I *computer crimes* definizioni ed elementi principali

Giovanni Felluga

Abstract

La rivoluzione e l'"alfabetizzazione" tecnologica hanno permesso la nascita di nuove condotte criminose che sfruttano l'utilizzo degli strumenti e dei sistemi informatici. Nel seguente articolo cercheremo di fare chiarezza sul problema definitorio dei reati informatici nonché sugli elementi principali che li caratterizzano e sulle diverse tipologie di condotte illecite con le quali essi si manifestano.

parole chiave

Computer crimes;
Reati informatici;
Evoluzione tecnologica;
Società dell'informazione;
Definizioni; Oggetto materiale;
Soggetti attivi; Condotte illecite.

Sommario

1. La società dell'informazione; 2. Gli effetti dell'"informatizzazione"; 3. Computer crimes, *una definizione ambigua; 4. Gli elementi principali del reato informatico; 4.1 L'oggetto materiale; 4.2 Il soggetto attivo; 5. Le condotte illecite; 5.1 Le condotte intrusive; 5.2 Le condotte manipolative; 5.3 Le condotte turbative e impeditive; 5.4 Le condotte distruttive.*

1. La società dell'informazione

Nel 1975 Herbert Simon, uno dei fondatori della scienza moderna, nel suo discorso per il conferimento del *Turing Award*, definisce il computer "*a physical simbol sistem*" ossia una macchina fisica capace di produrre, modificare e combinare tra loro dei simboli; di espletare dunque processi logici come fa la mente dell'uomo.

Questa definizione segna una tappa importante per l'evoluzione del computer e per la sua diffusione, poiché segna il suo passaggio dall'essere una semplice macchina calcolatrice all'essere un elaboratore idoneo ad acquistare esperienza per modificare le sue operazioni.

Alla stregua di quanto avvenne con l'invenzione dell'alfabeto o della stampa, la nascita del computer, inteso quale apparecchio elettronico in grado di svolgere operazioni matematiche e logiche e di memorizzare informazioni, assume la portata di una rivoluzione copernicana obbligando l'uomo ad adattarsi a un nuovo linguaggio, quello elettronico-artificiale parlato attraverso le macchine.

Come ben chiarisce il "padre dell'informatica giuridica italiana", Vittorio Frosini; il tratto fisionomico più caratterizzante dell'età in cui viviamo oggi, dell'età tecnologica, e quello che meglio di ogni altro ci permette di individuarla nella sua novità, è rappresentato dall'avvento dei calcolatori elettronici e dalla loro pervasiva diffusione. "Come la rivoluzione industriale moltiplicò l'energia fisica dell'uomo e ne diminuì la fatica, abituando l'uomo a convivere con le macchine [...] così la rivoluzione informatica allarga e potenzia le capacità della mente umana, obbligando la nostra intelligenza ad avvalersi di una protesi intellettuale"[1] e arricchendo la nostra percezione mentale con nuovi contenuti, prima neppure immaginabili.

1 V. Frosini, *Il diritto nella società tecnologica*, Milano, 1981, pp. 205 ss.

Le nuove tecnologie hanno favorito e accelerato il passaggio da un modo diretto e analogico di gestire i fatti, gli oggetti e i processi, a un modo discontinuo e indiretto, mediato dalla logica che governa i nuovi strumenti, dalla logica digitale.

Le reti informatiche interattive si sviluppano in maniera esponenziale creando nuove forme e canali di comunicazione nonché infinite connessioni tra campi diversi; la caratteristica comune delle nuove tecnologie risiede infatti nella loro divulgazione pervasiva ossia nella capacità di penetrazione in tutti i campi dell'attività umana.

Ecco allora che i computer entrano nelle case irrompendo nelle abitudini dell'uomo come beni di primaria necessità. Una connessione a internet poi continua il processo rivoluzionario iniziato con i mezzi tecnologici e consente all'uomo di esprimere, sfogare quella sua atavica esigenza di comunicare, conoscere, informarsi, quindi collegarsi col mondo.

Sorge così una società interconnessa in reti relazionali che risulta dinamica, interdipendente e globalizzata; una società trasformata nei modelli comportamentali, nei pensieri e nel modo di comunicarli; una società dissuasa e plasmata dalle nuove tecnologie; una società, per dirla con Virilio, "dove tutto arriva senza che sia necessario partire".

> Pare quindi che a mano a mano che le tecnologie informatiche si diffondono nel tessuto sociale, i modelli di lavoro, la vita familiare, gli svaghi, il tempo libero e perfino il modo in cui percepiamo noi stessi in quanto esseri umani, siano tutti destinati a subire importanti trasformazioni. Questo processo di sfaldamento di tradizioni e assetti sociali ormai dati per scontati è così generale da indurre molti ad invocare il concetto di "società dell'informazione" come griglia interpretativa di quanto sta avvenendo[2].

2. Gli effetti dell'"informatizzazione"

Prendendo atto quindi di quanto l'avvento dell'età cibernetica abbia posto l'umanità di fronte a una rivoluzione di tipo copernicano con la sua trasformazione da naturale in artificiale e da analogico a digitale, risulta necessario a questo punto fornire un giudizio valutativo sulle conseguenza sociali e sugli effetti palpabili di questa rivoluzione.

Ogni grande mutamento ha sempre portato con sé dei lati positivi e dei lati negativi; anche in questo caso, il concetto di società dell'informazione è infatti ambivalente, perché da una parte è centrato sullo sviluppo, sui nuovi modi di produrre, su un'informazione globalizzata e liberalizzata, sui nuovi valori, idee e significati dovuti all'introduzione dei nuovi strumenti; dall'altra è portatore anche dei rischi che sono direttamente connessi con il progresso e capaci di compromettere l'equilibrio del mondo.

Troviamo così tra gli effetti positivi, una forza trainante della tecnologia, capace di interagire sul sistema economico e informativo, dando vita a un processo di globalizzazione dei mercati, a un aumento della produttività, a nuove forme di lavoro più cooperative, a un ampliamento delle possibilità di ogni genere, a un abbattimento delle frontiere, una riduzione dei costi della manipolazione, conservazione e distribuzione dell'informazione.

Allo stesso tempo però l'avvento della tecnologia ha contribuito a generare timori e incertezze soprattutto nei confronti di chi non è apparso in grado di concepire e contenere la portata innovativa e rivoluzionaria di tale fenomeno; incertezze che crescono in maniera esponenziale alla luce degli effetti che il virtuale riversa con sempre maggiore frequenza e rilevanza nel mondo reale.

È vero quindi che le porte dell' informatizzazione si aprono verso nuovi spazi di applicazione per le attività e i pensieri dell'uomo, ma è vero anche che l'inaccessibilità a queste porte determina una pericolosa emarginazione e alienazione.[3]

2 D.Lyon, *La società dell'informazione*, Bologna, 1991, pp. 11 ss.

3 Il fenomeno in questione prende il nome di "digital divide" e si traduce appunto in quel divario digitale che separa la minoranza dei privilegiati "connessi" al mondo dalla grande maggioranza della popolazione mondiale che ancora non può accedere alle basilari infrastrutture di comunicazione. Ciò si spiega anche per la velocità. digitale che separa la minoranza dei privilegiati "connessi" al mondo dalla grande maggioranza della popolazione mondiale che ancora non può accedere alle basilari infrastrutture di comunicazione. Ciò si spiega anche per la velocità con cui è avvenuto il cambiamento, che non ha permesso a tutti di integrarsi e adeguarsi al meglio all'interno del sistema.

L'assunto cartesiano *cogito ergo sum* non si applica alle relazioni di rete: chi non comunica, chi non manifesta la sua esistenza attraverso l'interazione, la partecipazione a una *mailing list* o la presentazione di una pagina *web*, letteralmente non esiste da un punto di vista sociale.

Anche il *Dasein* Heideggeriano deve fare oggi i conti con il concetto di spazio virtuale; "l'esser-ci" diventa infatti "l'esser-ci-nel-mondo-digitale".

L'era informatica ridisegna inoltre la fisionomia dei territori, i confini vengono abbattuti col rischio e la paura che si crei un centro che è contemporaneamente ovunque e in nessun luogo; una "ubiquità virtuale" senza guardiani né documenti, il cui accesso è subordinato al solo possesso di un computer e di un modem.

Ad amplificare i pericoli del fenomeno, inoltre, c'è una generale e fisiologica inconsapevolezza sulle conseguenze che lo sviluppo tecnologico può apportare nella vita privata; ovvero l'incapacità di comprendere tale fenomeno come costellazione provoca incertezze e paure sui possibili risvolti futuri.

Insomma, forse dovremmo dirla con Adorno: "La dialettica del progresso incalza la nostra civiltà in una spirale fatale?".

Sulla base dell'esperienza acquisita nell'applicazione del computer, è facilmente dimostrabile che un uso distorto nella utilizzazione di questo strumento può certamente creare la base per nuove forme di criminalità; se è vero quindi che da un lato il binomio informatica-reti telematiche ha reso disponibili nuovi strumenti idonei allo sviluppo ed alla nascita di moderne e inedite opportunità su svariati livelli economici, sociali e comunicativi, dall'altro esso si è dimostrato terreno fertile per il proliferarsi di nuove e pericolose condotte criminose che prendono il nome di *computer crimes*.

Si riscontra infatti come

> la copertura tecnologica, figlia del post moderno informatico, abbia comportato inevitabilmente – così come sta comportando – una evoluzione megasoggettiva; cioè la strutturazione, sul piano della concezione, della prassi e della operatività di soggetti che veniamo a trovare nel commercio, nell'industria, nella editoria, allo stesso modo in cui li troviamo nella nuova criminalità; con la conseguente trasformazione della criminalità classica in maxicriminalità[4].

E la criminalità informatica rappresenta per ovvietà la componente principale di questa maxicriminalità.

Così, come ogni ambito dello scibile umano ha potuto sfruttare i nuovi mezzi tecnologici per potenziarsi, anche la mente del criminale ha trovato nuovi spazi e nuovi modi in cui sfogare inediti comportamenti illeciti.

3. I *COMPUTER CRIMES* UNA DEFINIZIONE AMBIGUA

Abbiamo osservato come la rivoluzione tecnologica abbia reso disponibile una serie di strumenti atti a creare nuove opportunità in ogni campo dell'agire umano; dall'altro lato però gli stessi nuovi mezzi si sono rivelati altrettanto idonei a porre in essere nuove e pericolose condotte criminose; anche i criminali hanno potuto (se non dovuto) familiarizzare con lo strumento informatico e aggiornare quindi in chiave tecnologica il repertorio delle proprie attività illecite.

Ma che cos'è il reato informatico? Quali sono gli elementi che lo caratterizzano?

"Individuare e definire compiutamente il fenomeno dei computer crimes è obiettivamente un compito arduo e complesso"[5], come sostiene Gianluca Pomante infatti, se si volesse identificare semplicisticamente come crimine del computer ogni comportamento previsto e punito dal codice penale in cui un qualsiasi strumento informatico o telematico ne rivesta un ruolo, si rischierebbe di escludere da tale definizione tutti quei comportamenti non ancora codificati a causa della continua e rapida evoluzione del settore informatico.

Ulteriori cause che incidono sulla difficoltà di elaborare una definitiva cornice descrittiva di tale fattispecie derivano inoltre "sia dalla eterogeneità delle modalità attraverso cui è possibile compiere un'azione inquadrabile

4 G. Ingrassia, *Comunicazione sociale: crimini e devianze nel post moderno informatico*, Torino, 1989, pp. 437 ss.

5 G. Pomante, *Internet e criminalità*, Torino, 1999, pp. 63 ss.

come crimine informatico, sia dal ruolo che lo strumento informatico può ricoprire"[6] all'interno dell'azione stessa.

Prendendo quindi atto della impossibilità di definire tale fenomeno come costellazione, vale a dire nella sua definitiva totalità, e della difficoltà di classificarlo sia sotto l'aspetto del *genus* che della *species*; non si potrà tuttavia prescindere da alcune definizioni generali elaborate da esperti del settore informatico e giuridico.

Una prima definizione efficace di *computer crimes*, la troviamo nel manuale preparato alla fine degli anni Settanta per il Dipartimento della Giustizia degli Stati Uniti, che individua i reati informatici nelle attività criminali per la cui esecuzione, scoperta e repressione si rendano necessarie particolari conoscenze nel campo della tecnologia dei computer; definizione questa non sufficientemente generica da farvi rientrare i c.d. "reati propri" (ovvero quelle condotte criminose, sempre più diffuse al giorno d'oggi, per la cui esecuzione non rileva alcuna particolare conoscenza informatica).

Secondo Tiedemann[7], i *computer crimes* appartengono al campo di indagine di quella speciale branca della criminologia che prende il nome di criminologia economica; non è erroneo infatti ritenere che alcuni (ma non tutti) di questi atti illeciti siano diretti a colpire interessi individuali, "abusando degli strumenti della vita economica e, conseguentemente, danneggiando anche gli interessi economici della collettività."[8].

Borruso, invece, sostiene che il crimine informatico deve per definizione riferirsi a un computer inteso però nella sua accezione più larga così da ricomprendere sia quelli a programma variabile, sia quelli c.d. dedicati, sia quelli nei quali il programma è inserito mediante supporto scritto. Lo stesso Borruso specifica inoltre che sono essenziali 4 condizioni:

1 – che si tratti di apparato elettronico;
2 – che utilizzi nel suo funzionamento un programma;
3 – che i segnali oggetto di elaborazione siano digitali e non analogici;
4 – che tale elaborazione avvenga sulla base della logica di Boole (and, or, not).

Un'ulteriore nozione di crimine informatico degna di rilievo è certamente quella elaborata dalla Commissione degli esperti OECD (Organisation for Economic Cooperation and Development) nell'incontro tenutosi a Parigi nel 1983; in quell'occasione si definì quali *computer crimes* "ogni condotta antigiuridica, disonesta o non autorizzata concernente l'elaborazione automatica e /o la trasmissione dei dati", "comprendendo pertanto in tale nozione anche le violazioni della privacy"[9].

Nonostante gli sforzi fatti dalla dottrina, le definizioni avanzate appaiono però tutte alquanto generiche e incapaci di cogliere ogni peculiarità del fenomeno:

> neppure l'accentuazione dei profili soggettivi e criminologici di questi reati – definiti come quegli illeciti in cui il computer si interpone tra l'autore del crimine e la vittima o comunque rappresenta lo strumento principale per eseguire una determinata azione criminale – ha in realtà permesso di individuare una nozione univoca a cui attribuire una precisa valenza tecnico-giuridica a fini esegetici[10].

Le definizioni fin qua riportate, fanno luce, ognuna a suo modo, sulle diverse forme che il reato informatico può assumere.

«La difficoltà di definire il concetto di crimine informatico si pone in tutta la sua evidenza se si osserva che, né a livello di legislazioni nazionali, né in ambito internazionale è stato possibile elaborare una definizione unitaria»[11]; questa difficoltà di definire porterà in Italia una nube di incertezza anche attorno all'esistenza di un bene giuridico unitario da tutelare – il bene giuridico informatico – facendolo coincidere con beni e interessi tradizionali e

6 G. Faggioli, *Computer Crimes*, Napoli, 1998, pp. 7 ss.

7 K.Tiedemann, *The international situation of research and legal reform work in the field of economic and business crime*, in "Ann. Internet. De Criminologie", 1978.

8 M.Correra, P.Martucci, *Elementi di criminologia*, Padova, 2006, p. 25.

9 P.Martucci, M.Correra, op. cit., pp. 169 ss.

10 M. Lanzieri, *I nuovi reati informatici*, Altalex eBook "Informatica Giuridica", 2010.

11 G. Faggioli, *op. cit,*. pag 10.

costringendo i penalisti ad estendere forme di tutela (già esistenti per le grandi categorie tradizionali) a fatti che vertono su oggetti informatici, negando così al nuovo bene informatico una tutela specifica.

Una chiara definizione di computer *crime*, non andrà quindi ricercata in una sequenza statica di parole, ma sarà più opportuno chiarirne il significato tramite una serie di distinzioni[12].

Alcuni autorevoli autori hanno fondato la definizione di reato informatico in una differenziazione basata sul ruolo che il computer può assumere nella perpetrazione del reato, potendo esserne oggetto, soggetto, strumento o simbolo.

Nel primo caso la condotta criminale include la distruzione, la manipolazione, la manomissione o l'inservibilità dell'elaboratore, dei dati e dei programmi in esso contenuti e delle relative apparecchiature di supporto (sabotaggio, vandalismo, danneggiamento informatico); nel secondo caso il sistema di elaborazione è inteso come "soggetto" quando rappresenta il luogo, il motivo o la fonte del crimine (appropriazione di programmi o informazioni, frodi elettroniche).

Nel terzo caso il computer può costituire strumento di reato quando ciò che avviene in relazione all'elaboratore non è di per sé illegale, ma è strumentale alla commissione di crimini di altro tipo quali i traffici di stupefacenti, l'usura, le scommesse clandestine.

Nell'ultimo caso il computer può rivestire fraudolentemente il ruolo di elemento di circonvenzione della vittima, in ragione dell'immagine di straordinaria efficienza tecnologica che il computer come simbolo esprime (come avviene nelle truffe realizzate a diverso titolo, utilizzando l'impatto psicologico favorevole indotto dalle tecnologie informatiche proprio su chi meno le conosce)[13].

Da questa classificazione è quindi possibile distinguere i reati informatici "tra reati "eventualmente informatici"(i c.d. *computer crime* in senso lato) e "necessariamente informatici"(i c.d. computer *crime* in senso stretto) a seconda che la diffusione delle tecnologie informatiche abbia solo ampliato le forme di manifestazione di un reato già esistente ovvero condotto alla configurazione di nuove figure in precedenza neppure ipotizzabili.

In quest'ottica, rientreranno nei reati informatici in senso stretto quelle particolari figure in cui il profilo informatico si presenta come imprescindibile elemento della condotta o dell'evento del reato; in altre parole non esisterà una fattispecie di reato per così dire "comune", omologa al reato informatico così definito.

Nei reati informatici in senso lato, al contrario, rientreranno tutte quelle fattispecie di reati "tradizionali" o "comuni" che, per le particolari modalità con cui vengono posti in essere si prestano ad implicazioni di carattere informatico, ma in maniera del tutto accidentale e assolutamente non caratterizzante.

Secondo questa impostazione il delitto di accesso abusivo a un sistema informatico andrà ricondotto alla categoria dei reati "necessariamente" informatici, mentre il furto o l'appropriazione indebita di fondi realizzati avvalendosi delle tecnologie informatiche a quella degli illeciti "eventualmente" informatici."[14].

Infine una seconda classificazione dei *computer crime*, forse la più esaustiva, permette di distinguerli in base:

a) *allo scopo perseguito dagli autori*; all'interno del quale trova spazio la suddivisione operata da Sarzana[15]che si esprime nelle seguenti categorie:

1 – fattispecie correlate all'uso del computer ed aventi per scopo la realizzazione di un profitto per l'autore e/o la produzione di un danno per la vittima;

2 – fattispecie dirette contro il computer-apparato, inteso cioè come entità fisica;

3 – fattispecie correlate all'uso del computer dirette a procurare danni fisici a individui o collettività;

b) *al modus operandi*; dove la variegata tipologia delle condotte viene continuamente aggiornata di pari passo con l'incalzante progres-

12 A nostro avviso il metodo delle classificazioni si rivela quello più opportuno a sopperire esigenze definitorie.

13 P. Martucci, M. Correra, *op.cit.*, pp. 170 ss.

14 M. Lanzieri, *op. cit.* pag 7.

15 C. Sarzana, *Criminalità e tecnologia: il caso dei computer crimes*, in "Rassegna Penitenziaria e criminologica", 1979, p. 59.

so tecnologico e la fantasia degli autori ma si può tuttavia raggruppare ulteriormente in:

1 – Reati commessi per mezzo del computer, quelli compiuti immettendo un'istruzione o una serie di istruzioni fraudolente nella memoria del computer o modificando i dati in esso già presenti, o aggiungendo dati alla memoria dello stesso tramite una linea esterna di natura telematica;

2 – Reati che sfruttano l'uso di un computer, i quali invece ineriscono transazioni telematiche non autorizzate, ed in questo caso il computer in sé non realizza nulla di irregolare, agisce per contro secondo i suoi fisiologici standard operativi, tuttavia per il suo tramite vengono preparati illeciti di penale rilevanza[16].

In conclusione possiamo rilevare che dal tenore di tali definizioni e distinzioni, appare evidente che l'unico dato unificante dei reati informatici è costituito dal coinvolgimento, attraverso differenti modalità, di strumenti informatici. Tuttavia, come correttamente è stato osservato, non tutti i comportamenti correlati all'uso del computer, ancorché penalmente rilevanti, possono farsi rientrare nel novero dei *computer crimes*, essendo tale qualifica da limitarsi ai soli casi in cui il sistema informatico o altri beni informatici costituiscano l'oggetto della condotta criminosa, ossia a quelle ipotesi in cui la particolare natura dei beni informatici comporti problemi di applicazione delle norme tradizionali e l'esigenza di nuove fattispecie penali[17].

4. Gli elementi principali del reato informatico

Abbiamo visto come il crimine informatico trova la sua genesi in un contesto complesso e caratterizzato da una continua evoluzione tecnologica e "come i reati informatici coinvolgono necessariamente l'utilizzo di un sistema di elaborazione, nel senso che la condotta dell'agente dev'essere rivolta verso un computer o, quantomeno, presuppone l'utilizzo di uno strumento tecnologico automatizzato"[18].

In questa sede è opportuno rilevare, come gli elementi fondamentali del reato informatico sono analoghi a quelli concernenti qualsiasi altro reato c.d. tradizionale [19]: avremo dei soggetti attivi che compiono una determinata azione od omissione, dei soggetti passivi che ne subiscono gli effetti, una condotta prevista e punita dall'ordinamento e un oggetto materiale su cui ricade la condotta medesima. A differenza degli altri fatti umani tuttavia, i reati informatici sono prodotti e si sviluppano all'interno di un contesto nuovo e di conseguenza sono sensibilmente caratterizzati dall'elemento tecnologico[20] il quale in varia misura, può assumere un determinato valore in relazione alle altre componenti del fatto.

L'influenza dell'elemento tecnologico può essere facilmente rilevata: ad esempio, sul piano dei soggetti attivi, sono individuabili persone dotate di particolari competenze informatiche quali gli operatori di sistema e i programmatori; allo stesso modo gli oggetti materiali della condotta possono essere costituiti da sistemi informatici e telematici, dalla corrispondenza telematica, da dati e informazioni elettroniche, ecc.

Nel soffermarci sull'analisi degli elementi tipici del reato informatico, inizieremo, per chiarezza espositiva, dall'oggetto materiale.

4.1 L'oggetto materiale

La legge 547 del '93 che ha introdotto i *computer crimes* nel nostro ordinamento, ha inserito nell'impianto del codice penale nuove fattispecie di reato, caratterizzate dall'oggetto materiale "informatico" dell'azione criminosa; in tali fattispecie infatti l'azione delittuosa colpisce i sistemi informatici e telematici, i programmi, i dati, le informazioni

16 P. Martucci, M. Correra, *op. cit.*, p. 170.

17 Così E. Giannantonio, *I reati informatici*, in "Il diritto dell'informazione e dell'informatica", Milano, 1992, p. 338, il quale rileva che considerando reati informatici tutte le ipotesi in cui un'attività criminosa venga realizzata mediante un computer, si finirebbe per etichettare come informatici la maggior parte dei reati, stante l'invadenza degli strumenti informatici in ogni settore dell'attività umana.

18 L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici*, Torino, 2009, p. 4.

19 G. Pomante, *Internet e criminalità*, Torino, 1999, p. 11.

20 P. Galdieri, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, p. 28.

in essi memorizzati, i documenti informatici, le comunicazioni informatiche / telematiche[21].Tuttavia il legislatore del '93 non ha fornito alcuna definizione di tali concetti, ma ne ha presupposto il significato ed i profili tecnici, lasciando così il compito di fornire definizioni legali alla prassi.

Il risultato di questa scelta è sicuramente una tecnica normativa difettosa e ambigua che ha creato non pochi dubbi interpretativi.

Iniziando tuttavia col cercare di definire il "sistema informatico" risulta opportuna una preliminare distinzione tra informatica e telematica:

Per informatica (espressione che risulta composta dalla fusione del sostantivo informazione con l'aggettivo automatica) si deve intendere la scienza e la tecnica dei fenomeni relativi al trattamento e alla trasmissione dell'informazione e degli strumenti di cui si serve; tuttavia, a questa definizione di ampia portata, appare preferibile una nozione più specifica di "scienza dell'uso del computer", non risultando giustificato far rientrare nella stessa ogni problematica relativa alla gestione dell'informazione, ed anche perché l'uso del computer consente non solo la gestione di informazioni bensì anche l'elaborazione di dati.

La telematica[22], invece, è sostanzialmente quel settore dell'informatica che si riferisce alle tecniche di diffusione dell'informazione, studia e definisce i supporti e gli strumenti per la trasmissione di suoni, immagini, informazioni ecc.: si tratta in sostanza dell'applicazione alla telecomunicazione dell'uso del computer.

Tanto l'informatica quanto la telematica si articolano in sistemi."[23]

Per sistema informatico deve intendersi il complesso degli strumenti, delle attività e delle risorse che utilizzano microprocessori per l'elaborazione di dati binari e per il trattamento automatico delle informazioni(raccolta, registrazione, elaborazione e conservazione).

Al fine di individuare le apparecchiature oggetto di tutela è necessario però che i singoli sistemi utilizzino, in tutto o in parte, tecnologie elettroniche che trattano e rappresentano informazioni attraverso simboli numerici ed elementari denominati "bit" che, organizzati in opportune combinazioni, vengono sottoposti ad elaborazione automatica.

Essenziale inoltre è che questa elaborazione dei segnali avvenga in formato digitale e non analogico[24], mediante una pluralità di istruzioni, che fa assumere rilevanza alla diversa programmabilità e alla variabilità dei risultati: ritenendo diversamente si rischierebbe infatti di confondere un sistema informatico con un semplice apparecchio elettronico.

Infatti, l'attitudine della macchina (*hardware*[25]) ad organizzare ed elaborare i dati sulla base di un programma (*software*[26]), per il perseguimento di finalità eterogenee, costituisce l'elemento essenziale che consente di distinguere ciò che è informatico da ciò che è invece solamente elettronico; in altre parole i termini "elettronico" e "informatico" non sono assimi-

21 Consiglio Superiore della Magistratura, incontro di studio sul tema "Criminalità informatica e protocolli investigativi", Roma 2006, relatore Dott. A. Calice.

22 La definizione di "telematica" deriva dalla contrazione semantica tra i termini "telecomunicazioni" e "informatica".

23 P. Martucci, M. Correra, *op. cit.*, p. 168.

24 Per formato "digitale" ci si riferisce a tutto ciò che viene rappresentato con numeri o che opera manipolando numeri; ciò che è digitale è contrapposto a ciò che è "analogico", cioè non numerabile, o meglio tutto ciò che non è analizzabile entro un insieme finito di elementi.

25 Per *hardware* si intende l'unità centrale, le memorie e le periferiche; ovvero tutte le parti fisiche di un personal computer (magnetiche, ottiche,meccaniche ed elettroniche) che ne consentono il funzionamento.

26 Per *software* si intende l'insieme dei programmi di elaborazione che permettono a un computer di operare. Essi, secondo Gallippi (*Dizionario di informatica inglese-italiano*, Milano, 2006), possono essere definiti come "sequenze ordinate di istruzioni destinate all'elaboratore elettronico, decisa a priori da programmatore mediante un'analisi del problema da risolvere e la definizione dell'algoritmo risolutivo". Sulla base delle funzioni (più o meno elementari o complesse) che i programmi sono in grado di risolvere, possono essere classificati in due gruppi distinti:1) I cd. Software di base o di basso livello, sono conservati nella memoria del computer con funzioni tanto elementari quanto fondamentali quali effettuare il controllo del corretto funzionamento della macchina alla sua accensione, il riconoscimento delle periferiche principali, il caricamento del sistema operativo, ecc..2) I cd. Software applicativi, sono posti a un livello superiore essendo quei programmi che consentono al sistema di svolgere i compiti impartiti dall'utente (per esempio l' elaborazione di un testo); in altre parole sono quei programmi che elaborano le informazioni richieste con l'utilizzo delle funzioni base del sistema operativo e restituendo i dati e le informazioni che sono stati così elaborati.

labili, poiché pur essendo elettronici il materiale ed i componenti, il sistema è informatico.

Oggetto della tutela saranno quindi solo i gruppi integrati di apparecchiature di elaborazione, composti sia dall' *hardware* che dal *software*, funzionanti in reciproca implementazione, ossia nell'insieme delle risorse di calcolo, delle procedure elettroniche, delle reti di comunicazione e degli apparati utilizzati per il trattamento di informazioni[27].Come accennato sopra, "in assenza di una classificazione legislativa, è stata la giurisprudenza a formare una definizione tendenzialmente valida per tutte le fattispecie incriminatrici, che fanno riferimento all'espressione sistema informatico"[28].

La Suprema Corte[29] infatti ha precisato che deve ritenersi "sistema informatico", secondo la ricorrente espressione utilizzata nella L. 547/93, "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente".

Nel caso di specie (in cui erano stati contestati i reati di accesso abusivo ad un sistema informatico e di frode informatica), la Cassazione ha riconosciuto la natura di "sistema informatico" alla rete telefonica fissa sia per le modalità di trasmissione dei flussi di conversazioni, sia per l'utilizzazione delle linee per il flusso dei cosiddetti "dati esterni alle conversazioni".

Si tratta certamente di una definizione di una certa complessità che, nella prassi, può determinare problemi di acquisizione della prova, per risolvere i quali si dovrà ricorrere a perizie ed accertamenti tecnici[30].Una definizione invece, certamente più semplificata di sistema informatico la troviamo nella Convenzione del Consiglio d'Europa sul "CyberCrime", tenutasi a Budapest il 23 Novembre 2001; all'art. 1, infatti, lo si definisce come " qualsiasi apparecchiatura isolata o un insieme di apparecchiature interconnesse o collegate, una o più delle quali, in basa e un programma, compiono l'elaborazione automatica dai dati".

Dai sistemi informatici si distinguono,come visto, i sistemi telematici i quali sono costituiti da un insieme combinato di apparecchiature idoneo alla trasmissione a distanza di dati e di informazioni, attraverso appositi programmi di gestione dei collegamenti; il collegamento tra più sistemi informatici deve però soddisfare alcuni requisiti essenziali:

a - la connessione deve avere carattere stabile (attraverso canali di comunicazione televisivi, satellitari, telefonici, via etere) o permanente (LAN o rete collegata via cavo);

b - lo scambio di informazioni e la connessione tra elaboratori distanti deve essere il mezzo necessario per conseguire le finalità operative del sistema.

Sul piano tecnico, l'applicazione delle procedure automatizzate alle reti di telecomunicazione, l'introduzione di nuovi mezzi trasmissivi (come il cavo in fibra ottica e il satellite), nonché la progressiva sostituzione dei sistemi analogici con quelli digitali, hanno prodotto il graduale superamento delle strutture tradizionali degli impianti di trasporto delle informazioni, da sempre basati sull'esistenza di reti distinte per organizzare servizi diversi.

Multimedialità e interattività sono l'effetto di un fenomeno di convergenza tecnologica in atto:

> l'accresciuta flessibilità dei sistemi di telecomunicazione consente di offrire a un numero sempre più ampio di soggetti una pluralità di servizi integrati e personalizzati che riguardano l'intrattenimento, l'informazione e l'accesso alle banche dati attraverso un solo punto di accesso.
> Tuttavia, la maggiore vulnerabilità degli strumenti telematici espone gli utenti a pericoli per la si-

27 L. Cuomo, R. Razzante, *op. cit.*, pp. 6 ss.

28 L. Cuomo, R. Razzante, *op.cit.*, p. 5.

29 Cass. Pen., sez VI, 4/10/1999, n. 3067, Pm. e Piersanti, RV.214945.

30 Consiglio Superiore della Magistratura, *op. cit.*, p. 6.

> curezza e per la riservatezza delle operazioni, per le tracce e le impronte elettroniche lasciate nella fruizione dei vari servizi, che rendono possibili controlli ed intromissioni nella vita privata[31].

Continuando nell'analisi delle componenti che costituiscono l'oggetto materiale del reato informatico, la legge 547 del 93 ha operato altresì una netta distinzione tra "dati" e "informazioni" in generale, da un lato, e "documenti informatici" e "corrispondenza informatica e telematica", dall'altro.

Per "dato" deve intendersi una parola, immagine, numero o suono convertito in una serie di bit, ossia "digitalizzato"; mentre l'"informazione" consiste nella connessione digitale che pone in relazione più dati; "essa è quindi composta da un insieme di dati interpretati e organizzati secondo un criterio logico che consenta di attribuire loro un significato ed un valore particolare per l'utente della macchina"[32].

I dati e le informazioni contenute e trasmesse dal sistema, costituiscono il vero patrimonio informatico esposto a pericolo.

Altro elemento di novità della legge 547 è l'introduzione, tra gli oggetti materiali del reato informatico, del documento informatico; il quale entrò a far parte del nostro ordinamento (art. 491 bis c.p.) come "qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".

Tuttavia questa nozione, pur riconoscendo una prima forma di efficacia probatoria al "supporto informatico", si mostrò da subito debole e inefficiente sul piano operativo, in particolare con riguardo alle possibili falsificazioni informatiche.

Le critiche maggiori erano rivolte al fatto che il documento così definito non fosse certo identificabile unicamente dal supporto, ma implicava un accento sul suo contenuto, ove questo avesse un senso e fosse riconducibile ad un determinato autore[33]. A superare tali difficoltà è intervenuto il "Codice di Amministrazione Digitale " entrato in vigore il 31/5/05 (Decreto legislativo 7 marzo 2005, n.82); il quale individuando il documento informatico nella "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", e integrando tale definizione alle disposizioni sulla firma digitale[34], consente un collegamento più penetrante tra "supporto", "contenuto" e "autore" e fornisce così le basi per una più opportuna tutela normativa del documento informatico.

Infine, la recente legge n. 48/2008 di ratifica della Convenzione di Budapest, ha provveduto a sopprimere il secondo periodo dell'art. 491 bis c.p., eliminando di fatto la prima e inadeguata definizione "penale" di documento informatico e slegando definitivamente la nozione di documento informatico dal mero supporto materiale. Ad oggi, in base al principio internazionale della c.d. "equivalenza funzionale" fra le categorie tradizionali e quelle informatiche, "se alcuna delle falsità [previste dal presente capo] riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private"[35]. La legge

31 L. Cuomo, R. Razzante, *op. cit.*, p. 8.

32 G. Pica, *Diritto penale delle tecnologie informatiche:* computer crimes *e reati telematici, internet, banche-dati e privacy*, Torino, 1999, pp. 26 ss.

33 V. L. Plantamura, A. Manna, *Diritto penale e informatica*, Bari, 2007, pp. 12 ss.

34 L'Art. 1 del Codice dell'Amministrazione Digitale definisce la "Firma elettronica" come "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"; la "Firma elettronica qualificata" come "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica"; la "Firma digitale" come "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

35 Art. 491 bis c.p. dopo la modifica della Legge 18 Marzo 2008 n. 48 in vigore dal 5 Aprile 2008.

547 del 93 individua in ultimo, tra i possibili obiettivi materiali della condotta illecita informatica, le "comunicazioni informatiche o telematiche"; tuttavia anche in questo contesto mancano indicazioni normative sul significato da attribuire al concetto.

L'art. 616, rubricato sotto "violenza, sottrazione e soppressione di corrispondenza", prevede nell'ultimo comma che "[...] per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza."

Va rilevato in primo luogo che l'oggetto della tutela sono i dati e le informazioni prodotte mediante le tecnologie informatiche, per cui non dovrebbe trarre in inganno l'uso dei termini "corrispondenza" e "comunicazione", in quanto il legislatore sembrerebbe aver utilizzato due termini apparentemente differenti sotto il profilo giuridico per descrivere il medesimo fenomeno tecnologico[36].

Quanto detto è stato ulteriormente posto in evidenza dalla dottrina, la quale ha affermato che la veste formale che assume la comunicazione telematica è sempre la stessa, e consiste in una rappresentazione di qualsiasi espressione di linguaggio in forma digitale, trasmissibile via cavo o via etere (cioè a mezzo di impulsi in radiofrequenza, anche via satellite), a prescindere da quale sia il contenuto della comunicazione[37].

Sia la dottrina che la giurisprudenza infatti, già prima della riforma del 1993 definivano il concetto di corrispondenza come ogni comunicazione di idee o notizie, intercorrente tra più persone, in modo diverso dalla comunicazione tra presenti; è pertanto ovvio che proprio per il riferimento alla comunicazione e quindi al contenuto del messaggio, non potrà mai essere considerato oggetto di tutela, quale "corrispondenza informatica", il supporto materiale su cui sono memorizzati i dati e le informazioni.

A questo punto si potrebbe affermare che le comunicazioni informatiche o telematiche, rilevanti ai fini dell'applicazione degli artt.616 e seguenti, consistono nell'attività di scambio e/o trasmissione di qualsiasi dato e/o informazione riservati tra due elaboratori fisicamente distanti, ma connessi tra loro. Questa sembrerebbe l'unica definizione in grado di soddisfare le esigenze ermeneutiche conformi, da un lato, ai principi di legalità e, dall'altro, alle tecnologie informatiche[38].

Concludendo, è sicuramente opportuno rilevare come l'applicazione delle tecnologie informatiche al campo delle comunicazioni abbia creato negli ultimi decenni, nuovi modi di trasmissione a distanza del pensiero, prima nemmeno immaginabili; esponendo però l'intero sistema di intercomunicazioni a profili sempre maggiori di vulnerabilità.

4.2 Il soggetto attivo

Genericamente viene definito soggetto attivo del reato, colui che realizza o concorre a realizzare il fatto conforme a una fattispecie astrattamente prevista dall'ordinamento giuridico come penalmente rilevante. In relazione alle ipotesi di reati informatici, la rivoluzione tecnologica, e in particolare l'avvento di internet, ha portato con sé la nascita di nuove figure di criminali: i c.d *computer criminals*.

Questo nuovo genere di autori del reato, agisce secondo modalità di esecuzione in larga misura diversificate a seconda del tipo di reato che commettono, della posizione che rivestono, dello scopo che li muove, ecc..

Sebbene i reati informatici non siano, tranne alcune eccezioni, sotto il profilo tecnico-giuridico dei reati propri, non essendo richiesta per la loro configurabilità una determinata qualifica soggettiva, ciò nonostante è evidente che talvolta gli stessi possono essere perpetrati, per le difficoltà di esecuzione che presentano, solo da soggetti dotati di conoscenze particolari. Secondo quanto sostiene Paolo Galdieri in "Teoria e pratica nell'interpretazione del reato informatico" infatti, si passa per gradi da reati che non richiedono alcuna competenza specifica, a reati che invece presuppongono un alto livello di specializzazione[39]. La stessa dottrina

36 Consiglio Superiore della Magistratura, *op. cit.*, p. 10

37 G. Pica, *op. cit.*

38 Consiglio Superiore della Magistratura, *op. cit.*, p. 11.

39 Un esempio chiarificatorio: l'ipotesi di frode informatica (ex art. 640 ter c.p.) richiede elevate conoscenze tecni-

ha infatti ritenuto opportuno distinguere i reati informatici in due fondamentali categorie; "delle quali la prima presuppone che il soggetto attivo sia un programmatore (cosiddetti "reati propri"), mentre la seconda si riferisce alle fattispecie che possono essere realizzate da chiunque"[40]In merito a quest'ultima tipologia di reati è in questa sede necessario accennare al fatto che negli ultimi decenni stiamo assistendo ad una intensificazione dei reati informatici presso fasce di persone sempre più vaste. Il diffondersi dell'"alfabetizzazione informatica" unita all'espansione di internet a livello globale, hanno facilitato la commissione sia dei crimini più tipici nell'ambiente tecnologico (quali l'accesso illecito a sistemi informatici, lo *spamming*, il furto di dati informatici, il deterioramento o il blocco di siti internet, la diffusione di virus informatici, ecc.), sia di quelli più "classici" (spionaggio, malversazioni finanziarie, pornografia infantile, vari tipi di truffe, ecc.) rendendoli più immediati da commettere e più impegnativi da reprimere.

Per quanto riguarda invece quelle tipologie di reati informatici che richiedono una qualche specializzazione nel settore per essere portati a termine, potremo distinguere ulteriormente i loro autori con riguardo, da un lato, alla specifica azione posta in essere e, dall'altro, alla qualifica soggettiva attribuita ad alcuni di essi.

Iniziando da questi ultimi possiamo dire che spesso

> il reato informatico può essere perpetrato proprio in virtù della posizione che un soggetto ha all'interno di un' organizzazione, posizione che sovente gli viene conferita dalla specifica qualifica professionale. Si è infatti osservato che spesso determinati reati si realizzano grazie alla complicità di un soggetto che, per il ruolo che riveste all'interno dell'organizzazione, ben può accedere alle risorse contro le quali dev'essere diretta l'azione delittuosa[41].

Il primo fra questi soggetti che per le sue qualifiche e competenze entrerebbe direttamente in cima alla lista dei sospettati di un reato informatico, prende il nome di "operatore di sistema".

La qualifica di operatore di sistema, può essere rivestita tanto da una persona fisica quanto da una impresa e nella pratica viene attribuita a chiunque può usufruire delle prestazione e delle risorse di un elaboratore elettronico. Nei sistemi monoutente l'operatore ha generalmente accesso a tutte le risorse del sistema in modo indiscriminato, compresa la possibilità di duplicare, esportare, cancellare o danneggiare irreparabilmente i dati e i programmi; nei sistemi multiutente, gli operatori si dividono in due grandi categorie: quella degli utenti "privilegiati", abilitati cioè a trattare tutte le informazioni, a gestire le risorse informatiche, ad organizzare gli archivi, e ad assegnare privilegi agli utilizzatori, secondo opportune gerarchie; e quella degli utenti "non privilegiati" i quali possono solo utilizzare programmi applicativi con precise restrizioni di accesso ai dati[42]. Frequentemente infatti viene sopravvalutato il rischio di aggressioni, accessi o intrusioni dall'esterno del sistema, mentre ben più insidiosi, a causa della conoscenza dei meccanismi virtuali di elusione delle misure di sicurezza, possono risultare le condotte poste in essere da dipendenti, collaboratori o soggetti interni all'organizzazione aziendale.

Alcune fattispecie di reati informatici, come l'accesso abusivo ad un sistema informatico o telematico (art. 615ter c.p.), l'intercettazione o interruzione illecita di comunicazioni informatiche (art. 617quater c.p.), l'installazione di apparecchiature atte a intercettare comunicazioni informatiche (art. 617quinquies c.p.), il danneggiamento di dati e sistemi informatici (art. 635bis, 635ter, 635quater, 635quinquies

che per la sua attuazione, mentre il reato di accesso abusivo (ex art. 615 ter c.p.) è realizzabile da chiunque fisicamente acceda a un sistema informatico abusivamente, senza una necessaria competenza nel campo informatico.

40 M. Correra, P. Martucci, *I reati commessi con l'uso del computer*, Padova, 1986, pp. 23 ss.

41 P. Galdieri, *op. cit.*, p. 29.

42 Secondo L. Cuomo e R. Razzante, possono assumere la qualità di operatore di sistema una vasta gamma di persone tra cui:-il soggetto preposto alle operazioni di "input" e di "output", di avviamento o di arresto dell'elaboratore elettronico;-il programmatore che scrive con appositi linguaggi le istruzioni e le operazioni che il computer è chiamato ad effettuare;-il sistemista che studia le possibili evoluzioni di un sistema per implementarlo-l'analista che sviluppa gli algoritmi per soddisfare specifiche esigenze.

c.p.) o la frode informatica (art.640ter c.p.), prevedono come ipotesi aggravate la commissione del fatto da parte di soggetti che ricoprono il ruolo di operatori di sistema e abusano di tale qualità[43]. Il fondamento dell'aggravante andrà ricercato nella speciale opportunità del soggetto attivo di sfruttare le proprie conoscenze per la commissione del reato a causa dell'esistenza di un rapporto giuridico di qualsivoglia natura, a carattere anche saltuario o temporaneo, con il bene su cui ricade la condotta materiale[44].

Altro soggetto particolarmente qualificato che può porre in essere la totalità dei reati informatici è il cosiddetto "provider", individuandosi con tale espressione il soggetto – sia esso persona fisica o ente collettivo – che fornisce a terzi l'accesso a internet gratuitamente o a pagamento.

Come è noto, le trasmissioni digitali all'interno delle reti telematiche avvengono raramente in modo diretto tra due o più soggetti interessati alla comunicazione, poiché i dati vengono resi accessibili al pubblico tramite la riproduzione, anche transitoria, dai supporti o dalle memorie su cui sono depositati in direzione del computer dell'utente finale, transitando attraverso percorsi di rete temporanei, più facilmente disponibili ed in grado di offrire connessioni maggiormente rapide ed efficienti; il soggetto che gestisce tale rete informatica su cui transitano le comunicazioni telematiche è, per l'appunto, il "provider"[45].

In sostanza, chiunque abbia intenzione di accedere alla rete internet, dovrà registrarsi presso un provider dichiarando il proprio "*user name*" (cioè il nome che lo identifica presso la struttura del provider) il quale abbinato a una password consente la navigazione appoggiandosi al *provider* stesso; il compito del *provider* sarà poi quello di registrare i dati relativi alla connessione effettuata da ciascun utente per consentire di individuarlo, di determinare la durata della sua connessione e di conoscerne i siti visitati.

> Il *provider*, ovviamente, come qualsiasi soggetto di diritto, può essere personalmente responsabile per illeciti che commette con la proprio condotta – si pensi ad esempio al provider che illecitamente diffonda dati personali di alcuni utenti registrati presso di lui-, ma evidentemente i profili più rilevanti attinenti alla responsabilità di tale soggetto riguardano però la possibilità che lo stesso sia chiamato a rispondere in relazione ad illeciti commessi da terzi, ovvero dagli utenti o soggetti che gestiscono un sito web o navigano sulla rete[46].

Passando ora ad analizzare le tipologie di *computer criminals* da un punto di vista delle specifiche azioni poste in essere e seguendo l'impostazione di P.Galdieri, si nota facilmente come sia possibile distinguere questi soggetti attivi in due figure principali:

La prima, prende il nome di "intrusore informatico" per ricomprendere al suo interno la vasta schiera di soggetti attivi che, privi di titolo o di autorizzazione, penetrano nel sistema eludendo le eventuali misure di sicurezza per portare a termine varie finalità e obiettivi.

L'intrusore presuppone gradi di conoscenza che differiscono a seconda del metodo utilizzato per l'intrusione; infatti, mentre è relativamente semplice accedere a un sistema di cui si conosca già la password d'accesso, non può dirsi lo stesso per le ipotesi in cui l'intrusore deve forzare sistemi di protezione ben protetti.

In questa categoria viene sempre più spesso utilizzato il termine onnicomprensivo di *hacker* per identificare un soggetto informatico di buon livello dedito ad attività illecite; in realtà, l'hacker comprende solo una tipologia di *computer criminal*, forse la più affascinante e complessa, sicuramente la prima della storia, ma oggi affiancata da una lunga serie di termini inglesi che stanno ad indicare i nuovi "cattivi" colleghi degli *hackers*, parliamo dei *cracker*, degli *irc warriors*, degli *swappers*, dei *chatters*, ecc.; tutti intrusori, nel senso più generico del termine ma caratterizzati da diverse condotte e mossi dalle più disparate motivazioni.

43 È da notare infatti come sia il termine "operatore di sistema" che "amministratore di sistema", assumono connotati negativi solo nel momento in cui l'agente abusa della sua particolare posizione per commettere un reato.

44 L Cuomo, R. Razzante, *op. cit.*, pp. 21 ss.

45 G. Amato, V. S. Destito, G. Dezzani, C. Santoriello, *I reati informatici*, Padova, 2010, p. 17.

46 G. Amato, V. S. Destito, G. Dezzani, C. Santoriello, *op. cit.*, p, 18.

L'ultima categoria di soggetto attivo "qualificato" è l'intercettore illegittimo o il c.d. *phreaker*; nel corso degli anni infatti, sono stati oggetto di studio da parte dei criminali informatici, non solo le tecniche e le modalità di accedere abusivamente a sistemi, dati e informazioni, ma anche i metodi di pirateria telefonica atti allo studio delle caratteristiche delle reti telematiche al fine di trovare nuovi metodi di chiamata senza addebito.

Il primo a dare il via a queste tecniche illecite fu John Drapher, conosciuto alle cronache come Captain Crunch, il quale scoprì come effettuare telefonate in teleselezione o addirittura intercontinentali senza pagare, tramite i fischietti che si trovavano in regalo nei pacchetti di cereali. Bastava infatti formare il numero della chiamata in teleselezione, attendere un momento e suonare con il fischietto nella cornetta; l'operazione riusciva in quanto la frequenza di 2600 hertz del fischietto, consentiva di disattivare il contascatti al centralino per la teleselezione.

A seguito di questa scoperta, tutto il mondo dei criminali, si adoperò per studiare e applicare metodi sempre più sofisticati di pirateria telefonica.

5. Le condotte illecite

L'ultimo elemento strutturale del reato informatico che andremo ad analizzare riguarda le diverse tipologie di condotte illecite tramite le quali il reato può essere perpetrato

> Con le tecnologie di comunicazione, il concetto di condotta, teorizzato per una realtà fisica nella quale le conseguenze sono esteriormente percepibili ed empiricamente verificabili nel luogo dove si trova l'agente, sfuma nella dimensione virtuale; dimensione dove tutte le azioni assumono l'aspetto di comportamenti comunicativi che consistono nella trasmissione o nel trasferimento di dati elettronici[47].

Infatti, a fronte di una usuale nozione di condotta quale comportamento esteriore che provoca (quanto meno nei reati commissivi) una modificazione del mondo esterno, nelle ipotesi delittuose in esame, l'azione del soggetto agente assume una dimensione affatto diversa, fino a modellarsi secondo evanescenti ed immateriali forme di trasmissione, immissione, gestione di dati a mezzo di impulsi elettronici[48].

Partendo da più lontano, abbiamo già avuto modo di osservare come l'oggetto materiale dei reati informatici si incarna in un "sistema informatico"; tale sistema viene definito – dall'art.1 della Convenzione europea di Budapest – come una "qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati".

Secondo questa prospettiva, ciò che caratterizza il sistema informatico è quindi la capacità dello strumento – sulla base di un apposito software – di organizzare *input* esterni e quindi elaborare dei dati in un formato digitale; detto in altre parole, un semplice gesto del soggetto agente, può attivare un impulso elettronico che richiede al *personal* computer di procedere ad una serie complessa di operazioni, il cui risultato è quanto mai distante – sotto un profilo temporale, geografico e di rilevanza – dal comando formulato dall'utente informatico[49].

Sotto il profilo ontologico, l'input (inteso come atto di volontà che si traduce in un impulso elettronico diretto al computer) rappresenta uno degli elementi costitutivi dei reati informatici; nel contesto virtuale però la possibilità di attribuire una condotta ad un determinato soggetto, si frantuma in ragione dei risultati espansivi provocati dalla rete, che può amplificare e moltiplicare le conseguenze dell'azione[50]. Inoltre, essendo l'azione telematica posta in essere tramite una connessione tra sistemi informatici distanti tra loro, gli effetti della condotta potranno esplicarsi in un luogo diverso da quello in cui si trova il soggetto agente.

La capacità di produrre, tramite l'uso delle tecnologie informatiche, conseguenze an-

47 L. Cuomo, R. Razzante, *La nuova disciplina dei reati informatici*, Torino, 2009, p.8.

48 G. Amato, V. S. Destito, G. Dezzani, C. Santoriello, *I reati informatici*, Padova, 2010, p. 14.

49 G. Amato, V. S. Destito, G. Dezzani, C. Santoriello, *op. cit.*, p. 15.

50 L. Cuomo, R. Razzante, *op. cit.* p. 9.

tigiuridiche lontane dal luogo in cui è stata compiuta l'azione, costituisce uno dei principali problemi in sede di accertamento del medesimo illecito; più in particolare, il problema attiene alla difficoltà nell'individuare l'autorità giudiziaria territorialmente competente.

Abbiamo già osservato come un' esaustiva classificazione dei *computer crimes* permette di distinguerli in relazione allo scopo della condotta o al "modus operandi" dell'autore; per quanto riguarda il primo criterio, i reati informatici possono poi ulteriormente distinguersi in:

1 - crimini correlati all'uso del computer ed aventi come finalità la realizzazione di un profitto e/o la produzione di un danno per la vittima; siamo nei casi di appropriazione o manipolazione di programmi e di informazioni, di frodi elettroniche, ecc.;

2 - crimini diretti contro il computer nella sua entità fisica allo scopo di provocarne la distruzione o l'inservibilità; è questo il caso del sabotaggio, del vandalismo o del danneggiamento informatico;

3 - crimini correlati all'uso del computer per procurare danni fisici a individui o a collettività; in questo caso le condotte illecite prendono forma nell'estorsione, nell'esercizio arbitrario delle proprie ragioni o ancora nell' attentato ad impianti di pubblica utilità, ecc.).

Per quanto attiene invece alle modalità di commissione dei *computer crimes*, abbiamo già rilevato come queste nascondano una variegata tipologia di condotte illecite che si rinnovano e si modificano allo specchio dell'evoluzione tecnologica.

Per fare un esempio, possiamo dire che fino a qualche anno fa, i comportamenti illeciti aventi ad oggetto un dispositivo informatico, sembravano richiedere necessariamente un alto grado di abilità tecnica da parte dei loro autori; quest'impostazione va oggi assolutamente smentita. Il processo di vascolarizzazione "digitale", la crescente "alfabetizzazione" informatica unita ad alcuni valori professati dall'"etica hacker" (come quello sulla totale libertà e accessibilità delle informazioni), hanno portato a un abbassamento delle difficoltà con cui porre in essere un *computer crime*; anche le violazioni più complesse possono essere oggi compiute da soggetti privi di competenze specifiche, semplicemente scaricando un programma da internet e avviandolo dal proprio computer. Si pensi alla diffusione dei virus o all'intercettazione di comunicazioni *on-line* o ancora alla possibilità di "craccare" reti *wireless* protette; operazioni oggi consentite da applicazioni pronte ad essere usate e condivise gratuitamente sul Web.

Inoltre, la necessaria perizia informatica nel compimento degli illeciti in questione, è smentita anche dagli strumenti rudimentali utilizzati in alcune tecniche di sabotaggio informatico: una semplice calamita sarà sufficiente a smagnetizzare i nastri interni alle memorie fisiche di computer così come basterà un semplice radiotrasmettitore (detto *blue box*) per disturbare le comunicazioni tra modem telefonici.

Proprio per questi motivi infatti, la tentazione al crimine informatico si è ampliata trascinandovi dentro una schiera di soggetti sempre più vasta e lasciando agli "*hacker* geniali" solo una minima percentuale della casistica complessiva.

Queste osservazioni inducono a ritenere come sia sempre più difficile inserire in un sistema coerente e definitivo un fenomeno tanto mutevole quanto eterogeneo come quello dei *computer crimes*.

Tuttavia l'esigenza di fare chiarezza in un mare così vasto di modalità criminose, impone un primo raggruppamento – di tali modalità – in categorie generiche di condotte.

5.1 Le condotte intrusive

Secondo l'impostazione di Paolo Galdieri[51], una prima categoria generale di condotte aggressive può essere individuata nell'intrusione all'interno di un sistema informatico o telematico.

Questa condotta può essere definita come il tentativo riuscito di effettuare nel sistema operazioni non consentite dai privilegi assegnati dall'amministratore del sistema e può comprendere tanto l'utilizzo di un sistema di

51 P. Galdieri, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, pp. 48 ss.

cui non si è utenti quanto l'abuso commesso su un sistema a cui si può accedere "legalmente" a qualunque altro titolo[52]. Tuttavia perché si possa parlare di intrusione è necessario che siano state superate tutte le protezioni di cui il sistema è fornito e ciò dovrebbe reclinare l'attenzione anche su quei soggetti, come gli amministratori di sistema, che dovevano predisporre le opportune misure di sicurezza ma non hanno provveduto a farlo[53].

La tematica sulla sicurezza informatica ricerca infatti quel punto di equilibrio tra la riservatezza di alcuni dati e la libertà di accesso ad altri; ma è un punto di equilibrio che non è fisso anzi varia a seconda che si tratti di un singolo elaboratore non collegato con altre postazioni di lavoro, o siano invece più sistemi collegati in rete. Nella prima ipotesi, quando cioè il computer è "stand alone", l'intrusione deve avvenire di persona, in modo diretto, e in questo caso il problema si pone nei termini di limitare il numero di soggetti che sono abilitati ad accedere a quella determinata postazione; nella maggior parte dei casi per ovviare al problema si ricorre all'utilizzo di apposite chiavi d'accesso (o *password*), all'inserimento delle quali viene fatto subordinare il funzionamento del sistema.

Nella seconda ipotesi invece è opportuna un'ulteriore distinzione a seconda che si consideri una rete chiusa o una rete aperta anche ad altri utenti esterni. Se non è previsto un collegamento con gli utenti esterni, (come può accadere nel caso di un'azienda i cui *computer* sono collegati in rete ma non hanno nessun contatto con altre macchine al di fuori di quelle facenti parte del *network*) il problema si pone in termini simili a quelle descritti in precedenza, ma in questo caso il punto di equilibrio va mediato dal concetto di "rete".

In un sistema dove più persone hanno la possibilità di accedere alle medesime informazioni tramite un accesso concorrente, sarebbe contrario alla *ratio* del sistema prevedere soluzioni che impediscano un accesso ai dati relativamente libero[54]. Come misure di sicurezza, si potranno quindi configurare diversi livelli di accesso e di privilegi, graduati in relazione all"importanza delle informazioni e dei soggetti legittimati a consultarle.

Infine, nel caso delle reti aperte, le intrusioni da parte di utenti esterni, si realizzano soprattutto attraverso gli accessi ad *Internet* o attraverso le linee telefoniche utilizzate dal soggetto colpito; in questo contesto il problema sulla sicurezza cresce in maniera esponenziale, tale da rendere assolutamente irrinunciabile e necessaria la predisposizione di adeguate misure e protezioni informatiche, capaci di crescere e aggiornarsi costantemente alle tecniche di chi è sempre intento a superarle.

Le modalità con cui vengono attuate le intrusioni nei sistemi informatici sono molto varie; in una parte della casistica, il comportamento volto a violare la sicurezza dei sistemi informatici e delle reti telematiche è un comportamento non animato da un fine di lucro ma più spesso da un mero scopo ludico. Tuttavia è da rilevare come in alcuni casi, il superamento delle barriere di protezione possa facilitare il soggetto infiltrato ad assumere condotte più invasive e aggressive; non è infrequente infatti che l'intruso decida di copiare le informazioni a cui ha avuto accesso illegalmente o inserire all'interno del sistema violato un programma dannoso (c.d. *malware).*

Come ci spiega G. Pomante in "Internet e criminalità", l'accesso non autorizzato ad un sistema informatico o telematico, può essere a seconda delle finalità perseguite, momento propedeutico alla commissione del reato vero e proprio, ovvero fine ultimo dell'assalto; se l'obiettivo della condotta delittuosa è l'acquisizione di informazioni riservate o il danneggiamento del sistema informatico, l'accesso diventa un percorso obbligato, una *conditio sine qua non*, per portare a termine l'attacco. Se invece il criminale è spinto del solo inten-

52 P. Galdieri, *op. cit.*, pp. 48 ss.

53 Tuttavia, per quanto P. Galdieri attribuisca una forte responsabilità su chi gestisce e mantiene il sistema di sicurezza, oggi vengono sperimentate e utilizzate nuove tecniche di intrusione che non lasciano scampo neanche al più accorto fra gli amministratori del sistema; per ottenere una password, non è più necessaria la collaborazione, dolosa o colposa che sia, di un operatore privilegiato, ma sarà sufficiente un programma moderno, in grado di calcolarla autonomamente.

54 P. Galdieri, *op. cit.*, p.50.

to di confrontarsi con le misure di sicurezza del sistema, l'assalto si esaurirà quando il soggetto agente avrà ottenuto l'accesso; da questo punto di vista alle condotte intrusive possono quindi fare seguito delle condotte modificative, turbative o, nei casi più gravi, delle condotte distruttive.

In tema di metodologie attuative dei *computer crimes*, è necessario distinguere innanzitutto fra un'aggressione "interna" e un'aggressione "esterna" ai sistemi informatici.

Con la prima espressione vanno intesi quegli illeciti commessi da dipendenti ai danni del proprio datore di lavoro[55]; in questo caso l'operatore che possiede già una legittimazione all'accesso in quanto utente privilegiato, abusa però del proprio strumento professionale e di solito lo fa perché spinto da finalità lucrative o da insoddisfazioni lavorative.

Nel secondo caso invece le tecniche intrusive necessitano di doti informatiche più elevate poiché il soggetto agente (molto spesso l'*hacker*) si inserisce abusivamente nelle reti non in quanto utente privilegiato ma in quanto utente esterno, che ha individuato una falla nella protezione del sistema.

Sebbene, risultino più frequenti le violazioni commesse sulle macchine aziendali da parte di dipendenti interni, repressi o da poco licenziati, in realtà gli accessi abusivi più insidiosi vengono compiuti a distanza da soggetti dotati di particolari conoscenze informatiche.

Per fare un esempio, secondo una prassi oggi sempre più diffusa, il soggetto che si infiltra in un sistema dall' esterno, comunica al titolare del computer o della banca dati di avere trovato il modo per superare le sue misure di sicurezza e di possedere quindi la soluzione al problema; fatta eccezione per i rari casi di segnalazioni gratuite, spesso tale comunicazione ha finalità ricattatorie, poiché se il proprietario non provvede a pagare l' *hacker* per risolvere il difetto di protezione, lo stesso *hacker* lo minaccerà di immettere nel sistema violato un programma distruttivo in grado di paralizzare il funzionamento del sistema. Si tratta di una nuova forma di estorsione non sempre facilmente documentabile poiché spesso le grandi aziende preferiscono pagare direttamente coloro i quali le minacciano piuttosto di far trapelare nel pubblico la notizia negativa di una falla nella sicurezza informatica.

5.2 Le condotte manipolative

Gli accessi non autorizzati nelle memorie elettroniche, non rappresentano di per sé la minaccia più grave alla sicurezza dei sistemi informatici; infatti, come abbiamo visto, se l'assalto si esaurisce nel semplice accesso – per quanto questo sia abusivo e quindi già di per sé illecito – non necessariamente avremo l' estrinsecazione di un danno effettivo.

Per rendere chiaro il concetto è utile fare riferimento all'art. 615 *ter* c.p. il quale punisce "chiunque abusivamente si introduce all'interno di un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo"; la pena è aggravata (dal secondo comma) se – tra le varie ipotesi – "dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti".

Dal testo normativo risulta chiaro come la previsione dell' aggravante nasconda un timore ulteriore rispetto alla mera condotta intrusiva; ovvero il timore che le finalità del soggetto attivo non si esauriscano col semplice accesso abusivo, ma continuino oltre, fino a prendere la forma di condotte ben più dannose.

Tra queste troviamo le condotte alterative o modificative, le quali hanno solitamente come oggetto materiale la componente "*software*" del sistema e presuppongono quindi la possibilità di avere pieno e completo accesso ai *file* contenenti il programma, nonché al sistema informatico su cui esso è installato.

Tali forme di aggressione sono finalizzate a modificare la funzionalità o l'aspetto esteriore del *software* o comunque a generare un prodotto diverso, ma basato sugli stessi principi ; ciò permette di ottenere un prodotto copiato e diverso dall'originale, ma la cui proprietà in-

55 P. Martucci, M. Correra, *Elementi di criminologia*, Padova, 1999, p. 173.

tellettuale è in larga misura del primo sviluppatore e non del "modificatore".

Questa operazione rispecchia la tecnica del cosiddetto *reverse engineering* (o ingegneria inversa) e cioè quel processo tramite il quale, nell'ambito informatico, si va ad analizzare nel dettaglio il funzionamento di un programma esistente così da poterne costruire uno nuovo che sia la rappresentazione ad alto livello di astrazione del primo programma. Il suo scopo principale è quello di ricostruire a fini di manutenzione una procedura di cui siano andati perduti i codici "sorgenti" per cause accidentali, salvaguardando così l'investimento effettuato in essa[56].

Tuttavia nulla impedisce l'utilizzo di questa tecnica per fini illeciti, poiché la stessa consente di generare programmi che in apparenza sembrerebbero originali ma in realtà sono copiati; in quanto solo da un'analisi approfondita e comparata delle strutture su cui lavora un programma "sospetto", si potrà provare la sua derivazione da altri programmi preesistenti.

Le alterazioni, invece, che colpiscono un programma in servizio, appartengono a un discorso diverso poiché queste possono essere tese a modificarne il funzionamento in favore di qualcuno o provocare errori che portino a conseguenze fraudolente o danneggiamenti per altre vie; per fare un esempio, nel caso in cui si alteri un programma che gestisca transazioni bancarie, si potranno ottenere accrediti inesistenti su altri conti.

5.3 Le condotte turbative e impeditive

Passando ora ad analizzare le condotte impeditive, possiamo dire che queste sono dirette solitamente a colpire il funzionamento di un sistema informatico o telematico provocandone una distorsione più o meno grave nelle sue normali funzionalità o privandolo di alcune sue componenti essenziali del *software* o dell' *hardware*.

La distinzione tra le suddette componenti risulta però fondamentale in quanto se il turbamento nel funzionamento della parte *hardware,* pur necessitando un accesso fisico nel luogo in cui lo stesso è situato, è tuttavia di facile esecuzione (basterà infatti sconnettere o recidere i cavi o provocare un danno meccanico) nonché di facile ripristino[57], nel caso invece in cui si voglia arrecare un danno alla componente *software*, non basterà la vicinanza materiale all'oggetto, ma servirà avere accesso alle parti "vitali" del sistema operativo il che implica la conoscenza delle chiavi di accesso del responsabile del sistema.

In questa prospettiva quindi, anche le condotte turbative presuppongono una preventiva condotta intrusiva.

Da ciò ne deriva che le alterazioni inducibili sul *software* sono generalmente più insidiose e provocano delle conseguenze più gravi. Inoltre occorre notare che il danno-*software* potrebbe non riguardare solo i programmi, ma estendersi anche ai dati con conseguenze ancora peggiori di quelle provocate dalla cancellazione del *software*: come la creazione di utenti abusivi, errori nella memorizzazione dei dati, malfunzionamenti nelle comunicazioni di rete, riduzione delle capacità elaborative o di memorizzazione del processore, ecc.

È possibile infine ottenere il blocco del sistema, sia totale che parziale, anche senza le cancellazioni al *software* ma lanciando un numero elevato di processi in contemporanea così da congestionare il sistema; tale effetto può essere raggiunto in modo automatizzato mediante l'uso di programmi "autoreplicanti" o generanti processi diversi a ripetizione come i *virus,* i quali hanno anche la capacità di installarsi in modo permanente nelle memorie di massa del *computer* continuando così l'infezione anche dopo l'intervento dell'operatore fraudolento[58].

5.4 Le condotte distruttive

In ultimo, per quanto attiene alle condotte distruttive, è necessaria una preliminare di-

56 P. Galdieri, *op. cit.*, p. 61.

57 Una manomissione al funzionamento dell'*hardware* può alterare i parametri di funzionamento causando improvvisi blocchi del sistema, ma generalmente il problema è facilmente risolvibile da un normale intervento di assistenza tecnica; a meno che non si siano verificati veri e propri danni fisici o perdite di dati in conseguenza della manomissione *hardware*.

58 P. Galdieri, *op. cit.*, p. 63.

stinzione tra i fatti diretti a danneggiare o distruggere interi sistemi informatici o telematici e i fatti diretti a danneggiare o distruggere dati, informazioni o programmi contenuti nel sistema o ad esso pertinenti.

In relazione alla prima categoria, valgono le stesse considerazioni già fatte in tema di condotte alterative sul funzionamento di un sistema estese però anche all'impiantistica associata al sistema informatico (come le linee di trasmissione o i collegamenti fra le periferiche e l'elaboratore principale o tra più elaboratori e periferiche).

In merito invece alle condotte di distruzione dei dati, esiste una duplice possibilità: che siano stati danneggiati i supporti di memorizzazione di massa (componenti *hardware*) oppure che siano state danneggiate le componenti *software* a seguito di accessi indesiderati con le modalità già descritte in precedenza.

In entrambi i casi le conseguenze possono essere molto gravi poiché la perdita di dati può provocare sia disservizi nel sistema sia la perdita del lavoro manuale che è stato necessario per creare i dati distrutti; il tutto è ulteriormente aggravato dal fatto che i dati possono essere non ricostruibili.

In questo contesto, l'unico rimedio in grado di sopperire a tali danneggiamenti è rappresentato dalle copie di sicurezza (*backup*), da eseguire con una frequenza proporzionale al grado di criticità dei dati oggetto della condotta lesiva.

Giovanni Felluga si è laureato in giurisprudenza presso l'Università degli Studi di Trieste sostenendo una tesi in antropologia criminale dal titolo I nuovi reati informatici.

giovannifelluga@hotmail.it