di “strutturare la nostra weltanschauung e proporre una nuova economia di rapporti tra il reale e le nostre rappresentazioni”.

## ***IL FENOMENO COMPUTER CRIME***

I primi fenomeni di “abuso informatico” agli inizi degli anni '60, sono condotti soprattutto ai danni delle grosse compagnie telefoniche americane, da parte di hackers animati da vari intenti. Alcuni sono semplicemente studenti di college che giocano occasionalmente con il nuovo giocattolo tecnologico, altri si identificano in una subcultura di area “yuppie” e considerano l'intrusione nelle reti telefoniche in modo più cosciente e legato all'esigenza di comunicare nonostante il loro deficit organizzativo. Negli anni '90, le implicazioni politiche, economiche e sociali legate al processo di informatizzazione del sistema sociale conduce inevitabilmente ad affrontare l'intangibile natura del ciber spazio come proprietà e il progressivo passaggio da una problematica criminologica legata a comportamenti genericamente trasgressivi ad una vera e propria definizione di categorie criminali correlate ad altrettante dinamiche in ambito normativo, di allarme sociale e di forme di controllo.

Il computer crime è un fenomeno con molteplici espressioni e con diversificate dinamiche di allarme sociale ad esse correlate.

Dietro un abuso informatico possono celarsi intenti ascrivibili a semplici curiosi in cerca di emozioni, ladri, spie, terroristi, pedofili, trafficanti di droga.

Nel caso del computer crime sembra configurarsi l'ipotesi di una vittima impersonale ed astratta che non risveglia reazioni di empatia e di identificazione come quelle che sorgono quando la vittima è una persona fisica. Molto importante è il "numero oscuro" che è un ostacolo conoscitivo per le ricerche empiriche sull'argomento. Le vittime sono riluttanti a palesare i fatti attraverso la denuncia alle autorità.

L'obiettivo della pirateria elettronica è quello di penetrare in sofisticati sistemi informatici, non per la sola soddisfazione di riuscirvi o per lasciare una testimonianza, una traccia del suo passaggio di solito consistente in un virus capace di danneggiare più o meno gravemente il sistema, ma anche per effettuare frodi di varia natura.

L'hacker (parola che in tedesco significa "contadino che zappa") o pirata informatico, è una figura ormai familiare nel mondo dell'informatica. L'hacker ha un'età compresa tra i 19 ed i 25 anni, è per lo più studente, ma alta è anche la percentuale di impiegati che

lavorano nella maggioranza dei casi in settori estranei all'informatica e predilige le ore notturne per compiere le proprie gesta.

Secondo l' "U.S. Secret Service", invece, si aggirerebbe attorno al mezzo miliardo di dollari l'ammontare delle truffe attraverso il furto da database on-line dei numeri di carte di credito di chi si affida al commercio elettronico. Altri lo stanno diventando, come il pirataggio informatico. Fra i casi più recenti quello del quindicenne di Montreal, detto "Mafiaboy", che in febbraio aveva messo in ginocchio numerose multinazionali del Web inviando milioni di messaggi di servizio da vari computer (controllati da una mano ignota) verso i loro siti. E' stato arrestato, multato e poi rilasciato perché minore, ma rischia comunque di farsi qualche anno in riformatorio visto che per questa "bravata" Yahoo!, CNN, Ebay, ZD Net, Etrade avevano perso decine di milioni di dollari. E' stato tratto in inganno dalla sua stessa vanità che lo ha spinto a gloriarsi dei suoi exploit nelle chat frequentate dagli hacker ed è stato così contattato dalla Polizia Canadese.

## -Tipologie di Autore-

Il computer crime sembra essere un tipo di comportamento illegale strettamente correlato ad alcuni prerequisiti funzionali indispensabili da parte degli autori, tra cui un certo livello di professionalità, di informazione, di conoscenza e delle specifiche competenze.

Quindi nell'ambito del computer crime un importante aspetto per una classificazione può essere il livello di professionalità criminale manifestato dagli autori nel corso dell'esecuzione dell'operazione in termini tecnologici e di comportamento in generale.

Alcune connotazioni ricorrenti sono:

- ? comportamento genericamente non-violento;
- ? finalità di produzione di guadagno;
- ? conoscenza di tecnica;
- ? pianificazione del reato;
- ? minimizzazione delle possibilità di cattura assumendo un comportamento definito un-noted.

Alcuni autori definiscono: **AMATEURS**: le persone dedite occasionalmente e con ridotta abilità a tali atti illeciti;

**Fraud Masters**: le persone in possesso di quelle prerogative richieste per queste forme di criminalità (raffinata abilità, competenza tecnica e destrezza; uso strumentale di tale attività al posto della violenza; raggiungimento

di notevoli profitti senza essere scoperti; connessione con una rete informale di professionals necessaria per scambio d'informazioni e per la reciproca assistenza; capacità di mantenere un comportamento un-noted), sono dei criminali spesso in grado di svolgere la loro attività illecita senza essere scoperti per lungo tempo, di non facile identificazione sociale, con non chiare connotazioni in grado di renderli riconoscibili ed isolabili, spesso apparentemente rispettabili cittadini ma con la particolarità di trarre il loro reddito dall'esecuzione sistematica di frodi.

Inoltre è stato studiato che il comportamento criminale verrebbe appreso all'interno di gruppi significativi; ciò che un individuo apprende a contatto con questi gruppi dipende dalla durata, frequenza e intensità dell'associazione.

## ***LA FORMAZIONE DELLE SUBCULTURE DEVIANTI***

La cultura di un gruppo, secondo ormai famose ricerche può essere considerata come una risposta ad un problema affrontato in comune da un gruppo di persone, nella misura in cui sono in grado d'interagire e comunicare efficacemente tra loro. Il fattore determinante è costituito proprio l'elemento "comunicazione" che costruisce valori ed identità di un aggregato sociale intorno a significati condivisi. La questione della formazione di una subcultura deviante proveniente da una rete d'interazioni tra soggetti devianti è stata affrontata da molti studiosi.

Becker sostiene che: "dove le persone che praticano attività devianti hanno l'opportunità d'interagire tra loro, è probabile che si sviluppi una cultura costruita intorno ai problemi emersi dalle differenze tra la loro definizione di ciò che fanno e la definizione sostenuta da altri membri della società". Nel mondo telematico esiste una dimensione, di interesse criminologico, relativa alla disponibilità di contesti di illegalità che offre notevoli possibilità di studio e approfondimenti.

Sulla rete Interne, ad esempio sono raggiungibili siti che contengono informazioni illegali di vario genere, dalle istruzioni per la

fabbricazione in casa di droghe ed esplosivi ai progetti per la realizzazione di virus informatici, nonché dati e materiale fotografico messi in rete da pedofili.

A volte questo materiale è protetto dagli utenti “normali” mediante procedure particolari tipo speciali codici o mediante cifratura dei testi, altre volte è liberamente fruibile da tutti. Nel caso della pornografia, si è attivato un acceso dibattito sulla questione della possibilità di censurare in qualche modo tali siti soprattutto per quanto riguarda la loro fruizione da parte dei minori che, navigando dentro altre reti telematiche, possono di fatto essere esposti a materiale che altrimenti difficilmente potrebbero visionare.

Un altro aspetto di indubbia rilevanza criminologica è rappresentato dal notevole incremento della prostituzione mediante le reti telematiche. Specie in Francia all'interno delle diffusissime BBS per cuori solitari in cerca di incontri si dissimulano sovente messaggi di professionisti della prostituzione ma anche di persone che cercano così di arrotondare il bilancio familiare aggirando, grazie il computer, il tradizionale impatto con il mondo del marciapiede le cui peculiarità di durezza e di violenza rappresentano una certa barriera per molti individui.

## ***ASPETTI CRIMINALI DELLA RETE INTERNET***

La grande popolarità e diffusione della rete internet che si sta proponendo come un vero e proprio luogo di dispiegamento di una nuova maniera di essere al mondo, di pensare il mondo e di agire su di esso è interessato a questioni di interesse criminologico. La presenza di svariate attività illegali su internet è cosa oramai assodata senza per questo voler criminalizzare tout court uno strumento di straordinaria utilità.

Le reti telematiche rispecchiano il mondo che le ha create.

Contengono pornografia, criminali, terroristi, truffatori, ma anche cultura, informazione, scienza e tutto ciò che è positività e progresso.

Alcune questioni effettivamente suscitano un certo allarme sociale come ad esempio la disponibilità di materiale pornografico per i minori, i casi di adescamento da parte dei pedofili, il furto d'informazioni, i sabotaggi di sistemi con virus, il gioco d'azzardo, le intrusioni clandestine da parte degli hackers. Un esempio di attività criminale che riteniamo opportuno ricordare, sono le comunicazioni illegali: pedofilia, traffico di droga, riuscendo a mantenere l'anonimato attraverso procedure tecnologiche, sfruttando il diritto

della privacy. E' particolarmente acceso il dibattito scientifico e politico sul delicato equilibrio tra la tutela della riservatezza e l'esigenza del controllo nelle comunicazioni telematiche che oramai sembra aver definito, da un lato, un fronte liberatorio che attribuisce enormi potenzialità di sviluppo di un nuovo modo di partecipare alla vita politica attraverso la formazione di "comunità elettive" che funzionino secondo un modello di tipo reticolare, deterritorializzato e libero da ogni forma di limitazione espressiva, privilegiando quindi la libertà di comunicazione senza vincoli e controlli e, dall'altro lato, un fronte che antepone alla libera e riservata espressione, la preoccupazione che venga a crearsi uno strumento comunicazionale dove qualsiasi fuorilegge possa effettuare i suoi traffici illeciti pressoché indisturbato.

## ***INTERNET E PEDOFILIA***

Internet è divenuto negli ultimi anni il modello alternativo della comunicazione sociale e delle relazioni interpersonali, specialmente nel campo della sessualità.

La pornografia ha sempre esplorato per prima tutte le nuove tecnologie nel campo della comunicazione (per esempio fotografia, videotape, internet etc.), che col passare del tempo si sono sempre più perfezionate. Si è stimato che le entrate dell'industria del porno on-line, abbia raggiunto nel 2001 ben 366 milioni di dollari (Sprenger, in Blue Money 1999). Il commercio on-line va dall'accesso in siti a pagamento dedicati al sesso convenzionale, del tipo Play Boy Magazine, alla vendita di materiale erotico, alla visione di veri e propri filmini hardcore e ancora allo scambio di foto e video pornografici.

La grande diffusione di Internet in questo campo è dovuto molto probabilmente oltre che alla facilità con cui è possibile accedervi (3 famiglie su 5 possiedono un collegamento ad internet, ISTAT 2000), anche per l'anonimato che la rete è in grado di fornire.

A mio parere l'anonimato può favorire soggetti con pedofilia che, spacciandosi per coetanei dei "piccoli", possono ottenere foto,

raccogliere informazioni e, a volte, organizzare incontri con le potenziali vittime.

Negli Stati Uniti, dove la navigazione da parte dei bambini è molto più diffusa che nei paesi Europei: dal 1993 gli arresti da parte dell' FBI, per crimini contro i bambini su internet, sono stati quasi 200.

In Italia di recente è stata scoperta un'organizzazione che trafficava bambini sulla rete, codificando la merce come se fosse vino: rosso per le femmine, bianco per i maschi; mentre la gradazione (che raramente superava i 14°) era riferita all'età.

Una ricerca di Serra e coll., utilizzando una tecnica di tipo antropologico-etnografico, l'osservazione sul campo, applicata all'attività di monitoraggio di una delle chat-line più utilizzate in Italia : "IRC Italia"; ha voluto misurare la frequenza dei tentativi di molestie e di adescamento da parte dell'adulto nei confronti della "bambina Virtuale" immesso nella rete. La tecnica dell'osservazione partecipante, prevede il coinvolgimento diretto del ricercatore con l'oggetto di studio, infatti la simulazione di identità di bambini compresi tra gli 8 e i 13 anni ha richiesto un lungo periodo di training formativo, durante il quale la "bambina virtuale", ha dovuto trascorrere molto tempo con minori della fascia d'età studiata per assimilare e metabolizzare il loro linguaggio e i loro valori. Allo

scopo di evitare, il più possibile, l'intrusione di variabili di disturbo si è stabilito un comportamento costante della bambina virtuale: un approccio il più possibile simile nei vari collegamenti, privo di atteggiamenti provocatori; nel caso di molestie verbali da parte dell'interlocutore adulto l'atteggiamento della bambina si caratterizzava da curiosità non eccessiva, al fine di proseguire la conversazione. Dall'analisi emerge che nell'84% dei collegamenti, non si è verificata alcun tipo di molestia e nessun tentativo di adescamento, mentre nel 12% dei casi, l'interlocutore adulto ha focalizzato la propria attenzione su racconti e descrizioni del minore rispetto alla propria sessualità, con tentativi di condurre il minore nel corso del collegamento, verso atti sessuali (come la masturbazione); e solo nel 4% dei casi si è verificato un vero e proprio tentativo di adescamento, in queste situazioni spesso l'interlocutore adulto cerca di ottenere il numero telefonico del bambino, assecondando gli interessi del minore, individuati durante l'interazione.

In sintesi, l'analisi quantitativa relativa agli eventi misurati nell'indagine sembra confermare l'ipotesi secondo cui è necessario ridimensionare l'allarme e l'idea creatasi nell'immaginario collettivo del binomio Internet/pedofilia, e indirizzare invece il dibattito verso una più consapevole e lucida attività di prevenzione.

Infatti, la disinformazione sulla realtà del drammatico problema degli abusi contro i minori, le ossessioni sessuofobiche che ancora caratterizzano la cultura politica italiana e l'irriducibile avversione contro ogni mezzo di comunicazione, sono le componenti costitutive di questa crociata politica e giornalistica contro il nuovo demone della "pedofilia telematica; mentre, basterebbe far riferimento ai dati relativi all'identità dei responsabili di violenza sessuale contro i minori. Infatti, secondo le statistiche dei procedimenti penali relativi a questi reati, il 90% dei casi degli abusi sessuali avviene in famiglia, l' 8% è agito da conoscenti (vicini di casa, scuola, chiesa etc.), e solo il 2 % chiama in causa persone sconosciute al minore.

Tuttavia esiste un'ampia varietà di filtri e di blocchi per evitare che i bambini che navigano in rete finiscano in siti non adatti a loro: alcuni hanno nomi suggestivi come: "La pattuglia cibernetica", "Il pastore della rete", "l'accompagnatore nel web", "La governante nella rete" ecc.; tra i più diffusi troviamo: Cyber Patron, Cibersitter, Net Nanny, Kidnet Explorer e Surfwatch. Questi funzionano generalmente con e tramite il browser (il programma che utilizziamo per navigare). Questi pacchetti filtro possono svolgere funzioni diverse, come ad esempio stabilire elenchi di indirizzi ai quali il browser non può accedere (black list). Un'altra tecnica diffusa si basa su etichette

elettroniche che possono essere aggiunte nelle varie pagine web per descriverne il contenuto; in tal modo il programma di controllo, in base al contenuto dell'etichetta, può effettuare una scelta, selezionando o meno il documento. Esistono pacchetti che consentono di controllare il flusso in ingresso o in uscita della e\_mail, consentendo in tal modo di ricevere e inviare posta solo a determinati indirizzi. Un buon numero di ISP (Internet Service Provider), come CompuServe o AOL, mette a disposizione, gratuitamente nel servizio, alcuni programmi filtro, ma la stragrande maggioranza dei navigatori internet non è a conoscenza e pertanto non fa uso di questi programmi.

In Italia, la legislazione, con l'introduzione della legge 66 del 1996, ha unificato il reato di violenza sessuale con gli atti di libidine (da ciò ne consegue che non è necessario il compimento del completo atto sessuale affinché si possa parlare di violenza), e ha ridefinito il reato di violenza sessuale da reato contro la morale a reato contro la persona, con l'applicazione di pene più severe per l'autore.

Inoltre, nei 19 articoli della legge 269 del 1998, contenente le norme contro la pedofilia, mantenendo l'impegno preso dall'Italia con la Convenzione di New York sui diritti del fanciullo del 1989, la magistratura si impegna a:

- 1) Rinforzare la repressione penale attraverso la creazione di nuove fattispecie delittuose quali: la prostituzione minorile, la pornografia minorile, la detenzione di materiale pornografico, e le iniziative turistiche finalizzate allo sfruttamento della prostituzione minorile;
- 2) Fornire, alle autorità giudiziarie, nuovi strumenti processuali come l'obbligo dell'arresto in flagranza, la possibilità del fermo dell'indiziato, l'applicazione della custodia in carcere o delle intercettazioni, l'utilizzo dell'audizione protetta per i minori di anni 16.
- 3) Facilitare la polizia giudiziaria nelle indagini, permettendo: l'acquisto simulato di materiale pornografico; l'apertura di siti Internet di "copertura" in grado di scovare chi partecipa alla distribuzione di materiale pornografico di minori per via telematica; il ritardo nell'esecuzione di provvedimenti, quali l'arresto o il sequestro qualora tale ritardo contribuisse all'identificazione di ulteriori autori di reato o organizzazioni criminose più vasti; l'infiltrazione di agenti all'interno di viaggi che tendono allo sfruttamento della prostituzione minorile.

Oltre le leggi citate, a partire dai primi del Novecento sono state stilate diverse convenzioni a livello internazionale che si possono far rientrare sotto l'etichetta "prevenzione della pedofilia", che sono riuscite nel tempo ad imporsi e a registrare indiscussi successi (vedi Tab. 1).

**Tab. 1 – Indice cronologico delle maggiori convenzioni internazionali per la protezione dell'infanzia**

E' possibile redigere un indice cronologico delle maggiori convenzioni che hanno in qualche modo contribuito alla tutela dell'infanzia:

1. 1902: Conferenza di diritto Internazionale Privato che considerò l'interesse del bambino come un criterio importante da inserire nelle convenzioni a tutela dei minori;
2. 1902: Convenzione dell'Aja sulla tutela dei minori;
3. 1923: Convenzione per la soppressione della circolazione e del traffico di pubblicazioni oscene;
4. 1924: Dichiarazione di Ginevra per il diritto del fanciullo ad una normale crescita psicofisica e spirituale e ad una protezione speciali che gli consenta di ricevere un'educazione e gli garantisca un futuro;
5. 1930: Convenzione dell'International Labor Organization sul lavoro Forzato;
6. 1949: Convenzione per la soppressione del traffico di persone e dello sfruttamento della prostituzione;
7. 1950: Convenzione Internazionale per la tutela dei diritti umani e delle libertà fondamentali
8. 1956: Convenzione integrativa sull'abolizione della schiavitù;
9. 1959: Dichiarazione dei diritti del bambino;
10. 1961: Carta Sociale Europea;
11. 1961: Convenzione dell'Aja sulla competenza delle Autorità e la legge applicabile in materia di protezione dei minori;
12. 1969: Convenzione Americana sui diritti umani;
13. 1973: Convenzione dell'International Labor Organization sull'età minima per limitare lo sfruttamento nelle attività economiche;
14. 1989: Convenzione Internazionale dei diritti del fanciullo, New York, ratificata in Italia con la legge n. 176 del 27 maggio 1991;
15. 1990: Dichiarazione Universale sulla sopravvivenza, protezione e sviluppo dei fanciulli e relativo programma d'azione;
16. 1990: Carta Africana dei diritti del fanciullo;
17. 1991: Raccomandazione n. R (91) 11 degli Stati Membri del Consiglio d'Europa;
18. 1991: Programma d'azione della Commissione O.N.U. per la prevenzione del traffico dei minori e della pornografia infantile;
19. 1994: Convenzione inter-Americana sul traffico internazionale dei minori;

Segue

20. 1995: Sentenza di condanna del Tribunale Permanente dei Popoli nei confronti di tutti gli Stati per le violazioni dei diritti fondamentali dell'infanzia e dei minori perpetrate da tutte le Nazioni
21. 1996: Convenzione Europea sull'esercizio dei diritti dei minori;
22. 1996: Dichiarazione finale della Conferenza Mondiale di Stoccolma contro il commercio e lo sfruttamento dei bambini;
23. 1996: Risoluzione del parlamento Europeo dei minorenni vittime di violenze
24. 1997: Risoluzione del parlamento Europeo sulla lotta al turismo sessuale e al rafforzamento della lotta contro l'abuso e lo sfruttamento sessuale dei bambini.

### **- Il caso Wonderland -**

Il primo Settembre in 31 città degli Stati Uniti e in 11 Paesi in tutto il mondo era scattata il raid contro la pedofilia più vasto fino ad oggi - "Operazione Cheshire Cat" negli Stati Uniti, "Operazione Cathedral" in Gran Bretagna e nel resto d'Europa - che aveva portato all'arresto di un centinaio di persone, tutti membri di un club, "Wonderland", il "Paese delle meraviglie" di Alice, la più sofisticata rete di pedofili on-line mai scoperta: 11 arrestati in Gran Bretagna, 32 negli Stati Uniti, 18 in Germania, 16 in Italia, otto in Norvegia, uno o due in Finlandia, Belgio, Austria, Francia, Svezia, Portogallo.

Tutti i membri di Wonderland arrestati in settembre avevano almeno diecimila immagini pornografiche sul loro computer: era la condizione per essere ammessi al club. Il gruppo, ha raccontato la polizia, usava tecniche molto sofisticate. Nelle riunioni virtuali

votavano su chi avesse i requisiti per diventare membro della comunità, che viveva nascosta nell'anonimato delle chat su IRC. Qui, nella parte più nascosta di Internet, con meno di 100 dollari al mese, i membri del club pedofilo compravano l'accesso alla chat segreta dove scambiavano file di foto pornografiche di bambini. Foto criptate con dei codici provenienti dal KGB, l'ex servizio segreto sovietico, in modo da impedire ai non membri di accedere alle immagini.

La prima traccia telematica dell'esistenza del club di pedofili on-line la polizia americana l'aveva trovata in un'inchiesta su un abuso sessuale di una bambina di dieci anni avvenuto nel 1996 a San Jose in California. La denuncia era partita dalla madre della bambina, che aveva chiamato la polizia dopo che la figlia aveva raccontato di essere stata molestata da un certo Ronald Allen Riva durante la sua festa. L'uomo era stato accusato e poi processato per aver offerto la bambina ad altri membri di una piccola rete di pedofili, l'Orchid Club. Dal computer di Riva, la polizia era risalita al Sussex, in Inghilterra, e da lì al più ampio club Wonderland.

Heinz Schaefer era uno dei membri di Wonderland. Dopo l'arresto aveva chiesto un'aspettativa dal lavoro. Il suo nome era comparso sul giornale locale, e quando si era collegato a Internet per comunicare la sua disavventura, i suoi amici, quei pochi che aveva al di fuori del

club Wonderland, lo avevano buttato fuori dalla chat, lasciandolo così senza il suo rifugio. E appena la polizia aveva reso noti i primi particolari dell'inchiesta, aveva deciso che il male minore, per lui, era togliersi la vita. Con il suicidio di Schaefers sale a dieci il numero di persone, tutti presunti membri del club di pedofili, che si sono tolte la vita. Il suicidio, in questi casi, sembra essere l'unica via d'uscita per non affrontare l'umiliazione di un processo e di una relativa incarcerazione.

## **OMICIDIO E INTERNET**

### **- Il caso Youens -**

Internet, come già abbiamo accennato prima, è un formidabile strumento di cultura, socializzazione ed intrattenimento, ma può diventare uno strumento estremamente pericoloso ed efficace nelle mani di un criminale.

Per un decennio intero, il giovane Liam Youens ha studiato il modo di uccidere un'ex compagna di scuola liceale, Amy Boyer, rea secondo la psiche distorta dell'assassino, di non aver corrisposto il suo amore ossessivo.

All'interno del suo personale sito internet, Youens scrisse: "Fu allora che io decisi di uccidere tutti e due, quello fu il mio unico, lucido piano per tutto il decennio successivo". Il giovane studiò il crimine per anni, in ogni minimo dettaglio, utilizzando il cyberspazio per scoprire ogni informazione personale sulla vittima, abitudini e spostamenti (attraverso le spese effettuate mediante carte di credito).

Alla fine, il 15 ottobre 1999, Youens si reca nello studio dentistico dove lavorava la ventenne Boyer e le scarica addosso tutto il caricatore del suo revolver, tenendo l'ultimo colpo per suicidarsi.

Youens aveva aperto più di un sito nei quali rifletteva sull'opportunità e le modalità per eliminare la ragazza responsabile, secondo lui, di tutta la sua sofferenza, descrivendo nei particolari ciò che avrebbe potuto fare. Tutte queste farneticazioni erano registrate in due siti di internet gestiti dalle società Geocites e Tripod. Nel frattempo, Youens ha versato diversi milioni di lire a servizi di ricerca on line che gli hanno fornito la data di nascita della Boyer, il suo numero di codice fiscale, indirizzo, numero telefonico e gusti nello shopping. I suoi messaggi telematici diventavano sempre più minacciosi, senza che le due società che gestiscono i siti abbiano preso nessuna iniziativa. Qualche mese prima dell'omicidio il ragazzo annota nei siti queste parole: “ *E' osceno quante informazioni sulla gente si riescono a trovare su internet...* ”

Forse quest'omicidio si poteva evitare, se solo fosse stato possibile poter mettere sotto controllo i siti del giovane Youens, ma quanto siamo disposti a perdere in termini di Privacy per la nostra sicurezza personale? Sarebbe veramente utile una legge che limiti la libertà di espressione e circolazione di idee nel cyberspazio, o, data la difficoltà tecnica di attuare un controllo così sistematico, diverrebbe presto solo un'ennesima Utopia?

## ***ASPETTI NORMATIVI***

Una delle basi conoscitive imprescindibili nell'ambito della ricerca criminologica è rappresentata dallo studio delle leggi che in definitiva, determinano l'esistenza o meno di un comportamento criminale.

In America esistono già organismi creati per la lotta al crimine informatico, come lo "U.S. Department of Justice Computer Crime and Intellectual Property Section", che si occupa di contrastare gli attacchi dei pirati informatici e che fornisce indicazioni su come denunciare frodi o crimini attuati attraverso Internet, o come la "Web Policy", agenzia governativa di lotta al crimine sul Web. Se il dibattito negli Stati Uniti è ormai in fase avanzata, in Europa, e soprattutto in Italia dove Internet si sta solo ora diffondendo, si è appena iniziato a discuterne: di recente il Consiglio d'Europa ha reso pubblico un primo progetto di convenzione internazionale sui crimini informatici; il testo ha il compito di armonizzare le legislazioni nazionali dei paesi membri del Consiglio in materia di crimini informatici, di facilitare le inchieste e di permettere una cooperazione efficace tra i diversi paesi.

Il progetto, che oltre ai 41 paesi europei coinvolge anche Canada, Giappone e Sud Africa, prende in considerazione tutti i cyber-crimini e incoraggia gli stati membri ad adottare gli stessi metodi di inchiesta per facilitare la collaborazione fra stati e per evitare che le frontiere diventino una protezione per i criminali informatici, che possono disperdere le prove della loro colpevolezza attraverso computer diversi nel mondo.

L'iniziativa ha già sollevato qualche perplessità da parte della comunità virtuale. Infatti uno degli strumenti che sarà utilizzato per combattere i crimini informatici è la "perquisizione informatica a distanza": una serie di tecnologie e procedure di controllo che dovrebbero consentire alle polizie dei vari paesi di perquisire i computer di chi è sotto inchiesta anche da lontano. Non sarebbe più insomma necessario sequestrare i computer per controllare gli hard disk, anche se sono ancora tutti da definire gli strumenti per assicurare alle forze dell'ordine questa facoltà.

Questo provvedimento, se indubbiamente rappresenta un passo avanti nella lotta ai criminali informatici, viola la privacy dei navigatori.

Nel panorama normativo italiano, da qualche anno, sono entrate in vigore la legge 23 dicembre 1993, n. 547 e il Decreto Legislativo 29 dicembre 1992, n. 518 che tendono verso l'allineamento del codice

penale con alcune nuove fattispecie criminose legate all'informatica e alla telematica.

La questione del rispetto della privacy in relazione all'esigenza dell'attività istituzionale di controllo e al generico trattamento dei dati informatici da parte dei privati, è sfociata in una produzione normativa; ricordiamo in proposito la legge 31 dicembre 1996, n. 675: "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".

## **BIBLIOGRAFIA**

- BISIO B., *Psicologia criminale*, Bulzoni, Roma, 1999
- BURKE, ANNE; SOWERBUTTS, SHAWN;(2002) *Child pornography and the Internet: Policing and treatment issues* in: *Psychiatry, Psychology & Law*. Vol 9(1), Apr 2002, pp. 79-84.
- COOPER, A., MCLOUGHLIN, I. P., & CAMPBELL, K. M. (2000). *Sexuality in cyberspace: update for the 21st century*, in: *Cyber Psychology & Behavior*, 3, 521-536.
- DE LEO G., *L'abuso sessuale infantile e la pedofilia*, Franco angeli, Milano, 1999.
- DE LEO G., *La spiegazione del crimine*, Il Mulino, Milano, 1998.
- DURKIN, K. (1997). *Misuse of the Internet by pedophiles: implication for law enforcement and probation practice*; in: *Federal Probation*, 61, 14-18.
- FERRARIS A., *Il volto e la maschera*, Ed. Valore scuola, Roma, 1999.
- FISHER WILLIAM A. & BARAK A., (2001) *Internet Pornography: A social psychological perspective on internet sexuality*, in: *The Journal of Sex Research*, Vol 38 (4), Nov 2001: pp. 312-323.
- FREEMAN-LONGO, ROBERT E; (2000) *Children, teens, and sex on the Internet Sexual Addiction & Compulsivity*; in: *Special Issue: Cybersex: The dark side of the force*. Vol 7(1-2), pp. 75-90.

- GRIFFITHS M., (2001) *Sex on the Internet: Observations and Implications for Internet Sex Addiction*, in: The Journal of Sex Research, Vol 38 (4), Nov 2001: pp. 333-342.
- GALIMBERTI U., *Psicologia*, Garzanti, modena, 1999.
- GULLOTTA, *Psicologia giuridica*, FrancoAngeli, Milano, 1998
- IZZO F., *Norme contro la pedofilia*, Simone, Roma 1998.
- LAMB, M. (1998). *Cybersex: research notes on the characteristics of visitors to online chat rooms*. In: Deviant behavior: An Interdisciplinary Journal, 19, 121-135.
- LAMB, M., *Psicologia*, Economica Laterza, Padova, 1997
- LINEHAN, C., QUAYLE, E., HOLLAND, G., & TAYLOR, M. (2001). *Virtual paedophile communities*; In: The Journal of Sexual Aggression, 6, 78-96.
- MCCABE, KIMBERLY, (2000). *A Child pornography and the Internet*; in: Social Science Computer Review. Vol 18(1), Spr 2000, pp. 73-76.
- NEGROTTI, *L'ombra di Wells e la società informatizzata*, Franco Angeli, Milano, 2000
- SERRA C., *Proposte di Criminologia Applicata*, Giuffrè, Milano, 2002.
- SERRA C., *Psicologia Penitenziaria*, Giuffrè, Milano, 2000 .
- SERRA C., STRANO M., *Nuove frontiere della criminalità. La criminalità informatica*, Giuffrè, Milano 1997.