

PREMESSA

La globalizzazione ha ristrutturato lo spazio-tempo all'interno del quale gli individui e i gruppi organizzano le loro esperienze di vita. Come scriveva McLuhan negli anni sessanta:

nell'era della meccanica avevamo operato un'estensione del nostro corpo in senso spaziale e, dopo oltre un secolo di impiego tecnologico dell'elettricità, abbiamo esteso il nostro stesso sistema nervoso centrale in un abbraccio globale che, almeno per quanto concerne il nostro pianeta, abolisce tanto il tempo quanto lo spazio ¹.

Grazie ai *media* globali le persone possono, ogni giorno, «attraversare» realtà radicalmente discontinue e opposte. Alla maggiore velocità di spostamento fisico si accompagnano flussi di comunicazione sempre più intensi e un'accresciuta capacità di mobilità virtuale, fino a raggiungere quello che il filosofo Jacques Attali definisce «nomadismo virtuale».

Di conseguenza, oggi, le tecnologie dell'informazione non solo coinvolgono emotivamente in quello che accade dall'altra parte del mondo, ma consentono anche di comunicare istantaneamente con chiunque abbia un *computer* e un *modem*, annullando di fatto la distanza fisica. Cambia, perciò, l'esperienza che si ha del mondo, viene confinata nel presente assoluto e nella molteplicità delle sue potenzialità spaziali: si vive, come afferma Jameson ², in una dimen-

¹ M. McLuhan, *Gli strumenti del comunicare*, tr.it., Milano, Garzanti 1974.

² F. Jameson, Notes on globalization as philosophical issue, in *The Culture of Globalization*, a cura di F. Jameson e M. Miyoshi, Durham, Duke University press, 1998.

sione sincronica piuttosto che diacronica. È indubbio, comunque, che le comunicazioni di massa abbiano prodotto effetti sociali positivi di notevole portata, primo fra tutti l'accelerazione dei processi di diffusione culturale³. Ma come avviene in tutti i fenomeni, sono diventate anche strumento del «mercato della violenza», violenza intesa come violazione delle norme sociali.

A noi, quindi, in quanto studiosi di criminologia, spetta il compito di rilevare l'altra faccia della medaglia: l'abuso deviante e criminale dei mezzi informatici e telematici. L'introduzione delle tecnologie dell'informazione nel mondo criminale, anche se relativamente recente, ha avuto un'immediata propagazione a tutti i livelli, dal singolo alle organizzazioni più sofisticate. Ciò ha posto non pochi problemi dal punto di vista sia criminologico sia giuridico.

Una prima questione riguarda la definizione stessa di *computer crime* e di *computer criminal*, data la varietà dei fenomeni interessati. La nozione di criminalità informatica è, tuttora, alquanto ambigua e le difficoltà di interpretazione hanno una ricaduta sulle norme giuridiche che necessitano di costanti adattamenti. Per non parlare, poi, della personalità del criminale informatico: come interpretarne i comportamenti e spiegarne le motivazioni dal momento che si spazia dall'*hacker* al pedofilo, al cyberdipendente?. È praticamente impossibile, o perlomeno molto difficile, utilizzare le conoscenze classiche della criminologia in questo settore. Peraltro, in molti casi, non è né un marginale né un disadattato, ma un soggetto ben integrato nell'ambiente sociale e professionale.

Un'ulteriore difficoltà di analisi è dovuta, inoltre, al «numero oscuro». La criminalità informatica è in gran parte dissimulata; spesso non vi è un'interazione diretta tra autore e vittima; quest'ultima è non di rado la collettività; la dimensione spazio-temporale è dilatata o non identificabile. Questi e altri motivi ne riducono la individuazione e, di conseguenza, la misurazione in termini statistici.

Last, but not least, si pone il fondamentale problema della sicurezza che coinvolge tutti: dal padre di famiglia che deve proteggere i figli dal rischio pedofilia, al cittadino che utilizza tessere bancomat e carte di credito, all'azienda che deve prevenire azioni fraudolente sempre più «creative» di *insider* e *outsider*, agli Stati che devono di-

³ O. N. Larsen, Social effects of mass communication, in *Handbook of Modern Sociology*, a cura di R. E. L. Faris, Chicago, Rand McNally, 1964, pp. 348-381.

fendersi da organizzazioni criminali di tipo mafioso e terroristico. Di nuovo, la complessità del fenomeno implica la necessità di individuare misure di protezione e di sicurezza adeguate.

Il volume *Tecnologie dell'informazione e comportamenti devianti* vuole affrontare, se non tutte, alcune delle problematiche fin qui evidenziate. Lo scopo è quello di offrire uno strumento conoscitivo sulle possibili minacce ai sistemi informatici e telematici, sui metodi di attuazione, sui diversi tipi di criminalità informatica, nonché sulle misure di sicurezza e sulle metodologie investigative. Nei limiti della obiettiva difficoltà dei temi trattati, si è cercato di esporli nella forma più semplice possibile in considerazione del fatto che è destinato a studenti di diversi corsi di laurea e, quindi, con differenti *background* culturali.

La raccolta comprende i saggi di autori con formazioni molto diversificate che hanno, però, come comune denominatore il fatto di essere esperti, ognuno per il proprio settore, nel campo della criminalità e devianza informatica.

Il percorso inizia con il lavoro di Isabella Corradini, psicologa del lavoro, e Chiara Di Fede, sociologa, dal titolo *La criminalità informatica: un'analisi socio-criminologica*. Le autrici rivolgono l'attenzione al fenomeno ponendo in risalto come la cultura tecnologica, oltre a modificare le relazioni comunicative, abbia prodotto nuove sfide per la criminologia.

Paolo Galdieri, avvocato e docente di Diritto penale dell'informatica presso l'Università di Roma «La Sapienza», nel capitolo su *Il reato informatico affronta diffusamente le problematiche giuridiche connesse*. Come si vedrà, per quanto riguarda il nostro Ordinamento, non esiste un *corpus* unico di norme ma, data la varietà, i reati perpetrati con il mezzo tecnologico sono previsti in diversi articoli del codice penale e di altre leggi. Merito dell'autore è stato quello di riuscire, in poco spazio, a dare un quadro chiaro ed esaustivo della normativa.

Il Crimine informatico in azienda, trattato dalla Corradini, offre un'ampia panoramica delle tipologie, del *modus operandi*, degli autori e delle reazioni in relazione al fenomeno nello specifico mondo aziendale. Anche in questo caso l'esiguità dello spazio non ha pregiudicato la completezza dell'esposizione.

Collegato al precedente si colloca il tema *La sicurezza dei sistemi informatici aziendali*, sviluppato da Gianluigi Me, capitano dell'Arma

dei Carabinieri, nonché ingegnere informatico docente presso l'Università di Roma «Tor Vergata». L'analisi, ricca di figure esplicative, verte sugli attacchi informatici e sulle misure di sicurezza atte a contrastarli, senza trascurarne il problema dell'amministrazione in quanto al costo, alla pianificazione e ai rischi. L'osticità dell'argomento è resa chiara dalla penna dell'autore.

L'affascinante discorso su *L'Information Warfare* nel terzo millennio, ad opera di Roberto Di Pietro, capitano dell'Arma dei Carabinieri, ingegnere dell'Informatica e docente presso l'Università di Roma «La Sapienza», e del precitato Me, introduce in un settore del tutto nuovo per la nostra materia: la conduzione degli «affari» di guerra. Dimostra come la rivoluzione tecnologica stia mutando anche il modo di gestire la dimensione militare nel campo dell'*intelligence*, della guerra psicologica e della «guerra alle e delle informazioni» non solo durante i conflitti bellici.

Altro argomento di grande interesse è quello svolto da Antonio Picci, avvocato e criminologo, e da Paolo Galdieri su *Nuove tecnologie e terrorismo*. Come il precedente, anche il cyberterrorismo rappresenta un *humus* recente per gli studi di criminologia. I due autori lo affrontano dal punto di vista sia criminologico (tipologie, utilizzazione delle reti, ecc.) sia giuridico (normativa comunitaria, questioni di diritto processuale, ecc.), mettendone in risalto l'annoso dilemma della scelta tra maggiore sicurezza e minore libertà.

Hacker e Internet crime è il capitolo scritto dalle già menzionate Di Fede e Corradini. Dalla storia del fenomeno si passa alle tipologie di autori, per poi affrontare il collegamento con il terrorismo e la valutazione del rischio.

Il tema *La c. d. «pedofilia telematica»*, di Valentina Guiducci, laureata in Scienze della Comunicazione e collaboratore della cattedra di Criminologia della stessa Facoltà, viene sviluppato in tutti i vari aspetti con particolare attenzione ai siti e alle modalità di comportamento del pedofilo telematico.

Strettamente connesso al precedente si configura il capitolo *Brevi cenni sui metodi di investigazione nella pornografia minorile* di Giorgio Stefano Manzi, maggiore dell'Arma dei Carabinieri consulente della Commissione Bicamerale per l'Infanzia. L'autore mette in evidenza le difficoltà e la complessità delle indagini sulla pedo-pornografia in rete, anche alla luce della normativa internazionale. Va dato atto sia

al Manzi sia alla Guiducci di aver trattato un tema così delicato (in quanto coinvolge i bambini) non solo con professionalità e chiarezza espositiva (il che era scontato), ma soprattutto con particolare tatto.

Segue *Le investigazioni informatiche nel processo penale* dei predetti Me e Di Pietro, che ci accompagna nei meandri del mondo digitale connesso al processo penale. Così si affronta la problematica dell'analisi forense dei dispositivi digitali, i tipi di investigazione, l'utilizzo della prova digitale e le relative metodologie di analisi.

L'ultimo capitolo di Corradini e Galdieri è sulle *Tecnologie dell'informazione e psicopatologie: le nuove dipendenze e ripercussioni sull'accertamento della colpevolezza informatica*. Nella prima parte, di impostazione psicologica, si spiegano le varie forme di *net addiction* e le caratteristiche dei soggetti affetti da questa nuova psicopatologia; nella seconda si affronta la materia sul piano giuridico con particolare attenzione all'imputabilità del delinquente informatico e ai relativi motivi a delinquere.

In conclusione, l'intento dell'opera collettanea è quello di «navigare» nel complesso mondo della criminalità informatica, evidenziandone le problematiche criminologiche e giuridiche degli scenari più attuali. Tale intento si è potuto realizzare, come si è visto, solo grazie alla collaborazione di professionalità diverse. Gli studi in questo ambito, infatti, necessitano di un sincretismo tra varie discipline. Come affermano Morcellini e Fatelli⁴ riguardo alla comunicazione:

La difficoltà principale non consiste nell'«indeterminismo» concettuale o banalmente terminologico, e neppure nell'obiettiva difficoltà a tenere insieme una materia omogenea e coerente. L'oggetto non resta fondamentalmente misterioso per questa ragione; anzi, la sovrabbondanza di immagini in qualche modo rende retorica la domanda su che cosa sia la comunicazione: tutti sappiamo di che cosa più o meno si stia parlando e siamo pertanto in grado – mescolando un po' gli ingredienti – di trovare un'etichetta da appiccicare sulla scatola. Il problema risiede invece nella corretta individuazione della scatola e nell'esame del contenuto.

In altre parole, questo è il problema anche nostro. Tutti sanno che cosa sia la criminalità informatica (l'etichetta), ma poi risulta difficile

⁴ M. Morcellini, G. Fatelli, *Le scienze della comunicazione*, Roma, Carocci, 2002.

individuare le variegata sfaccettature, esaminarle, trovare le modalità per investigarle, prevenirle e contrastarle. Ciò è possibile attraverso il lavoro di équipe di esperti nei settori di interesse ed è quello che si è cercato di fare, se non completamente, perlomeno in parte.

* * *

Il lavoro collettaneo, qui presentato, va visto in collegamento con *Teorie criminologiche. Da Beccaria al post-moderno*, a firma di chi scrive, testo suggerito per il corso omonimo impartito presso le Facoltà di Scienze della Comunicazione e Giurisprudenza. Si aggiunge ad un'ulteriore opera, dal titolo *Temi di Criminologia*, a firma di altri autori. In sostanza le due «Lecture» sono connesse al manuale completandolo nei settori di specifica trattazione.

Si coglie l'occasione per affermare il concetto che la responsabilità dei singoli contributi appartiene ai relativi autori.

Come è ovvio, gli scambi di idee tra chi scrive e i diversi «contributori», come del resto tra di essi, sono stati continui e intensi così da dare una veste unitaria alle due «Lecture» e, al contempo, arricchire le reciproche conoscenze.

Mi è grato esprimere agli autori tutti di questo volume il mio più vivo apprezzamento per il loro impegno.

Roma, 30 luglio 2004

Gemma Marotta

1.

LA CRIMINALITÀ INFORMATICA: UN'ANALISI SOCIO-CRIMINOLOGICA

Isabella Corradini - Chiara Di Fedè

1.0. INTRODUZIONE *

Le tecnologie informatiche e telematiche costituiscono alcuni degli aspetti integranti della vita quotidiana, in tutte le sue espressioni, e non solo quelle professionali. Se, da un lato, l'informatizzazione dei processi e delle relazioni rappresenta una nuova modalità di interazione socio-economica, dall'altro si correla a nuove esigenze di *security*. Il reato informatico e le conseguenze derivanti ne testimoniano l'importanza. Per comprendere appieno l'entità del rischio derivante dai c. d. «crimini informatici» e per valutare l'esigenza di pianificare una strategia di *e-security* globale, è necessario proiettarsi in quello che gli addetti ai lavori definiscono come «il settimo continente»¹: un mondo virtuale e globale che si sovrappone a quello tradizionale e nel quale la percezione del Sé individuale e collettivo² assume significati inaspettati anche nella definizione di condotte devianti e criminali. La globalizzazione, letta attraverso i suoi elementi cultura-

* Paragrafo redatto da Chiara Di Fedè.

¹ Sul tema Cfr. A. Contaldo, T. M. Mazzatosta, *Il lavoro sul Settimo continente*, Roma, Edizioni SEAM, 1998.

² Sul tema Cfr., L. Arcuri, A. Maass, Le dimensioni sociali del sé, in L. Arcuri, *Manuale di Psicologia sociale*, Bologna, Il Mulino, 1995.

li, assume un carattere particolarmente incisivo e determinante, in termini di «svuotamento», sui significati dell'azione sociale e individuale rispetto ai sistemi esperti e astratti della scienza e della tecnologia ³.

1.1. ALLE ORIGINI DELLA RETE *

Scaturita dalla convergenza tra la tecnologia della telecomunicazione e la tecnologia dell'informazione, la *Rete Internet* si è evoluta in ambienti nei quali la ricerca concilia standard e metodologie nell'innovazione tecnologica: quello militare e quello universitario. La prima apparizione di questa forma d'interconnessione risale al 1969 ⁴, quando il Ministero della Difesa Statunitense, durante il periodo della guerra fredda, creò un'agenzia, ARPA (*Advanced Research Project Agency*), preposta allo sviluppo di una rete di fondamentale importanza strategica volta a garantire i collegamenti tra i reparti in caso di guerra globale, connettendo in modo sicuro gli elaboratori allora esistenti. Il progetto coinvolse centri di ricerca, università e qualche azienda privata, tutti in qualche modo legati all'attività militare e dotati di *computer* che all'epoca costituivano quanto di più moderno la tecnologia informatica americana potesse offrire.

Il primo appalto per la costruzione della rete fu concesso a una società chiamata *Bolt, Beranek and Newman* (BBN) che collegò quattro università diverse: *Stanford University*, *UCLA* (*University of California at Los Angeles*), *UCSB* (*University of California at Santa Barbara*) e la *University of Utah*, usando linee telefoniche e installò in ciascuna di queste un particolare *computer* che gestiva il traffico in rete (*Information Message Processor*). L'IMP fungeva da intermediario tra linee di connessione e mainframe. Il progetto, chiamato ARPANET, divenne attivo il 2 settembre 1969. Nel 1972 l'Università dello Utah realizzò un sistema per controllare un *computer* a distanza su ARPA-

³ Sul punto Cfr. R. Caccamo, A. Ferrara, *Globalizzazione e multiculturalismo*, in E. V. Trapanese (a cura di), *Sociologia e modernità*, Roma, NIS, 1997.

* Paragrafo redatto da Chiara Di Fede.

⁴ Sull'evoluzione di *Internet* Cfr G. Bettetini, F. Colombo, *Dall'alfabeto alle reti*, Roma, SEAM, 1996.

NET e divenne possibile trasferire *file* da un *computer* all'altro per mezzo del protocollo ftp (*File Transfer Protocol*). Nel 1980 ARPANET divenne uno strumento vitale per le università e per i centri di ricerca americani, che avevano un bisogno sempre maggiore di scambiare informazioni e di coordinare le proprie attività. Nacque così la posta elettronica che si affiancava al semplice trasferimento di *file*. Nel 1983 *Internet* divenne a tutti gli effetti la rete delle reti, utilizzando ARPANET come dorsale⁵. Nel 1991 il governo degli Stati Uniti ha emanato una legge, l'*High Performance Computing Act*, che decretava la nascita della *National Research and Education Network* (detta anche «autostrada elettronica») il cui scopo è quello di costituire reti ad alta velocità che uniscano le varie università e i vari centri di ricerca americani, fornendo anche l'infrastruttura per eventuali attività commerciali. Sempre quello stesso anno, il CERN (Consiglio Europeo per la Ricerca Nucleare) poneva le basi per una nuova architettura capace di semplificare enormemente la navigazione di *Internet*, la *World Wide Web*. Nel 1993 è stato inventato il primo strumento grafico per esplorare *Internet*, il programma *Mosaic*. A partire dal 1994 la *World Wide Web* ha trasformato *Internet* in uno strumento di *mass-communication*. A differenza delle quattro università che parteciparono alla versione originale di ARPANET, l'*Internet* moderna si compone di migliaia di singole reti, ciascuna che raccoglie a sua volta un numero più o meno grande di *host* (macchine individuali). Il termine non si riferisce ai singoli oggetti fisici al suo interno, bensì allo spazio complessivo che questo insieme di *computer* rappresenta e che può essere attraversato in lungo e in largo da chi cerca notizie, documenti, messaggi e *file* da scaricare. Si tratta di un mondo in continua trasformazione, con pezzi che si aggiungono e pezzi che scompaiono, ma nel suo insieme lo spazio *Internet* è sempre disponibile, a qualsiasi ora, e la sua esistenza non dipende dall'iniziativa di una singola azienda oppure di un singolo governo.

⁵ Rete ad alta velocità che unisce tra loro altre reti locali.

1.2. PROCESSO DIGITALE E INNOVAZIONE CRIMINALE *

Il prevalere della *technology culture* ha fatto emergere l'importanza degli elementi astratti del processo comunicativo, definendo un ruolo e una funzione del tutto nuova dell'interazione comunicativa ⁶: si assiste ad una riduzione dei rapporti empatici insiti nei rapporti *face to face* e allo sviluppo di flussi linguistici codificati secondo modelli lineari di tipo digitale.

Nel processo evolutivo, attraverso la tecnologia informatica, che coinvolge la società dell'informazione, si definiscono, inoltre, nuovi modelli di comportamento e di costruzione dell'identità. A tale proposito Baudrillard ⁷ afferma che:

la sfera privata cessa d'essere il palcoscenico dove noi esistiamo come attori poiché siamo divenuti i terminali di reti multiple.

Lo spazio pubblico dell'arena sociale tende a sintetizzarsi nello spazio privato del *Personal Computer*, nella quale gli individui assumono un ruolo di perfetta sovranità ormai infinitamente distanti dall'universo originario: l'identità è ora creata tramite strategie simboliche e credenze collettive che nascono, si sviluppano e muoiono nella Rete.

Il successo della Rete, nell'ultimo decennio, è dovuto a quattro elementi operativi fondamentali perfettamente interdipendenti ⁸:

1. L'applicazione di una gestione interattiva a contenuti organizzati e potenzialmente universali.
2. La costruzione di una memoria di contenuti immediatamente accessibile.
3. Una struttura di costi non dipendente dalla distanza (come il telefono), dalla quantità di informazioni messa a disposizione (come i libri stampati), dall'audience (come la radio o la televisione). Per questo i suoi costi di distribuzione sono inferiori agli altri media.
4. Una dimensione interattiva che ha determinato la nascita della

* Paragrafo redatto da Chiara Di Fedè.

⁶ G. Mazzoli, *Profili sociali della comunicazione e nuove tecnologie*, Milano, Franco Angeli, 1998.

⁷ J. Baudrillard, *The Ecstasy of Communication*, New York, University Press, 1987.

⁸ J. Jacobelli (a cura di), *Dall'analogico al digitale*, Bari, Laterza, 1996.

comunità virtuale.

Internet rappresenta non solo una Rete, ma un concetto molto articolato; nel riferirci ad esso dobbiamo prendere atto:

- dell'affermarsi sempre crescente di una nuova filosofia comunicativa: la *computer communication* ⁹;
- della diffusione reale di tale fenomeno;
- del diffondersi di un processo di socializzazione emergente che contribuisce alla definizione di un Io collettivo virtuale;
- degli effetti sociali della *web revolution* anche in termini di devianza e di criminalità.

Le innovazioni culturali e scientifiche dell'era post-industriale, indotte dalla «rivoluzione digitale», si sono imposte parallelamente all'incremento di una *new crime's way* particolarmente complessa, poiché sfrutta le possibilità d'anonimato che lo strumento informatico offre, favorita dalle oggettive difficoltà, a livello complessivo, di prevenzione e di contrasto. Questa rivoluzione digito-globale se da un lato ha determinato una maggiore efficienza del *working-network*, dall'altro ha aperto nuove problematiche relative al *technology risk assessment*.

Kling ritiene che una corretta valutazione dei livelli di sicurezza dei sistemi e della vulnerabilità sociale, impone di tener conto della ormai costante penetrazione del *computer* nel contesto quotidiano e il ruolo che esso ha assunto nei trasporti, nella difesa nazionale, nelle comunicazioni, nelle operazioni finanziarie e commerciali, nella nell'industria e nei servizi sociali ¹⁰.

La rapida evoluzione dei mezzi elettronici non ha, inoltre, determinato un simultaneo aggiornamento della cultura socio-istituzionale creando, di conseguenza, le condizioni per attacchi al sistema informativo, mediante la diffusione di *virus* ¹¹, la manipola-

⁹ Sul tema Cfr. A. Contaldo, T.M. Mazzatosta, *op. cit.*, p. 1.

¹⁰ R. Kling, *Computerization and Controversy, value conflicts and social choices*, in U. Rapetto, R. Di Nunzio, *Le nuove guerre*, Milano, BUR, 2001.

¹¹ I primi virus si diffondono tra il 1986 e il 1987, attraverso l'infezione di *floppy disk* usati come mezzo di scambio di informazioni in formato digitale. Il virus «Brain» impiega 5 anni per raggiungere l'apice dell'infezione. Negli anni '90, con l'avvento del *web*, il mondo dei virus si evolve in quantità e in qualità. Nel Marzo del '99 il virus «Melissa» (*macro-virus per Word'97*), infetta 150.000 sistemi in 4 giorni, provocando danni per circa 300 milioni di dollari; nel Maggio 2000 il virus «I Love You» (*virus per Outlook*) infetta 500.000 sistemi in meno di 24h, provocando danni

zione o il furto di dati e la manifestazione di un sommerso innovativo¹² a base tecnologica. Tale fenomeno è stato inserito nell'inglobante classe dei «Crimini ad Alta Tecnologia», definiti nella riunione dell'Ottobre 1999 dal comitato scientifico del G8¹³. I Crimini ad Alta tecnologia comprendono qualsiasi attività illegale compiuta con l'ausilio di sistemi elettronici avanzati come PC, cellulari, lettori magnetici; la manipolazione del flusso d'informazioni che viaggia nelle reti telematiche, può determinare una catena di crimini di difficile contrasto come frodi, rapine, furti, falsificazioni e minacce.

Attualmente, i crimini ad alta tecnologia, interessano prevalentemente:

1. *Computer Crime* (crimini informatici): raccolgono una vasta classe di crimini perpetrati per mezzo di *computer* e reti telematiche.
2. Cellulari: impiegati sia come oggetto della frode (clonazione/alterazione), che come mezzo di trasmissione a scopo criminale.
3. Carte di credito e *Smartcard*: clonazione e riutilizzo delle carte plastiche di pagamento.
4. *Video-game* illegali.
5. Clonazione di CD musicali e riproduzione illegale di *software* privo di licenza.

Gli esperti del settore hanno proposto diverse definizioni del crimine informatico, anche a causa dell'eterogeneità dei modi con cui può essere compiuto.

Secondo il Dipartimento di Giustizia degli Stati Uniti, si intende per reato informatico qualsiasi atto illegale nel quale la conoscenza della tecnologia informatica è utilizzata per commettere una infrazione.

Ceccacci afferma che:

per circa 10 miliardi di dollari; tra Luglio e Settembre 2001, i virus «*Red Code*», «*Red Code II*» e «*Nimda*» (apparso dopo l'11 Settembre) infettano 160.000 *host* in 7 ore; nel 2002 il virus «*Slammer*» infetta 75.000 *host* in 10 minuti e si moltiplica ogni 8,5 secondi.

¹² Sul punto Cfr. R. Bettini, *Sociologia del diritto positivo*, Milano, Franco Angeli, 1998.

¹³ M. Mattiucci, *Le investigazioni*, relazione presentata al Convegno «*Computer Crime*», Roma, biblioteca del CNEL, 27 Aprile 2000.

il crimine informatico rappresenta qualsiasi atto o fatto contrario alle norme penali, nel quale il *computer* è stato coinvolto come strumento, simbolo od oggetto del fatto ¹⁴

per Martella e Cremonesi il crimine informatico è

Un crimine nel quale un sistema di elaborazione, o una sua parte, ricopra uno dei seguenti ruoli: oggetto (distruzione o manipolazione dei dati e dei programmi contenuti nell'elaboratore o delle relative apparecchiature di supporto); soggetto, quando l'elaboratore è l'origine del crimine. In sostanza un sistema di elaborazione o un suo prodotto è utilizzato come mezzo per compiere frodi, falsificazioni ¹⁵.

Sul versante del diritto, la dottrina offre numerosi spunti classificatori. Sarzana ¹⁶, ad esempio, propone una suddivisione basata sullo scopo dell'azione criminosa:

- I crimini correlati all'uso del *computer* e aventi per scopo la realizzazione di un profitto per l'autore e la produzione di un danno per la vittima (appropriazione di dati e di informazioni dai *computer*, crimini finanziari).
- I crimini diretti contro il *computer* come entità fisica, aventi per scopo un danneggiamento parziale o totale del sistema; esempi ne sono il sabotaggio industriale e il vandalismo tramite l'immissione di programmi *virus*.
- I crimini correlati con l'uso del *computer* e diretti a provocare danni fisici a gruppi o persone.

Per Tiedemann ¹⁷, nel concetto di criminalità da *computer* devono essere considerati, poiché ben contraddistinti

tutti quei comportamenti anti-giuridici, o in ogni modo socialmente dannosi, che sono attuati utilizzando un elaboratore elettronico di dati.

Effettuando un'analisi in ottica sistemica e interazionista, il *computer*

¹⁴ G. Ceccacci, *Computer Crimes*, Milano, Fag, 1994.

¹⁵ G. Martella, C. Cremonesi, *I crimini informatici: storia, tecniche e difese*, Milano, Mondadori, 1994.

¹⁶ C. Sarzana, *Informatica e diritto penale*, Milano, Giuffrè Editore, 1994.

¹⁷ G. Ingrassia, *Comunicazione sociale: crimine e devianza nel post-moderno informatico*, Torino, Giappichelli editore, 1990, p. 451.

* Parte redatta da Isabella Corradini.

crime potrebbe comprendere tutti i casi in cui un mezzo telematico si interpone tra autore e vittima del reato rappresentando lo strumento principale di esecuzione dell'azione criminale e alterando la percezione della gravità del crimine stesso.

1.3. CRIMINOLOGIA E COMPUTER CRIME *

Qual è l'interesse della criminologia per il fenomeno del *computer crime*?

In senso lato, per *computer crime* s'intende il reato commesso con l'uso di un *computer*.

Il punto, però, deve essere approfondito. Occorre, in particolare, chiedersi se alcune attività realizzate con l'ausilio di mezzi elettronici siano attività lecite o illecite, etiche o no, e in quali casi sia possibile considerarle reati da perseguire.

È difficile stabilire un criterio distintivo tra giusto e ingiusto, anche perché un tale criterio può differenziarsi da individuo a individuo.

Tuttavia, il concetto di crimine è stato spiegato con maggior chiarezza da illustri criminologi, come Sutherland e Cressey che ne hanno fornito ampia analisi nel testo *Principi di Criminologia*.

Il comportamento criminale è una violazione della norma penale. Un atto, non importa quale sia il grado di immoralità, repressibilità o indecenza, non è un crimine a meno che esso sia proibito dalla legge, intesa convenzionalmente come un corpo di regole specifiche riguardanti la condotta umana, promulgate da autorità politiche che le applicano a tutti i membri della comunità in modo uniforme e che sono rinforzate dalla punizione amministrata dallo stato ¹⁸.

L'espansione della tecnologia informatica ha oggi aperto un solco sempre più profondo tra le attività illecite legate all'uso improprio del *computer* e la criminologia.

(segue)

¹⁸ E.H. Sutherland, D. Cressey, *Principles of Criminology*, Philadelphia, LIPPINCOTT Co., 1960 cit., in R. Goyal, M. Pawar, *Computer Crimes: Concept, Control and Prevention*, Sysman Computers, 1994.

4.

LA SICUREZZA DEI SISTEMI INFORMATICI AZIENDALI

Gianluigi Me

4.0. INTRODUZIONE

4.0.1. *L'importanza della sicurezza informatica*

I sistemi di produzione industriale hanno subito, negli ultimi trenta anni, drastici mutamenti, sotto la spinta di evoluzioni tecnologiche e organizzativo-gestionali. Le *Information e Communication Technology* (ICT) hanno giocato, infatti, un ruolo decisivo sia nel cambiamento dei sistemi di produzione, sia nell'integrazione dei processi intra-impresa e inter-impresa mediante, ad esempio, gli strumenti di lavoro collaborativi (*Groupware*), l'*Internet* e l'*E-business*. La creazione di nuovi modelli d'impresa, quali, ad esempio, «la flotta di piccole imbarcazioni» (rete di imprese) in luogo «della corazzata» (modello fordista/taylorista)¹, si basa sull'utilizzo delle ICT quale strumento imprescindibile per la creazione del valore. Appare chiara, perciò, la primaria e centrale importanza ricoperta dal sistema informatico all'interno delle imprese e, quindi, la necessità di proteggerlo nel modo più appropriato, che, in unione con la crescente complessità dei sistemi, ha portato alla creazione di una vera e propria disciplina riguardante la «sicurezza informatica».

Dal principio, infatti, quando i sistemi informatici erano usati

¹ P. F. Drucker, *The Emergency Theory of Manufacturing*, *Harvard Business Review*, vol. 68, n.3, 1990, 94-102.

da un utente alla volta e non erano collegati in rete, la sicurezza del calcolatore consisteva, in maggior parte, dalla sicurezza fisica, prevedendo, ad esempio, che i *computer* e le loro periferiche fossero chiusi a chiave in un'area sicura ad accesso controllato, tale da identificare l'utente prima dell'autorizzazione all'ingresso. La rapida evoluzione e obsolescenza delle tecnologie dei sistemi informatici ha aumentato la complessità del loro studio, specializzandolo in modo sempre più spinto, in modo da poter raggiungere metodologie e tecniche di protezione sempre più efficaci e, conseguentemente, più sofisticate. Si è passati, perciò, nell'arco di breve tempo, dalla esclusiva sicurezza fisica alla sicurezza olistica, intesa come protezione completa del patrimonio informativo aziendale attraverso una struttura di sicurezza generale e coerente con gli obiettivi, le regole e le priorità dell'azienda. Il breve percorso scientifico, ma di portata assai vasta, è stato racchiuso in una disciplina autoconsistente, la «sicurezza informatica».

Parallelamente al rapido progresso delle tecnologie e allo sviluppo della disciplina «sicurezza informatica», anche la disciplina del diritto ha dovuto affrontare nuovi percorsi di conoscenza e di ricerca, definendo nuovi reati in relazione ai nuovi scenari che progressivamente venivano a delinearsi. I crimini commessi con l'uso di tecnologie informatiche, tra cui gli attacchi ai sistemi informatici rappresentano, infatti, una nuova forma di crimine, denominata, in accezione generale, *e-crime*, cui la *National High Tech crime Unit* riconosce una duplice tipologia:

- *Nuovi crimini, nuovi strumenti*, commessi contro sistemi informatici e reti telematiche che presentino nuove opportunità per i criminali e nuove sfide per le Forze di Polizia;
- *Vecchi crimini, nuovi strumenti*, intendendo crimini tradizionali supportati dall'uso della Internet e dell'alta tecnologia, come frodi, estorsioni, pedofilia, furto d'identità.

Gli *e-crime* possono rappresentare una doppia preoccupazione per il mondo aziendale, considerata la vulnerabilità agli attacchi di duplice tipologia:

- *Centripeta*, con attacchi diretti dall'esterno verso l'interno;
- *Endogena*, con attacchi provenienti dall'interno dell'azienda, e diretti all'esterno o all'interno della stessa azienda.

Un quadro sintetico esplicativo dei danni economici causati dagli *e-*

crime è dato annualmente dal CERT (*Computer Emergency Response Team*), l'organo che svolge un ruolo di supervisione sull'attività in Rete. La situazione del 2003, ad esempio, rileva che, dal 1999 ad oggi, gli attacchi informatici sono diminuiti, pur se i valori rimangono ancora nella soglia di attenzione. Un dato ancora più allarmante è che ne sono vittime anche le grandi organizzazioni che hanno investito molto su tecnologie all'avanguardia nell'ambito della sicurezza. Ciò si palesa con rilevanti perdite economiche aziendali, riassunte in *Figura 1*, da cui si evince che le maggiori perdite sono legate alla sicurezza fisica dei dispositivi portatili, ad *e-crime* quali attacchi ad abbattimento del servizio, diffusione dei *virus* e furto di informazioni private. Nei prossimi capitoli saranno analizzate le diverse tecniche dell'attacco e le metodologie di difesa, focalizzandosi proprio su quelle che attualmente costituiscono le minacce più preoccupanti.

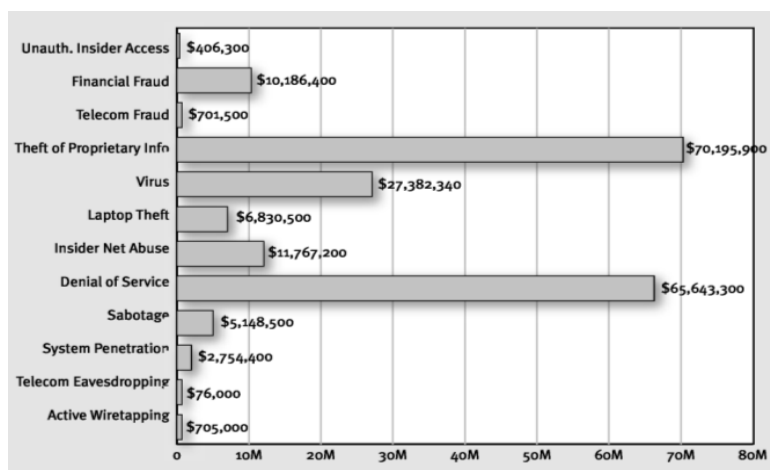


Figura 1: Ammontare in dollari delle perdite causate dalle diverse tipologie di attacchi informatici.

4.0.2. Definizioni di base

Un approccio sistematico alla sicurezza informatica, per quanto generale, come quello presentato in questo capitolo, non può prescindere da una esatta definizione dei termini, quali vulnerabilità, mi-

naccia e controllo, che verranno più frequentemente trattati nei prossimi paragrafi.

La vulnerabilità è una debolezza del sistema di sicurezza (ad esempio, i pneumatici di una automobile). Nella programmazione del *software*, una porzione di codice sorgente scritta in maniera corretta nella soddisfazione dei requisiti funzionali, ma scorretta, rispetto all'uso delle risorse del sistema, può generare malfunzionamenti.

La minaccia ad un sistema è un insieme di circostanze che può causare danneggiamenti o perdite al sistema stesso (ad esempio, gli oggetti sparsi sul fondo stradale, le imperfezioni del manto rappresentano la minaccia per il regolare proseguimento). Il controllo è una misura protettiva, ovvero un'azione, un dispositivo, una procedura o una tecnica che rimuove o riduce la vulnerabilità. La minaccia è bloccata dal controllo della vulnerabilità.

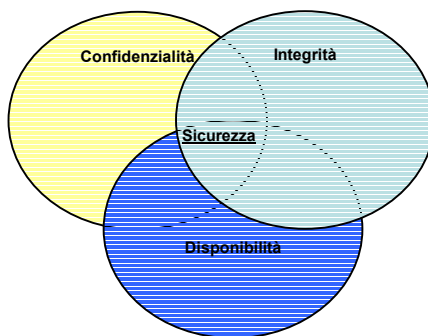


Figura 2: La sicurezza informatica secondo la definizione ISO.

Con il termine *sistema informatico* si intende l'insieme di risorse computazionali (ad esempio *computer*), di comunicazione (ad esempio reti locali) e di informazioni trattate dai precedenti due insiemi di risorse. Con il termine *sicurezza informatica*, secondo la definizione dell'International Standard Organization, si intende l'insieme delle misure atte a garantire, ad un sistema informatico, le seguenti proprietà delle informazioni (Figura 2):

- *Confidenzialità*: il patrimonio informativo (*asset*) deve essere acceduto solamente da soggetti autorizzati. Perciò, solamente coloro

in possesso di adeguata autorizzazione possono leggere, stampare, copiare o essere a conoscenza dell'esistenza di una determinata risorsa;

- *Integrità*: L'asset informatico può essere modificato solo se autorizzati (persone, applicazioni). Tale autorizzazione individua anche un livello di accesso alle risorse al quale sono associate un insieme definito di operazioni permesse: ad esempio, un utente potrebbe accedere in lettura ad un *file*, ma non in scrittura;
- *Disponibilità*: L'asset deve essere acceduto dalle persone autorizzate nei tempi prestabiliti. Ad esempio, una persona o applicazione, che detenga un'autorizzazione valida per qualche risorsa, non deve averne l'accesso negato. La disponibilità è la caratteristica da preservare negli attacchi di abbattimento del servizio (*Denial of Service*, DoS).

Una ulteriore definizione, meno formale, ma più pratica, della sicurezza informatica, dovuta a Garfinkel S. L. et al.² è:

Un *computer* è sicuro se ne si ha il controllo e il *software* si comporta come ci si aspetta.

Questo concetto è spesso chiamato «fiducia»: si ha fiducia nel sistema che conserva e protegge i dati. La valenza di questa definizione risiede nel concetto esplicito di protezione dai disastri naturali e dai programmi con malfunzionamenti che possano minare la sicurezza dell'intero patrimonio informativo.

Nei successivi paragrafi verranno delineate le linee generali della sicurezza informatica in azienda, tenendo sempre in mente i due interrogativi alla base di un generico progetto di difesa:

- Quali risorse sto cercando di proteggere?
- Da cosa bisogna difendere il sistema informatico?

4.0.3. Fondamenti di crittografia

L'esigenza di modifica volontaria del testo per occultarlo a «sguardi indiscreti» risale ad alcuni secoli a. C., a testimonianza dell'esigenza,

² S. L. Garfinkel, et al., *Practical Unix and Internet security*, seconda edizione, O'Reilly, 1996.

da sempre, dell'uomo di proteggere la propria riservatezza. Racconta Svetonio, nella *Vita dei dodici Cesari*, che Giulio Cesare proteggeva la propria corrispondenza personale con i Druidi utilizzando un codice di sostituzione molto semplice, nel quale ogni lettera del messaggio originale veniva sostituita dalla lettera che la seguiva di tre posti nell'alfabeto (ad esempio la lettera C dalla F, e così via, fino a sostituire le ultime tre lettere dell'alfabeto con le prime).

Il codice di Cesare rappresenta esattamente il primo esempio noto di crittografia.

In una definizione più formale, la crittografia è la scienza che si occupa di fornire:

- *Confidenzialità* (segretezza), con obiettivo di proteggere le informazioni rendendole incomprensibili a chiunque diverso dal legittimo destinatario (ad esempio, un intercettatore);
- *Autenticazione*, con obiettivo di accertare la reale origine di un messaggio, evitando che un intrusore si mascheri, ad esempio, da utente autorizzato;
- *Integrità*, con obiettivo di consentire al destinatario di un messaggio di verificare che non sia stato modificato durante il tragitto. Un intrusore non deve essere in grado di sostituire un messaggio vero con uno falso;
- *Non ripudio*, con obiettivo di impedire al mittente di negare di aver inviato un messaggio.

La *crittoanalisi* è, invece, la scienza che si occupa della lettura delle informazioni crittografate attraverso la rottura dei sistemi cifranti.

Il messaggio da proteggere è detto *testo in chiaro*, mentre quello trasformato in modo da essere incomprensibile è detto *testo cifrato* (*crittogramma*); la trasformazione da testo in chiaro a testo cifrato si definisce *cifatura*, mentre la trasformazione inversa si definisce *decifatura*. La modalità di trasformazione crittografica è dettata da un *algoritmo di cifatura* che definisce puntualmente i passi per tradurre il testo in chiaro in quello cifrato. Affinché questa trasformazione possa essere finalizzata, occorre utilizzare un ulteriore elemento, una chiave k , indispensabile per personalizzare la confidenzialità. Nel caso del codice di Cesare, l'algoritmo è la sostituzione con lettere dell'alfabeto successive e la chiave (k) è 3. Due persone che volessero scambiarsi messaggi segreti potrebbero farlo mettendosi

d'accordo sulla chiave k e sostituire con le k successive lettere dell'alfabeto ogni lettera delle parole da scambiare, come previsto dall'algoritmo del codice di Cesare. Sapendo che due persone si scambiano messaggi con il codice di Cesare, un crittoanalista potrebbe risalire al testo in chiaro, una volta in possesso del crittogramma scambiato, provando tutti i possibili k (25, nel caso dell'alfabeto inglese).

In generale, nello studio della robustezza della crittografia si suppone che l'algoritmo sia noto a tutti, mentre la chiave sia la parte assolutamente segreta della comunicazione (*Principio di Kerckhoff*): un sistema crittografico basato sulla segretezza dell'algoritmo è, perciò, assolutamente inaffidabile.

Esistono 2 diversi schemi di crittografia:

1. Basato su *chiave segreta*, e denominata *crittografia simmetrica* (Figura 3), in cui cifratura e decifratura sono effettuate utilizzando la stessa chiave;

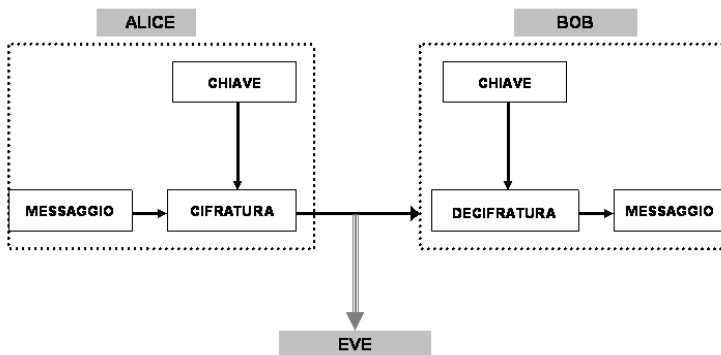


Figura 3: Crittografia simmetrica.

2. Basato su *chiave pubblica*, denominata *crittografia asimmetrica* (Figura 4), in cui è richiesto l'uso di due chiavi complementari. Una chiave, la chiave pubblica, usata per cifrare il messaggio, può essere liberamente distribuita a chiunque, mentre la seconda chiave, chiamata chiave privata, usata per decifrare il messaggio, deve essere conservata in maniera sicura (tipicamente su una *smart card*) e mai divulgata in alcun modo.

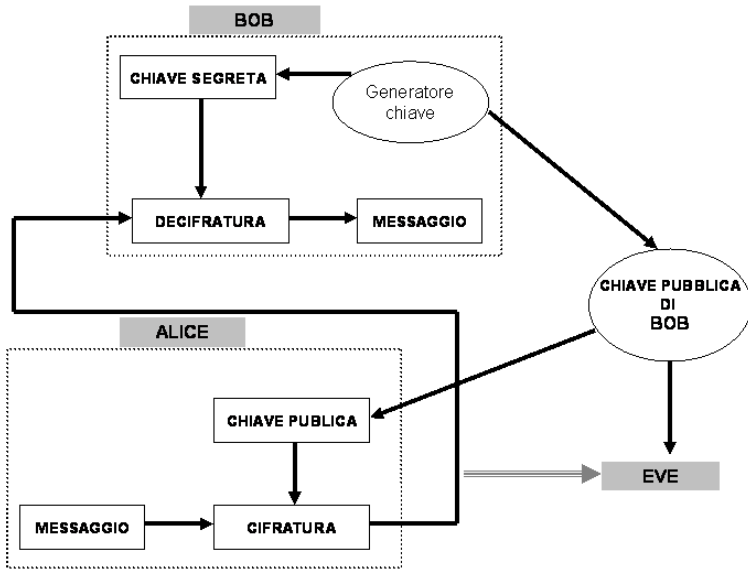


Figura 4: Crittografia asimmetrica..

Una funzionalità supplementare consentita dalla crittografia asimmetrica è la *firma digitale*: utilizzando le caratteristiche di integrità e non ripudio (esclusiva, quest'ultima, della crittografia asimmetrica) il mittente di un messaggio può firmarlo grazie alla sua chiave privata (che solo lui possiede) e tutti sono in grado di verificare l'autenticità della firma grazie alla chiave pubblica del mittente (che è, appunto, nota). Da quanto espresso finora, si potrebbe essere indotti a considerare che le funzionalità offerte dalla crittografia simmetrica siano un sottoinsieme di funzioni della crittografia asimmetrica, delegando perciò a quest'ultima una sorta di predominio della disciplina. Assolutamente falso, poiché la crittografia simmetrica, a dispetto di quella asimmetrica, ha il grande vantaggio di essere poco affamata di risorse computazionali. Una soluzione frequentemente adottata è, infatti, la cascata dei due schemi, proprio per esaltare i benefici di ognuno: viene utilizzata la crittografia asimmetrica per concordare una chiave segreta da utilizzare, poi, per scambiarsi i messaggi tramite un algoritmo simmetrico: in questo modo l'algo-

ritmo a chiave pubblica, divoratore di risorse computazionali, viene usato solo per trasmettere una piccola quantità di dati (la chiave segreta), mentre, per il restante scambio dei dati, viene usato un algoritmo a chiave segreta, più adatto ad uno scambio copioso di messaggi.

4.0.4. I principi di sicurezza

Alcuni principi generali di sicurezza, di natura non tecnica, ma di carattere generale, con forti ripercussioni sulle responsabilità delle persone interne all'azienda, si sono evoluti nel tempo fino a diventare largamente accettati. Essi sono:

- *Minimo privilegio* (non solo in ambito informatico): è, forse, il principio fondamentale della sicurezza. Tale principio indica che ogni risorsa (informatica, umana) deve avere soltanto le autorizzazioni di cui ha bisogno per compiere il proprio lavoro. Niente di più.
- *Difesa in profondità* (non solo in ambito informatico): non bisogna fare affidamento soltanto su un meccanismo di sicurezza, anche se ritenuto estremamente valido e affidabile. L'adozione di molteplici sistemi di sicurezza in grado di coprire eventuali malfunzionamenti di altre contromisure evita la compromissione del sistema (ad esempio, nelle automobili, la serratura degli sportelli e il sistema di bloccaggio del motore senza chiavi nel quadro d'accensione).
- *Punto di transito di semplice controllo*: un punto d'accesso facilmente controllabile permette una bassa percentuale di errori e una loro immediata individuazione. Un esempio è costituito dalla linea dei *metal detector* in aeroporto, la coda per il controllo dei biglietti a teatro.
- *Anello debole*: la sicurezza, proprio per il secondo principio enunciato, è rappresentabile come una catena di contromisure tanto forte quanto l'anello più debole. Chiunque vorrà attaccare il sistema lo farà nella parte maggiormente vulnerabile, ovvero quella con la contromisura più debole.
- *Fallimento in regime di sicurezza*: quando una contromisura fallisce, lo deve fare in maniera «sicura». Ciò vuol dire che se un sistema di sicurezza ha un malfunzionamento non deve consentire l'ac-

cesso all'intruso, anche a costo di negarlo ai legittimi utenti. Istanze di questo principio sono:

- a) tutto ciò che non è espressamente consentito è vietato;
 - b) tutto ciò che non è espressamente vietato è consentito.
- *La partecipazione universale*: la maggior parte dei sistemi di sicurezza richiede la partecipazione universale (o, almeno, l'assenza di opposizione attiva) delle risorse umane coinvolte. Ad esempio, se qualcuno all'interno dell'azienda non è disciplinato nell'adozione delle misure previste dalla politica di sicurezza, allora un'attaccante potrebbe utilizzare il suo *computer* per poter arrivare, dall'interno, alla risorsa d'interesse per l'attacco.
 - *Diversità della difesa*: è strettamente collegata alla profondità della difesa, diversificandosi nell'organizzazione della sicurezza. Non occorrono diversi strati di sicurezza, ma differenti tipi di difesa. Ad esempio, aggiungendo un sistema d'allarme all'interno dell'autovettura, equipaggiata con i sistemi citati nell'esempio precedente, si aggiunge la diversità alla profondità della difesa;
 - *Semplicità*: è una strategia di sicurezza per due ragioni: la semplicità, che consente la più larga e veloce comprensione, rende chiaro cosa accade, rendendo più facile capire se si è sicuri. Inoltre, la complessità fornisce nicchie dove poter nascondere oggetti: è molto più facile rendere sicuro un monocale rispetto ad una villa a due piani con giardino!
 - *Security through obscurity*: è il principio di proteggere gli oggetti, nascondendoli. È un principio molto usato nella vita di tutti i giorni (nascondere le chiavi in un posto segreto, la borsa nel portabagagli dell'automobile), ma in informatica è soltanto una valida tattica di sicurezza: senza una reale protezione adottata, è assolutamente inefficace (è il caso, ad esempio, degli algoritmi di cifratura del GSM).

Questi principi generali sono alla base di principi tecnici per la costruzione di sistemi sicuri, codificati, ad esempio, per i sistemi operativi, da Saltzer J. et al. ³

³ J. Saltzer, et al., The Protection of Information in Computing System, *Proceedings of the IEEE*, v. 63 n. 9, 1975, p. 1278-1308.

4.1. LA SICUREZZA INFORMATICA IN AZIENDA

L'esigenza della sicurezza nasce dal fatto che possono accadere eventi indesiderati che determinano un degrado nelle caratteristiche di integrità, disponibilità e riservatezza del sistema informatico. Un evento indesiderato è costituito da qualsiasi accesso (a servizio o informazione) non previsto dalla politica di sicurezza, sia esso un attacco deliberato, sia un semplice evento accidentale. Analogamente alla funzione dei castelli nelle città medievali, le reti telematiche possono essere difese perimetralmente, dai *firewall*, dove le torri hanno l'equivalente negli *Intrusion Detection System*, capaci di intercettare nuove strategie di attacchi;

Controllare il perimetro, però, come insegna la storia di Troia, assediata per 10 anni e beffata da una astuzia di Ulisse, non è sufficiente. Occorre anche una difesa in profondità: il rischio di cavalli di troia, *virus* e *worm*, memori della fine disastrosa di Troia, non possono essere sottovalutati.

La lezione imparata nei secoli è, perciò, di non sottovalutare alcun aspetto della protezione, poiché la sicurezza dell'intero sistema informatico è data dalla parte più debole del sistema di sicurezza. Nonostante tutto ciò sia abbondantemente noto, la situazione reale non è così confortante. In viene illustrato, ad esempio, la diffusione degli attacchi inclusi nel report 2003 CSI/FBI FBI.

Per questo motivo, occorre partire da una seria analisi funzionale dell'organizzazione, delle esigenze, delle priorità, delle relazioni umane e del comportamento delle persone: il piano di sicurezza sarà tanto più efficace quanto più sarà basato su un processo ben definito e su un'approfondita formazione e coscienza condivisa da tutte le persone direttamente o indirettamente coinvolte. Tale processo, dal punto di vista aziendale, è, invece, spesso, sottovalutato, analogamente alle profezie di Laocoonte, e concepito come fonte di puri costi (o spese), a volte nemmeno inseriti nel budget, ignorando il conseguente rischio di gravi danni. Nei prossimi paragrafi saranno, quindi, illustrate le metodologie di attacco e di difesa in unione alle problematiche di gestione della sicurezza, al fine di comprendere, dal punto di vista aziendale, come suggerisce B. Schneier, il processo «sicurezza».

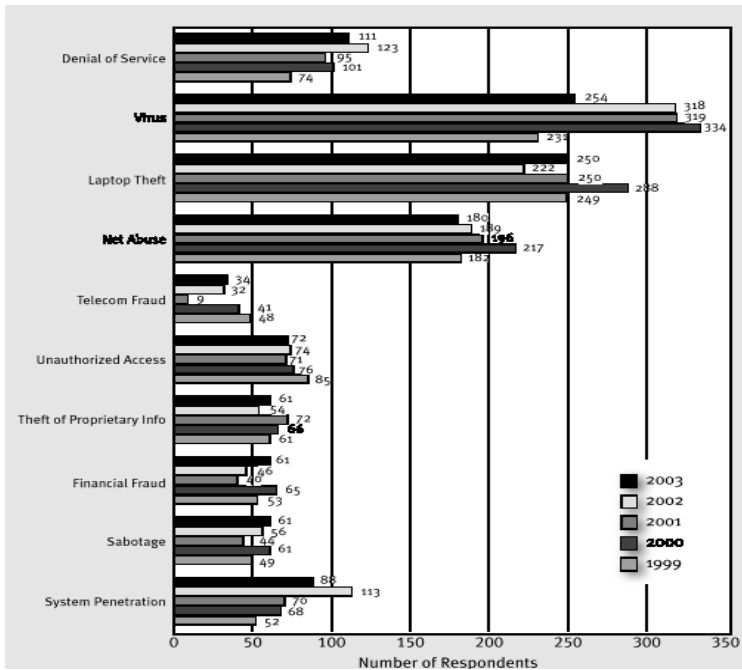


Figura 5

4.1.1. Gli attacchi

Un attacco informatico è, tecnicamente, una violazione della sicurezza informatica. Dalla definizione presentata nel paragrafo 4.0.2., una possibile definizione di attacco informatico è, perciò,

la violazione della confidenzialità, disponibilità e integrità di un sistema informatico.

Tra le molteplici tassonomie e classificazioni presenti in letteratura, verranno presentate, ai fini di una impostazione metodologica, J. D. Howard ⁴ e W. Stallings ⁵.

⁴ J. D. Howard, *An Analysis Of Security Incidents On The Internet 1989-1995*,

La prima classificazione è utile ad individuare le categorie degli attaccanti al fine di comprendere rapidamente, seppur in maniera approssimativa, quali fini e quali mezzi possono essere a disposizione, in funzione della risorsa informatica aziendale da proteggere, di colui che avanza la minaccia al sistema informatico. Howard divide gli attaccanti in sei categorie, come indicato in *Figura 6*.

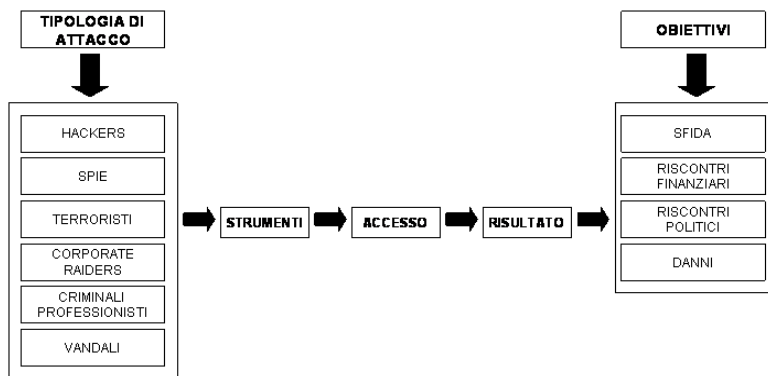


Figura 6

- *Hacker*: attacco a primario scopo dimostrativo e di sfida tecnica;
- *Spie*: attacco per furto di informazioni al fine di guadagnare potere politico;
- *Terroristi*: attacco per infondere paura utile all'acquisizione di potere politico;
- *Corporate raiders*: attacco portato dai dipendenti di una azienda ai danni di sistemi dei concorrenti, finalizzato al guadagno economico aziendale;
- *Criminali professionisti*: attacco per guadagno economico personale;
- *Vandali*: attacco al fine di causare danni;

In relazione alla tipologia di risorsa informatica da proteggere è possibile capire quali sono i possibili attaccanti interessati e quali sono i mezzi a disposizione per l'attacco: **(segue)**

<http://www.cert.org/research/JHThesis/Chapter6.html>, 1997.

⁵ W. Stallings, *Network and Internetwork Security Principles and Practice*, Englewood Cliffs, NJ., Prentice Hall, 1995.

11.

TECNOLOGIE DELL'INFORMAZIONE E PSICOPATOLOGIE.

Le nuove dipendenze e ripercussioni
sull'accertamento della colpevolezza informatica

Isabella Corradini - Paolo Galdieri

11.0. INTRODUZIONE *

Le tecnologie, in particolare quelle informatiche e telematiche, hanno determinato nuove modalità di relazione socio-economica, incidendo sullo stile di vita dell'uomo e sui processi di socializzazione e di comunicazione interindividuale.

Nell'attuale fase storica dell'IT (*Information Technology*), sembra che non si riesca più a vivere senza essere «bombardati» dalle informazioni.

Questa attività di pressione continua sui processi mentali dell'uomo produce effetti sorprendenti, poiché, nonostante l'efficienza garantita dai nuovi mezzi digitali, si pone il problema dell'adattamento cognitivo dell'essere umano, ancora lontano dall'essere completo, ed è facile pensare che ciò non avverrà facilmente data l'estrema rapidità con cui si evolvono le tecnologie.

In questi ultimi anni, stanno insorgendo nuove psicopatologie legate all'uso della tecnologia e allo sviluppo di nuovi modelli sociali.

* Paragrafo redatto da Isabella Corradini

11.1. TECNOLOGIA E COMUNICAZIONE *

Il rapporto tra comunicazione e tecnologia sta evidenziando alcune peculiarità su cui vale la pena di riflettere se si vuole comprendere lo sviluppo delle nuove psicopatologie correlate alla tecnologia.

Innanzitutto l'informazione. Il tempo intercorrente tra produzione e diffusione delle informazioni è sempre più ridotto, il che implica intervalli molto brevi nei processi di acquisizione e di assimilazione delle stesse. A ciò si correla il reperimento immediato delle informazioni di cui si ha bisogno: in ogni momento, collegandosi ad *Internet*, è possibile ottenere molte nozioni sulle tematiche di interesse.

D'altro canto, quando parliamo di tecnologia, non ci riferiamo solo a quella informatica, ma anche ad altri strumenti utilizzati nella comunicazione, come il cellulare, diventato ormai indispensabile sia per l'attività professionale che di relazione.

Quali ragioni sembrano privilegiare l'uso di tali tecnologie nei processi di comunicazione e di reperimento delle informazioni?

A parte l'efficienza e la disponibilità immediata, ci sono importanti fattori da considerare, legati alle caratteristiche stesse della tecnologia in uso, sia che si tratti di *computer*, sia che si tratti di telefono cellulare.

Riguardo alla tecnologia informatica e in particolare ai servizi dalla stessa offerti, come *Internet*, le caratteristiche principali consistono in:

1. *Ipertestualità*: un testo non è lineare e sequenziale, ma costituito da parti (ipertesti) alle quali si può accedere attraverso i collegamenti, i *link*.
2. *Annullamento dei limiti tempo-spazio*: attraverso speciali servizi offerti dalla Rete (IRC - *Internet Related Chat*, *e-mail*) è possibile comunicare con qualsiasi persona, in qualunque parte del mondo e soprattutto in qualsiasi momento.
2. *Identità virtuale*: è possibile comunicare con chiunque mantenendo l'anonimato, sperimentando identità diverse che possono essere create all'occorrenza, a seconda delle esigenze del momento.

Anche per la tecnologia cellulare, permangono le caratteristiche di

* Paragrafo redatto da Isabella Corradini

annullamento tempo-spazio e la possibilità di sperimentare (sia pure solo in parte) l'anonimato. L'interazione odierna della tecnologia informatica con quella cellulare sta implementando nuovi servizi di telecomunicazione tanto che è oggi possibile navigare su *Internet* attraverso il proprio telefonino. Vale a dire che i telefonini vanno sempre più assumendo le caratteristiche della tecnologia informatica.

In entrambi i casi, sotto il profilo psicologico, fa spicco la possibilità di evitare l'impatto emotivo che generalmente scaturisce dal relazionarsi con l'altro. Il che riveste particolare rilievo se teniamo conto della tipologia di comunicazione oggi preferita dal mondo giovanile (e non solo): si privilegiano i dialetti ipertecnologici fatti di simboli e di *emoticon* (faccine, sorrisi, rabbia, ammiccamento) per indicare i propri stati d'animo e le emozioni del momento. Si è anche ipotizzato che in questo modo si possa arrivare a compromettere nei ragazzi la capacità di interpretazione delle espressioni vocali e comportamentali di chi li circonda.

Ci troviamo di fronte a nuovi modelli sociali e comportamentali e i processi comunicativi sembrano orientarsi verso una trasmissione non più di gesti ed espressioni, ma di «segni».

Anche la comunicazione aziendale privilegia sempre più la tecnologia informatica per le sue attività di gestione esterna e interna: la Rete *Intranet* viene concepita quale mezzo informativo generale, per convocare riunioni, inviare aggiornamenti, pubblicizzare attività interne, per dare consigli al personale.

Se si confrontano i dati relativi alla vendita di *computer* e delle schede *sim*, ci si rende conto di quanto oggi le tecnologie informatiche e i cellulari abbiano acquisito un ruolo privilegiato quali strumenti di comunicazione, soprattutto se si tiene conto dei servizi che offrono all'utente. Acquistato un *Personal Computer*, si pone con immediatezza la necessità di avere un collegamento ad *Internet*, così come comprato un cellulare ci si informa sulla possibilità di sperimentarne tutti i servizi (sms, mms, fotocamera, ecc.).

Alcuni dati fanno emergere l'enorme diffusione dell'uso di tali tecnologie e dei servizi annessi ¹.

Secondo quanto indicato dall'Autorità per le garanzie nelle

¹ www.netdipendenza.it

comunicazioni, nell'anno 2003 le schede sim vendute sono state circa 54 milioni, e il 91% degli italiani possiede un cellulare.

Le stime di Telecom Italia Lab, riguardo l'uso degli sms, indicano uno smistamento di circa 23 miliardi di messaggi ogni anno.

Si tratta tuttavia di dati non quantificabili in modo definito, variabili di giorno in giorno.

Uno studio della Università Bocconi di Milano ha messo in evidenza che:

1. circa 3,3 milioni di Italiani navigano su *Internet* quotidianamente;
2. circa 1,7 milioni di italiani navigano dalle due alle tre volte durante la settimana.

L'utilizzo del servizio *e-mail* sta assumendo proporzioni vertiginose, sembra che ci si stia avviando verso primati da record: una ricerca del Sole 24 Ore ha indicato un flusso di *e-mail* annuale pari a 1 miliardo e 300 milioni nella sola Svezia.

Ed il popolo di *Internet* continua ad aumentare.

Tuttavia, l'eccessivo utilizzo della tecnologia ha anche fatto emergere dati inquietanti sugli effetti che ne possono derivare: i fenomeni di dipendenza ne sono un esempio.

11.2. *NET ADDICTION*: DEFINIZIONE E CARATTERISTICHE *

Quando si parla di dipendenza, generalmente si fa riferimento ad una sostanza chimica (come nel caso della tossicodipendenza), ma è anche possibile che sia la ripetizione di certi comportamenti a determinare una dipendenza; esempi comuni sono il gioco d'azzardo e il comportamento bulimico.

Le dipendenze che sembrano destare oggi un certo interesse sotto il profilo psicologico sono quelle «tecnologiche», le *net addiction*, che hanno per oggetto la tecnologia e che, in quanto di natura comportamentale, possono rientrare nella categoria delle *new addiction*, legate ai processi di trasformazione socio-economica e a nuovi modelli di relazione.

Secondo Mark Griffith ², esse costituiscono un sottoinsieme

* Paragrafo redatto da Isabella Corradini.

² Cfr. T. Cantelmi, M. Talli, C. Del Miglio, A. D'Andrea, *La Mente in Internet*,

di dipendenze comportamentali che vanno a condividere i componenti nucleari della dipendenza (dominanza di una certa attività, alterazione del tono dell'umore, tolleranza, astinenza, conflittualità, ricaduta nella condotta di dipendenza).

Più specificatamente l'Autore individua le dipendenze tecnologiche come forma di interazione uomo-macchina, sia in senso passivo (es. la televisione) che attivo (es. i videogiochi).

Generalmente, la caratteristica delle *new addiction* è che i soggetti sviluppano la dipendenza da ciò che fanno e da ciò che provano mentre lo fanno.

Il primo a parlare di dipendenza è stato Ivan Goldberg, psichiatra, creatore di un gruppo di supporto (*Internet Addiction Support Group*) che ha coniato nel 1995 il termine *Pathological Internet Use* (PIU).

Nonostante tale definizione, gli studi successivi non evidenziano un'omogeneità nell'utilizzo dei termini.

Oggi si parla di IAD (*Internet Addiction Disorder*), PIU (*Pathological Internet Use*), IRP (*Internet Related Psychopathology*) per indicare la varietà delle dipendenze che si sviluppano a seconda dei servizi utilizzati nella Rete e dei bisogni che questi soddisfano.

La maggior parte delle ricerche si sono sviluppate nel contesto americano, anche se in Italia ci si sta approntando a studiare il fenomeno con attenzione.

Si tratta di una patologia che non è stata ancora inserita nel DSM IV (Manuale Diagnostico e Statistico dei Disturbi Mentali) ma che sembra inquadarsi nell'ambito dei disturbi del controllo degli impulsi, come nel caso del gioco d'azzardo patologico.

Un interessante lavoro in proposito è quello condotto dalla psicologa americana Kimberly Young, che ha fondato il centro COLA (*Center for On-line Addiction*) per sensibilizzare alla problematica della dipendenza da *Internet* e fornire consigli sul tema.

La Young³ ha indicato i principali segni clinici per la diagnosi di dipendenza da *Internet*:

1. essere mentalmente assorbito da *Internet*;
2. avvertire il bisogno di utilizzare *Internet* sempre più a lungo per sentirsi soddisfatto;

Padova, Piccin, 2000.

³ K. Young, *Center for on-line addiction*. www.netaddiction.com.

3. essere incapace di controllare il proprio utilizzo della rete;
4. sentirsi inquieto o irritabile mentre si tenta di ridurre o interrompere l'utilizzo di *Internet*;
5. utilizzare *Internet* come mezzo per fuggire dai problemi o alleviare il senso di abbandono, impotenza, ansia, depressione;
6. mentire ai familiari o agli amici per nascondere il proprio grado di interesse per la rete;
7. avere messo a repentaglio o aver rischiato di perdere una relazione significativa, il lavoro o opportunità di studio o di lavoro a causa di *Internet*;
8. tornare in rete anche dopo aver speso grandi somme di denaro per i collegamenti;
9. ritiro sociale quando si è *off-line* (non collegati): in questi casi si denota nei soggetti dipendenti un aumento degli stati ansioso-depressivi;
10. rimanere collegati più a lungo di quanto si era programmato all'inizio.

Analizzando i criteri diagnostici indicati dalla Young, è evidente come una *net addiction* possa coinvolgere l'individuo nella sua complessità, in particolare negli ambiti di natura fisica, relazionale, professionale, economica.

Secondo l'autrice, è importante tener conto di alcuni fattori nella predisposizione alla dipendenza da *Internet*. In particolare l'*accessibility*, il *control* e l'*excitement* (Modello ACE) ne costituirebbero i principali elementi.

L'*accessibility* (accessibilità) quale requisito fondamentali della Rete, permette di esplorare e navigare in siti di non facile portata (es. siti del gioco d'azzardo) e con estrema rapidità.

Il controllo (*control*) favorisce la possibilità per l'utente di consultare facilmente attività personali gestite *on-line* (es. la contrattazione di titoli).

L'*excitement* (eccitazione) rappresenta l'elemento di «attrazione» per chi utilizza *Internet*, percepito quale strumento affascinante e misterioso per le opportunità che favorisce, come quella di assumere identità e ruoli diversi a seconda delle situazioni.

Naturalmente non tutti coloro che utilizzano in modo intenso la tecnologia informatica e la Rete sviluppano la dipendenza, ma è indubbio che i tre elementi indicati dalla Young, inducano l'indivi-

duo a privilegiare sempre di più l'utilizzo di tale mezzi per svolgere gran parte delle proprie attività.

11.3. IL PERCORSO DELLA NET ADDICTION*

È possibile ipotizzare un «percorso virtuale» attraverso il quale si sviluppa la dipendenza da *Internet*: il soggetto sperimenta un bisogno sempre più intenso di collegarsi alla Rete e l'incapacità di esercitarne il controllo, non riuscendo ad interrompere i prolungati collegamenti in *Internet*. Sono state evidenziate due fasi nello sviluppo della dipendenza tecnologica⁴: tossicofilica e tossicomantica, caratterizzate da:

FASE TOSSICOFILICA	<ol style="list-style-type: none"> 1. attenzione ossessiva per la <i>mail box</i>; 2. atteggiamento esplorativo della Rete (<i>lurker-guardoni</i>); 3. focalizzazione su tutto ciò che riguarda la Rete; 4. incremento del tempo trascorso in Rete (anche notturno); 5. primi sintomi di malessere <i>off-line</i> (quando non si è collegati); 6. tipologia di servizi utilizzati: <i>chat room</i> e gruppi di discussione;
FASE TOSSICOMANICA	<ol style="list-style-type: none"> 7. collegamenti intensi e incontrollati; 8. distorsione del tempo (<i>Terminal Time Wharp</i>); 9. alterazione dei ritmi di vita del soggetto sotto il profilo professionale, relazionale, sociale; 10. tipologie di servizi utilizzati: <i>chat</i> e <i>MUDs</i> (giochi di ruolo).

* Paragrafo redatto da Isabella Corradini.

⁴ Cfr. T. Cantelmi, M. Talli, C. Del Miglio, A. D'Andrea, *op. cit.*

L'utilizzo patologico della Rete può arrivare a compromettere la vita del *net slave* sotto il profilo relazionale, sociale e professionale: la focalizzazione su tutto ciò che riguarda la Rete, comporta una scarsa (se non assente) concentrazione nel proprio lavoro e in ambito relazionale. Non di rado sono messi in discussione rapporti di lunga data per sperimentare le «novità» offerte dal virtuale.

Nella fase tossicomantica, vero e proprio sviluppo della dipendenza, si assiste ad una preferenza per alcune attività, come le MUD, i giochi di ruolo ove è possibile sperimentare identità fittizie creando personaggi di natura fantastica nei quali potersi identificare, o il *cybersex*, nel quale si interagisce «eroticamente» attraverso i servizi di *e-mail* o le *chat-room*.

In una delle prime ricerche sul tema, analizzando le risposte dei partecipanti ad un questionario elaborato appositamente, la Young⁵ ha individuato tre fasi distinte attraverso le quali gli utenti di *Internet* sviluppano la dipendenza:

1. *Coinvolgimento*: la possibilità di sperimentare la tecnologia e i servizi della Rete stimolano la curiosità a utilizzare con un certo interesse ciò che viene offerto (*chat room, newsgroup*).
2. *Sostituzione*: alla curiosità segue l'interesse e la crescente fiducia per chi, nella *chat room*, mostra attenzione ai problemi esposti, sempre pronto a fornire in qualsiasi momento un sostegno morale e parole di comprensione. Le persone e gli amici con i quali si condivideva la quotidianità cominciano a perdere di importanza, ci si allontana da loro per conoscere i nuovi amici in Rete.
3. *Fuga*: in questa fase la sostituzione delle conoscenze virtuali a quelle reali diventa quasi completa; i collegamenti sempre più lunghi producono una eccitazione emotiva, i problemi e la solitudine sembrano allontanarsi grazie alla costante presenza di persone in Rete cui ci si può rivolgere in qualsiasi momento, anche di notte, con un semplice *click*.

Ma quando il *computer* viene spento, si ritorna alla realtà e ai problemi di tutti i giorni.

⁵ K. Young, *Presi nella Rete*, Milano/Bologna/Roma, Calderini edagricole, 2000.

11.4. PROFILI E SOGGETTI NELLA *NET ADDICTION**

Non è ancora possibile tracciare un profilo del *net slave* (schiavo della Rete): il solo tempo trascorso in Rete (il limite critico per lo sviluppo della dipendenza sembra essere individuabile tra le 5/6 ore giornaliere) non può di per sé causare dipendenza, altrimenti non si spiegherebbe perché mai soggetti che passano tanto tempo collegati non arrivino a sviluppare una patologia da *Internet*.

È invece plausibile ritenere che la variabile «tempo» sia da correlarsi ad altre variabili, *in primis* le caratteristiche di personalità dei soggetti.

Le ricerche finora effettuate sembrano evidenziare problematiche di fondo in coloro che sviluppano una patologia da Rete: difficoltà relazionali, disagi psicologici, tratti ossessivo-compulsivi, sono le caratteristiche maggiormente riscontrate in questa tipologia di soggetti. Sembra che gli uomini rispetto alle donne utilizzino con maggior frequenza i servizi della Rete, anche se le motivazioni di fondo sono di diversa natura: gli uomini, nella ricerca di affermazione e di potere, sono maggiormente orientati all'utilizzo di *chat* con connotazioni sessuali esplicite, giochi di ruolo e ricerca di informazioni. Le donne invece, ricorrono alle *chat* per avere un sostegno ai problemi che vivono in famiglia, o sono alla ricerca del partner «ideale».

È possibile indicare due tipologie di *retomani*: coloro nei quali è presente a priori una psicopatologia e coloro che non presentano alcun disagio preesistente.

Evidentemente ci sono persone maggiormente esposte al rischio di sviluppare la dipendenza, esprimendo in tal modo il proprio disagio: *Internet* può rappresentare la fuga, l'evasione dai problemi. Individui che magari vivono situazioni difficili in famiglia o sul lavoro, adolescenti che si sentono non compresi: problemi quotidiani che in una personalità emotivamente fragile, caratterizzata da scarsa autostima e insicurezza, trovano terreno fertile. Così chi vive un disagio di natura relazionale, può trovare in *Internet* il modo per superarlo: assumendo un'altra identità, può descriversi al meglio, apparire divertente, affascinante, e in quel momento, «accettarsi»

* Paragrafo redatto da Isabella Corradini.

completamente. Ma prima o poi, con il ritorno alla vita reale, riergono nella loro concretezza. L'immagine creata virtualmente si riaffercherà solo nel momento in cui ci si collegherà di nuovo alla Rete.

Sembra dunque che soggetti più a rischio di sviluppare una dipendenza da *Internet* soffrano di difficoltà relazionali e comunicative e presentino frequentemente problemi psicologici e psichiatrici ⁶.

Attraverso *Internet* si dà sfogo alle proprie ansie e frustrazioni, si ascoltano i pareri più diversi e soprattutto si ha la possibilità di esprimere concetti e opinioni che magari nella realtà non si ha il coraggio di manifestare: se qualcuno in collegamento non approva la conversazione, v'è sicuramente qualcun altro pronto a condividerla.

Sembra anche che *Internet* rappresenti per molti adolescenti uno strumento per combattere il disagio culturale dei nostri tempi, l'incapacità e la difficoltà di comunicare all'interno della famiglia.

Diventa prioritaria l'interpretazione del cyberspazio, da intendersi come un complemento della realtà, e non il luogo dove vivere completamente le proprie emozioni.

Se tale spazio diventa il centro dell'interesse dell'individuo, le esigenze relazionali soddisfatte dalla Rete finiscono per non trovare corrispondenza nella realtà; in tal caso, fenomeni di dissociazione e assunzione di identità virtuali possono compromettere l'equilibrio emotivo dell'individuo.

Uno dei problemi che emerge nella *net addiction* è quello della «dissociazione», quando non si riesce ad integrare la vita reale con quella virtuale: quest'ultima diventa infatti dominante nel soggetto dipendente, provocando il fallimento dell'esame di realtà.

La dissociazione induce il soggetto dipendente a considerare il cyberspazio l'unica realtà di vita. **(segue)**

⁶ N. A. Shapira., T. D. Goldsmith., P. E. Keck., et al, Psychiatric features of individuals with problematic Internet use, in *Journal Affective Disorders*, 2000.