IL REATO DI FRODE INFORMATICA

Una rilettura alla luce delle recenti pronunce giurisprudenziali

Dott. Giovanni Modesti[1]

Sommario: INTRODUZIONE 1. I REATI INFORMATICI 2. IL REATO DI TRUFFA - 3. IL REATO DI FRODE INFORMATICA – 3.1 ALCUNE IPOTESI DI FRODE INFORMATICA: PHISHING, DIALER, ECC 3.2 LE CIRCOSTANZE AGGRAVANTI - 4. LA GIURISPRUDENZA. - CONCLUSIONI

INTRODUZIONE

Il recente sviluppo della tecnologia informatica[2], unito al rapido diffondersi dell'utilizzo dei sistemi di comunicazione telematica, ha

[1] L'Autore è docente incaricato di Diritto Privato presso la Università degli Studi "Gabriele D'Annunzio", al C.d.L. in Scienze Infermieristiche ed Ostetriche – Specialistica.

[2] Bibliografia: **Corrias L.**, Informatica e Diritto Penale: elementi per una comparazione con il diritto statunitense; 1987; **Vaccaio D.,** L'evoluzione del concetto di misura di sicurezza a protezione del sistema informatico alla luce dell'art. 615-ter e del Disciplinare Tecnico; in www.computerlaw.it,; 2004; **Guida normativa Il sole 24 Ore,** AA.VV., 2004; **Rossi D.,** Personal computer…home sweet home; e Dialer, trojan horse. Cosa si nasconde dietro un click; su WWW.filodiritto.com; **Farolfi F.**, I crimini informatici, in www.ei.unibo.it/materie/pdf/reati_informatici.pdf, opera alla quale si rimanda per una lucida analisi sulla incidenza che la frode informatica ha in materia di risk analisis aziendale; **Pomante G.**, Frode informatica, la soluzione arriva dall'art. 640 ter, su www.pomante.com, i quale analizza la tematica avendo come punto di partenza una analisi dei rischi al fine di individuare, successivamente, le fattispecie criminose; **Parodi C.,** La tutela penale dei sistemi informatici e telematici: le fattispecie penali; **Stilo L.,** Il crimine informatico: tra esigenze di riforma, protocolli operativi omogenei ed approcci criminologici, su www. diritto.it; **Sinibaldi A.**, "Risk Management", Hoepli 2007; **Sabato G.,** La Responsabilità Amministrativa degli Enti: i reati informatici in www.diritto.it (2009); **Marino G.,** La competenza territoriale in materia di reati informatici, fra giurisdizione di legittimità e profili di incostituzionalità: brevi note a margine della sent. Cass. pen. n. 45078/2008 in www.diritto.it (2009); **Logroscino S.** Analisi e considerazioni sul delitto di Frode informatica quale autonoma figura di reato rispetto al delitto di Truffa , www.diritto.it (2011); al quale si rimanda per la interessante tesi relativa al collegamento (rectius: concorso) che esisterebbe tra il phishing con i delitti di Truffa e di Frode informatica**.**

indotto il legislatore – a livello planetario – a dovere affrontare il problema derivante dalla necessità di dovere disciplinare ambiti prima "sconosciuti".
Le ricadute economiche prodotte dalla commissione dei reati c.d. informatici richiede un tempestivo intervento delle autorità statali e comunitarie al fine di regolamentare un settore in progressiva espansione.
La diffusione dell'uso di Internet, la "rete delle reti", richiede risposte certe e sistematiche anche, e soprattutto, in termini di legislazione penale; tali risposte devono essere coordinate a livello di comunità sovra statali atteso che trattasi di un fenomeno non circoscrivibile - proprio per le sue peculiarità – ad un singolo Stato.
Negli anni '80 e '90 dello scorso secolo le macro aree che hanno cominciato ad affrontare il problema in termini sistematici sono state il Nord America e l'Europa.
L'approccio degli Usa[3] è stato quello di partire da una definizione dei termini utilizzati per descrivere tali fattispecie (computer, dispositivo elettronico[4], sistema informatico[5], sistema telematico[6], malware[7], etc.) per poi individuare entro quali ambiti dovere intervenire

---

[3] **Corrias Lucente G.**, *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in *Diritto dell'informazione e dell'informatica*, 1987, **Salvatori I.,** L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cooking, in Rivista Italiana di Diritto e Procedura Penale, (2008). **Romani M. e D. Liokopoulos,** La globalizzazione telematica. Regolamentazione e normativa nel diritto internazionale e comunitario, ed. Giuffrè, (2009)

[4] Si differenzia dal sistema informatico in quanto non consente, di per sé, la organizzazione né la elaborazione dei dati; ci si riferisce, quindi, ad es. ad un video registratore, ecc.

[5] Si caratterizza per consentire di elaborare ed organizzare dei dati, che potranno essere utilizzati per svariate finalità. Tale termine comprende anche il software di base (che consente all'elaboratore di funzionare), quello applicativo (che permette all'utente di scrivere testi, disegnare grafici, ecc.). La **Cass. Sez. VI, 4 ottobre 1999** ha fornito la seguente definizione: *"un sistema informatico o telematico, intendendosi, per quest'ultimo … 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 una 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 combinazioni diverse, e della 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 consente loro di esprimere un particolare significato per l'utente"*.

[6] E' costituito da una pluralità di sistemi informatici tra loro collegati onde consentire la trasmissione e la comunicazione a distanza delle informazioni.

[7] Nella sicurezza informatica il termine **malware** indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer o un sistema informatico su cui viene eseguito. (tratto da: WIKIPEDIA) I virus ed i worms fanno parte di questa tipologia di attacchi con la seguente differenza: mentre i virus per propagarsi richiedono una qualche azione da parte dell'utente, i worms sono programmi autoreplicanti che una volta eseguiti di propagano senza l'intervento di chi li ha creati.

Pur dovendo operare un netto distinguo tra la legislazione federale e quella prodotta dai singoli Stati, occorre dire che l'attenzione è stata posta sui computer e sui sistemi telematici mentre la normativa non ha intaccato l'ambito, residuale, dei sistemi elettronici con modeste capacità di elaborazione.
In Europa, a parte la Gran Bretagna, che ha imboccato negli anni '90 una propria strada individuando una serie di ipotesi di comportamenti delittuosi, l'imput è venuto dalla legislazione comunitaria che ha fatto da pungolo verso gli Stati membri.
In Italia, la stessa legge n. 547 del 23.12.1993, è stata promulgata sulla spinta di una Raccomandazione del Consiglio di Europa del 1989[8].
Il legislatore italiano ha introdotto, quindi, nel codice penale nuove fattispecie incriminatici elaborando una concezione che vedeva lo strumento informatico assurgere al ruolo di mezzo e non di fine.

1 I REATI INFORMATICI

La trafila che ha portato alla promulgazione della Legge n. 547/1993 è stata lunga e laboriosa ed ha visto la partecipazione di molteplici giuristi oltre che di esperti informatici.
Partendo dalle due liste[9], minima e massima, stilate dal Comitato di esperti nominato dal Consiglio d'Europa, nel 1989 fu istituita in Italia – su iniziativa del Ministero della Giustizia - una commissione composta da giuristi ed informatici, con il compito di valutare – in prima battuta – se fosse possibile inserire talune delle fattispecie criminali in preesistenti fattispecie penali oppure se fosse necessario provvedere ad una elaborazione di nuove forme di reato.
La difficoltà di elaborare figure delittuose estremamente specialistiche, legata al difficile contemperamento tra istituti e regole giuridici declinati su fattispecie penali "passate" con concetti "nuovi" relativi all'I.C.T. (Information communication tecnology), alla security aziendale, ha condotto, come esito finale, alla introduzione nel codice penale di figure

[8] Ci riferiamo alla "Reccomandation n. R 899 du Comitè des Ministres aux etats membres sur la criminalità en relation avec l'ordinateur (adoptè pour le Comitè des Ministres le 13 septembre 1989, lors de la 428° reunion des Delegues des Ministres ».

[9] La lista minima contemplava le ipotesi di reato più diffuse: la frode informatica, il sabotaggio informatico, l'accesso non autorizzato, ecc. La lista facoltativa conteneva ipotesi delittuose quali: il reato di alterazione dei dati o dei programmi informatici, il reato di spionaggio informatico, ecc.

nuove di reato, anche se alcune ricalcate – almeno in parte – su vecchi canovacci (vedasi il reato di truffa informatica, ex art. 640 ter c.p. con le sue assonanze con il reato di truffa ex. art. 640 c.p. così come il reato di accesso abusivo a sistemi informatici o telematici di cui all'art. 615 ter c.p.[10]).
E prese di posizione assunte dalla dottrina a momento del varo di tale legge non furono delle più lusinghiere se si pensa che lo sforzo compiuto dal legislatore fu, complessivamente, ritenuto inadeguato a compito che egli si era posto.
E criticità maggiori furono individuate nei seguenti aspetti: pesatura della sanzioni, mancata individuazione del giudice competente, assenza di procedure atte a favorire una cooperazione internazionale, atteso che spesso tali fattispecie delittuose hanno un ambito non circoscrivibile ad un singolo Paese; ecc.
Al termine di tale lavoro fu "partorito" il testo della legge n. 547/93, titolata "modificazioni e integrazioni delle norme del codice penale e del codice di procedura penale in materia di criminalità informatica".

2 IL REATO DI TRUFFA

Poiché il punto di partenza per tentare un inquadramento giuridico del reato di frode informatica[11] è la truffa (Antolisei F., Manuale di diritto

[10] Sull'argomento sia consentito rimandare a **Modesti G.**, **Commento al reato di accesso abusivo ad un sistema informatico, di cui all'art. 615-ter c.p., alla luce delle pronunce giurisprudenziali**, su www.filodiritto.com/diritto/privato/informaticagiuridica/accessoabusivosisinformaticogiurispmodesti.htm; ottobre 2005; e su www.diritto.it/archivio/1/20950.pdf; (2005); **Danneggiamento dei sistemi informatici ed accesso abusivo ai sensi dell'art. 615 ter del c.p. (Corte di Appello di Bologna, Sezione II Penale, Sentenza 30 gennaio 2008, depositata il 27 marzo 2008), in www.diritto.it** e in **Il Nuovo Diritto – Rassegna Giuridica Pratica n. 3-4/2008; La copiatura dei file aziendali non configura il reato di furto ma, forse, quello di accesso abusivo ad un sistema informatico o telematico** (nota a sentenza Cassazione n. 44840/10); in **Quaderni Amministrativi** – Periodico di dottrina, giurisprudenza e legislazione del Centro Studi Amministrativi di Torino n. 1/2011; e **Commento al reato di accesso abusivo ad un sistema informatico, di cui all'art. 615 ter c.p.** alla luce delle recenti sentenze giurisprudenziali; in **RAGIUSAN** – Rassegna giuridica della Sanità, Fascicolo 331/332, a. 2011.

[11] Da una attenta lettura delle fattispecie declinate dagli artt. 615 ter c.p. e 640 c.p. è possibile evincere la esistenza di un rapporto tra le due ipotesi di reato, in quanto 'azione fraudolenta potrebbe essere compiuta da un soggetto non autorizzato ad accedere al sistema informatico o telematico oppure da un soggetto che agisca da 'remoto'. In entrambe le ipotesi l'accesso abusivo è finalizzato a commettere la frode costituendone una condotta necessaria dell'azione fraudolenta.

penale – Parte Speciale I; Ed. Giuffrè) altro non ci resta che esaminare tale figura delittuosa per vagliarne le eventuali assonanze e/o differenze.
Nucleo essenziale del delitto in parola è l'inganno. Il consenso della vittima, carpito fraudolentemente, caratterizza il reato e lo distingue sia dal furto sia dall'appropriazione indebita. Ambedue questi reati presuppongono il dissenso della vittima.
Scopo della incriminazione della truffa è: 1. la protezione del patrimonio e 2. la tutela della libertà del consenso nei negozi patrimoniali.
La fattispecie oggettiva della truffa consta dei seguenti elementi: a) un particolare comportamento del reo (= artificio o raggiro); b) la causazione di un errore, il quale deve a sua volta dare origine a una disposizione patrimoniale; c) un danno di natura patrimoniale derivato dall'inganno con conseguente ingiusto profitto per l'agente o altra persona.
Con il termine "artificio" si intende ogni studiata trasfigurazione del vero, ogni camuffamento della realtà effettuato sia simulando ciò che non esiste sia dissimulando – cioè nascondendo –ciò che esiste.
Il "raggiro" è un avvolgimento ingegnoso di parole destinate a convincere, quindi, una menzogna corredata da ragionamenti idonei a farla scambiare per verità.
In entrambi i casi, il comportamento dell'agente deve determinare un errore, deve essere causa di un inganno.
Requisito tacito della truffa è la disposizione patrimoniale.
Soggetto passivo dell'errore deve essere una persona determinata, mentre l'inganno può essere esercitato anche su persona diversa da quella che subisce il danno.
Il danno ha natura patrimoniale, dovendo consistere in una deminutio patrimonii e al nocumento deve corrispondere un profitto per chi inganna o per altri.
Il delitto di truffa è aggravato, e si procede d'ufficio mentre nelle ipotesi non aggravate il reato è punibile a querela dell'offeso, nei seguenti casi: **1**. se il fatto è commesso a danno dello Stato o di un altro ente pubblico; **2**. se il fatto è commesso col pretesto di fare esonerare taluno dal servizio militare (a significare che l'agente non ha fatto nulla per fare ottenere l'esonero.); **3**. se è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità.

3 IL REATO DI FRODE INFORMATICA

Alla fattispecie classica della truffa, la Legge n. 547/93 ha introdotto una specifica figura di frode patrimoniale che ricalca si a precedente ma presuppone ‘impiego de computer.
Tale nuova fattispecie penale non nasce solo con lo scopo di definire un complesso di sanzioni più incisivo bensì con quello di evitare che determinati comportamenti non assimilabili ictu oculi alla truffa, sic et simpliciter, benché riprovevoli non potessero essere perseguiti.
Un primo problema che il legislatore ha dovuto affrontare fu quello riguardante la distinzione tra due condizioni psicologiche: l‘errore dell’uomo e quello del computer, in relazione all’effettivo destinatario dell’artificio e/o raggiro.
La dottrina più evoluta
La frode informatica è una fattispecie penalmente rilevante di recente istituzione, introdotta dalla legge n. 547/1993 e disciplinata dall’art. 640 ter del c.p[12].; tale figura delittuosa costituisce il reato più importante, in termini quali-quantitativi, del commercio elettronico.
Il delitto di frode informatica è commesso da “*chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati*[13]*, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51,64 euro a 1.032,91 euro”.*

[12] **Art. 640 ter Frode informatica** 1 *Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad essi pertinenti, procura a sè o ad altri un ingiusto profitto con altrui danno è punito con la reclusione da sei mesi a tre anni e con la multa da 51 a 1032 euro. 2. La pena è della reclusione da uno a cinque anni e della multa da 309 a 1549 euro se ricorre una delle circostanze previste dal secondo comma numero 1 dell´articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore di sistema. 3. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un´altra circostanza aggravante*" (*Articolo aggiunto dall’art. 10, L. 23 dicembre 1993, n. 547.)*

[13] **Pomante G.,** op. cit., “tecnicamente, per ‘dato’ si intende un qualsiasi elemento processabile da un sistema informatico, per il quale la rappresentazione della realtà esterna non ha alcun significato ed è quindi assolutamente ininfluente ai fini dell’elaborazione, oltre che ingestibile. E’ quindi individuabile come dato un numero, un colore, un valore, indipendentemente dal contesto in cui è inserito. Proprio detto contesto…consente di trasformare i dati in informazioni”.

Una corretta interpretazione della norma ci consente di affermare che la fattispecie in trattazione, id est: la frode informatica, si realizza attraverso due condotte tra loro alternative: la prima prevede l'alterazione "*in qualsiasi modo*- del … *funzionamento di un sistema informatico o telematico…*»; mentre la seconda è una condotta di intervento "*senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti ….».*
La prima condotta si realizza quando viene alterato il sistema informatico o telematico in modo da indurre in errore l'utente.
La seconda condotta ha per oggetto i dati o i programmi installati nell'hardware del computer che vengono manipolati 'senza diritto' da parte di un soggetto privo sia del consenso del titolare dei dati e che, inoltre, agisce con modalità estranee a quanto stabilito dalla normativa di settore.
La necessità di introdurre tale specifica ipotesi delittuosa è data dalla obiettiva difficoltà di potere regolamentare la frode informatica sulla falsariga della truffa, atteso che un elemento di quest'ultima – la induzione in errore – non poteva essere speso per la prima.
Ciò è quanto emerso, anche, in sede di redazione della relazione ministeriale al disegno di legge sui reati informatici, ove è stato osservato che "*la discussa compatibilità del reato di truffa in caso di analogo illecito informatico, in particolare per l'aspetto attinente all'induzione in errore, impone per detto illecito la creazione di una nuova figura di reato, nella quale la comune condotta di artificio o raggiro è più specificamente integrata dall'alterazione di sistemi informatici o dall'abusivo intervento con ogni mezzo effettuato su dati, informazioni o programmi contenuti in un sistema anche telematico*".
In merito alla possibilità, in linea teorica, di induzione in errore di un elaboratore elettronico rileva una divergente "visione" da parte della dottrina meno aperta alle problematiche sorte con i "computer crimes" e la giurisprudenza.
La dottrina tradizionale, infatti, partendo dal concetto che la induzione in errore deve essere rivolta comunque ad una persona fisica, riteneva che fosse impossibile, quindi, che ad essere indotto in errore potesse essere un computer.
La giurisprudenza, invece, ha affrontato tale nodo allargando il proprio campo visivo ed arrivando ad affermare che l'induzione in errore, nel caso di frode informatica, attenesse non al computer sic et simpliciter bensì ai

soggetti preposti al controllo del sistema informatico o telematico il cui comportamento era stato alterato.
Le condotte fraudolenti poste in essere attraverso tale reato sono tre:

1. alterazione del funzionamento del sistema informatico o telematico, mediante una modifica del regolare svolgimento di un processo di elaborazione o di trasmissione dati; la alterazione provoca i suoi effetti materiali sul sistema informatico o telematico.
2. intervento, senza diritto, con qualsiasi modalità, su dati, informazioni o programmi contenuti nel sistema, e pertanto ogni forma di interferenza diversa dall'alterazione del funzionamento del sistema. L'intervento senza diritto ha per oggetto i dati, le informazioni o i programmi[14]. Solitamente questa seconda condotta rappresenta la modalità attraverso cui viene realizzata la alterazione del sistema informatico.
3. intervento sulle informazioni, ovvero sulle correlazioni fra i dati contenuti in un elaboratore o in un sistema.

La alterazione può cadere sia sul programma, facendo compiere al computer operazioni in modo diverso da quelle programmate (ad es. cambiando la funzione dei tasti di addizione e/o di sottrazione), così come può avere ad oggetto le informazioni contenute nel sistema informatico. Oggetto della alterazione resta, comunque, il dato.
In entrambi i casi, comunque, il bene giuridico offeso è il patrimonio, di qui la collocazione del delitto di frode informatica tra i reati contro il patrimonio.
L'evento si realizza con il danno patrimoniale altrui e l'ingiusto profitto dell'agente o di un terzo.
L'intervento senza diritto a cui fa menzione il legislatore nel primo comma dell'art. 640 ter c.p si verifica quando l'agente non è autorizzato – né da una legge né dal titolare – ad eseguire quella attività sul sistema informatico.
Il delitto di frode informatica si consuma allorché l'agente procura a sé o ad altri un ingiusto profitto con altrui danno; ciò vuol dire che non si tiene conto né del luogo ove si è verificato l'evento informatico né del momento in cui risulti posta in essere l'alterazione o l'intervento senza diritto sul sistema informatico o telematico.

[14] Si pensi all'inserimento in un elenco dei fruitori di una elargizione da parte di un ente pubblico di nominativi di persone non aventi diritto; oppure, l'inserimento nel programma di un istituto di credito di un programma in grado di spostare somme di denaro da un conto all'altro, ecc.

Il reato risulta commesso, quindi, nel luogo ove l'agente consegue la concreta disponibilità del bene con l'effettivo altrui danno rappresentato dalla perdita di quel dato bene da parte della vittima della condotta criminosa.
Il profitto in questione attiene alla effettiva verificazione di una deminutio patrimonii, ciò consente di classificare tale reato tra quelli di danno, in quanto la condotta criminosa comporta la effettiva lesione del bene tutelato.
Alla stregua della truffa, la frode informatica richiede il dolo generico, cioè la coscienza e la volontà di realizzare il fatto tipico che, per l'appunto, consiste nell'ottenere o nel procurare un ingiusto profitto con altrui danno.

3.1 ALCUNE IPOTESI DI FRODE INFORMATICA: PHISHING, DIALER, ECC

Il phishing è una forma di truffa via Internet con la quale gli aggressori cercano di ingannare gli utenti spingendoli a divulgare informazioni personali sensibili oppure dati finanziari, ecc.[15].
Tale truffa solitamente ha come campo di azione le banche e l'e-commerce e può essere perpetrata in due modalità:

a. l'utilizzo di tecniche di "Social Engineering"[16], mediante l'invio di una pagina web, che in realtà è una copia di quella originale, nella quale l'utente deve inserire i propri dati; (un caso eclatante di phishing è l'attacco rivolto negli ultimi anni ai clienti di Pay Pal).
b. con l'aiuto della tecnologia, allorché si inserisce nel sistema operativo un trojan (Il trojan è un programma che sotto forma di applicazione può introdurre un virus oppure un keylogger) che può includere una Keylogger[17]. Quando l'utente visita il sito bancario o un sito per la vendita per corrispondenza, la Keylogger si attiva e registra tutti i numeri e le lettere digitate sulla tastiera.

[15] **Flor R.,** Phishing, identità theft e identità abuse. Le prospettive applicative del diritto penale vigente, in Riv. It. Dir. Proc. Pen. (2007); Frodi identitarie e diritto penale, www.penale.it (2008).
[16] Si tratta di tecniche definite di "ingegneria sociale", "*basate su processi cognitivi di influenzamento, inganno e manipolazione psicologica finalizzate all'ottenimento di informazioni riservate o dati sensibili"*da ASSOSECURITY, La dimensione psicologica nella sicurezza informatica: un approccio cognitivo.(2011)
[17] Il Keylogger è un programma che, oltre registrare le battute fatte sulla tastiera, esegue anche delle istantanee dello schermo per mostrare a chi ricorre a tale frode con quali finestre l'utente ha lavorato. Cattura, inoltre, anche informazioni sull'uso di Internet.

Questa tecnica solitamente prevede e-mail fraudolente e siti web che si fingono legittimi.
Gli utenti vengono così spinti a rispondere poiché non sono in grado di controllare l'autenticità dei messaggi o dei siti web.
Esistono, quindi, rischi elevati di furti di dati, di identità personali e di perdite finanziarie causate da transazioni fraudolente[18].
Un altro caso di frode informatica si realizza attraverso i "dialer"[19] (Dialer, dall'inglese "to dial", significa che una volta composto un numero telefonico il modem del proprio provider viene disconnesso, fraudolentemente, per creare un collegamento ad un altro provider che utilizza una connessione ad elevata tariffazione.) Il tutto si svolge all'insaputa del navigatore che si accorge della truffa allorché gli arriva la bolletta telefonica!
Il dialer arriva solitamente visitando i siti che offrono la possibilità di scaricare gratuitamente programmi, suonerie, filmati pornografici, ecc.
Tale forma di truffa informatica può realizzarsi anche attraverso l'uso dei telefonini; a volte, messaggi indicanti premi da ritirare telefonando ad un certo numero che comincia con 899, sono in realtà casi di dialer.
Ulteriore, ma non ultima, ipotesi di frode informatica, attinente all'alterazione della componente hardware di un sistema informatico o telematico, riguarda il caso di chi inserisce un chip in grado di dare vita ad un traffico telefonico non reale ma fittizio, che avviene all'insaputa dell'utente.

3.2 LE CIRCOSTANZE AGGRAVANTI

Le circostanze aggravanti del delitto di frode informatica sono indicate nel secondo comma dell'art. 640- ter del c.p. nel quale si fa riferimento alle aggravanti di cui al secondo comma dell'art. 640 in tema di truffa. E' stata però aggiunta una specifica circostanza aggravante che è riferita alla commissione del reato in qualità di operatore di sistema[20].

---

[18] *"L'uso di queste informazioni nella strutturazione di attacchi di phishing…,aumenta notevolmente la possibilità di strutturare un contatto credibile e di sfruttare al meglio una più ampia gamma di vulnerabilità di natura sociale."* Cfr. ASSOSECURITY, op. cit.

[19] La maggioranza di programmi *dialer* sono creati per connettersi a numeri a tariffazione speciale, ad insaputa dell'utente. Solo una frazione limitata di questi dispositivi contiene l'indicazione corretta e visibile del costo, mentre la maggior parte dei dialer impostati per connettersi a numeri a tariffazione speciale utilizza metodi illegali, rientrando così nel reato di truffa. (wikepedia)

[20] Su questa specifica figura sia consentito rimandare a Modesti G., **Il ruolo dell'Amministratore di Sistema (La sicurezza nel trattamento dei dati personali in ambito sanitario)** in **Panorama**

Le circostanze sono, le seguenti:

1. se la truffa è commessa a danno dello Stato o di un altro ente pubblico o col pretesto di fare esonerare taluno dal servizio militare[21];
2. se la truffa è commessa ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità;
3. se la truffa è commessa per il conseguimento di erogazioni pubbliche (contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, concesse o erogate da parte dello Stato, di altri enti pubblici o delle Comunità Europee).
4. se la truffa è commessa con abuso della qualità di operatore di sistema. Da rilevare che tale circostanza aggravante è prevista anche per il delitto di cui all'art. 615 ter del c.p. "Accesso abusivo ad un sistema informatico o telematico". In merito alla definizione di operatore di sistema ci sembra che tale figura attenga sia a chi, professionalmente, opera sul sistema, quindi: programmatore, sistemista, analista, ecc, sia chi, in base alla propria posizione nell'organizzazione del lavoro ha il potere di intervenire - in maniera diretta o indiretta – sui dati o sui programmi. Tale circostanza aggravante è da valutare attentamente solo se si pensi che la maggior parte dei crimini informatici arriva non dall'esterno della struttura ma dal suo interno[22]!

---

della Sanità, n. 7 del 23 febbraio 2009; L'Amministratore di Sistema e le problematiche relative alla sua disciplina in ambito aziendale; in **www.bancamatica.it;** in **Quaderni di management**, n. 43 , gennaio-febbraio 2010, E.G.V. Edizioni; e in **e-Health care**, a. 2, n. 1, Gen – Feb 2010.

[21] Vista la poco o nulla attinenza della truffa finalizzata a fare esonerare taluno dal servizio militare con il reato di frode informatica, era forse il caso di evitare un rimando così "generico" alle circostanze aggravanti desunte da un'altra fattispecie delittuosa!

[22] Su questo specifico aspetto sia consentito rimandare a **Modesti G., Il trattamento dei dati sensibili a livello di azienda: aspetti normativi e di sicurezza** ", su www.diritto.it/articoli_materiali/privacy/diritto_privacy.html; (2005); **La responsabilità oggettiva e lo svolgimento delle attività pericolose ai sensi dell'art. 2050 codice civile, con particolare riferimento al trattamento dei dati personali alla luce del decreto legislativo n. 196/2003,** su **www.diritto.it ;** e su **www.dirittosuweb.com; (giugno 2006).** Per un approccio al tema della sicurezza informatica focalizzato sul ruolo giocato dall'individuo, quale soggetto capace con il proprio operato di scardinare le più efficienti policy di sicurezza aziendale, si rimanda al testo curato da ASSOSECURITY, op. cit.

In presenza di una circostanza aggravante il reato è perseguibile d'ufficio e la pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1549 euro.

4 LA GIURISPRUDENZA.

La Cassazione penale, Sezione VI, sentenza del 4 ottobre 1999, n. 3065 apre dei grandi 'squarci' sul reato di frode informatica[23], in quanto ci consente di acquisirne una prima importante definizione che si aggiunge a quella fornita da Legislatore, integrandola.

"*Il reato di frode informatica…ha la medesima struttura, e quindi i medesimi elementi costitutivi, della truffa…, dalla quale si distingue solamente perché l'attività fraudolenta della gente investe non la persona* (soggetto passivo), *bensì il sistema informatico* (significativa è la mancanza del requisito della 'induzione in errore') *che gli perviene: elemento, questo, che sembra anche costituire la ragione per la quale il legislatore ha ritenuto di farne un reato autonomo*".

A tale proposito la Cassazione ha fatto riferimento, e non poteva essere altrimenti, alla legge 547/93, che – lo ribadiamo - ha introdotto in Italia la disciplina dei crimini c.d. informatici e che ha collocato il delitto di frode informatica tra i delitti contro il patrimonio.

"*L'elaborazione giurisprudenziale relativa alla truffa – che si attaglia…anche al reato di frode informatica – è pervenuta alle conclusioni che il reato si consuma nel momento in cui l'agente consegue l'ingiusto profitto, con correlativo danno patrimoniale altrui, e che il carattere dell'ingiustizia è attribuito al profitto per il fatto di essere stato realizzato sine jure, tanto che l'arricchimento in cui esso si risolve, risulta conseguito sine causa*".

---

[23] **Sitografia**: http://www.ildirittoamministrativo.it/altri-approfondimenti/giurisprudenza-penale/index.php?anno=2009; http://www.penale.it/page.asp?mode=1&IDPag=94; http://www.dirittoeprocesso.com/index.php?option=com_content&view=section&id=10&Itemid=28 ; http://www.altalex.com/index.php?idnot=16607 ; http://www.iureconsult.com/areeatema/informatica/frode_informatica_e_accesso_abusivo_a_sistema/index.htm ; http://computerlaw.wordpress.com/about/; www.compliancenet.it/documenti/tesi-alessandra-paolella-2011-rici; www.francoangeli.it/Area_PDFDemo/1360.30_demo.pdf; http://www.iso27001security.com/html/others.html; http://www.enisa.eu/doc/pdf/deliverables/WGRARM/ENISA_RM-__Deliverable2-Final-Version-v1.0-2006-03-30.pdf; http://www.bpmn.org; http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2; http://www.sans.org/whatworks; http://www.isecom.org/;

Una successiva decisione ci permette di determinare l'ambito del reato in trattazione allorchè afferma che **"***per la configurabilità del delitto di frode informatica di cui all'articolo 640 ter C.p., era richiesta l'alterazione del funzionamento ovvero l'intervento su dati e programmi del sistema informatico, con conseguente arbitraria modificazione dello stesso allo scopo di profitto*"[24]. **Corte di Cassazione, Sezione II Penale, 10 luglio 2003 (dep. 31 luglio 2003), n. 32440**

Nella stessa direzione va una sentenza dell'anno successivo in cui si è ribadito che *«(omissis) per la giurisprudenza di questa Corte, il reato di frode informatica - che postula necessariamente la manipolazione del sistema - presenta la medesima struttura e gli stessi elementi costitutivi della truffa, con l'unica differenza che non viene indotto in errore la persona del soggetto passivo, ma l'attività fraudolenta dell'agente investe il sistema informatico riferibile al suddetto (omissis).* **Cass. pen. 5 febbraio 2004, n. 4576, *Giur. it.*, 2004,**

All'interno di una lunga teoria di decisioni adottate dalla Suprema Corte negli anni a venire che consentono allo studioso di potere parlare di un tracciato giurisprudenziale ormai consolidato, va citata **Cass. pen. 26 febbraio 2009, n. 8755**, la quale nel ribadire la esattezza della definizione sopra riportata, afferma che tale fattispecie costituisce una ipotesi specifica della truffa, con conseguente possibilità di estendere alla prima gli schemi e aggravanti che tipizzano quest'ultimo reato.

Tra le due fattispecie vi sarebbe un rapporto di specialità reciproca che esclude ogni possibilità di concorso.

Ciò significa che quando il reato di frode informatica viene commesso non solo con abuso della qualità di operatore di sistema, ma anche in pregiudizio dello Stato o di altra Pubblica Amministrazione, trova applicazione la fattispecie di cui al comma 2 dell'art. 640 c.p. e le circostanze aggravanti non sono da intendersi alternative ma integrative della stessa ratio legis.

Una recente sentenza, del giudice di legittimità, contiene una interessante precisazione sia in merito alla autonomia del delitto di Frode informatica rispetto a quello di Truffa: "*E' … indubbio … che la fattispecie di cui*

[24] "La tutela di cui agli articoli 420, 635-bis e 640-ter va estesa anche ai programmi, informazioni e dati archiviati separatamente per ragioni di sicurezza e che hanno lo scopo di consentire, ove del caso, il ripristino del funzionamento del sistema." **Relazione del Disegno di legge n. 2773, presentato dal Ministro di Grazia e Giustizia – Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica (XI Legislatura)**

all'art. 640 ter integri senz'atro un'autonoma figura di reato, a differenza di quanto si è invece ritenuto in giurisprudenza a proposito della ipotesi di truffa aggravata per il conseguimento di erogazioni pubbliche, prevista dall'art. 640-bis cod. pen., ormai pacificamente ricondotta nel novero delle circostanze aggravanti rispetto al reato "base" di truffa ex art 640 cod. pen."; sia in relazione alla perimetrazione del bene giuridico oggetto di tutela attraverso tale ipotesi delittuosa: "*Il bene giuridico tutelato dal delitto di frode informatica, non può, dunque, essere iscritto esclusivamente nel perimetro della salvaguardia del patrimonio del danneggiato, come pure la collocazione sistematica lascerebbe presupporre, venendo chiaramente in discorso anche l'esigenza di salvaguardare la regolarità di funzionamento dei sistemi informatici - sempre più capillarmente presenti in tutti i settori più importanti della vita economica, sociale, ed istituzionale del Paese - la tutela della riservatezza dei dati, spesso sensibili, ivi gestiti, e, infine, aspetto non trascurabile, la stessa certezza e speditezza del traffico giuridico fondata sui dati gestiti dai diversi sistemi informatici."* **Cassazione, I sez. Penale, n. 17748/11**
Si tratta, pertanto, di una pluralità di interessi coinvolti tali da connotarne, otre al "*tratto di fattispecie plurioffensiva, anche i connotati di figura del tutto peculiare, e quindi "speciale", nel panorama delle varie ipotesi di "frode" previste dal codice e dalle varie leggi di settore*".

CONCLUSIONI

Ci sembra, quindi, di potere affermare che a distanza di circa venti anni dalla entrata di in vigore della Legge n. 547/93, sia necessario un ripensamento della legge stessa unitamente ad un ripensamento dell'approccio culturale, sociologico e, soprattutto, giuridico da rivolgere al tema del crimine informatico.
A fronte di una evidente difficoltà che colpisce il legislatore penale nell'arduo compito di decifrare la realtà occorre rifarsi ai principi base sanciti dagli articoli 25[25], che sancisce il principio di irretroattività della legge, e 27[26] della Costituzione. Tali principi dovranno rappresentare,

[25] **Art. 25:, comma 2, Cost.** "Nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso".
[26] **Art. 27, commi 1 e 2, Cost.** "1. La responsabilità penale è personale. 2. L'imputato non è considerato colpevole sino alla condanna definitiva".

tanto per il legislatore quanto per il giudice e il giurista, le “categorie” di pensiero da utilizzare in questa affannosa rincorsa a volere/dovere coprire tutte le fattispecie che vengono ad esistenza e che assumono una rilevanza penale.
Va, pertanto, rielaborata a teoria giuridica che è alla base della materia riconoscendo un ruolo strategico a concetto di dato, inteso come informazione con tutto ciò che ne deriva in termini di suo trattamento.
E’ innegabile che alla luce dei progressi della tecnica in campo informatico e dell’utilizzo sempre più massivo degli elaboratori elettronici sia necessario adottare un approccio strategico al problema al fine di sottoporre il diritto penale dell’informatica ad una completa revisione. Tale opera, affinché sia credibile, va compiuta all’interno di una cornice legislativa che abbia come orizzonte la normativa comunitaria. Senza tralasciare, inoltre, di considerare gli aspetti criminologici e psicologici ai quali le nuove scienze attribuiscono sempre maggiore evidenza per la comprensione dei comportamenti penalmente sanzionabili.