DIPARTIMENTO DI GIURISPRUDENZA

TESI DI LAUREA MAGISTRALE A CICLO UNICO

LUISS GUIDO CARLI

LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI GIURISPRUDENZA

A.A. 2014/ 2015

TESI IN INFORMATICA GIURIDICA

Computer crimes: frode informatica e phishing

RELATORE: Prof. Gianluigi Ciacci

CORRELATORE: Prof.ssa Barbara Sargenti

CANDIDATA: Emanuela Caputo

MATR.: 105963

Indice

Capitolo III. Casi pratici di phishing

Introduzione

Oggigiorno la maggior parte delle attività sociali, lavorative, di svago si svolgono anche e sempre di più tramite l'utilizzo di mezzi tecnologici e di internet. Questo ha sicuramente comportato ampie possibilità di crescita per la società, in quanto l'e-commerce, l'e-government, l' home banking, il trading online rendono più efficienti e veloci gli scambi e le comunicazioni, ma, parallelamente, sono aumentate le possibilità che vengano commessi reati c.d. informatici.

Con il presente elaborato si intende trattare ed approfondire una fattispecie di reato "*di nuova concezione*", la frode informatica, a cui è connessa una "*nuova*" attività illecita, il c.d. phishing, volta a carpire informazioni personali tramite svariate modalità fraudolente al fine di commettere illeciti attraverso la rete.

Il primo capitolo sarà interamente dedicato alla trattazione del reato di frode informatica. La prima parte di esso avrà la finalità di introdurre, in linea generale, il fenomeno e di spiegare come, nel tempo, l'ordinamento giuridico italiano si sia uniformato, adeguato e protetto dalla costante evoluzione dei crimini informatici derivante dall'esponenziale crescita dell'uso e abuso della tecnologia in ogni suo aspetto, introducendo il reato di frode informatica. La trattazione proseguirà con l'analisi della fattispecie di reato, con particolare attenzione ai suoi elementi strutturali, per poi passare all'esame del rapporto intercorrente tra questa fattispecie criminosa ed altre figure delittuose, tra cui la truffa, la frode del certificatore, l'accesso abusivo, il danneggiamento informatico, il falso informatico e la falsificazione di carte di pagamento. Infine, verrà effettuata un'analisi del reato in chiave comparatistica,

analizzando le scelte legislative attuate dai vari legislatori stranieri, precisamente quello statunitense, quello tedesco e quello francese, in materia di frode informatica.

Il secondo capitolo sarà incentrato sull'analisi del phishing, ponendo l'attenzione sulla diffusione del fenomeno, sulle modalità dei phishing attack, sulle tipologie esistenti e sulle loro evoluzioni legate allo sviluppo tecnologico. Si spiegherà, infatti, la nascita di nuove tipologie di phishing, quale ad esempio il pharming, l'smshishing, il fast flux, il tabnabbing o il vishing, rinvenendo contestualmente lacune nel nostro ordinamento in merito ad una specifica disciplina giuridica che punisca l'attività di phishing.

Infine, nel terzo capitolo verranno analizzati tre leading case in relazione a condotte di phishing, affrontando il tema dell'inquadramento giuridico delle condotte poste in essere a seconda del caso analizzato.

Capitolo I. La frode informatica

1.1 **La frode informatica: cenni introduttivi**

Il crescente sviluppo della tecnologia e il sempre maggiore utilizzo dei computer in ogni settore delle attività umane hanno comportato la possibilità, sempre crescente, che gli strumenti informatici possano essere oggetto o strumento di attività illecita e hanno, quindi, reso necessario l'intervento del legislatore, sul piano penale, per introdurre nuove fattispecie criminose definite "*computer crimes*" o "*reati informatici*". Tra i reati informatici, peculiare rilevo assume la frode informatica, introdotta nel nostro ordinamento con la legge n. 547/1993[1] e disciplinata dall'art. 640 *ter*, inserito nel Libro II titolo XIII capo II del Codice Penale, tra i *"delitti contro il patrimonio mediante frode*", che mira a reprimere le ipotesi di illecito arricchimento attraverso l'uso fraudolento di un computer. La *ratio* dell'introduzione di questa fattispecie criminosa sta proprio nell'impossibilità di applicare l'ipotesi tradizionale di truffa ai casi di aggressione al patrimonio altrui, a scopo di lucro, mediante manipolazione o utilizzazione in modo fraudolento di processi o sistemi automatizzati di elaborazione, trattamento o trasmissione dati. La fattispecie in esame è appunto collocata, al pari della truffa, da cui si distingue in quanto manca un qualsiasi riferimento ad artifizi e raggiri ed all'induzione in errore, tra i delitti contro il patrimonio mediante frode poiché è riscontrabile una oggettiva idoneità ingannevole dell'azione, universale caratteristica del concetto astratto di frode, attuata attraverso l'alterazione dei sistemi informatici o telematici e la conseguente modifica del corretto

[1] Legge n. 547 del 23 dicembre 1993, G. U. n. 305 del 30 dicembre 1993, "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*".

risultato del processo di elaborazione, con un ingiusto profitto del soggetto agente e un danno per il proprietario del sistema, coerenti con le intenzioni dell'agente di un ingiusto profitto, ma diverse da quelle volute dal proprietario del sistema.

1.2 **Prima e dopo la legge n. 547/1993**

In Italia, prima della legge n. 547 del 1993, i comportamenti illeciti realizzati mediante o aventi ad oggetto il computer, soprattutto il complesso di dati e informazioni contenute nel sistema, potevano assumere rilevanza penale solo in quanto riconducibili ad una figura di reato tradizionale. Nel caso di danneggiamento o di furto di dati o informazioni, era problematico ricondurre tali fattispecie a quelle di danneggiamento *ex* art. 635 c.p. e di furto *ex* art. 624 c.p., essendo difficile affermare la fisicità di dati e informazioni per includerli tra "*i beni materiali*" tutelati dall'art. 635 c.p. ovvero tra le "*cose mobili*" menzionate nell'art. 624 c.p.: inoltre, il più delle volte, il furto veniva realizzato con la duplicazione dei dati, senza cancellazione dell'originale, e, dunque, senza "*spossessamento*" fisico del bene, elemento essenziale del reato. Ciononostante, gran parte della giurisprudenza e della dottrina[2] avevano ritenuto applicabili, a seconda dei casi, l'art. 635 c.p.[3] (danneggiamento), l'art. 392 c.p.[4] (esercizio arbitrario delle proprie ragioni con violenza sulle cose), l'art. 624 c.p. (furto), l'art. 420 c.p.[5] (attentato

[2] Corrias Lucente G., *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in *Diritto dell'informazione e dell'informatica*, 1987, p. 531; Marini G., *Condotte in alterazione del reale aventi ad oggetto nastri ed altri supporti magnetici e diritto penale*, in *Riv. it. dir. proc. pen.*, 1986, p. 381; Pica G., *Diritto penale delle tecnologie informatiche*, 1999, Torino, p. 27.

[3] Cass. Pen., Sez. Un., 9 ottobre - 13 dicembre 1996, n. 1282.

[4] Trib. di Torino, 12 dicembre 1983 (in *Giur. it.*, 1984, II, p. 352): "*Il reato di esercizio arbitrario delle proprie ragioni specificamente si concretizza ricorrendo, tra gli altri, il requisito di violenza sulle cose: il danneggiamento di un programma per elaboratore - precisamente di un bene immateriale, nella specie di opera dell'ingegno - realizza il suddetto requisito di violenza sulle cose*".

[5] Trib. di Firenze, 27 gennaio 1986 (in *Foro it.*, 1986, II, p. 359): "*Costituiscono atti genericamente qualificabili di 'sabotaggio' di un impianto di elaborazione di dati, quelle alterazioni magnetiche che rendono impossibile l'accesso e l'utilizzo delle informazioni memorizzate in dischi, così da risultare in pratica distrutte, anche se il*

ad impianto di pubblica utilità) o anche l'art. 171 della legge n. 633 del 1941[6] sul diritto d'autore.

Per quanto, invece, attiene le truffe a mezzo di computer, già nei primi anni ottanta si erano manifestati comportamenti consistenti nell'alterazione del funzionamento dei sistemi informatici, in particolare quelli bancari, percepiti da tutti come comportamenti gravi ed illeciti, aventi rilevanza penale, verosimilmente configuranti gli estremi di una truffa *ex* art. 640 c.p.. In pratica, però, mancavano gli elementi chiave del delitto di truffa e cioè gli "*artifizi o raggiri*" per indurre taluno in errore, in quanto si trattava di incidere sul funzionamento di un elaboratore, ma, ciononostante, in tali circostanze, in mancanza di una disciplina ad hoc, veniva applicato l'art. 640 c.p.[7].

Queste nuove condotte connesse ad attività svolte mediante l'uso della tecnologia necessitavano, per le loro caratteristiche, sempre più, di una normativa specifica, per evitare che, con l'estensione della normativa applicabile alle figure criminose tradizionali, potesse configurarsi una violazione del principio di tassatività. Inoltre, l'intervento del legislatore era necessario anche per adeguare la legislazione italiana alle direttive impartite da organismi sovranazionali. In particolare, ai fini

---

danno arrecato ai supporti debba considerarsi riparabile (nella specie, pur essendosi accertata la volontaria causazione, mediante l'uso di magneti, di numerose alterazioni e manomissioni di dischi in uso presso l'elaboratore dati del centro di calcolo di un'università, l'imputato è stato prosciolto dall'imputazione di cui all'art. 420 c.p., per mancanza di prove circa la commissione del fatto da parte sua)".

[6] Cass. Pen., Sez. II, n.13166 del 24 novembre 1986.

[7] Trib. di Roma, 20 giugno 1984, "*Testa ed altri*" (in *Dir. Inf.*,1986, p. 166 ss.): caso riguardante l'immissione nell'elaboratore elettronico dell'I.N.P.S. di dati non veritieri relativi a contributi in realtà non versati; si è ritenuto che in tal modo fossero ingannati i dipendenti preposti al controllo del versamento dei contributi e all'esazione degli stessi, e non il computer. E Trib. di Roma, 14 dicembre 1985, "*Manenti ed altri*" (in *Dir. Inf.*,1988, p. 487 ss.): era stata ravvisata la truffa aggravata nel caso di un dipendente bancario che, inserendo falsi dati nell'elaboratore, aveva ottenuto che risultassero come avvenuti per contanti versamenti effettuati mediante assegni, al fine di occultare il maggior rischio assunto con la negoziazione di assegni prima che ne fosse stata confermata la copertura e per procurare il maggior lucro ai correntisti attraverso il riconoscimento della valuta liquida; si è ritenuto che fossero stati ingannati gli organi di controllo della banca e non il sistema di elaborazione.

dell'intervento normativo italiano in materia, ha assunto un ruolo determinante la Raccomandazione "*Sur la criminalitè en relation avec l'ordinateur*" adottata dal Comitato dei Ministri del Consiglio d'Europa il 13 settembre del 1989[8], che, ponendo l'attenzione sul crescente fenomeno della criminalità informatica e sulle sue diverse manifestazione, ha ripartito tutti quei comportamenti percepiti come offese perpetrate attraverso o sulle nuove tecnologie in due gruppi, relativi rispettivamente, alle condotte che gli Stati dovevano necessariamente punire con sanzione penale (c.d. lista minima[9]), ovvero alle condotte, meno gravi, che gli Stati potevano eventualmente punire con sanzione penale (c.d. lista facoltativa[10]).

Dunque, nel 1993, il legislatore italiano è intervenuto con la legge n. 547, recante "*Modificazioni e integrazioni delle norme del codice penale e del codice di procedura penale in materia di criminalità informatica*".

Prima dell'intervento legislativo del '93 poco era stato fatto in materia di repressione dei reati informatici: la legge n. 191/1978[11], che introduceva nel codice penale l'art. 420 contro l'attentato ad impianti di elaborazione dati; la legge n. 121/1981[12] relativa alla prima forma di tutela dei dati archiviati in un sistema informatico; la legge n.

[8] Council of Europe - Recommandation Nº R (89) 9, in *Riv. Trim. dir. pen. econ.*, 1992, p. 378.

[9] Fatti contemplati nella lista minima: frode informatica, falso informatico, danneggiamento dei dati o programmi informatici, sabotaggio informatico, accesso non autorizzato, intercettazione non autorizzata, riproduzione non autorizzata di un programma informatico protetto, riproduzione non autorizzata di una topografia.

[10] Fatti previsti dalla lista facoltativa: alterazione dei dati o dei programmi informatici, spionaggio informatico, utilizzazione non autorizzata di un elaboratore, utilizzazione non autorizzata di un programma informatico protetto.

[11] Legge n. 191 del 18 maggio 1978, G. U. n. 137 del 19 maggio 1978, "*Conversione in legge, con modificazioni, del decreto legge 21 marzo 1978 n. 59 concernente norme penali e processuali per la prevenzione e repressione di gravi reati*".

[12] Legge n. 121 del 1 aprile 1981, G. U. n. 100 del 10 aprile 1981, "*Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*".

197/1991[13] che, all'art. 12 punisce l'indebito utilizzo delle carte di credito; il d. lgs. n. 518/1992[14] che, con l'art. 10, mira a punire, anche se solo genericamente, i reati di "*pirateria informatica*". Ma è con la legge n. 547/1993 che si pongono le basi per una reale lotta al crimine informatico e, con essa, da una parte, vengono inserite nuove fattispecie nel codice penale[15] e, dall'altra, vengono aggiornate alcune tradizionali fattispecie codicistiche[16] al fine di renderle atte a ricomprendere, senza le incertezze del passato, le condotte proprie della fenomenologia informatica. L'estensione normativa del significato di nozioni già presenti nel codice penale, nelle intenzioni del legislatore, era finalizzata a sollevare l'interprete dal compito di verificare se quelle nozioni avessero potuto o meno ricomprendere anche fenomeni informatici e ad evitare interpretazioni analogiche vietate in ambito penale: è stato allora definito, con la l. 547/1993, il "*documento informatico*" (art. 3) ai fini dell'applicazione delle norme sulla falsità in atti, il "*documento*" ai sensi della disposizione dell'art. 621 c.p. (art. 7), la "*corrispondenza*", ricomprendendovi quella "*informatica o telematica ovvero*

[13] La legge n. 197 del 5 luglio 1991, G. U. n. 157 del 6 luglio 1991, "*Conversione in legge, con modificazioni, del decreto legge 3 maggio 1991 n. 143 recante provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio".*

[14] Decreto legislativo n. 518 del 29 dicembre 1992, G. U. n. 306 del 31 dicembre 1992, "*Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore*".

[15] Le nuove fattispecie inserite sono: l'art. 491 *bis* c.p., rubricato *documenti informatici*, collocato nel Libro II, titolo VII, capo III; l'art. 615 *ter* c.p., rubricato *accesso abusivo ad un sistema informatico o telematico*, collocato nel Libro II, titolo XII, capo III, sezione IV; l'art. 615 *quater* c.p., rubricato *detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*, collocato nel Libro II, titolo XII, capo III, sezione IV; l'art. 615*quinquies* c.p. , rubricato *diffusione di apparecchiature,dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*, collocato nel Libro II, titolo XII, capo III, sezione IV; l'art. 617 *quater* c.p., rubricato *intercettazione,impedimento o interruzione illecita di comunicazioni informatiche o telematiche*, collocato nel Libro II, titolo XII, capo III, sezione V; l'art. 617 *quinquies* c.p., rubricato *installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*, collocato nel Libro II, titolo XII, capo III, sezione V; l'art. 617 *sexies* c.p., rubricato *falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*, collocato nel Libro II, titolo XII, capo III, sezione V; l'art. 635 *bis* c.p., rubricato *danneggiamento di sistemi informatici o telematici*, collocato nel Libro II, titolo XIII, capo I; l'art. 640 *ter* c.p., rubricato *frode informatica*, collocato nel Libro II, titolo XIII, capo II.

[16] Le fattispecie tradizionali che vengono aggiornate sono: l'art. 392 c.p., rubricato *esercizio arbitrario delle proprie ragioni con violenza sulle cose*, collocato nel Libro II, titolo III, capo III; l'art. 420 c.p., rubricato *attentato a impianti di pubblica utilità*, collocato nel Libro II, titolo V; l'art. 621 c.p. , rubricato *rivelazione del contenuto di documenti segreti*, collocato nel Libro II, titolo XII, capo III, sezione V; l'art. 623 *bis* c.p., rubricato *altre comunicazioni e conversazioni*, collocato nel Libro II, titolo XII, capo III, sezione V.

effettuata con ogni altra forma di comunicazione a distanza" (art. 5), o la "*violenza sulle cose*", quale condotta che può ricadere anche su un programma informatico o sul funzionamento di un sistema informatico o telematico (art. 1). Occorre, però, osservare che il legislatore se, da un lato, ha disciplinato la materia anche attraverso l'introduzione di nuove definizioni giuridiche, dall'altro non ha previsto definizioni di ordine tecnico, lasciando alla dottrina e alla giurisprudenza il compito di dare una definizione a concetti quali "*sistema informatico o telematico*", "*dati*", "*informazioni*", "*programma*", o "*operatore di sistema*". I nuovi illeciti introdotti con la legge n. 547/1993 corrispondono alle figure rientranti in entrambi i gruppi indicati nella Raccomandazione del Consiglio d'Europa del 1989, che dunque hanno trovato una soluzione normativa di carattere penale, salvo la "*riproduzione non autorizzata di una topografia*", per la quale, ad oggi, sono previste solo sanzioni amministrative[17] e "*l'uso non autorizzato di un elaboratore*" che, al pari del "*furto*" di dati, può trovare tutela, anche se solo in via indiretta, attraverso la norma sull'accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.).

Il legislatore italiano, nel redigere la legge del '93, ha avuto la possibilità di seguire l'esperienza statunitense degli anni '80, adottando una legge speciale che disciplinasse in modo organico l'intera materia dei reati informatici[18], ma ha preferito modificare ed integrare l'impianto del codice penale inserendovi, in punti diversi, le nuove figure criminose. Le ragioni di tale soluzione normativa sono legate, da un lato, alla volontà di evitare di introdurre l'ennesima legge speciale, e dall'altro, alla considerazione che

[17] Legge n. 70 del 21 febbraio 1989 ("*Norme per la tutela giuridica delle topografie e dei prodotti a semiconduttori*").
[18] Frosini V., *Introduzione*, in Borruso R., Buonomo G., Corasaniti G., D'Aietti G., *Profili penali dell'informatica*, Milano, 1994, p. XIII s..

le condotte da incriminare non sono configurabili come aggressioni ad un nuovo oggetto unitario, ma nuove forme di aggressione a beni giuridici già oggetto di tutela in diverse norme del codice penale[19]. Parte della dottrina[20], tuttavia, ha sostenuto che dalle nuove tecnologie sono scaturiti nuovi beni giuridici cui sono attribuite diverse denominazioni e che sarebbe stato, quindi, necessario un trattamento autonomo, anche in ambito codicistico. Infatti, l'informatica costituisce una tecnologia innovativa che tende a penetrare in ogni settore dell'attività umana prospettando così, da un lato, nuovi beni giuridici da tutelare anche penalmente ma, dall'altro e principalmente, nuovi strumenti e forme di aggressione ai beni già tutelati dal sistema penale. Il settore dell'informatica è, inoltre, in continua evoluzione e un intervento normativo in tale settore dovrebbe sempre prevedere meccanismi di tempestivo adeguamento della normativa a tali cambiamenti. Se così non fosse potrebbero venirsi a creare problemi riguardanti, da un lato, l'estensione di concetti tradizionali ad ipotesi sempre diverse, e dall'altro, la messa in discussione della compatibilità logico-giuridica[21] della struttura e della modalità esecutiva delle condotte.

La tutela contro le aggressioni informatiche è stata, poi, ulteriormente rafforzata con la legge 18 marzo 2008 n. 48, di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica (cybercrime), svoltasi a Budapest il 21 novembre 2001. Con la Convenzione per la lotta contro la criminalità informatica era stata ribadita l'esigenza di prevedere, nelle legislazioni interne, norme penali idonee a sanzionare determinate condotte legate all'uso delle tecnologie informatiche e telematiche,

[19] Pica G., *Diritto penale delle tecnologie informatiche*, 1999, Torino, p. 31 e ss.
[20] Militello V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ.*, 1992, p. 372 s.; Sieber V., *La tutela penale dell'informazione*, in *Riv. Trim. dir. pen. econ.*, 1992, p. 492.
[21] Picotti L., *Commento all'art. 5 della legge n. 547 del 1993*, in *Legislazione penale*, 1996, p. 109.

disposizioni processuali idonee a rendere effettivamente punibili tali condotte, nonché previsioni normative che contemplassero una responsabilità delle aziende per reati informatici commessi al loro interno, nella convinzione della necessità di armonizzazione delle legislazioni dei vari Paesi facenti parte dell'Unione Europea, essendo la criminalità informatica ormai di carattere transnazionale. Nel recepire tali indicazioni, la legge n. 48/2008 è intervenuta sia sul piano sostanziale, con l'inserimento di altre fattispecie a tutela del patrimonio, della fede pubblica e della sicurezza e riservatezza informatica nel codice penale[22] e con l'aggiornamento di alcune fattispecie già esistenti[23], sia sul piano processuale, in materia di raccolta delle fonti di prova, ispezioni, perquisizioni, sequestri, con modifiche del codice di procedura penale[24], sia sul piano della rilevanza penale di alcune condotte in ambito aziendale, con estensione della disciplina della legge n. 231/2001[25] sulla responsabilità amministrativa delle società e degli enti dipendente da reato ai delitti informatici, se commessi da vertici o dipendenti nell'interesse o a vantaggio dell'ente.

[22] Le nuove fattispecie inserite sono: l'art. 495 *bis* c.p., rubricato *falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri*, collocato nel Libro II, titolo VII, capo IV; l'art. 635 *ter* c.p., rubricato *danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*, collocato nel Libro II, titolo XIII, capo I; l'art. 635 *quater* c.p., rubricato *danneggiamento di sistemi informatici o telematici*, collocato nel Libro II, titolo XIII, capo I; l'art. 635 *quinquies* c.p., rubricato *danneggiamento di sistemi informatici o telematici di pubblica utilità*, collocato nel Libro II, titolo XIII, capo I; l'art. 640 *quinquies* c.p., rubricato *frode informatica del soggetto che presta servizi di certificazione di firma elettronica*, collocato nel Libro II, titolo XIII, capo II.

[23] Le fattispecie modificate sono: l'art. 420 c.p., rubricato *attentato a impianti di pubblica utilità*, collocato nel Libro II, titolo V; l'art. 491 *bis* c.p., rubricato *documenti informatici*, collocato nel Libro II, titolo VII, capo III *;* l'art. 615 *quinquies* c.p., rubricato *diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*, collocato nel Libro II, titolo XII, capo III, sezione IV*;* l'art. 635 *bis* c.p., rubricato *danneggiamento di informazioni,dati e programmi informatici*, collocato nel Libro II, titolo XIII, capo I.

[24] E'stato modificato l'art. 51 del c.p.p.. Sono state apportate modifiche al Libro III, titolo III, del codice di procedura penale, agli artt. 244, 247, 248, 254, 256, 259, 260, ed è stato inserito l'art. 254 *bis*; sono state apportate modifiche al Libro V, titolo IV, del codice di procedura penale, agli artt. 352, 353 e 354.

[25] E'stato inserito l'art. 24 *bis*, rubricato "*Delitti informatici e trattamento illecito di dati"*.

Nel febbraio del 2012, il legislatore nazionale ha emanato un altro provvedimento, la legge n. 12/2012[26], recante norme in materia di misure per il contrasto ai fenomeni di criminalità informatica. Tale legge, composta da soli tre articoli, ha previsto, innanzitutto, un'importante modifica dell'art. 240 c.p., con l'introduzione della confisca dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione di alcuni reati informatici[27]. Inoltre, ha introdotto l'art. 86 *bis* del d. lgs. n. 271/1989, prevedendo che i beni e gli strumenti informatici o telematici oggetto di sequestro che, a seguito di analisi tecnica forense, risultino essere stati in tutto o in parte utilizzati per la commissione di alcuni reati[28] sono affidati dall'autorità giudiziaria in custodia giudiziale con facoltà d'uso, salvo che vi ostino esigenze processuali, agli organi di polizia che ne facciano richiesta per l'impiego in attività di contrasto ai crimini informatici, ovvero ad altri organi dello Stato per finalità di giustizia. La legge n. 12/2012 ha anche previsto che gli stessi beni e strumenti, ove acquisiti dallo Stato a seguito di procedimento definitivo di confisca, possono essere assegnati alle amministrazioni che ne facciano richiesta e che ne abbiano avuto l' uso ovvero, ove non vi sia stato un precedente affidamento in custodia giudiziale, agli organi di polizia che ne facciano richiesta per l'impiego in attività di contrasto ai crimini informatici o ad altri organi dello Stato per finalità di giustizia. La finalità di tale legge, data l'introduzione della pena accessoria della confisca dei beni collegati all'esecuzione di fatti criminosi, si può ravvisare proprio nell'esigenza di

[26] Legge n. 12 del 15 febbraio 2012, G.U. n. 45 del 23 febbraio 2012, "*Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica*".

[27] Si tratta dei reati di cui agli artt. 615 *ter*, 615 *quater*, 615 *quinquies*, 617 *bis*, 617 *ter*, 617 *quater*, 617 *quinquies*, 617 *sexies*, 635 *bis*, 635 *ter*, 635 *quater*, 635 *quinquies*, 640 *ter* e 640 *quinquies* del codice penale.

[28] Si tratta dei reati di cui agli artt. 473, 474, 615 *ter*, 615 *quater*, 615 *quinquies*, 617 *bis*, 617 *ter*, 617 *quater*, 617 *quinquies*, 617 *sexies*, 635 *bis*, 635 *ter*, 635 *quater*, 635 *quinquies*, 640 *ter* e 640 *quinquies* del codice penale.

evitare che la disponibilità di cose funzionali o conseguenti al reato possa spingere nuovamente il reo a delinquere.

La criminalità informatica è stata contrastata non soltanto tramite provvedimenti di carattere nazionale, ma anche tramite provvedimenti emanati a livello europeo, quale, in particolare, la Decisione Quadro 2005/222/GAI[29], che ha avuto l'obiettivo di ravvicinare le legislazioni penali nazionali degli Stati membri in riferimento agli attacchi informatici, ad oggi sostituita dalla Direttiva 2013/40/EU[30] del Parlamento e del Consiglio,che mira a combattere la criminalità informatica e a promuovere la sicurezza informatica mediante leggi nazionali più incisive, sanzioni penali più severe e una maggiore cooperazione tra le autorità competenti. I reati compiuti a mezzo informatico sono stati e devono continuare ad essere contrastati sia a livello nazionale sia a livello comunitario, cercando di creare una normativa omogenea e comune. Inoltre, è importante coltivare, ai fini di una graduale riduzione del crimine informatico ed in parallelo allo sviluppo coordinato delle normative transnazionali, una nuova cultura informatica, che sappia ben informare e sensibilizzare l'utenza sui vantaggi ma anche sui rischi che è possibile correre attraverso un incauto utilizzo delle nuove tecnologie informatiche e telematiche.

[29] Decisione Quadro 2005/222/GAI del Consiglio del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione; http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2005.069.01.0067.01.ITA

[30] Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio; http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32013L0040

1.3 **Art. 640 *ter* cod. pen.: fattispecie ed oggetto di tutela**

La fattispecie incriminatrice della frode informatica è stata inserita nel codice penale nel Libro II, titolo XIII, capo II, tra i delitti contro il patrimonio mediante frode, dall'art. 10 della legge n. 547 del 1993, all'art. 640 *ter* che punisce, con la reclusione da sei mesi a tre anni e con la multa da 51 a 1032 euro, «*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 esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno*». La pena si aggrava, con la reclusione da uno a cinque anni e con la multa da 309 a 1549 euro, se «*ricorre una delle circostanze previste dal numero 1 del secondo comma dell'articolo 640*[31]*, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema*». Dal 2013, con l'art. 9 del d.l. n. 93[32], così come modificato dalla legge di conversione, la legge n. 119/ 2013[33], è stato aggiunto il terzo comma che punisce, con la reclusione da due a sei anni e con la multa da 600 a 3000 euro, le ipotesi in cui il fatto « *è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*». Lo stesso art. 9 del d.l. n. 93/ 2013 ha modificato l'ultimo comma che recita: «*Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante».*

[31] Le circostanze previste all'art. 640 c.p., rubricato *Truffa*, al secondo comma n. 1 sono *:"fatto commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare*".

[32] D. l. n. 93 del 14 agosto 2013, G. U. n. 191 del 16 agosto 2013, "*Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonche' in tema di protezione civile e di commissariamento delle province*".

[33] Legge n. 119 del 15 ottobre 2013, G. U. n. 242 del 15 ottobre 2013, "*Conversione in legge, con modificazioni, del decreto legge 14 agosto 2013, n. 93, recante disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonchè in tema di protezione civile e di commissariamento delle province*".

Per quanto concerne la fattispecie di cui all'art. 640 *ter* c.p., ci si deve chiedere quale sia il bene giuridico che il legislatore abbia ritenuto meritevole di tutela. In generale, bisogna capire se le fattispecie concernenti i reati informatici tutelino un bene giuridico unitario, inteso come «*intangibilità informatica*»[34] o come «*diritto alla personalità*» in relazione alla libertà informatica.

Il delitto di cui all'art. 640 *ter* c.p. è un tipico reato informatico e, in quanto tale, tutela il regolare funzionamento dei sistemi informatici e telematici, ma il primo obiettivo perseguito da tale fattispecie è quello di punire quei "*comportamenti comunicativi*" che cagionano un danno patrimoniale ed economico, anche attraverso il solo spostamento di informazioni o dati[35].

Tale fattispecie è posta a tutela del patrimonio, inteso come l'insieme di tutte quelle disponibilità finanziarie "*immateriali*" di cui si può disporre anche attraverso un computer[36], e ciò si evince sia dalla sua collocazione nel codice penale tra i delitti contro il patrimonio mediante frode, sia dalla struttura della fattispecie, clonata sulla base di quella della truffa[37].

Dunque, in seguito alla commissione del delitto di frode informatica i danni[38]cagionati dal reo possono essere sicuramente economici, direttamente ricollegabili alla

[34] L'intangibilità informatica può essere definita come «*l'esigenza di non alterare la relazione triadica fra dato della realtà, rispettiva informazione, e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento, ricezione)*», o anche come «*bene immateriale con carattere di diritto reale, ossia di inerenza del diritto al bene che ne rappresenta l'oggetto*».

[35] Pica G., *Internet*, in *Dig. pen*., Aggiornamento, I, Torino, 2007, p. 433 e ss.

[36] Mantovani F., *Diritto penale*, pt. spec., II, *Delitti contro il patrimonio*, III ed., Padova, 2009, p. 210.

[37] Cass. Pen., Sez. II, 24 febbraio 2011, n. 9891, in *DeJure.*

[38] Il danno patrimoniale derivante dalla condotta descritta dalla norma comporta, in primis, una *deminutio patrimonii* subita dal soggetto passivo e, successivamente, una serie di danni "*riflessi*" derivanti dal ristabilimento della situazione *quo ante* del sistema informatico o telematico alterato o derivanti dalla disfunzione del sistema o dalla perdita dei dati. L'individuazione e la qualificazione di tali danni "*riflessi*" è legata al contenuto e alla funzione dei dati, si pensi ad esempio a lesioni della privacy o riservatezza, all'abusiva utilizzazione di strumenti di pagamento, alle violazioni del diritto d'autore, alle violazioni di segreti o alla lesione della segretezza e della libertà della corrispondenza. Quanto alla posta di danno non patrimoniale, è

collocazione della norma tra i delitti contro il patrimonio, ma possono anche essere lesi beni di nuova generazione, quali, ad esempio, la regolarità dei sistemi informatici e la riservatezza informatica[39]. Anche la giurisprudenza di legittimità[40] ha affermato che tra i beni protetti vi sono la riservatezza, la regolarità dei sistemi informatici, il patrimonio altrui e la libertà negoziale del danneggiato. La norma sanziona anche le condotte lesive dell'integrità, della riservatezza e del regolare funzionamento del sistema informatico in quanto strumentali ad aggressioni patrimoniali realizzate con la fraudolenta manipolazione dello strumento elettronico.

1.3.1 **Definizione di sistema informatico e telematico e di dati, informazioni e programmi**

Oggetto della condotta della frode informatica sono, oltre ai dati, informazioni e programmi (c.d. software), anche i sistemi informatici o telematici e, pertanto, per inquadrare la portata applicativa dell'art. 640 *ter* c.p., è necessario individuare la nozione e le caratteristiche di dati, informazioni e programmi, nonché del sistema informatico e telematico, anche alla luce dell'interpretazione giurisprudenziale.

I dati sono le informazioni codificate ed interpretabili dal computer; le informazioni sono le notizie che devono essere poste ad oggetto dell'elaborazione tramite computer; i programmi sono i gruppi di istruzioni che servono per far lavorare i computer al fine di realizzare un compito.

Per sistema informatico si intende ogni sistema di trattamento automatico dell'informazione attraverso mezzi elettronici e possono ricomprendersi in tale

pacifico che sussista il risarcimento derivante da reato secondo quanto prescritto dall'art. 185 c.p., la cui liquidazione è rimessa in via equitativa al giudice.

[39] Campeis C., *Frode informatica*, in AA. VV. (a cura di), *Reato e danno*, Milano, Giuffrè, 2014, p. 923.

[40] Cass. Pen., Sez. V, 24 novembre 2003, n. 4576.

nozione i sistemi che utilizzano bande magnetiche, microchip, cd o lettori ottici, apparecchiature di input e output. La legge 23 dicembre 1993, n. 547 non ha enunciato una definizione di «*sistema informatico*» e, quindi, in assenza di una classificazione legislativa, è stata la giurisprudenza[41] a definirlo come una "*pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche*". Il sistema informatico deve presentare tre essenziali caratteristiche: la registrazione o memorizzazione, per mezzo di impulsi elettronici e su supporti adeguati, di dati rappresentati mediante simboli numerici in combinazioni diverse; l'elaborazione automatica da parte della macchina dei dati così registrati o memorizzati; l'organizzazione di tali dati secondo una logica che consenta loro di esprimere un particolare significato per l'utente (utilità)[42]. Esso è un apparato elettronico in grado di elaborare, in formato digitale, un elevato numero di dati o di informazioni opportunamente organizzato, capace di restituire un altro insieme di elementi codificati in maniera leggibile, grazie ad un programma in grado di far cambiare lo stato interno dell'apparato e di mutarne all'occorrenza il risultato. L'attitudine della macchina ad organizzare ed elaborare i dati sulla base di un programma costituisce l'elemento essenziale che consente di distinguere ciò che è «*informatico*» da ciò che è invece solamente «*elettronico*», in modo da evitare che qualsiasi apparato tecnologicamente avanzato possa essere considerato un sistema informatico.

Il sistema telematico è, invece, l'insieme di sistemi informatici connessi tra loro attraverso una rete elettrica ovvero mediante un sistema di trasmissione via etere al

[41] Cass. Pen., Sez. VI, 4 ottobre 1999, n. 3065, De Vecchis, in *Cass. pen*., 2001, p. 481.

[42] Stalla G., *L'accesso abusivo ad un sistema informatico o telematico,* http://www.penale.it/commenti/stalla_01.htm

fine di trasmettere e ricevere informazioni, come ad esempio internet. Il collegamento tra più sistemi informatici, per formare quello telematico, deve soddisfare due requisiti essenziali, quali una connessione avente carattere stabile o permanente e uno scambio di informazioni e una connessione tra elaboratori distanti come 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, 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 ad 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 sicurezza 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[43].

1.3.2 **Condotte tipiche**

La fattispecie di frode informatica prevede in via alternativa le due condotte di "*alterazione, in qualsiasi modo, del funzionamento di un sistema informatico o*

[43] Valastro A., *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. e proc. pen*., 1999, 3, p. 989; Librando V., *La tutela della riservatezza nello sviluppo tecnologico*, in *Dir. inf. e informatica*, 1987, p. 487.

telematico" e l'attuazione "*dell'intervento, senza diritto, con qualsiasi modalità, su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti*". L'art. 640 *ter* del codice penale è una norma che presenta una struttura a forma libera, prevedendo due fattispecie alternative di condotta, come si evince dalle espressioni "*in qualsiasi modo*" e "*con qualsiasi modalità*"[44]. Dalla lettura della rubrica di tale articolo, sorge il dubbio se il termine frode possa sottintendere il fatto che, anche in tale fattispecie criminosa, si richieda, come per la truffa, l'induzione in errore di un soggetto attraverso artifizi o raggiri, ma l'evidenza letterale della norma smentisce tale ipotesi in quanto non è presente alcun riferimento all'induzione in errore ed, anzi, il legislatore, ben conscio dell'impossibilità di trarre in inganno una macchina, ha delineato il verificarsi del delitto di frode informatica semplicemente in conseguenza di una delle due condotte alternative descritte. Ai fini della rilevanza penale della condotta ciò che risulta determinante è che essa incida, in qualsiasi modo, sui meccanismi fisici e logici di funzionamento di un sistema informatico o telematico, con un ingiusto profitto e l'altrui danno.

La prima delle due condotte, quella di alterazione, investe le modalità di funzionamento del sistema informatico o telematico, potendo consistere sia in una manomissione delle componenti fisiche del sistema (hardware), per rendere impossibile o difficoltoso il suo corretto funzionamento, sia in un'artificiosa manipolazione del complesso delle istruzioni che ne consentono il funzionamento (software), in modo che l'output sia reso impossibile o viziato nel contenuto. Ciò potrebbe, ad esempio, accadere nel caso di alterazione della modalità di log-in e log-

[44] Dello Iacono A., *Articolo 640 ter: truffa o furto? La Frode informatica e il «modello 640»*, in *Temi Romana*, 1996, p. 597.

out del sistema da un determinato sito internet, di tal che, ove il computer rimanesse collegato alla rete e al sito nonostante la convinzione dell'utilizzatore di aver effettuato il log-out, ciò comporterebbe un ingiusto guadagno per il gestore del sito e, specularmente, il danno economico in capo all'utente. Nel caso dell'alterazione di un sistema informatico o telematico non è rilevante se chi agisce è legittimato o meno a farlo e, inoltre, l'intervento manipolativo può anche essere tale da modificare gli scopi cui il sistema informatico è destinato. Il reato ricorre anche quando, pur nel rispetto della destinazione del sistema, vengano manipolati i contenuti dello stesso. Rilevano sia le modificazioni delle componenti fisiche riguardanti l'unità centrale, l'architettura di sistema e i collegamenti interni, in modo da destinare gli impianti a scopi diversi da quelli per cui sono stati programmati, sia ipotesi di inserimento e attivazione di altre schede o periferiche tali da causare anomalie nel funzionamento[45].

La seconda condotta alternativa è quella dell'intervento abusivo su dati, informazioni e programmi e il suo disvalore si incentra proprio sulla circostanza che colui che ha agito lo ha fatto "*senza diritto*". L'intervento, per configurare la condotta descritta dalla fattispecie *ex* art. 640 *ter* c.p., deve essere, appunto, "*senza diritto*" e, dunque, non solo senza il consenso necessario del titolare di dati, informazioni e programmi contenuti nel sistema informatico, ma anche abusando di un diritto di cui si è titolari o secondo modalità non consentite da norme giuridiche, né da altre fonti. L'intervento abusivo, elemento di tipicità del fatto, può riguardare sia i dati, le informazioni ed i programmi contenuti in un sistema informatico o telematico, sia quelli "*pertinenti*" ad un siffatto sistema, e cioè tutti quei dati che, pur essendo contenuti in supporti

[45] Campeis C., *Frode informatica*,in AA.VV. (a cura di), *Reato e danno*, Milano, Giuffrè, 2014, p. 920.

materiali esterni (come, ad esempio, i cd, o anche i floppy) sono o input o output e quindi i risultati dell'elaborazione[46]. Non occorre che il sistema informatico o telematico sia altrui, né che lo siano i dati, le informazioni o i programmi, ma risulta necessario che il soggetto operi senza diritto di modificare il funzionamento del sistema e di intervenire su dati, informazioni o programmi. Diversamente, ove il soggetto agente versi nella convinzione di agire con il diritto di effettuare l'intervento, il reato può essere escluso per sussistenza di errore di fatto. Infine, in dottrina[47] ci si è chiesti se le condotte descritte dall'art. 640 *ter* c.p. possano essere commesse in forma omissiva e la risposta sembrerebbe essere positiva solo se, nel caso di specie, vi sia l'obbligo giuridico di impedire l'evento in capo al soggetto agente (posizione di garanzia).

1.3.3 **Elemento soggettivo**

In riferimento all'elemento soggettivo del reato, frode informatica è un delitto doloso, dovendosi escludere, in capo al reo, la rilevanza della colpa e della preterintenzione per l'assenza di un'espressa previsione in tal senso nel testo della norma. Per quanto riguarda il grado della volontà criminosa, la fattispecie prevista dall'art. 640 *ter* c.p. è compatibile, per la natura stessa del reato, tanto con il dolo di proposito, tanto con la premeditazione, ma va, invece, esclusa la compatibilità con il dolo d'impeto, sia per la natura del reato, in quanto la commissione di un delitto come la frode informatica, solitamente, richiede del tempo per l'ideazione e per la predisposizione dei mezzi prodromici al compimento del reato, sia in quanto tale manifestazione del dolo attiene

[46] Pecorella C., *Commento Art. 640 ter c.p.*, in *Codice penale commentato, Artt. 575-734 bis*, a cura di E. Dolcini e G. Marinucci, III ed., Milano, 2011, p. 6417 e ss.
[47] Masi A., *Frodi informatiche e attività bancarie*, in *Riv. Pen. econ.*,1995, p. 428.

tipicamente ai reati contro la persona. Se invece si considera il dolo sulla base del grado di rappresentazione dell'evento, sia il dolo intenzionale che quello diretto possono integrare l'elemento soggettivo del delitto in parola e lo stesso può dirsi in riferimento al dolo indiretto. Sulla compatibilità del delitto in questione con il dolo eventuale, si osserva che proprio lo specifico contesto, quello informatico- virtuale, in cui viene posta in essere la condotta criminosa, suggerisce la conclusione opposta. Infatti, se, ad esempio, si pensa alla condotta di alterazione del sistema informatico e alle scarse possibilità di insuccesso che essa presenta, non si vede come il reo possa rappresentarsi l'esito di tale condotta come solo probabile o, addirittura, meramente possibile, finendo per sostituire alla propria volontà criminosa, la mera accettazione del rischio-reato. Infine, va esclusa la compatibilità dell'art. 640 *ter* con il dolo specifico, in quanto tale norma, nell'omettere qualsiasi riferimento espresso al fine specifico cui è rivolta la condotta criminosa, richiede solamente la sussistenza del dolo generico[48]. Il soggetto attivo, quindi, ha coscienza e volontà di porre in essere l'alterazione del sistema informatico o l'intervento senza diritto su dati e di cagionare, loro tramite, il duplice evento dell'altrui danno e dell'ingiusto profitto. Il dolo, per svolgere una propria funzione selettiva sulla tipicità, si deve ritenere sussistente soltanto se il reo, nel momento in cui ha agito, ha avuto consapevolezza di esercitare il proprio dominio sull'intero processo causale, che inizia con la condotta che cagiona il risultato irregolare e continua con l'ingiusto profitto e l'altrui danno. Non vale ad escludere il dolo l'eventuale errore sulla natura informatica o meno del sistema, o sulla pertinenza dei dati ad un sistema, avendo questi errori, normalmente e salvo casi particolari, i tratti propri degli errori che cadono sulla legge penale e non sul fatto.

[48] Pica G. , *Diritto penale delle tecnologie informatiche*, Torino, 1999, p. 154.

1.3.4 **Momento consumativo e tentativo**

La frode informatica è un tipico reato di evento, in quanto l'alterazione del sistema e l'intervento senza diritto, che comportano l'irregolare processo di elaborazione, possono dirsi in un rapporto di causa-effetto con gli eventi, che la norma individua espressamente nel conseguimento di un ingiusto profitto per sé o per altri e dell'altrui danno. Dunque, per la consumazione di tale delitto, è necessario che il soggetto agente procuri a sé o ad altri un ingiusto profitto e che cagioni ad altri un danno. Per quanto attiene alla nozione di ingiusto profitto, esso, affinchè possa qualificarsi quale ingiusto, deve essere stato ottenuto dal soggetto agente in modo illecito, quindi contrario rispetto all'ordinamento giuridico. L'ingiusto profitto può essere conseguito tanto dall'autore di una delle condotte previste dalla norma, tanto "*da altri*" , soggetti terzi rispetto al reo. Per comprendere la natura del profitto in riferimento al delitto di frode informatica si deve tenere in considerazione la dottrina e la giurisprudenza in riferimento a tale analogo requisito nel delitto di truffa. Il profitto, nella frode informatica così come nella truffa, non necessariamente deve avere natura economica, ben potendo rilevare anche un vantaggio di tipo affettivo o morale[49] e deve avere come diretta conseguenza un danno alla persona offesa dal reato, o meglio al soggetto passivo del reato. Il danno, nella frode informatica, assume i tratti di un vero e proprio secondo evento, che si pone in un rapporto di causa-effetto con il profitto. L'evento dannoso viene scomposto in danno emergente e lucro cessante e, ad oggi, il danno patrimoniale non può essere qualificato solo come la differenza negativa per il soggetto passivo tra il valore del bene da questi corrisposto e quello minore del bene acquisito, ma anche come il conseguimento di qualcosa di diverso da ciò che era

[49] Cass. Pen., Sez. Un., 16 dicembre 1998, n. 24 , Messina, m. 212076.

atteso. Invero, se si muove dalla premessa che la frode informatica tutela direttamente il patrimonio e, soltanto indirettamente, il regolare funzionamento dei sistemi e la c.d. riservatezza informatica, non si può non riconoscere che è proprio il danno patrimoniale subito dalla vittima della frode, quel *quid pluris* che differenzia la frode dagli altri reati informatici, il cui danno si potrebbe anche dire è *in re ipsa*. Ed ancora, le riflessioni sviluppate nell'ambito della truffa in relazione agli elementi dell'ingiusto profitto e dell'altrui danno assumono rilievo per determinare il *locus commissi delicti*, che dovrà essere ravvisato non nel luogo in cui è stata realizzata l'alterazione del funzionamento del sistema informatico, ma in quello in cui il soggetto 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[50]. Il danno, nel delitto di truffa e di conseguenza anche in quello di frode informatica, è stato considerato come una situazione precedente o prodromica alla causazione dell'evento penalmente rilevante. Tuttavia, se così fosse, il delitto di truffa, e conseguentemente anche quello di frode informatica, non sarebbe più considerato come un reato di evento ma di pericolo e, a conferma di ciò, si può osservare come eventuali situazioni prodromiche alla produzione del danno altrui potrebbero avere un'autonoma rilevanza penale ai sensi del combinato disposto degli artt. 56 c.p. (delitto tentato) e 640 o 640 *ter* c.p.. E', dunque, configurabile, per il delitto di frode informatica, anche se di non facile prova[51], il tentativo, che consiste nel porre in essere, da parte del reo, la manipolazione o l'intervento senza diritto, ma senza

[50] Parodi C., *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in *Criminalità informatica*, Sarzana Di S. Ippolito F. (a cura di), in *Diritto e procedura penale*, 1997, p. 1539 e ss.
[51] Masi A., *Frodi informatiche e attività bancarie*, in *Riv. Pen. econ.*,1995, p. 428.

ottenere l'ingiusto profitto e l'altrui danno o atti idonei all'azione criminosa, senza, poi, compierla concretamente.

1.3.5 **Soggetti attivi, circostanze aggravanti e procedibilità**

La frode informatica è un reato comune, può essere commessa da "*chiunque*" e, dunque, qualsiasi persona può essere soggetto attivo di tale reato. Solitamente ad aggredire i sistemi informatici e telematici sono coloro che hanno conoscenze e capacità tecnico-informatiche, definiti hacker e cracker, ma soggetto attivo può essere chiunque ponga in essere le condotte descritte dalla fattispecie criminosa. Se si tratta di un operatore del sistema, il quale agisce con abuso della sua qualità, il delitto è aggravato e si procede d'ufficio.

Le circostanze aggravanti del delitto di frode informatica sono previste dall'art. 640 *ter* ai commi secondo e terzo. Il secondo comma richiama le aggravanti del secondo comma n. 1 dell'art. 640 in tema di truffa, cioè quella del fatto commesso in danno dello «*Stato o di un altro ente pubblico*», e quella del fatto commesso «*col pretesto di far esonerare taluno dal servizio militare*» ed, inoltre, prevede come aggravante specifica la circostanza che il fatto sia commesso con abuso della qualità di operatore del sistema. La dottrina[52] non ha mancato di rilevare che, proprio per la *ratio* della fattispecie di frode informatica, il legislatore avrebbe dovuto elencare in modo esplicito le singole aggravanti, evitando di richiamare le circostanze, come ad esempio quella concernente il pretesto di far esonerare taluno dal servizio militare, che risultano incoerenti con le finalità e la struttura della norma incriminatrice.

[52] Pica G., *Diritto penale delle tecnologie informatiche*, 1999, Torino, p. 158.

La circostanza aggravante dell'abuso della qualità di operatore del sistema è stata dettata da maggiori possibilità materiali di intervenire abusivamente sui dati e i programmi da parte di chi ricopre tale posizione, con una conseguente accentuata vulnerabilità per i dati e un maggiore disvalore dell'offesa così arrecata. Si tratta di una condotta connotata da una maggiore pericolosità per la violazione del dovere di fedeltà nei confronti del titolare o dell'utente del sistema informatico, sia delle persone i cui interessi economici sono gestiti da quel sistema[53]. L'operatore del sistema si viene a trovare, in ragione delle sue funzioni o della sua attività, in un'evidente posizione di vantaggio dal punto di vista attivo, nel senso che la possibilità di accedere al sistema, ad aree riservate dello stesso e di controllarne le operazioni rende più semplice la commissione del reato.

La previsione dell'aggravante in questione, quindi, si giustifica proprio per punire più severamente comportamenti illeciti più facili da porre in essere e per sanzionare il tradimento della fiducia riposta dal titolare in chi professionalmente dovrebbe curarsi del sistema e che, invece, approfitta delle proprie personali e particolari conoscenze, non astrattamente intese, ma concretamente riferibili al sistema sul quale opera e che lo privilegiano, di conseguenza, nella possibilità di commettere il reato.

E' controverso se debba qualificarsi quale operatore del sistema soltanto il c.d. system administrator[54], e cioè il tecnico informatico che ha il controllo *de facto* di tutte le fasi di elaborazione dati, con esclusione del semplice operatore addetto a funzioni esecutive e manuali, oppure se ci possa riferire a qualsiasi tecnico legittimato ad

[53] Campeis C., *Frode informatica*,in AA.VV. (a cura di), *Reato e danno*, Milano, Giuffrè, 2014, p. 946.
[54] Pecorella C., *Il diritto penale dell'informatica*, CEDAM, Padova, 2000, p.353.

operare sul computer[55]. L'opinione[56] che prevale è però quella, intermedia, per cui si deve intendere operatore del sistema qualsiasi soggetto che possa legittimamente contattare, in via continuativa, il sistema e che disponga della qualificazione professionale o di conoscenze ulteriori e specifiche rispetto a quelle di qualsiasi altro soggetto.

La previsione legislativa non è ancorata ad una specifica qualifica lavorativa o ad una determinata qualità tecnico-professionale astratta del soggetto, poiché, in tal caso, da un lato, la disposizione perderebbe qualsiasi garanzia di certezza e tassatività e rischierebbe di restare in balia delle categorie professionali che nel settore informatico sono soggette a continue mutazioni, dall'altro, vedrebbe snaturata la sua funzione di aggravare la pena non per le conoscenze teoriche dell'agente, ma per l'"*abuso*" del rapporto funzionale di cui era investito nei confronti del sistema. Ciò che è importante, affinchè sussista l'aggravante, è che tale soggetto abbia "*abusato*" della sua "*qualità*", cosa che si verifica tutte le volte in cui questi eccede i limiti dei compiti ad esso affidati[57].

Non è necessario che sussista un rapporto di dipendenza tra il titolare del sistema informatico e il soggetto agente, potendo ravvisarsi l'abuso dell'operatore del sistema anche da parte di un socio, di un collaboratore esterno o di un soggetto che, pur godendo di una posizione di autonomia ed indipendenza rispetto al titolare, si trova a

[55] Secondo Borruso sono ricompresi nella categoria in esame tutti i tecnici dell'informatica, trattandosi di persone che operano sul computer; anche D'Aietti dà un'interpretazione molto lata dell'espressione "*operatore del sistema*" , definendolo "*chiunque sia legittimato ad operare sul sistema, anche nella qualifica di semplice addetto alla immissione dei dati*"- in Borruso R., Buonomo G., Corasaniti G., D'Aietti G., *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pgg. 33 e 74.

[56] Mucciarelli F.,*Commento all'art. 10 della legge n. 547 del 1993*, in *Legislazione penale*, 1996, p. 102.

[57] Pica G., *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999, p. 76.

poter operare sul sistema informatico in forza di un titolo che glielo consenta o glielo imponga[58].

Il d. l. n. 93/ 2013, convertito con modifiche nella legge n. 119/ 2013, ha inserito il terzo comma dell'art. 640 *ter*, che disciplina un'ulteriore ipotesi aggravante, cioè quella per cui la frode informatica sia commessa, a danno di uno o più soggetti, con furto o indebito utilizzo dell'identità digitale. Il testo originario del decreto legge non faceva riferimento al furto o all'indebito utilizzo, bensì alla "*sostituzione dell'identità digitale*", espressione ritenuta ambigua, poiché evocava, piuttosto che l'indebito utilizzo dell'identità, la sua surrogazione con altra al fine di accedere ai dati raggiungibili con quella sostituita e cioè fattispecie diversa e ben più specifica di quella ipotizzata in precedenza, ma di dubbia rilevanza[59]. La legge di conversione ha modificato la disposizione, facendo esplicito riferimento al furto e all'indebito utilizzo dell'altrui identità digitale, purché commessi in danno di uno o più soggetti. Al di là di una residua imprecisione nella tecnica di normazione, in quanto potrebbe non essere del tutto chiaro il motivo per il quale il furto o l'indebito utilizzo debba avvenire in danno di uno o più soggetti, atteso che l'altrui danno è già evento del delitto di frode informatica[60], tale previsione normativa è sicuramente in grado di rafforzare la tutela penale dell'identità digitale in ogni sua concreta lesione effettuata tramite la rete Internet. Ai fini della commissione di frode informatica aggravata dal furto o indebito utilizzo dell'identità digitale, quindi, rilevano l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare suo utilizzatore, sotto un processo di identificazione che consiste nella validazione dell'insieme di dati attribuiti

[58] Può verificarsi nel caso di un contratto per l'assistenza e la manutenzione del sistema informatico.
[59] Pistorelli L., Relazione dell'Ufficio Massimario della Corte di Cassazione, n. III/1/2013.
[60] Pistorelli L., Relazione Ufficio del Massimario, cit..

in modo esclusivo ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.

Secondo quanto prescrive l'art. 640 *ter* all'ultimo comma, la frode informatica è perseguibile, normalmente, a querela della persona offesa e, nelle ipotesi aggravate, d'ufficio. Il soggetto legittimato a proporre querela non è né il proprietario del sistema o dei dati, né colui che ha la disponibilità di questi ultimi, bensì il soggetto che subisce il danno patrimoniale, non rilevando che quest'ultimo possa essere anche colui che ha disponibilità del sistema o dei dati alterati o manipolati.

La competenza per territorio spetta al giudice del luogo in cui è stato conseguito il profitto, essendo, a tal fine, irrilevante il luogo in cui è stata posta in essere la condotta[61]; la competenza per materia è del Tribunale in composizione monocratica, con udienza preliminare per le ipotesi aggravate. Le misure cautelari limitative della libertà personali possono essere applicate solo nelle ipotesi aggravate, ma mai possono disporsi le intercettazioni *ex* art. 266 ss. c.p.p..

1.3.6 **Responsabilità delle persone giuridiche**

Il delitto di frode informatica è uno dei reati presupposto per la responsabilità amministrativa delle persone giuridiche secondo quanto disposto dall'art. 24 del d. lgs. 231/2001[62]. Ai sensi di tale decreto, la frode informatica rileva se commessa in danno

[61] Alesiani V., *Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione*, in *Cass. pen*., 2001, p. 485 ss.

[62] Art. 24 d. lgs. 231/2001, Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico *: " In relazione alla commissione dei delitti di cui agli articoli 316 bis, 316 ter, 640 comma 2 n.1, 640 bis e 640 ter se commesso in danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.*
Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità, si applica la sanzione pecuniaria da duecento a seicento quote.

dello Stato o di altro ente pubblico: tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico. L'ipotesi di reato si potrebbe, inoltre, ricondurre all'alterazione di registri informatici della Pubblica Amministrazione per far risultare esistenti condizioni essenziali per la partecipazione a gare ovvero per la successiva produzione di documenti attestanti fatti e circostanze inesistenti o, ancora, per modificare dati fiscali o previdenziali di interesse dell'azienda, già trasmessi all'Amministrazione. Il reato in esame potrebbe anche configurarsi qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico della Pubblica Amministrazione al fine di inserire un importo superiore a quello legittimamente ottenuto. Il reato di frode informatica, se commesso in danno dello Stato o di altro ente pubblico, può dar luogo a responsabilità dell'ente collettivo, quando commesso nell'interesse o vantaggio dell'ente da soggetti apicali o sottoposti alla direzione o vigilanza degli stessi. Essendo prevista la responsabilità amministrativa, è richiesta, all'interno dell'ente, un'organizzazione, riguardante l'analisi delle procedure di accesso o di utilizzo dei sistemi informatici o telematici dell'ente, tale da rimuovere o, comunque, ridurre il rischio di commissione di reati. Se il modello manca o non è idoneo, sono previste sanzioni interdittive e pecuniarie che incidono sulle attività dell'ente, tanto da causarne la paralisi temporanea o permanente: interdizione dall'esercizio dell'attività, sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, divieto di pubblicizzare beni o servizi ed anche sanzioni

---

Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)."

pecuniarie, computabili per numero di quote a seconda della gravità del fatto e per importo delle medesime a seconda delle condizioni economiche e patrimoniali dell'ente.

La legge n. 119/2013 ha modificato l'art. 24 *bis* del d. lgs. 231/2001[63] e, ad oggi, la responsabilità amministrativa dell'ente è stata ampliata e sussiste anche per altre ipotesi di reati informatici, tra cui quello di frode informatica commessa con sostituzione di identità digitale. Sull'ampliamento dei reati presupposto per la responsabilità amministrativa degli enti si è soffermata la Corte di Cassazione nella sua Relazione n. III/01/2013 del 22 agosto 2013. La Corte ha affermato che l'inserimento sia del reato di frode informatica aggravata dalla sostituzione dell'identità digitale, ma soprattutto dei delitti in materia di violazione della privacy nel decreto legislativo n. 231/2011 risulta di grande impatto poiché comporta l'obbligo per le imprese di prevedere e implementare nelle policy interne misure organizzative e di prevenzione per questi nuovi delitti. Infatti, gli enti devono, per limitare al massimo la commissione di tale tipo di reati, partire da una responsabilizzazione di tutti i soggetti che ivi lavorano. A tal fine potrebbe essere utile predisporre corsi di formazione interna in grado di spiegare ai vertici ed ai dipendenti dell'azienda ciò che si può e ciò che non si deve fare con gli strumenti informatici o,

[63] Art 24 bis d.lgs. 231/2001, *Delitti informatici e trattamento illecito di dati*:" *In relazione alla commissione dei delitti di cui agli articoli 615 ter, 617 quater, 635 bis, 635 quater, 635 quinquies terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*
In relazione dalla commissione dei delitti di cui agli articoli 615 quater e 615 quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.
In relazione dalla commissione dei delitti di cui agli articoli 491 bis e 640 quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica la sanzione pecuniaria sino a quattrocento quote.
Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9 comma 2 lettere a), b), ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9 comma 2 lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2 lettere c), d) ed e)."

anche, redigere un vero e proprio codice di comportamento informatico, i cui principi fondamentali potrebbero essere addirittura inseriti all'interno del contratto di lavoro.

1.4 **Rapporti tra la frode informatica ed altre figure delittuose**

La fattispecie di frode informatica, per la sua genesi e la sua natura, si trova inevitabilmente in rapporto e confronto con altre figure delittuose, quali in particolare la truffa *ex* art. 640 c.p., la frode informatica del soggetto che presta servizi di certificazione di firma elettronica *ex* art. 640 *quinquies*, l'accesso abusivo ad un sistema informatico o telematico *ex* art. 615 *ter* e il danneggiamento di sistemi informatici o telematici *ex* art. 635 *bis*.

1.4.1 **La frode informatica e la truffa: analogie e differenze tra le due fattispecie**

La fattispecie di frode informatica è sicuramente accostabile a quella della truffa *ex* art. 640 c.p., infatti la norma del 640 *ter* è modulata sulla falsariga del reato di truffa ma con particolarità proprie dettate dalle modalità tipiche di azione connessa agli strumenti elettronici, a cui la tradizionale fattispecie non risultava estensibile.

Il delitto di truffa si basa sull'esistenza di una relazione intersoggettiva tra persone fisiche, in quanto la vittima viene determinata a compiere atti di disposizione patrimoniale a seguito dell'attività ingannatoria, consistente in artifizi e raggiri, posta in essere da altri, mentre nella frode informatica vi è un indebito arricchimento a seguito di modificazioni o alterazioni sugli strumenti elettronici. I tentavi di estendere

la norma della truffa alle ipotesi di frodi elettroniche[64] hanno trovato l'ostacolo del divieto di analogia in malam partem, rendendo improrogabile la distinzione tra le ipotesi in cui l'ingiusto profitto fosse conseguito con l'alterazione della volontà del soggetto agente tramite artifizi e raggiri, da quelle in cui si agiva direttamente sullo strumento elettronico. Ci si chiede, dunque, se il delitto di frode informatica possa essere considerato una autonoma fattispecie di reato o se tra esso e la truffa vi sia un rapporto di species a genus. Secondo un certo orientamento, il delitto previsto dall'art. 640 *ter* c.p. costituirebbe un'ipotesi di reato speciale rispetto a quella generale di truffa[65], ma tale assunto non è condivisibile dal momento che la fattispecie dell'art. 640 *ter* c.p. presenta elementi d'autonomia tali da rendere strutturalmente impossibile l'esistenza di un rapporto di specialità tra le due fattispecie delittuose[66].

In particolare, rispetto alla fattispecie che disciplina la truffa, nell'art. 640 *ter* non vi è alcun riferimento a una condotta vincolata, posta in essere, cioè, mediante artifici o raggiri tesi a indurre in errore il soggetto passivo o altro soggetto terzo e a fargli compiere un atto di disposizione patrimoniale che altrimenti non porrebbe in essere. Nella fattispecie di frode informatica il reo, lungi dall'indurre taluno in errore, nel porre in essere una condotta libera di alterazione del funzionamento del sistema informatico o telematico ovvero di intervento abusivo su dati, informazioni o programmi in esso contenuti , rivolge la propria condotta fraudolenta direttamente sul

[64] Trib. di Roma, 14 dicembre 1985, "*Manenti ed altri*", in *Dir. Inf.*, 1988, p. 487.
[65] Pica G., *Diritto penale delle tecnologie informatiche*, 1999, Torino, p. 141 e p. 162.
[66] Fanelli A., *Telefonate abusive e frode informatica*, in *Foro italiano*, 1999, III, p. 610, nonché Marini G., *Truffa*, in *Dig. Pen*., 1999, XIV, p. 394 e ss..

sistema informatico o telematico[67] e, da tale condotta, derivano direttamente e simultaneamente gli eventi dell'ingiusto profitto e dell'altrui danno.

Nonostante queste differenze, le due fattispecie di reato, pur nella loro autonomia, presentano indubbi elementi in comune. Ci si riferisce, in primo luogo, al fatto che entrambe le fattispecie normative sono poste a tutela del patrimonio, e poi agli eventi di ingiusto profitto e di altrui danno e al momento di consumazione dei reati che è, appunto, quello in cui si verifica l'effettivo conseguimento dell'ingiusto profitto, con correlativo danno nella sfera patrimoniale della persona offesa ; ma anche all'elemento soggettivo richiesto, che è costituito , per entrambe le fattispecie criminose, dal dolo generico, indiretto o eventuale, quale coscienza e volontà di porre in essere le condotte tipizzate dalle norme e di cagionare un ingiusto profitto con l'altrui danno, alla procedibilità, che è a querela della persona offesa, salvo non ricorra un'aggravante, nonché alla disciplina delle circostanze aggravanti, in quanto il secondo comma dell'art. 640 *ter* opera un rinvio espresso alle circostanze aggravanti previste dal numero 1) del secondo comma dell'art. 640 c.p..

1.4.2 **La frode informatica e l'art. 640 *quinquies* cod. pen.**

La legge n. 48/2008, come già anticipato, ha introdotto nel codice penale l'art. 640 *quinquies*, rubricato "*frode informatica del soggetto che presta servizi di certificazione di firma elettronica*", che disciplina la fattispecie "*propria*" commessa dal soggetto che presta servizi di certificazione di firma elettronica, completando la disciplina in materia di frode informatica.

[67] Cass. Pen., Sez. II, 11 novembre 2009, n. 44720.

La norma sanziona colui che, prestando servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto ovvero arrecare ad altri un sanno, viola gli obblighi previsti dalla legge per il rilascio del certificato qualificato. Nonostante l'art. 640 *ter* e l'art. 640 *quinquies* presentino la medesima rubrica, quest'ultimo non presenta riferimenti all'alterazione del funzionamento del sistema informatico né ad indebite intromissioni richiedendo, invece, la violazione di obblighi di legge previsti per il rilascio del certificato. Anche la frode del certificatore, in relazione al suo oggetto giuridico, rientra nel novero dei delitti contro il patrimonio mediante frode, anche se alcuni ritengono impropria tale collocazione poiché mancano, nella condotta tipica, i caratteri dell'azione fraudolenta in senso tecnico. La condotta punibile, infatti, consiste nella mera violazione di obblighi di legge riguardanti il rilascio della certificazione della firma elettronica, anche se finalizzata all'ingiusto profitto e l'altrui danno. Una tale anticipazione della tutela è sicuramente giustificabile alla luce della delicatezza e della rilevanza delle funzioni attribuite al soggetto certificatore, anche per l'avvenuta liberalizzazione del servizio, che non è più necessariamente garantito dalla presenza di un'autorità pubblica al vertice di esso e non necessita più di un'autorizzazione preventiva per il suo svolgimento.

Per quanto attiene l'elemento soggettivo, il reato è punibile a titolo di dolo specifico di profitto o di danno, ma è anche richiesto che il certificatore abbia la coscienza e la volontà di violare gli obblighi che la legge prevede a suo carico. A differenza della frode informatica, l'art. 640 *quinquies* è un reato proprio, in quanto soggetto attivo può essere soltanto il soggetto che presta il servizio di certificazione ed eventuali soggetti

sprovvisti di tale qualifica potranno, se del caso, risponderne a titolo di concorso, sempre che abbiano contribuito alla realizzazione della condotta criminosa.

1.4.3 **La frode informatica e l'accesso abusivo ad un sistema informatico o telematico**

Il delitto di frode informatica *ex* art. 640 *ter* può essere messo a confronto anche con la fattispecie disciplinata dall'art. 615 *ter* c.p., ossia l'accesso abusivo ad un sistema informatico o telematico. Tra le due norme non si ravvisa un rapporto di specialità, in quanto ciascuna attiene a fatti diversi, ma, tra le due fattispecie, possono porsi problemi di correlazione nei casi in cui l'azione fraudolenta a fini di ingiusto profitto sia intentata tramite un accesso abusivo, da lontano per via telematica, o anche da vicino, da persona non abilitata. In tali casi, l'azione di accesso abusivo non è fine a se stessa, né rivolta all'esclusiva conoscenza di informazioni contenute nel sistema violato, ma è finalizzata alla commissione della frode e, dunque, costituisce una modalità necessaria, anche se prodromica, dell'azione fraudolenta, poiché l'agente, se prima non si introduce nel sistema altrui, non può neppure realizzare le manipolazioni descritte dall'art. 640 *ter* c.p.. Tuttavia, la necessaria prodromicità logica e fisica dell'azione di accesso abusivo, non comporta l'esclusione della possibilità di un concorso fra le due ipotesi di reato, e ben può ritenersi che ci si trovi di fronte ad un caso di concorso apparente di norme. L'azione di accesso abusivo non rientra nello schema tipico della fattispecie di frode informatica, che è articolata sull'azione di manipolazione del sistema, e ci si trova di fronte a due diverse fattispecie, delle quali l'una inglobi strutturalmente e tipicamente elementi dell'altra, perciò appare

ipotizzabile il concorso di reati. Tale concorso può manifestarsi in un vero e proprio concorso formale, nel caso in cui l'azione tecnica di accesso abusivo rechi già in sé anche la manipolazione necessaria per l'indebito profitto, come ad esempio nel caso in cui si violi il sistema remoto introducendovi contestualmente un nuovo *software* che trasferisce a nome dell'agente un blocco più o meno ampio di poste economiche attive; od anche nel caso in cui l'unicità dell'azione sia data dal compimento di operazioni, anche se non contestuali, comunque consecutive e quindi in stretta connessione logica e cronologica. Oppure il concorso potrà essere materiale, come ad esempio nei casi in cui la frode sia realizzata con ripetuti accessi e successive operazioni, logicamente correlate, ma distanti nel tempo e, in questi casi, tale pluralità di reati troverà confluenza nella figura del reato continuato (*ex* art. 81 cpv. c.p.). Quindi, nei casi in cui l'accesso riesca, ma la frode, per qualsiasi motivo, non sia commessa, appare configurabile il concorso tra il reato di accesso abusivo consumato ed il tentativo di frode informatica. Egualmente sarà configurabile il concorso, nella forma della continuazione, tra i reati consumati di accesso abusivo e di frode informatica, nei casi in cui l'accesso riesca, e,grazie ad esso, riesca anche la frode informatica, nel senso che il reato di frode sia consumato, con l'acquisizione dell'ingiusto profitto. Se l'agente non riesce a porre in essere l'accesso abusivo nel sistema, la finalità di frode sarà irrilevante penalmente, restando ancora sul piano delle intenzioni del reo, mentre sarà punibile il tentativo di accesso abusivo.

Tuttavia, in dottrina vi è chi critica la possibilità di concorso formale tra i due reati[68] in quanto, anche se è vero che le due norme incriminatrici tutelano differenti beni giuridici e che è possibile commettere una frode informatica anche senza accedere

[68] Fanelli A., *La truffa*, GIUFFRE', 1998, p. 423.

abusivamente ad un sistema informatico, da una parte, il criterio della diversità degli interessi tutelati, ai fini dell'affermazione della sussistenza del concorso di reati, è assai criticato dalla dottrina più autorevole, dall'altra, i casi più comuni di frode informatica sono realizzabili proprio mediante abusivo accesso ad una rete informatica. Per tali motivi, sembrerebbe che in tali fattispecie, qualora vi sia il conseguimento da parte dell'agente di un profitto con danno di altri, l'accesso abusivo costituisca un ante factum non punibile, poiché esso, secondo l'id quod plerumque accidit, rappresenta lo strumento normalmente utilizzato per la commissione del più grave reato di frode informatica.

Talvolta, inoltre, è possibile che si configuri il reato di accesso abusivo ma non di quello di frode informatica, come può leggersi in una sentenza del 1997 del Tribunale di Torino[69], che ha affermato che la duplicazione dei dati acquisiti in occasione dell'accesso abusivo a sistema informatico o telematico non integra l'elemento materiale della frode informatica, in quanto tale reato colpisce solo gli interventi che consistono nell'adibire l'apparato a scopi diversi da quelli per cui era stato destinato o nel manipolarne arbitrariamente i contenuti, bensì tale duplicazione è da considerarsi condotta tipica del reato di cui all'art. 615 *ter* c.p., potendo "*l'intrusione informatica*" sostanziarsi sia in una semplice lettura dei dati, che nella copiatura di essi.

[69] Trib. di Torino 4 dicembre 1997, *Zara e altro*, in *Dir. informazione e informatica*, 1998, p. 354.

1.4.4 **La frode informatica e il danneggiamento dei sistemi informatici o telematici**

Il delitto di frode informatica può essere accostato anche al delitto di danneggiamento dei sistemi informatici e telematici, disciplinato dall'art. 635 *bis* c.p.[70]. Sicuramente tale ultima disposizione, come si evince dal testo della norma, ha natura residuale in quanto vi è la clausola "*salvo che il fatto costituisca più grave reato*". Dunque, in concreto, tutte le volte che ad una condotta di distruzione, deterioramento, cancellazione, alterazione o soppressione di sistemi informatici altrui si accompagna il conseguimento di un ingiusto profitto con altrui danno, elemento non richiesto invece dall'art. 635 *bis*, troverà applicazione la fattispecie della frode informatica, poiché punita più gravemente, in quanto alla medesima pena detentiva si aggiunge anche la pena della multa[71].

1.4.5 **La frode informatica e il falso informatico**

Prima dell'entrata in vigore della legge n. 547/1993, nei casi di manomissione di dati informatici a fine di indebito profitto, si riteneva sussistente il concorso tra i reati di truffa e di falso. In tal senso si è orientata la giurisprudenza in una vicenda che aveva visto un agente modificare i dati memorizzati nell'archivio informatico di un ufficio I.N.P.S., in modo da far figurare i contributi versati a favore di una persona in entità tale da far ritenere maturato il diritto alla pensione[72], e, in tal caso, è stato ravvisato il

[70] Art. 635 *bis* c.p., *Danneggiamento di sistemi informatici e telematici*: "*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio."
[71] Masi A. , *Frodi informatiche e attività bancarie*,in *Riv. Pen. Econ*., 1995, p. 430.
[72] Trib. di Como, Sez. Pen., 21-25 settembre 1995, n. 611.

concorso del reato di truffa con quello di falso in atto pubblico[73], disciplinato all'art. 476 c.p..

Il Tribunale di Como, nel caso di specie, ha disatteso l'assunto dell'imputato secondo cui le falsità poste in essere sui documenti informatici sarebbero state punite solo a seguito dell'entrata in vigore della legge n. 547/1993, che ha introdotto l'art. 491 *bis* c.p.[74] nel codice penale, per cui tale condotta illecita prima di tale legge non rientrava nella fattispecie di reato prevista dall'art. 476 c.p. e non risultava punibile in forza di altra disposizione normativa; ed ha ritenuto che le alterazioni dei dati dell'archivio magnetico pubblico configurassero non solo il delitto di cui all'art. 476 c.p., ma anche quello di tentativo di truffa, in quanto tali alterazioni possono essere considerate come atti idonei e non equivoci diretti a far conseguire all'imputato un ingiusto profitto con corrispondente danno dell'ente pubblico.

Con l'introduzione della fattispecie di frode informatica, l'intervento "*con qualsiasi modalità su dati, informazioni o programmi*", nel quale si sostanzia anche ogni forma di falsificazione di dati informatici, è divenuto elemento tipico e costitutivo del reato di frode informatica. Ad ogni modo, tra le fattispecie di falso e quella di frode informatica vi è una netta demarcazione quanto alle esigenze di tutela ed all'oggetto giuridico dei due reati, che rende tuttora ipotizzabile il concorso di reati. Parte della dottrina[75] propende, appunto, per la configurabilità del concorso tra la frode informatica e il falso informatico, reato che risulta dal combinato disposto dell'art. 491 *bis* e delle norme che puniscono le varie ipotesi di falsità in atti, e, a tal fine, fa

[73] Pica G., *Diritto penale delle tecnologie informatiche. Computer's crimes e reati telematici Internet Banche-dati e privacy*, UTET, 1999, pgg. 160-161.
[74] Art. 491 *bis* c.p., *Documenti informatici*: "*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*."
[75] Fanelli A., *La truffa*, GIUFFRE', 1998, pgg. 426-427.

l'esempio dell'alterazione di dati o dell'immissione abusiva di dati fittizi, ma tale conclusione non può considerarsi scevra da dubbi. La giurisprudenza, invece, afferma unanimemente il concorso formale tra truffa e reati di falso, ma nel caso della frode informatica e del falso informatico il problema assume una connotazione diversa. A differenza della truffa, l'art. 640 *ter* fa esplicito riferimento ad una condotta di alterazione o di intervento su dati, informazioni o programmi e, dunque, un'attività *lato sensu* falsificatoria è necessariamente presupposta nella commissione di tale reato. Ed è vero che l'art. 491 *bis* si riferisce al concetto di "*documento informatico*", pubblico o privato, come tale intendendosi "*qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*", e che non ogni alterazione di dati costituisce per ciò solo falsificazione di un documento informatico, occorrendo, a tal fine, che oggetto della falsificazione siano solo quelle registrazioni magnetiche di fatti rilevanti a fini probatori che, per essere immagazzinate su di una memoria, interna o esterna all'elaboratore, sono destinate ad essere conservate per un ragionevole lasso di tempo, come si richiede per i documenti tradizionali; tuttavia, anche in caso di alterazione di un documento informatico, condotta teoricamente idonea ad integrare il reato di falso informatico e al tempo stesso finalizzata alla commissione di una frode, non è sempre facile ravvisare la lesione del patrimonio della vittima ed anche del bene giuridico della fede pubblica. Una tale lesione può verificarsi in relazione a certi documenti pubblici, quale ad esempio il certificato di residenza contenuto nella memoria del terminale di un ufficio amministrativo, ma riguardo ad altri documenti informatici privati, quale ad esempio un conto corrente bancario il cui ammontare viene alterato,

la lesione della fede pubblica sfuma nella lesione patrimoniale, che è alla base del reato disciplinato dall'art. 640 *ter*, in quanto esso implica necessariamente la manipolazione e alterazione dei dati informatici. In altre parole, nella suddetta condotta, se mantenuta nei limiti indicati, non sembrano distinguibili due autonomi disvalori dell'azione posta in essere e, dunque, l'uno viene assorbito nell'altro, determinando, in virtù del principio del *ne-bis in idem* sostanziale, l'applicazione della sola e più grave fattispecie della frode informatica.

1.4.6 **La frode informatica e la falsificazione di carte di pagamento**

La frode informatica può essere anche rapportata, per valutarne analogie e differenze, con la fattispecie di falsificazione di carte magnetiche di pagamento, secondo quanto disposto dall'art. 12[76] della legge n. 197/1991[77]. Innanzitutto, bisogna tenere in considerazione la distinzione tra *documenti informatici* e *documenti elettronici*, per cui i primi sono documenti formati, elaborati e gestiti da sistemi informatici e la cui alterazione o manipolazione può configurare il reato di cui all'art. 640 *ter* c.p.; mentre i secondi sono individuabili in tutti i tesserini, di solito magnetici, a rilevazione elettronica, che consentono il riconoscimento del titolare di esso o il suo accesso ad apparecchiature o a procedure elettroniche di vario genere, quali ad esempio il Bancomat, e la cui falsificazione o le altre condotte illecite ad essi relative non si attua

[76] Art. 12 l. 197/1991- *Carte di credito, di pagamento e documenti che abilitano al prelievo di denaro contante*: " *Chiunque, al fine di trarre profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni. Alla stessa pena soggiace chi, al fine di trarre profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi*."

[77] Pecorella C., *Il nuovo diritto penale della carte di pagamento*, in *Riv. it. dir. proc. pen*., 1993, p. 235; Pecorella C., *L'abuso dei distributori automatici di banconote*, in *Riv. it. dir. proc. pen*, 1990, p. 573; Corrias Lucente G., *I reati in materia di carte di credito nella legge 5 luglio 1991 n. 197*, in *Dir. informaz. informat*., 1991, 3, p. 763.

attraverso la manipolazione di *files* o *softwares*, ma attraverso la materiale contraffazione del tesserino e l'uso di questo. Tali ultime condotte non rientrano nel campo di applicazione della norma del codice penale sulla frode informatica, ma sono disciplinate dall'art. 12 della legge n. 197/1991 appositamente creata dal legislatore. Venendo, invece, più nello specifico, ai rapporti che intercorrono tra le due ipotesi criminose si può dire, per prima cosa, che nel caso in cui l'agente consegua un ingiusto profitto mediante la falsificazione di una carta personale di pagamento, non si avrà concorso di reati con la frode informatica, ma concorso apparente di norme. In relazione ai rapporti fra il reato di cui all'art. 12 della legge n. 197/1991 e la truffa ordinaria *ex* art. 640 c.p., la giurisprudenza è incline ad ammettere la configurabilità del concorso formale, ma la questione assume toni differenti in riferimento alla frode informatica: infatti, il concetto di "*dati pertinenti ad un sistema informatico*" di cui all'art. 640 *ter* c.p. può teoricamente estendersi sino a ricomprendere frodi commesse mediante falsificazione di carte di credito, e ciò, quindi, configura l'ipotesi di cui all'art. 12 quale una particolare specie di frode informatica. In realtà, fra le due disposizioni non intercorre un rapporto di specialità vero e proprio, in quanto nella seconda è richiesto un *quid pluris* rispetto alla prima: nell'art. 640 *ter* il profitto è l'evento e dunque deve essere effettivamente realizzato, mentre nell'art. 12 il profitto è previsto a titolo di dolo specifico. Ad ogni modo, l'esclusione del concorso di reati e l'applicazione della sola più grave norma prevista dalla legge n. 197/1991 possono fondarsi su un rapporto di specialità reciproca fra le due fattispecie, e quindi il conseguimento dell'ingiusto profitto può essere visto come un post-factum non punibile, poiché la pena più severa prevista per il reato di falsificazione di carte di

credito è in grado di assorbire anche l'eventualità di un profitto realmente conseguito e non solamente perseguito[78].

Inoltre, la previsione del dolo specifico, che consiste nel fine di trarre profitto per sé o per altri, in riferimento all'art. 12 è molto importante anche per consentire di distinguere i casi in cui l'agente è sorretto da scopi illeciti dai casi in cui, per diverse e molteplici ragioni, agisce senza alcuna volontà di illecito profitto. Vi possono essere, infatti, casi in cui il titolare utilizzi la propria carta, senza accorgersi della sopravvenuta scadenza temporale: in tale ipotesi, dal momento della scadenza egli non è più titolare della carta e quindi si verifica la qualità soggettiva richiesta dalla prima parte della disposizione; ma, se l'uso della carta è dovuta a mera distrazione, non può ascriversi a carico dell'agente il reato in esame, avendo egli agito per errore su un elemento normativo della fattispecie, cioè la titolarità o meno della carta, ed essendo escluso il dolo da tale situazione di errore[79].

Dunque, in conclusione, può dirsi che l'art. 12 è una norma molto importante in quanto prevede e punisce un nuovo tipo di reato che prima non era facilmente configurabile e quindi punibile, né come truffa né come furto; anzi, la nuova fattispecie può concorrere con il reato di furto, mentre si ritiene che assorba il reato di truffa in quanto si tratta di una previsione più specifica dell'induzione in errore mediante artifici o raggiri.

1.5 La frode informatica in una prospettiva comparatistica: il sistema statunitense

[78] Blaiotta R., *I reati commessi con le carte di pagamento nel sistema penale*, in *Critica del dir.*, 1996, p. 195.
[79] Articolo 47, 3° comma c.p.

Gli Stati Uniti sono, ad oggi come in passato, un Paese fortemente colpito dalle frodi informatiche. Negli Stati Uniti si ritiene che le frodi informatiche possono integrare gli estremi dei reati *federali* di "*wire fraud*" e di "*mail fraud*". Precisamente, il reato di "*wire fraud*" si ha quando "*qualcuno sia ricorso o abbia avuto intenzione di ricorrere a qualsiasi mezzo o artificio per frodare o per procurarsi danaro o altre utilità a mezzo di falsi o ingannevoli pretesti e trasmette o fa in modo che sia trasmessa mediante telegrafo un qualsiasi scritto, firma, segno, disegno o segnale acustico allo scopo di realizzare tale mezzo o artificio*": qui si prende in considerazione la frode per mezzo delle telecomunicazioni. Si ha, invece, reato di "*mail fraud*" quando si utilizza il servizio postale tra i diversi Stati o con l'estero per progettare o eseguire una frode.

L'ampia formulazione delle due ipotesi criminose e, in particolare, la mancata previsione dell'induzione in inganno di una persona come necessario estremo costitutivo del reato, ha permesso facilmente alla dottrina di far rientrare in tali ipotesi le nuove figure delle frodi telematiche. In particolare, la dottrina statunitense ha considerato i collegamenti telematici equivalenti, ai fini della configurabilità dei reati in questione, alle comunicazioni telegrafiche. Data l'espansione del fenomeno, a metà degli anni ottanta, sono stati emanati il *Counterfeit Access Device and Computer Fraud and Abuse Act* in materia di accesso abusivo ai sistemi informatici, e il *Credit Card Fraud Act* per reprimere in modo specifico le frodi compiute con le carte di credito.

Con la prima disposizione, si è prevista una figura di accesso non autorizzato ad un "*sistema informatico di interesse federale*" (*Federal interest computer*) qualificato dall'intento di commettere una frode (18 U. S. C. § 1030(a)(4)) (*computer access*

fraud): una disposizione che, benché osteggiata nel corso dei lavori preparatori della legge, ritenendosi inutile e fuorviante il presupposto dell'accesso abusivo al sistema informatico utilizzato per utilizzare la frode, è rimasta pressoché immutata anche dopo i numerosi interventi legislativi che hanno interessato il § 1030 U. S. C. nel corso di questi anni; le sole modifiche apportate con il più recente "*National Information Infrastructure Protection Act"* del 1996, d'altra parte, se da un lato mirano piuttosto ad un restringimento dell'ambito di operatività della norma, attraverso l'estromissione dei casi di mero utilizzo indebito dell'elaboratore, che abbia comportato un costo complessivo non superiore a 5.000 dollari nell'arco di un anno; dall'altro lato, attraverso la sostituzione della locuzione "*sistemi informatici di interesse federale*" con quella più ampia di "*sistema informatico protetto*" (protected computer), destinata ad operare per tutte le disposizioni del § 1030, si limitano ad ampliare l'ambito dei sistemi informatici il cui impiego fraudolento determina la rilevanza penale a livello federale della condotta del reo.

La seconda norma, invece, prevede varie ipotesi criminose: a) quando si produca, si usi o si trasferisca uno o più strumenti di accesso contraffatti; b) quando si utilizzino uno o più strumenti di accesso non autorizzati durante il periodo di un anno e mediante tale condotta ci si procuri un ingiusto profitto pari o superiore a 1000 dollari per il periodo in questione; c) quando si possieda 15 o più strumenti contraffatti o non autorizzati; d) quando si detenga, si possieda o si traffichi con attrezzature per realizzare strumenti di accesso. Tutti questi reati presuppongono un elemento soggettivo costituito non soltanto dalla coscienza e dalla volontà della condotta, ma anche dalla consapevolezza della natura degli strumenti utilizzati o detenuti e

dall'intento specifico di frodare. La prima ipotesi è punita con una pena pecuniaria non superiore a 50.000 dollari o al doppio del valore ottenuto con il reato e/o con una pena detentiva non superiore a 15 anni; nel caso che il reato sia stato commesso dopo la reclusione per un altro reato dello stesso tipo, o dopo un tentativo di commettere un reato dello stesso tipo, la sanzione è costituita da una pena pecuniaria non superiore a 100.000 dollari o al doppio del valore ottenuto con il reato e/o con la pena detentiva non superiore a 20 anni. La seconda e terza ipotesi sono considerate meno gravi e punite con una pena minore; la quarta ipotesi, invece, è punita come la prima, ma non è previsto l'inasprimento della pena per la recidiva. Si tratta di sanzioni che costituiscono un notevole inasprimento delle pene previste nel "*Truth in Lending Act"* e nell'"*Electronic Fund Transfer Act"* e tuttavia molto elastiche, in modo da consentire al giudice un elevato margine di discrezionalità in ordine alla misura concreta della pena e alla possibilità di applicare la sola pena pecuniaria senza un minimo edittale. La norma detta, inoltre, una serie di definizioni dei termini usati nella legge stessa. In particolare, definisce la nozione di strumento di accesso come "*ogni carta, targhetta, codice, numero di conto o altri mezzi di accesso al conto che possono essere usati, da soli o insieme con altri strumenti di accesso, per ottenere danaro, beni, servizi o qualunque altra cosa di valore e che possono essere usati per attivare un trasferimento elettronico di fondi, esclusi quelli originati solamente da uno strumento cartaceo*".

L'espressione "*altri mezzi di accesso al conto*" è anch'essa di significato molto ampio e comprende, ad esempio, il numero di identificazione personale, il cosiddetto P.I.N. e gli altri mezzi biometrici di identificazione della persona. L'espressione "*strumento di*

accesso contraffatto" comprende ogni strumento di accesso che sia contraffatto, fittizio, alterato o falsificato o un identificabile componente di uno strumento di accesso o di un contraffatto strumento di accesso.

Per "*componente*" si intendono, invece, gli strumenti di accesso incompleti come le carte di credito in bianco, i microchips, le firme, gli ologrammi e le strisce magnetiche. Strumento di accesso non autorizzato è ogni strumento smarrito, rubato, revocato o cancellato, ovvero che è stato ottenuto con l'intento di frodare.

Infine "*produrre*" vuol dire disegnare, alterare, autenticare, duplicare o assemblare; "*trasferire*" significa, invece, vendere, affittare, prestare, distribuire, acquistare, ottenere il possesso o la detenzione. La norma provvede anche a istituire un Ufficio del Servizio Segreto degli Stati Uniti per accertare i reati previsti dalla legge secondo le modalità stabilite tra il Segretario del Tesoro e il *General Attorney*. A livello statale, invece, è controverso anche negli Stati Uniti se siano applicabili le norme in tema di truffa alle frodi informatiche nonostante la mancanza dell'induzione in inganno di una persona.

Le controversie della dottrina hanno indotto alcuni Stati ad emanare norme legislative con le quali si estendono le norme in tema di truffa alle frodi informatiche; altri Stati, invece, hanno preferito emanare disposizioni che prevedono la truffa informatica come figura autonoma di reato.

1.4.7 **Il sistema tedesco**

In Germania il § 264 del codice penale (Strafgesetzbuch) disciplina la truffa affermando che: "*Chi, nell'intento di procurare a sé o a un terzo un vantaggio patrimoniale illecito, danneggia il patrimonio di altri, inducendolo o mantenendolo in*

errore mediante affermazione di circostanze false oppure mediante alterazione o dissimulazione di circostanze vere, viene punito per il reato di truffa con il carcere, oltre al quale può essere inflitta la pena pecuniaria o la perdita dei diritti civili e onorifici". L'inapplicabilità della norma alle frodi elettroniche è stata espressamente affermata dalla Commissione di esperti per la lotta contro la criminalità economica. In particolare, la Commissione ha affermato che la fattispecie della truffa risulta spesso inapplicabile in quanto presuppone che l'offeso venga dolosamente indotto in errore. L'uomo si serve di un elaboratore per compiere determinati atti di disposizione patrimoniale, come ad esempio nello sviluppo dei rendiconti delle operazioni di conto corrente, nella contabilità delle paghe del personale di un'impresa, e, qualora tali dati siano oggetto di manipolazione nelle singole fasi, ricorreranno gli estremi della truffa solamente a condizione che sussista il raggiro delle persone addette al controllo delle operazioni di elettronica.

La lacuna di perseguibilità penale che si evidenzia nell'ambiti della truffa deriva, dunque, dal fatto che, in luogo del processo decisionale umano che conduce all'operazione di disposizione patrimoniale, in alcuni settori è subentrato l'elaboratore che non può essere dolosamente indotto in inganno, ragion per cui non ricorre un elemento essenziale della fattispecie della truffa. Il legislatore ha quindi emanato la legge sui reati patrimoniali in materia di informatica che ha introdotto, tra l'altro, l'articolo 263a del codice penale intitolato "*frode informatica*".

1.4.8 **Il sistema francese**

In Francia le manipolazioni di dati sono state ricondotte senza alcuna esitazione alla fattispecie di *escroquerie* contemplata dall'articolo 405 del *code pènal* del 1810, alla

luce della interpretazione estensiva dei suoi diversi elementi, tradizionalmente accolta dalla giurisprudenza: sia in riferimento alla nozione di *manoevrues frauduleuses*, al cui ambito vengono ricondotti comportamenti fraudolenti diretti anche solo mediatamente all'uomo, sia in riferimento all'oggetto della *remise*, che viene ritenuto individuabile anche nella moneta scritturale. Di conseguenza, non sorprende che la legge 5 gennaio 1988 n. 88-19, con la quale il legislatore francese ha provveduto ad aggiornare il *code pènal* sul fronte degli abusi dell'informatica, non preveda alcuna disposizione sulla frode informatica; del resto neanche nel nuovo *code pènal*, entrato in vigore il 1° marzo 1994, è stata inserita alcuna disposizione specifica per le frodi informatiche, anche se viene ritenuta applicabile ad esse, oltre alla nuova fattispecie di *escroquerie*, prevista dall'articolo 313-1 del *code pènal*, anche la fattispecie di accesso abusivo, prevista all'articolo 323-1 del *code pènal* nonché, data la genericità del dettato normativo, quella che punisce l'introduzione, la soppressione o la modifica fraudolenta di dati, prevista dall'articolo 323-3 del *code pènal*.

Capitolo II. Il phishing

2.1 **La tecnica del phishing: fenomeno e diffusione**

Il phishing, nella traduzione italiana "*spillaggio*", è una variante del termine inglese "*fishing*", letteralmente traducibile "*pescare*", ormai entrato a far parte dell'odierno linguaggio criminologico, che consiste in una tecnica fraudolenta mirante a carpire informazioni personali e sensibili, quali dati anagrafici, user id e password per i conti correnti online, codici di carte di credito, facendo leva sugli aspetti c.d. sociali di internet, con il fine di porre in essere illeciti bancari attraverso la rete, accendendo ai sistemi di home banking ovvero a conti correnti e servizi online per disporre dei depositi attraverso operazioni e bonifici attuati in frode ai titolari.

Il phishing può essere definito come una tecnica di social engineering che, tramite l'invio da parte di truffatori di messaggi di posta elettronica ingannevoli, spinge le vittime a fornire volontariamente informazioni personali.

L'etimologia del termine ne indica un'origine dubbia, derivante dall'unione delle parole "*harvesting*" con "*password*", ovvero "*password*" con "*fishing*"o, ancora, "*fishing*" con "*phreaking*". Ma, al di là dell'etimologia della parola, gli obiettivi del phishing attack sono sia quello di portare l'utente a fornire informazioni e dati personali, riguardanti principalmente le credenziali di autenticazione per accedere ad aree informatiche esclusive o servizi bancari online, numeri di carte di credito, identificativi per le abilitazioni all'accesso a siti di vario genere, numero di conto corrente, numero ed estremi della carta di identità o della patente e sia quello di

utilizzare i dati ottenuti per conseguire l'abilitazione all'accesso ai servizi on line, assumendo virtualmente l'identità del legittimo titolare o utente[80].

La frode sottesa alla tecnica del phishing trae origine, solitamente, dall'invio casuale di e-mail ad un elevato numero di persone[81] contenti messaggi, immagini ed informazioni appositamente formulati in modo da influenzare la psicologia del destinatario, il quale, ricevendo tali comunicazioni, apparentemente provenienti da enti, istituzioni o società reali, viene indotto a collegarsi a pagine web o siti non autentici, ma del tutto simili a quelli delle citate istituzioni o società o enti, e indotto ad inserire le proprie credenziali per l'accesso ad aree riservate, servizi on line, in particolare l'home banking, cliccando sui link o sui form creati *ad hoc* dal phisher, ovvero operando un collegamento *ex novo* dal proprio computer che è stato già infettato da un trojan dal phisher[82].

Il phishing è un fenomeno che ha cominciato a diffondersi nella metà degli anni '90 e, ad oggi, la tecnica con cui viene posto in essere si è affinata e diffusa, non limitandosi necessariamente al perseguimento di un lucro pecuniario, ma investendo anche in tecniche e forme più sofisticate[83], tali da mettere in allarme i settori della sicurezza informatica, dei servizi finanziari e della tutela dei consumatori. Inizialmente, il phishing era un fenomeno generato, principalmente, dall'invio massivo di e-mail e diffuso maggiormente nei Paesi del Nord America, ma, successivamente, tale tecnica si è diffusa anche in altri Paesi, tra cui l'Italia, che ha subito il primo attacco nel marzo 2005, tramite e-mail inviate ai clienti di Poste Italiane.

---

[80] Flor F., *Phishing, identity theft e identity abuse:le prospettive applicative del diritto penale vigente*, in RIDPP, 2007, p. 899.

[81] Tale tecnica è denominata *spamming.*

[82] Tale tecnica è denominata *pharming.*

[83] Massa R. G., *Il phishing*, 2008 http://www.pmi.it/impresa/normativa/articolo/1999/il-phishing.html

In Italia, fino a poco tempo addietro, anche se erano già circolate e-mail esca provenienti da phishers esteri, il fenomeno era piuttosto contenuto e non vi erano stati grandi problemi, soprattutto perché le e-mail erano scritte in lingua inglese e riferite ad istituti di credito esteri. Dalla fine del 2005 il panorama è cambiato, sono cominciate a circolare e-mail riferite ad istituti di credito nazionali in un italiano sempre più corretto e anche l'Italia ha cominciato ad assumere un ruolo sempre più importante nella classifica delle nazioni con maggior numero di istituti bancari colpiti da tali attacchi[84]. Per comprendere l'effettivo numero di attacchi posti in essere in Italia, possiamo prendere in considerazione i report resi noti da Anti-Phishing Italia, un osservatorio sul mondo degli illeciti legati alla rete, per contrastarli e arginarli, promosso da uno staff formato da informatici, giornalisti, avvocati e aperto a collaborazioni esterne. Nel primo trimestre del 2007, dunque nei mesi gennaio-marzo, sono stati rilevati 225 tentativi di phishing, con una media di 2,5 attacchi giornalieri: un dato preoccupante considerando che, nello stesso periodo del 2006, il numero totali di attacchi è stato di 12 e, nel solo mese di gennaio 2006, il numero di attacchi è stato pari a zero. Nei successivi tre mesi del 2007, gli attacchi sono ulteriormente aumentati, con una crescita del 940% rispetto al primo trimestre.

Gli obiettivi più colpiti sono stati Poste Italiane, con una frequenza di due attacchi al giorno, probabilmente perché i conti Banco Posta e le carte prepagate Poste Pay sono particolarmente diffuse e utilizzate anche per gli acquisti in rete, Banca Intesa, con una percentuale di attacchi pari al 6% e il sito di aste online eBay, che è stato fortemente attaccato con l'utilizzo della tecnica di keylogger. Con il passare degli anni, gli attacchi di phishing in Italia si sono moltiplicati, infatti nel 2014 e nel 2015 è alto il

[84] Cajani F., Costabile G., Mazzaraco G., *op. cit.*, p. 32.

numero di attacchi registrato e si rileva anche l'utilizzo di diverse piattaforme di attacco e cioè i social network, in particolare Facebook e Twitter[85].

Pian piano, con il tempo, le tecniche di phishing si sono anche perfezionate e, ad oggi, si parla di phishing tramite VoIP, fax, sms, tutte varianti che permettono di mietere più vittime, anche grazie all'inflazionamento del fenomeno e alla diffusione di kit software *"all inclusive"* che permettono anche ai soggetti più inesperti di porre in essere tentativi, abbastanza credibili, di truffa[86].

I phishing attacks sono in continua e rapida crescita e, per comprendere la reale dimensione del fenomeno a livello mondiale, considerando che alcuni tentativi di phishing non sono riportati o rilevati, può farsi riferimento all'analisi dei Phishing Activity Trends Reports, elaborati dall'Anti Phishing Working Group[87]. I risultati dei rapporti evidenziano, in modo particolare, una crescita del fenomeno sia in riferimento ai casi segnalati, sia in riferimento al numero dei nuovi siti di phishing. Il settore più colpito rimane quello relativo ai servizi finanziari, mentre il Paese che ospita il maggior numero di host sono gli Stati Uniti, seguiti da Corea, Cina e Germania; la durata minima e massima di vita di un phishing site è rilevante perché varia da un minimo di 4 ad un massimo di 27 giorni, elemento questo che inevitabilmente incide sul piano dell'accertamento del fatto e dell'individuazione del suo autore[88].

---

[85] Picotti L., *I diritti fondamentali nell'uso e abuso dei social network. Aspetti penali*, *Giur. merito*, fasc.12, 2012, p. 2522.

[86] Massa R. G., *Il phishing*, 2008 http://www.pmi.it/impresa/normativa/articolo/1999/il-phishing.html

[87] L'Anti Phishing Working Group (APWG) è stato fondato nel 2003 da David Jevans con lo scopo di creare un consorzio internazionale, che ad oggi conta più di 3000 membri, formato da aziende leader nel campo della sicurezza informatica e finanziaria per tutelarle da attacchi di phishing. Sono membri dell'APWG BitDefender, Symantec, McAfee, Gruppo ING, VISA, Mastercard, ecc.

[88] Cajani F., *Profili penali del phishing*, in CP, 2007, p. 2294.

Fortunatamente, però, anche se il numero di phishing attacks in Italia, e nel mondo, continua ad essere alto, quelli che effettivamente vanno a buon fine sono in un numero sempre minore grazie alla maggiore sensibilizzazione nei confronti di tale fenomeno e alla diffusione di metodi per evitare di incorrere in questo tipo di situazioni.

2.1.1 **Le fasi del phishing attack**

Il phishing attack si articola essenzialmente in sei fasi, miranti a conseguire l'obiettivo proprio del phishing e cioè il furto di informazioni e dati personali dell' utente.

La prima fase è quella del "*Planning*" e cioè quella in cui l'attaccante, dunque il phisher, determina chi colpire, cosa colpire, quali tecniche adoperare e quali sono gli obiettivi della frode. In seguito, egli si adopera a configurare i tools e i meccanismi necessari a poter sferrare l'attacco, cercando anche informazioni utili sulle potenziali vittime e passando, quindi, alla seconda fase, che è quella del "*Setup*".

Inizia, poi, l'attacco vero e proprio, dunque la fase c.d. "*Attack*", in cui l'attaccante inizia ad instaurare un contatto con le potenziali vittime, utilizzando tutte le tipologie di strumenti che internet mette a disposizione, quali e-mail, dialer, news group, instant messaging, chat web site, malware, bacheche elettroniche. L'intento di tale contatto dell'attaccante con le vittime è quello di indurle a realizzare azioni che possano portarlo a conoscere le loro credenziali, in modo da passare alla fase c.d. "*Collection*", in cui l'attaccante sottrae realmente ed effettivamente le credenziali alle vittime.

Una volta sottratte le credenziali, l'attaccante pone in essere l'attività fraudolenta vera e propria, nella fase denominata "*Fraud*": utilizzo delle credenziali per l'acquisto di beni, furto di denaro dal conto della vittima, uso delle credenziali per furto di identità o per riciclaggio di denaro.

Infine, vi è l'ultima e finale fase, quella del "*Post Attack*", in cui l'attaccante, dopo aver conseguito i propri scopi fraudolenti, pone in essere qualsiasi azione volta a coprire le proprie tracce e a disattivare i meccanismi con cui ha potuto perpetrare l'attività fraudolenta, verificando anche il successo dell'attacco e cominciando a pianificare i prossimi attacchi[89].

2.1.2 **Tipologie di phishing**

Il phishing, finalizzato all'ottenimento e al successivo utilizzo per scopi fraudolenti delle credenziali dei soggetti lesi, può essere posto in essere mediante diversi tipi di attacchi, in cui è possibile comunque rintracciare le varie fasi tipiche sopra descritte.

2.1.2.1 Deceptive phishing

La tipologia di attacco più utilizzata e comune tra i phisher è quella del "*deceptive phishing*", traducibile come "*phishing ingannevole*", ossia quando il phisher invia ad un gran numero di potenziali vittime un messaggio di posta elettronica ingannevole, con un invito a fare clic su un collegamento web. L'utente, vittima del phisher, viene reindirizzato ad un sito che permette al phisher di raccogliere informazioni riservate riguardanti l'utente, per poi potersi spacciare per quest'ultimo o trasferire denaro o, ancora, acquistare merce o porre in essere qualsiasi altro tipo di danno. In molti casi, il phisher non provoca direttamente un danno economico alla propria vittima, ma rivende le informazioni ottenute fraudolentemente su un mercato secondario tramite forum di mediazione online e canali chat.

[89] Cajani F., Costabile G., Mazzaraco G., *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008, p. 16.

Esistono molte variazioni negli schemi di phishing ingannevole: può, ad esempio, essere presentata una replica della pagina di login a chi legge messaggi in formato HTML direttamente nel testo dell'e-mail, in modo che non vi sia necessità di cliccare su un collegamento web; o, ancora, può essere utilizzato un indirizzo IP numerico in luogo del nome dell'host nella stringa di collegamento ad un sito di phishing, in modo che, per prendere il controllo della barra degli indirizzi di un browser, deve essere usato Javascript oppure c'è bisogno di ingannare in altro modo l'utente facendogli credere che sta comunicando con un sito legittimo.

Le e-mail di phishing, inizialmente, anche in Italia, solo in inglese e poi in un italiano sempre più corretto, prendono come modello una reale comunicazione di servizio della società o ente di riferimento, imitando alla perfezione non solo la grafica del messaggio ma anche il linguaggio adoperato. Cliccando, poi, sul link proposto nel testo della e-mail, la pagina caricata non è quella del sito della società o ente, bensì un sito web fittizio, creato dal phisher, per sottrarre e memorizzare le informazioni fornite dagli ignari utenti. Dunque, possono essere inviate, da parte del phisher, e-mail che invitano ad accedere al sito della propria banca per ottenere il pin di sicurezza; e-mail contenenti un avviso di addebito in conto di un alto importo e la richiesta di cliccare un link per ottenere user id e password dell'utente; e-mail che invitano ad accedere al sito della propria banca proprio perché dei phishers avrebbero attentato alla sicurezza del conto corrente del cliente per raccogliere i dati digitati dalla vittima e inviarli ad un hacker o una banda criminale. Proprio quest'ultimo caso ci fa comprendere come il fenomeno illecito si stia aggravando e allargando, anche grazie all'impiego di tecniche diverse da quella dell'invio di e-mail, e cioè l'utilizzo di virus per carpire informazioni

riservate sui conti bancari o per dirottare gli utenti a veri e propri siti clone al momento della digitazione del sito della propria banca[90].

2.1.2.2 Phishing basato su malware

Con l'espressione phishing basato su malware si intende, generalmente, un tipo di attacco che comporta l'esecuzione di un software o codice maligno sul computer dell'utente a sua insaputa, utilizzando inganni di social engineering o sfruttando le vulnerabilità del sistema di sicurezza. Un tipico inganno di social engineering è quello di convincere un utente ad aprire un allegato di una e-mail oppure a scaricare un file da un sito web, spesso sostenendo che esso sia di carattere pornografico, oppure contente foto particolari o gossip su personaggi celebri; inoltre, anche software scaricabili da internet possono contenere un codice maligno. Il codice suddetto può essere diffuso anche tramite attacchi alla sicurezza, sia mediante la propagazione di worm o virus che approfittano di una vulnerabilità del sistema per installare il codice maligno, sia rendendo disponibile il codice su un sito web che sfrutta una vulnerabilità di sicurezza. La navigazione internet può essere ridirezionata su un sito web fraudolento tramite social engineering, come avviene nei casi di messaggi spam, oppure inserendo un contenuto accattivante per gli utenti su un sito web legittimo, sfruttando una debolezza nella sicurezza del web server[91].

Il phishing basato sul codice maligno può assumere diverse e varie forme: quella della "*session hijacking"*, in italiano "*dirottatori di sistema"*, che è un attacco con cui vengono monitorate le attività di un utente, di solito tramite una componente non legittima del browser, per cui quando egli immette le proprie credenziali di un account

[90] Tale tecnica è denominata "*hijacking".*
[91] C.d. "*Cross-site scripting*".

o effettua una transazione, il software dirotta la sessione per eseguire le azioni miranti a frodarlo; quella dei "*web trojans"*, ossia cavalli di troia sul web, che sono programmi che si agganciano agli schermi di login per prelevare le credenziali, per cui l'utente crede di inserire i propri dati su un certo sito web ma in realtà le informazioni sono immesse localmente e dunque trasmesse al pisher per un uso fraudolento di esse; quella degli "*attacchi di configurazione del sistema"*, tramite i quali vi è una modifica delle impostazioni sul computer dell'utente provocando la compromissione dei dati, come ad esempio quando vengono modificati i server DNS dell'utente, dirottando la sua navigazione su internet verso altri siti fraudolenti. Altra forma di phishing basato su codice maligno è quella dei "*keylogger"*, traducibile in "*registratori di tasti*", che sono programmi che si auto-installano sia nel browser web che nel driver del dispositivo di input, per osservare i dati immessi e inviare quelli che interessano ad un server di phishing. Tali keylogger possono essere implementati tramite l'ausilio di vari strumenti, tra cui un oggetto di help del browser che rileva le modifiche delle URL e registra le informazioni quando l'URL si riferisce ad un sito designato per la raccolta di credenziali, un driver di dispositivo che controlla l'immissione dei dati da tastiera e da mouse e contemporaneamente controlla le attività dell'utente, uno screenlogger che controlla sia le immissioni dell'utente sia le visualizzazioni a video per contrastare le misure di sicurezza sulle immissioni alternative su schermo. I keylogger possono raccogliere credenziali relative ad un'ampia gamma di siti e spesso sono realizzati per monitorare la posizione dell'utente e trasmettere soltanto le credenziali relative a particolari siti. Tali attacchi di phishing tramite codice maligno, molto spesso, proprio

perché possono essere ottenute grandi quantità di dati, anche e soprattutto sensibili, sono utilizzati per il furto di dati finalizzato allo spionaggio industriale.

2.1.2.3 Phishing basato sui motori di ricerca

Il phisher può porre in essere il suo attacco anche mediante la creazione di pagine web dedicate a prodotti fittizi, che vengono poi indicizzate nei motori di ricerca e, in tal modo, gli utenti, facendo un ordine o un'iscrizione o un trasferimento di somme, immettono i loro dati e informazioni, divenendo, così, di dominio del phisher. Tali pagine, tipicamente, offrono prodotti ad un prezzo molto vantaggioso e, in particolare, sono stati utilizzati con successo siti web di banche fraudolente: il phisher crea una pubblicità per un conto corrente con tasso di interesse leggermente più alto di qualsiasi altra banca non fittizia, le vittime trovano la banca tramite i motori di ricerca e inseriscono le credenziali del loro conto bancario per un trasferimento somme verso il nuovo conto[92].

2.1.2.4 Phishing "*Man in the middle*"

Un attacco man in the middle è una forma di phishing con il quale il phisher si interpone tra l'utente e il sito legittimo: i messaggi destinati al sito legittimo passano attraverso il phisher, che salva tutte le informazioni e i dati che possono essere di suo interesse, inoltra i messaggi al sito legittimo e poi inoltra all'utente le risposte di ritorno. Gli attacchi man in the middle possono essere utilizzati anche per il dirottamento delle sessioni con o senza la memorizzazioni delle credenziali compromesse dell'utente. Questo tipo di attacco è difficile da scoprire per l'utente poiché il sito funziona correttamente e può anche non esserci alcuna indicazione

[92] Cajani F., Costabile G., Mazzaraco G., *op. cit.*, p. 30.

esterna che faccia capire che c'è qualcosa di sospetto. Di solito, il traffico Secure Socket Layer (SSL)[93]sul web non è vulnerabile a questo tipo di attacco, in quanto il traffico SSL viene criptato usando la chiave di sessione in modo che non possa essere decodificato da un intercettatore.

Tuttavia, un attacco basato sull'utilizzo di un codice maligno può modificare la configurazione di un sistema per installare una nuova autorità di certificazione fidata e, in tal caso, un man in the middle può creare i propri certificati per un sito protetto con SSL, decriptare il traffico, estrarre le informazioni riservate e poi criptare nuovamente il traffico per comunicare con l'altra parte[94].

2.1.2.5 Rock Phish Kit

Il "*Rock Phish Kit*" è un software reperibile on line che permette di creare siti clone, con aspetto e grafica simile a quelli ufficiali, ma che all'interno contengono una serie di form da compilare tramite i quali vengono sottratti i dati sensibili alle ignare vittime. Il "*Rock Phish Kit*" sfrutta un insieme di software per creare non solo numerosi siti clone, ma anche un'e-mail da utilizzare per lo spam con all'interno i link che reindirizzano al sito clone, sul medesimo server, in modo da attaccare più obiettivi diversi contemporaneamente. Tale tecnica permette, quindi, di trasformare ciascun server in una base da cui far partire attacchi multipli e diversificati, in modo tale da massimizzare le possibilità di riuscita prima che le forze dell'ordine e i gruppi antiphishing riescano a neutralizzare l'attacco.

[93] E' il protocollo standard che garantisce la sicurezza durante il trasferimento di dati da un browser ad un server web.
[94] Cajani F., Costabile G., Mazzaraco G., *op. cit.*, p. 29.

Praticamente, il phisher installa un pacchetto multiplo contente i siti clone di entità finanziarie italiane o straniere, clonando loghi, testi, grafica, trasformando il server ospite in un arsenale pronto a sferrare l'attacco e a trarre in inganno i malcapitati utenti[95].

2.2 **Evoluzione delle tecniche di attacco. Il pharming**

Attualmente, il phishing è in continua evoluzione e, con il passare del tempo e l'evolversi delle tecnologie, si evolvono anche le tecniche di attacco. Infatti, una ancor più pericolosa evoluzione del phishing è il pharming, termine composto dalle parole phishing e farming, che consiste in una tecnica di cracking, capace di colpire più utenti contemporaneamente, volta ad ottenere l'accesso ad informazioni personali e riservate, senza la necessità di aprire alcuna e-mail.

Il pharming è una tecnica di truffa on line che consiste nella manipolazione degli indirizzi di DNS (Domain Name Server) che utilizza l'utente, in modo tale che le pagine web visualizzate dall'utente, create ad hoc dai pirati informatici, non siano quelle originali, anche se il loro aspetto è identico. Per comprendere meglio il pharming, bisogna innanzitutto comprendere che cosa si intende per manipolazione degli indirizzi DNS. Quando si inserisce un determinato indirizzo di una pagina web nel proprio browser in forma alfanumerica, lo stesso viene tradotto automaticamente in un indirizzo IP numerico che serve per raggiungere in internet il server web corrispondente a quel dominio, poiché sarebbe estremamente complesso dover ricordare sequenze di numeri che identificano tutte le pagine web da visitare. Infatti, è più facile scrivere nel motore di ricerca, ad esempio, www.bancadiroma.it e poi

[95] Cajani F., Costabile G., Mazzaraco G., *op. cit.*, p. 30.

lasciare che il server DNS del provider lo traduca in un indirizzo IP in formato numerico. La tecnica del pharming, attaccando i server DNS, mira a cambiare la corrispondenza numerica di tali server DNS, in modo tale che essi decodifichino una corrispondenza numerica distinta da quella reale e portino l'utente ad una pagina identica a quella di riferimento, ma creata dai pirati informatici. A questo punto, l'utente sarà convinto di navigare sul sito giusto e, nel momento in cui utilizza le proprie credenziali di accesso, esse, automaticamente, sono conosciute anche dal soggetto attaccante.

Un altro tipo di pharming, anche più pericoloso e dannoso, è quello che si realizza a livello locale, cioè in ogni computer: è necessario modificare una cartella chiamata "*HOSTS*", contenuta in qualsiasi computer che utilizzi Windows come sistema operativo ed Internet Explorer per per la navigazione in Internet, poiché nell'archivio "*HOST*" vi è immagazzinata una piccola tabella con gli indirizzi di server e indirizzi IP più utilizzati dall'utente e modificandola accadrà che, nel momento in cui si scriverà la URL nel motore di ricerca, automaticamente si verrà reindirizzati alla pagina web fittizia. Il pirata informatico potrà entrare nel computer della vittima o in forma remota, o sfruttando qualche vulnerabilità del sistema, o attraverso un virus.

In generale, un attacco di pharming deve rivolgere le proprie attenzioni agli anelli più deboli della catena di macchine che servono per connettersi ad un "*HOST*" ed, infatti, sempre più spesso una modalità di attacco consiste nell'infettare i router casalinghi, usati per connettersi all'adsl, di solito poco protetti.

La maggiore pericolosità di questo tipo di attacchi consiste nel fatto che non occorre convincere l'utente a visitare siti fasulli, né occorrono e-mail esca, la vittima non ha

alcun elemento per ipotizzare di essere connessa ad un server "*trappola*" in quanto esso è perfettamente somigliante a quello vero, inoltre l'evidenza dell'attacco può essere facilmente rimossa e, quindi, la rilevanza delle attività di indagine è fortemente ridotta.

Il pharming è in relativa crescita, soprattutto grazie all'incremento della presenza di malware, in quanto, ormai spesso, programmi all'apparenza innocui nascondono al loro interno malware capaci di modificare le componenti del sistema operativo, attivando servizi di pharming all'insaputa dell'utente. Tale fenomeno è, come già detto, molto più pericoloso del phishing tradizionale, proprio a causa della portata delle modifiche che un sistema di pharming riesce a compiere sul sistema operativo della macchina target, poiché le tecniche di difesa sono le stesse adottate per i sistemi di anti-malware.

Nei prossimi anni, il fenomeno è destinato ad una forte crescita, anche a causa dell'incremento degli attacchi con tecniche di rootkit[96], in riferimento ai quali spesso i sistemi antimalware si trovano in difficoltà. In Italia un attacco simile si è verificato nell'ottobre del 2006, da un provider russo, in riferimento ad un indirizzo che apriva una pagina del tutto simile a quella del sito di Poste Italiane, con la richiesta di inserimento di user name e password e, successivamente, l'inserimento delle 10 cifre del codice dispositivo. La complessità di tale attacco risiedeva nel fatto che l'indirizzo

[96] Il Rootkit è un tipo di malware usato per attaccare i computer ed eludere i sistemi di sicurezza, studiato in modo tale da non essere rilevato dalle applicazioni anti-malware e dai principali strumenti di controllo e sicurezza; esso permette all'hacker di installare una serie di strumenti che gli danno accesso al computer da remoto in modo che egli possa rubare password, informazioni bancarie e dati di carte di credito, bot per attacchi DDos e diverse funzionalità in grado di disabilitare i software di sicurezza.

del sito era visibile soltanto dai computer infettati da specifici malware e non rintracciabile con i tradizionali metodi di analisi[97].

2.2.1 **Smshishing**

Lo Smshishing, ossia SMS phishing, è la nuova frontiera del phishing: attraverso l'uso di sms o di applicazioni cosiddette "*malevole*" sugli smartphone, i pirati informatici si impossessano dei dati degli utenti. All'ignaro utente viene inviato un messaggio sul cellulare, presumibilmente da una fonte affidabile, con l'invito a cliccare su un link e la promessa di un premio o comunque con una proposta particolarmente vantaggiosa e, una volta cliccato, si apre un sito creato ad hoc nel quale l'utente deve inserire le proprie credenziali, che diventeranno, poi, di dominio anche dell'attaccante.

Gli attacchi tramite la tecnica di Smshishing sono iniziati quando gli aggressori hanno cominciato ad utilizzare servizi automatizzati che consentono l'invio di molti messaggi sms in una sola volta. Infatti, gli attaccanti inviano messaggi, facendo figurare che il mittente sia un soggetto affidabile, come ad esempio la banca di cui la vittima è correntista, che di solito seguono uno stesso modello, cioè avvisano le vittime di un determinato urgente bisogno da soddisfare e della necessità di mettersi in contatto con il soggetto di riferimento. Quando la vittima chiamerà il numero indicato nel messaggio, una voce registrata gli chiederà i dettagli di numero di carta di credito e il codice PIN, o altri dati e informazioni sensibili: l'attaccante ha, quindi, ottenuto ciò per cui ha posto in essere l'attacco.

Anche la stessa tecnica del Smshishing, con il tempo, si è evoluta e sempre più spesso il contenuto degli sms truffaldini ricevuti dai malcapitati utenti chiedono non più di

[97] Cajani F., Costabile G., Mazzaraco G., *op. cit.*, p. 40.

chiamare un numero telefonico, bensì di aggiornare i propri account o promettono ricariche premio gratuite, invitandoli a visitare pagine web di siti commerciali e di istituti di credito, chiedendo dunque l'inserimento delle credenziali tramite internet.

Gli attacchi di questo tipo sono particolarmente pericolosi in quanto fanno leva sull'affidamento che un utente ripone negli sms ricevuti da un mittente che, all'apparenza, è conosciuto e aventi un contenuto che sembra, sempre all'apparenza, avere carattere di urgenza, senza immaginare che essi possano invece avere carattere truffaldino. Però, non sempre tali attacchi sono posti in essere con un meccanismo sofisticato: infatti, spesso, il numero da comporre non riesce a gestire più di una chiamata alla volta, oppure la qualità della chiamata non è delle migliori e la connessione non funziona come dovrebbe.

Ad ogni modo, per difendersi da tale tipo di attacchi, sarebbe necessario, una volta ricevuto il messaggio, chiamare la propria banca o il soggetto che figura come mittente per accertarsi dell'effettiva autenticità dell'sms.

2.2.2 **Fast Flux**

Il metodo denominato Fast Flux, anch'esso evoluzione delle tecniche di attacco phishing, è quello che consente di modificare continuamente, ad intervalli brevissimi di tempo, gli indirizzi IP e domain server dei computer infettati da virus e utilizzati per ospitare siti di phishing. I domini Fast Flux stanno notevolmente aumentando, sono sempre più utilizzati dai phisher in quanto rendono più difficile l'identificazione dei siti clone ed è, dunque, più difficile la loro chiusura. In questi casi, il phisher evolve la propria metodologia di attacco: invia una e-mail contenente un messaggio di collegamento al sito clone all'utente, che, confidando dell'autenticità del messaggio,

clicca sul link che appartiene alla rete di personal computer infettati da malware rispondenti ai comandi da remoto del phisher[98] ed inserisce le proprie credenziali sul sito clone[99], che cattura le credenziali e reindirizza automaticamente l'utente sul sito originale, così che non possa accorgersi di nulla. In tali casi, l'indirizzo IP a cui si connetterebbe il browser dell'utente cambia randomicamente ogni tre minuti, collegandosi a differenti computer facenti parte della rete dei computer infettati da malware e controllati dal phisher: in questo modo, con il cambiamento continuo, è difficile risalire al server principale che ospita il sito clone ed è anche più facile per l'aggressore disporre di computer c.d. "*zombies*[100]" attivi e pronti all'uso.

Ad oggi, esistono due tipologie di rete Fast Flux: una prima, denominata Singol Flux ed un'altra, denominata Double Flux, che sfrutta una complessa tecnica basata su un doppio livello di cambiamento degli indirizzi IP.

Di recente, le aziende produttrici di software antivirus hanno individuato un particolare tipo di virus, il virus storm worm, quale veicolo principale di diffusione degli attacchi, stimandolo in circa due milioni di unità e la propagazione massima è stata registrata tramite alcuni filmati caricati sul sito YouTube.

Un esempio di Fast Flux si può rintracciare prendendo in considerazione un attacco ai clienti di Poste Italiane, che, digitando l'URL del sito di Poste Italiane, di cui l'attaccante aveva creato un sito clone, hanno involontariamente attivato un javascript nascosto che ha scaricato automaticamente sul loro computer un trojan, facendo sì che anche l'attaccante potesse avere accesso al computer del cliente.

[98] C.d. *Botnet-fast flux.*
[99] C.d. *Back-end.*
[100] Un computer c.d. "*zombies*" è un computer infettato da un codice maligno in attesa di essere attivato.

Nonostante i gruppi anti-phishing e i responsabili della sicurezza informatica degli enti colpiti abbiano condotto studi che hanno permesso di individuare le strategie idonee ad identificare l'indirizzo IP del sito clone e di effettuarne la chiusura, il Fast Flux rimane comunque una tecnica di attacco molto pericolosa, in quanto vi è forte difficoltà a procedere ad una veloce individuazione e chiusura del sito clone, che spesso viene anche occultato mediante proxy e, quindi, rimane la tecnica che permette massimizzazione di profitti con il minimo degli sforzi[101].

2.2.3 **Tabnabbing**

Il Tabnabbing è una nuova forma di phishing, letteralmente significa "catturare *la scheda di un browser*" e sfrutta l'abitudine degli utenti di aprire più schede, cosiddette "*tabs*", all'interno del browser durante la normale navigazione, per consultarle poi una ad una. Infatti, tramite la tecnica del tabnabbing, la vittima, navigando in Internet, clicca su un link e si apre una pagina dall'aria del tutto innocua, che non richiede l'inserimento di password o di altri dati, ma che ha,anzi, un contenuto interessante, spesso immagini osè o simili, e, quindi, l'utente non la chiude, passando ad un'altra scheda del browser. Quello che l'utente non si aspetta è che la pagina-trappola, mentre egli continua a navigare consultando altre pagine del browser, si trasforma e cambia la propria icona[102] e il proprio contenuto, diventando una pagina che richiede l'autenticazione per un servizio adoperato dall'utente: per esempio, la login della propria banca, della propria web mail, del proprio account Facebook o Twitter. L'utente, vedendo l'icona del sito noto sulla scheda, pensa di averla aperta e, visitandola, si trova davanti una pagina familiare, che richiede l'inserimento delle

[101] Cajani F., Costabile G., Mazzaraco G., *op. cit.*, p. 41 e ss..
[102] C.d "*Favicon*".

proprie credenziali di accesso e, dunque, egli fornisce i propri dati di autenticazione senza controllare che l'URL della pagina sia corretto: a questo punto l'aggressore entra in possesso delle credenziali dell'utente tramite lo script truffaldino che le memorizza e porta poi l'utente, ignaro e senza alcuna percezione di essere stato derubato del proprio account, sulla vera pagina, autenticandolo realmente.

Tale tecnica si basa sull'idea, sbagliata, dell'utente medio che utilizza Internet, che una scheda del browser sia immutabile e usa il forte richiamo visivo di un'icona, ancora più forte se si tratta di un'icona conosciuta dall'utente.

La soluzione migliore contro questo tipo di trappola è aprire sempre una scheda nuova per fare login a qualunque servizio e immettere manualmente l'indirizzo oppure prenderlo dai Preferiti, a maggior ragione perché e quando viene richiesto l'inserimento delle proprie credenziali di accesso.

2.2.4 **Vishing e financial manager**

Sempre più sofisticate sono le tecniche finalizzate a "*pescare*" i dati finanziari e quelli sensibili degli utenti in rete e va, quindi, diffondendosi un nuovo fenomeno dai risvolti penalmente rilevanti, il vishing, termine coniato dall'unione delle parole VoIP (Voice over Internet Protocol) e phishing.

La tecnica del vishing si articola nell'invio, dal parte del cosiddetto visher, di una e-mail che simula nella grafica e nel contenuto una società o un ente noto al destinatario, quale ad esempio la sua banca o un sito a cui il destinatario è realmente iscritto, contenente avvisi di particolari situazioni o problemi verificatisi con il proprio conto corrente o account, quale ad esempio un addebito economico o l'avvenuta scadenza dell'account, e invita il destinatario a comporre un numero telefonico per evitare

l'addebito o regolarizzare la sua posizione con l'ente o la società. Il destinatario, composto il numero telefonico, avrà contatti con un falso centralinista che gli chiederà di fornire i propri dati personali, in particolare il numero di conto corrente o di carta di credito: le informazioni così raccolte finiscono nelle mani del visher, che le utilizzerà per acquistare beni, trasferire somme di denaro o anche solo come strumento per ulteriori attacchi, magari utilizzando l'identità di un altro individuo[103].

Un'altra tecnica di vishing è quella che consiste nell'attivazione di un account VoIP e nell'avvio di un sistema di chiamata automatico per contattare le potenziali vittime ed invitarle, tramite la riproduzione di una registrazione vocale, a comporre un numero telefonico, che viene fatto credere di essere di un call center in grado di risolvere problemi o fornire comunicazioni urgenti sul proprio conto corrente bancario o sulla propria carta di credito, previo inserimento de dati personali, ma in realtà è il numero VoIP del visher. Infatti, il fenomeno dei falsi call center è in forte crescita: i truffatori puntano sul fatto che vi è meno diffidenza a comunicare le proprie informazioni personali a voce, ad una persona che lavora per un call center e non rispondere ad una semplice e-mail[104].

Strettamente connesso al fenomeno del vishing è il ruolo dei financial manager, soggetti che mettono a disposizione i propri conti correnti per il deposito delle somme di denaro sottratte dai phisher alle vittime tramite le descritte tecniche illecite, per poi, una volta ricevuto l'accredito, prelevarle e ritrasferirle all'estero dietro compenso. I phisher necessitano, infatti, di essere affiancati da un financial manager poiché, dopo

[103] Surace C., *Dal Phishing al Vishing: l'evoluzione della truffa come conseguenza dell'evoluzione tecnologica* (a cura di) , Ricerca svolta presso l'Osservatorio CSIG (Centro Studi Informatica Giuridica) di Reggio Calabria, in www.filodiritto.com, 2007

[104] Sambucci L., *Falsi call center sul VoIP: la nuova truffa si chiama Vishing*, in www.anti-phishing.it , 2006

l'acquisizione delle credenziali e la possibilità di disporre di bonifici online in frode, nasce il problema di come incassare le relative somme, dal momento che l'home banking italiano non consente bonifici verso l'estero se non tramite ulteriori controlli degli istituti bancari. Dunque, quasi contemporaneamente all'invio delle e-mail di phishing, si registra la richiesta, preferibilmente sempre veicolata da messaggi di posta elettronica provenienti da fantomatiche società estere, di collaborazione indirizzata a cittadini italiani o residenti in Italia. A tali soggetti, per adempiere al ruolo di financial manager, viene chiesto di comunicare le coordinate del proprio conto corrente, in quanto l'attività loro proposta consisterà proprio nel prelevare somme di denaro di volta in volta accreditate su tali conti e apparentemente provenienti da clienti di tali società, ma che in realtà provengono dai soggetti frodati, al fine di ritrasferirle all'estero[105]. Il reato in questo caso integrato è quello di riciclaggio di denaro: il financial manager trasferisce risorse provenienti da un'attività illecita da parte di un soggetto estraneo alla commissione del reato presupposto, così come previsto e sanzionato, appunto, dall'art. 648 bis c.p..

2.3 **Il phishing nel nostro ordinamento: norme applicabili**

L'attualità del fenomeno non ha permesso il formarsi, nell'ordinamento giuridico italiano, di una normativa ad hoc atta a regolare, definire e sanzionare la pratica illecita del phishing. Gli illeciti connessi a tale fenomeno vengono ricondotti, di volta in volta, a seconda della manifestazione e del *modus operandi*, nell'alveo delle diverse

[105] Cajani F., *Profili penali del phishing*, in CP, 2007, p. 2294.

fattispecie di natura civile e penale già disciplinati e puniti dalla legge, senza pretesa alcuna di esaustività, trattandosi di un fenomeno dinamico e in continua evoluzione.

Dopo i primi casi di phishing nel 2005 e la crescita di tale fenomeno nei successivi anni, vi sono state due interrogazioni parlamentari[106] volte a mettere alla luce la necessità di incrementare e migliorare gli interventi della polizia postale e di porre in essere iniziative concrete per debellare alla fonte tali azioni delittuose dei pirati informatici. La risposta a tali interrogazioni[107] è stata quella di informare che sul piano della prevenzione, la polizia postale, in collaborazione con l'ABI[108] e con Poste Italiane, ha avviato un'attività di sensibilizzazione degli utenti che, attraverso gli istituti bancari, sono avvisati del pericolo rappresentato dal fenomeno del phishing. Invece, sul piano della repressione, la polizia postale ha avviato circa 1200 indagini di iniziativa propria e circa 900 su richiesta dell'autorità giudiziaria e tali interventi hanno permesso di denunciare circa 80 persone e di procedere a perquisizioni, nonché di appurare che la maggior parte delle minacce proveniva dall'est Europa.

Tutt'oggi il nostro legislatore non si è ancora occupato di porre in essere una normativa che disciplini i casi di phishing attacks e, dunque, per comprendere quali norme vigenti possono essere applicate, a seconda dei casi, alle violazioni riconducibili alla pratica del phishing, è indispensabile tenere in considerazione ciascuna delle tre fasi in cui esso può suddividersi. A tal fine, possono distinguersi: una prima fase, consistente nell'invio di un messaggio di posta elettronica, contenente

[106]Camera dei Deputati, Resoconto stenografico seduta n. 82 del 5 dicembre 2006- Allegato B, pp. 2708 ss. in http://www.camera.it/_dati/leg15/lavori/stenografici/sed082/pdfbt01.pdf ; Camera dei Deputati, Resoconto stenografico seduta n. 100 del 30 gennaio 2007- Allegato B, p. 3537 in http://www.camera.it/_dati/leg15/lavori/stenografici/sed100/pdfbt07.pdf

[107] Camera dei deputati, Resoconto stenografico seduta n. 101 del 31 gennaio 2007, pp. 40 ss. In http://www.camera.it/_dati/leg15/lavori/stenografici/sed101/s000r.htm

[108] Associazione Bancaria Italiana.

il link di indirizzamento alla pagina web non autentica, diretto ad indurre un soggetto utente o fruitore di un servizio on line a rivelare informazioni personali di carattere riservato; una seconda fase, di "*raccolta*" o "*pesca*" dei dati riservati del soggetto utente o fruitore del servizio on line tramite tale sito, ovvero attraverso un form da compilare contenente le stringhe corrispondenti alle informazioni personali richieste; ed una terza fase, in cui vi è l'utilizzo delle informazioni raccolte per accedere abusivamente ai servizi on line o ad aree riservate, o per utilizzare indebitamente carte di credito o di pagamento, realizzando un profitto.

Già da questa schematizzazione appare evidente che i phishing attacks non aggrediscono immediatamente il patrimonio del soggetto passivo, ma esprimono una autonoma dimensione offensiva, il cui fulcro si concretizza in una forma di "*identity theft"*, ovvero in un *"furto di dati*" identificativi o, *latu sensu,* riservati, che si traduce nella realizzazione di una serie di attività riconducibili all'uso non autorizzato di dati fraudolentemente raccolti.

Venendo, quindi, all'esame delle norme penali vigenti astrattamente applicabili, appare opportuno procedere mantenendo la distinzione fasica, pur nella consapevolezza che alcune manifestazioni criminose possono assumere una valenza plurioffensiva o astrattamente riconducibile a più fasi. Con riferimento alla prima fase dei phishing attacks, relativa all'invio di messaggi di posta elettronica solo apparentemente provenienti da mittenti "*reali*", potrebbe anzitutto prospettarsi l'applicazione, seppur limitata, della norma di cui all'art. 494 c.p., qualora vengano utilizzati on line gli estremi identificativi di un mittente reale, così da integrare le modalità tassativamente previste della sostituzione illegittima di persona, o

dell'attribuzione *"a sè o ad altri di un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici*". Le condotte concrete caratterizzanti questa prima fase possono essere realizzate anche nella terza fase, in cui il phisher utilizza i dati "*pescati*" nella seconda fase, per accedere ad aree o servizi on line riservati e porre in essere attività illecite. Se la condotta volta all'acquisizione delle credenziali viene posta in essere attraverso la collocazione di un virus, su un sito internet appositamente creato oppure in un allegato ad un messaggio di posta elettronica preventivamente inviato all'utente, può ritenersi, altresì, applicabile, nella prima fase, l'art. 615 *quinquies* c.p.,disciplinante l'ipotesi di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

La dimensione offensiva del fenomeno del phishing trova la sua peculiare manifestazione nella sua seconda fase, cioè nell'attività diretta a "*pescare*" i dati riservati degli utenti. Ci si chiede, perciò, se questa fase dei phishing attacks possa essere riconducibile alle condotte tipiche previste dall'art. 615 *quater* c.p., rubricato "*detezione e diffusione abusiva dei codici di accesso a sistemi informatici o telematici*", nonché se fra le modalità di realizzazione del fatto tipico possa essere incluso anche l'invio di una e-mail con contenuto tale da indurre il destinatario a fornire informazioni riservate.

Tale norma deve essere letta ed interpretata considerando il requisito di illiceità speciale caratterizzante le condotte, il quale coinvolge le stesse modalità fraudolente di raccolta dei codici di accesso, per cui il legislatore non ha espressamente previsto delle forme vincolate. Non vi sono ostacoli, quindi, per

ritenere incluso nella locuzione "*procurarsi abusivamente*" anche l'invio di una e-mail che contribuisca all'effettiva raccolta di detti codici.

Questi ultimi rappresentano l'oggetto materiale su cui ricade l'attività del reo, tecnicamente comprendono un qualsiasi codice numerico, alfabetico e alfanumerico e, grazie alla clausola estensiva prevista al comma 1, includono certamente fra gli "*altri mezzi idonei all'accesso"* anche l'indirizzo e-mail o il numero di carta di credito, ove svolgano le funzioni tipiche di identificazione dell'utente per abilitarlo all'accesso ai servizi on line, in abbinamento con passwords o parole chiave.

La "*pesca*" dei dati personali dell'utente, con evidente sottrazione ed impossessamento di essi, hanno fatto pensare alla possibile applicazione, nella seconda fase dell'attività di phishing, della fattispecie penale disciplinante il furto. Non è però possibile applicare l'art. 624 c.p., in quanto la "*raccolta*" o l'"*acquisizione*" di dati riservati non costituisce né un "*impossessamento"* né una "*sottrazione"* di una *"cosa mobile altrui"*. Infatti, i dati e le informazioni riservate o personali dell'utente non sono propriamente *res*, bensì oggetti per natura immateriali e non idonei ad essere "*sottratti*", in quanto essi rimangono a disposizione anche del titolare e non si verifica l'acquisizione a favore del phisher di un potere di dominio esclusivo. Inoltre, le modalità tipiche di manifestazione delle condotte di furto presuppongono l'usurpazione unilaterale e il dissenso del soggetto passivo, che non si realizza nella seconda fase dei phishing attacks, in quanto vi è una cooperazione della vittima che, anche se indotta in errore tramite il contenuto dell'e-mail ed il sito non autentico, fornisce i propri dati.

La terza ed ultima fase dei phishing attacks è quella diretta all'utilizzo delle informazioni raccolte. A tale fase della condotta dei phishers è possibile applicare la fattispecie di frode informatica, qualora, però, sussistano gli elementi costitutivi del reato di cui all'art.640 *ter* c.p.: ad esempio, se essi, tramite l'utilizzo delle informazioni raccolte, intervenissero, per via informatica, sui dati, sulle informazioni o sui programmi dell'utente, modificando i dati relativi alle operazioni bancarie e finanziarie, oppure inerenti al conto corrente, al fine di procedere ad addebiti, a trasferimenti di fondi, all'utilizzo indebito di carte di credito o di pagamento o ad ogni altro abuso di simili servizi on line. Se, invece, simili operazioni, riconducibili a tale ultima fase, venissero effettuate mediante o a seguito di un accesso abusivo ad uno o più sistemi informatici, potrebbe configurarsi un concorso formale di reati con l'art. 615 *ter* c.p., astrattamente ammissibile. Inoltre, l'utilizzo dei dati e delle informazioni è, per la maggior parte delle volte, legato all'accesso abusivo ad aree informatiche riservate o a servizi online per eseguire operazioni bancarie o finanziarie, dunque è astrattamente applicabile anche il solo art. 615 *ter* c.p.. A tale ultima fase è possibile applicare anche l'art. 640 c.p.[109], disciplinante la truffa, in quanto il phisher, mediante artifici e raggiri realizzati attraverso l'invio di false e-mail e la creazione di false pagine web in tutto simili a quelle di primari istituti di credito, dopo aver indotto in errore l'utente ed essersi fatto rivelare le credenziali di accesso, si introduce nel servizio di home banking della vittima per effettuare operazioni di prelievo o bonifico on line non autorizzate. Infine, riferendoci alla fase dell'utilizzo dei dati, è possibile anche

[109] E'possibile applicare la fattispecie di truffa anche alle prime due fasi dei phishing attacks: false e-mail e falsi siti web quali artifici e raggiri, in riferimento alla fase dell' "*esca*"; successivamente, l'induzione in errore e la rivelazione da parte dell'utente delle credenziali, in riferimento alla fase della "*pesca*".

applicare l'art. 12 del d.l. n. 143/ 1991, in quanto, dopo aver carpito le credenziali delle carte di pagamento delle vittime, i phishers utilizzano in modo indebito le stesse.

2.3.1 **Truffa attraverso il phishing**

L'attività di phishing può essere ricondotta alla fattispecie di truffa, disciplinata dall'art. 640 c.p., quando il soggetto agente, mediante gli artifici e i raggiri derivanti dalla sostituzione di persona, realizzata attraverso la creazione ed utilizzazione di un account di posta elettronica ed attribuzione falsa delle generalità di un diverso soggetto, dopo avere indotto in errore la vittima ed essersi fatto rivelare le credenziali di accesso, si introduce nel suo servizio di home-banking, compiendo un atto dispositivo che comporta una depauperazione del patrimonio della vittima, con pari profitto in proprio favore.

L'elemento oggettivo è perfettamente integrato dalla condotta del reo, che fa credere alla persona offesa di essere chi non è, ad esempio la banca di fiducia o una nota società di e-commerce, di modo che la vittima venga indotta in errore e comunichi i propri dati. Successivamente, il soggetto indotto in errore pone in essere l'atto di disposizione patrimoniale, che è effetto dell'errore in cui è stato indotto e, allo stesso tempo, causa dell'ingiusto profitto con altrui danno. Del resto, l'appropriazione fraudolenta di codici e password non è altro che il mezzo con cui il reo può ottenere, con gli artifici e raggiri tipici del phishing, l'indebito profitto patrimoniale[110] e ciò,senza dubbio, realizza la condotta e l'evento propri della truffa.

[110] Fanelli A., *Commento all'art. 640 C.P.*, in Lattanzi-Lupo, Codice Penale, *Rassegna di giurisprudenza e di dottrina*, Giuffrè, 2005, p. 157.

A conferma del fatto che il comportamento criminoso del phisher può essere idoneo ad integrare lo schema dell'induzione in errore del soggetto passivo, che rappresenta il modus operandi tipico della fattispecie di truffa, vi è una nota sentenza[111] del 2011 emanata dal Tribunale di Milano. In tale sentenza, si è affermato che possono essere considerati artifici e raggiri quelli che pone in essere chi utilizza una e-mail in cui vengono riprodotti colori, marchi ed altre caratteristiche degli enti reali. Inoltre, sono stati considerati come realizzati anche gli altri elementi costitutivi della fattispecie, in particolare il danno è risultato di evidente e rilevante gravità per le ignare vittime.

La truffa, tipico delitto fraudolento contro il patrimonio, si caratterizza per l'inganno con cui un soggetto viene indotto a compiere un atto che determina una deminutio del suo patrimonio, consistente, nel caso di utilizzo della tecnica di phishing, nell'invio massiccio di messaggi di posta elettronica falsi e ingannevoli apparentemente provenienti da enti affidabili, che invitano a comunicare le proprie credenziali o codici di accesso. Dunque, le ipotesi più comuni di phishing, consistenti nell'abusiva captazione di dati personali poi utilizzati per sottrarre somme di denaro, rientrano nella fattispecie di cui all'art. 640 c.p.: ricorrono nelle false e-mails inviate l'elemento degli artifici e raggiri, l'induzione in errore del cliente della banca e l'ingiusto profitto con l'altrui danno[112].

2.3.2 **Frode informatica attraverso il phishing**

La condotta di phishing potrebbe anche integrare gli estremi del reato di frode informatica, di cui all'art. 640 *ter* c.p., in quanto essa comporta l'induzione in errore

[111] Trib. di Milano, Sez. 8, 7 ottobre 2011, n. 11696.
[112] Amore S., Stanca V., Staro S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Massa Carrara, 2006, p. 73 ss.

della persona, che inconsapevolmente fornisce i propri dati personali e l'intervento, sine titulo, nel sistema informatico di un istituto di credito o altro ente. Infatti, l'agire del phisher sembrerebbe potersi ricondurre ad una frode abilmente compiuta con mezzi informatici, anche in considerazione dei beni giuridici tutelati da tale norma, costituiti dal patrimonio del danneggiato, dall'interesse alla regolarità del funzionamento dei sistemi informatici ed alla riservatezza che ne deve accompagnare l'utilizzazione. Ma l'elemento oggettivo di tale fattispecie richiede la necessaria realizzazione di una delle due condotte tipiche prefigurate dalla norma, l'alterazione del funzionamento di un sistema informatico oppure l'intervento su dati, informazioni o programmi contenuti nel sistema.

Quindi, la semplice acquisizione o duplicazione di dati non vale ad integrare, di per sé, l'elemento materiale della frode informatica, ma possono considerarsi riconducibili a tale reato solo quegli interventi volti a porre in essere alterazioni del funzionamento del sistema o manipolazioni arbitrarie dei contenuti: così, ad esempio, l'utilizzazione della password, illecitamente ottenuta, per entrare nel sistema informatico di home-banking del correntista, per poi effettuare un ordine di bonifico dal conto corrente[113]; o, ancora, in quei casi in cui vengano utilizzati i c.d. programmi key-logger, per l'intrusione nei computer degli utenti e l'estrazione abusiva di dati e informazioni sulle operazioni compiute attraverso quei sistemi informatici. Dunque, nei casi di phishing basato su malware, il ricorso ad un software malevolo che va ad auto-installarsi sul personal computer dell'utente, potrebbe integrare gli estremi del reato di frode

[113] Cass. Pen., Sez. II, 24 febbraio 2011 n. 9891.

informatica, in quanto comunque, con la sua condotta, il phisher provvede ad inserire un elemento logico senza il consenso espresso o tacito dell'utente[114].

L'attività di phishing, prevedendo l'invio, da parte del phisher, di e-mails che riproducono grafica e loghi ufficiali di siti aziendali o istituzionali come quelli postali o bancari ad un elevato numero di destinatari, integra, indubbiamente, il furto o l'indebito utilizzo dell'identità digitale di uno o più soggetti, circostanza aggravante del reato di frode informatica[115]. E' necessario, a questo punto, verificare il rapporto tra l'art. 494 c.p., così come esteso in via interpretativa dalla Corte di Cassazione[116] al mondo online, e l' art. 640 *ter* c.p..

La presenza nel testo dell'art. 494 c.p. di una clausola di riserva ben definita , "*se il fatto non costituisce un altro delitto contro la fede pubblica*", a prima vista non porrebbe alcun problema circa la possibilità di un concorso materiale tra i due reati, attesi i beni e gli interessi differentemente tutelati. Tuttavia, pur riconoscendosi in astratto una non perfetta sovrapponibilità tra la condotta di chi "*sostituisca illegittimamente la propria all'altrui persona, o attribuisca sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici*" e quella di chi "*rubi o indebitamente utilizzi una identità digitale con altrui danno*"[117], pare forse più correttamente sostenibile, nella maggior parte dei casi concretamente

[114] Flor R., *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen*., 2007, p. 905.

[115] Tale circostanza aggravante è stata introdotta al terzo comma dell'articolo 640 ter dalla legge n. 93/2013.

[116] Cass. Pen., Sez. V, 8 novembre 2007, n. 46674, in C.E.D. Cass., n. 238504. La massima: *"Integra il reato di sostituzione di persona, art. 494 c. p., la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale)".*

[117] Flor R., *Phishing, identity theft e identity abuse:le prospettive applicative del diritto penale vigente*, in RIDPP, 2007, p. 908.

ipotizzabili, la tesi di un concorso formale tra reati, attribuendo così la natura di reato complesso alla nuova previsione dell'art. 640 *ter* comma 3 c.p..

E', poi, opportuno anche verificare l'applicabilità del comma 3 dell'art. 640 *ter* ad altre ipotesi fattuali quali, ad esempio, le c.d. truffe su piattaforme di commercio elettronico, fenomeno in continua crescita e con un *modus operandi*, o i casi di acquisizione indebita di un account personale e/o profilo di piattaforma di social network.

Il fenomeno delle c.d. truffe su piattaforme e-commerce, infatti, sconta gli effetti del furto di identità sotto una duplice fenomenologia: da un lato, vi è il furto dell'identità dell'utente tramite e-mail di phishing apparentemente provenienti dalle società che gestiscono le piattaforme di commercio elettronico; dall'altro, una volta acquisita tale falsa identità digitale, vengono effettuate inserzioni di vendita fittizie, allo scopo di ottenere pagamenti anticipati tramite carte ricaricabili, anch'esse oggetto di un precedente furto di identità. La nuova disposizione *ex* art. 640 *ter* comma 3 c.p. sembrerebbe essere astrattamente idonea a disciplinare tali ipotesi illecite in maniera più adeguata, rispetto agli artt. 494 e 640 c.p., in quanto non vi è dubbio che, nella condotta immediatamente successiva al furto di identità digitale e consistente nella realizzazione delle inserzioni di vendita fittizie, possa concretizzarsi l'ipotesi di un intervento senza diritto sui dati e/o informazioni contenuti nel sistema informatico messo a disposizione dell'utente originario dalle richiamate società di e-commerce. Analogo discorso potrebbe essere fatto in relazione alle ipotesi, fino ad oggi inquadrabili negli artt. 494 e 615 *ter* c.p., di acquisizione indebita di un account personale e/o profilo di piattaforma di social network. Anche in tali casi, infatti,

immediatamente dopo la condotta di accesso abusivo al relativo sistema informatico, si configura, nella condotta volta all'utilizzo, a fine di profitto e con altrui danno, della identità digitale così illecitamente acquisita, un intervento senza diritto su dati e/o informazioni contenuti nel suddetto sistema informatico.

Altro elemento a favore della configurabilità del reato di frode informatica nel caso di attività di phishing è l'evento di tale fattispecie di reato, che consiste nel conseguimento, da parte del soggetto attivo, di un ingiusto profitto con altrui danno[118], di carattere economico-patrimoniale: nel caso del phishing il profilo economico avuto di mira dall'hacker integra perfettamente tale astratta determinazione di depauperamento patrimoniale cui corrisponde l'ingiusto arricchimento del reo.

2.3.3 **Accesso abusivo a un sistema informatico o telematico attraverso il phishing**

L'accesso all'account della vittima senza aver nessun titolo ed eludendo le misure di autenticazione e identificazione predisposte per garantire la tutela dei dati in esso contenuti, vale a dire l'esatta condotta del phisher, può integrare il reato di "*accesso abusivo ad un sistema informatico o telematico*", disciplinato dall'art. 615 *ter* c.p..

Tale reato si perfeziona con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, dunque quando, ad esempio, il phisher accede al servizio di home banking della vittima, dopo aver carpito illecitamente le sue credenziali di accesso.

L'abusiva intrusione o l'indebita permanenza nel collegamento con i sistemi informatici, contro la volontà dell'avente diritto, persona fisica o persona giuridica,

[118] Cass. Pen., Sez. V, 24 novembre 2003, n. 4576, in *Giur. It.*, 2004, p. 2363.

comporta la lesione dell'interesse specificamente tutelato da questa norma, e cioè la riservatezza del domicilio informatico, inteso come "*luogo in cui può estrinsecarsi la personalità individuale*", che rappresenta la trasposizione sul piano virtuale dello *jus excludendi alios*, ovvero il diritto del titolare di vietare ad altri l'accesso indesiderato allo spazio informatico di sua pertinenza, protetto da misure di sicurezza[119].

Il delitto previsto e punito dall'art. 615 *ter* c.p. si configura anche a carico di chi, pur essendo autorizzato all'accesso ad un sistema informatico per determinate finalità, utilizzi tale facoltà per finalità diverse rispetto a quelle per le quali vale la sua autorizzazione. Dunque, l'art. 615 *ter* c.p. punisce non solo chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza, come afferma la prima parte del comma 1 della norma, introduzione abusiva che non è configurabile in capo a colui che è autorizzato all'accesso al sistema e che è quindi munito delle chiavi necessarie per superare le misure di protezione senza violarle, ma anche colui che, introdottosi lecitamente nel sistema, vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, come afferma la seconda parte del comma 1 della norma.

Il soggetto che sfrutta la sua possibilità di accesso al sistema per effettuarvi operazioni diverse rispetto a quelle per le quali è autorizzato tiene un comportamento che equivale al mantenersi nel sistema contro la volontà tacita di chi ha il diritto di escluderlo e che, pertanto, rientra nell'ipotesi prevista e punita dalla seconda parte del comma 1 dell'art. 615 *ter* c.p.[120]. Dunque, si realizza il reato di accesso abusivo ad un sistema informatico o telematico ogni qual volta un soggetto, con la propria condotta,

[119] Flor R., *op. cit.*, p. 930.
[120] Trib. di Nola, 11 dicembre 2007, n. 488.

acceda senza alcuna autorizzazione della vittima ad informazioni contenute nel sistema, al di là del loro carattere personale o meno, rilevando l'intrusione non autorizzata in quanto tale, anche nei casi in cui l'elaboratore non contenga alcun dato[121]. In tal modo, però, sorge il rischio che l'ordinamento offra tipi di tutela meramente formali che esporrebbero la norma a censura di incostituzionalità per violazione del principio di proporzione e, per questo, sarebbe auspicabile, in questo settore, l'intervento del legislatore, volto a selezionare con maggiore chiarezza i comportamenti di illecita intrusione nei sistemi informatici protetti.

In un phishing attack appare difficile immaginare un accesso abusivo cui non segua anche una alterazione o, comunque, un intervento sul sistema informatico oggetto dell'attacco, se non altro in quella fase, detta "*Post Attack*", in cui il phisher interviene per nascondere le tracce dell'accesso abusivo realizzato: in tali casi la sua condotta integrerà gli estremi del reato di frode informatica punito dall'art. 640 *ter* c.p.. A tal proposito la Corte di Cassazione ha chiaramente affermato che i due reati possono concorrere, avendo essi diversi presupposti giuridici[122], nonché per la diversità dei beni giuridici tutelati, per l'elemento soggettivo e per la previsione della possibilità di commettere il reato di accesso abusivo solo nei riguardi di sistemi protetti, caratteristica che non ricorre nel reato di frode informatica[123].

2.3.4 **Detenzione e diffusione abusiva di codici di accesso ad un sistema informatico attraverso il phishing**

[121] Cass. Pen., Sez. VI, 4 ottobre 1999, n. 214945, in *Dir. Inf.*, 2001, p. 485. Questa è la soluzione che meglio si attaglia alla lettera della legge, perché la norma non opera distinzioni tra sistemi a seconda dei contenuti, ma soltanto delle misure di sicurezza e allo scopo della legge, perché l'interpretazione contraria porterebbe all'esclusione dalla tutela di aspetti non secondari, quali per esempio quelli connessi ai profili economico-patrimoniali dei dati.

[122] Cass. Pen., Sez. II, 24 febbraio 2011, n. 9891.

[123] Cass. Pen., Sez. V, 1 ottobre 2004, n. 2672.

L’attività di phishing potrebbe integrare anche il delitto rubricato “*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici*”, disciplinato dall’art. 615 *quater* c.p., che prevede e sanziona la condotta di chi, al fine di procurare a sé o ad altri un profitto e arrecare ad altri un danno, abusivamente si procura codici o altri mezzi idonei all’accesso ad un sistema informatico protetto, vale a dire esattamente la condotta del phisher.

Il pisher, infatti, si procura abusivamente, con artifizi e raggiri quali ad esempio l’uso di un layout simile o uguale alla potenziale banca del destinatario, avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente, o anche tramite l’ invio di un trojan dopo che la vittima abbia fatto accesso al sito fake, le password, i codici cliente, i numeri di carte di credito e quant’altro gli consenta di accedere al conto corrente della vittima e di ripulirlo. Tali credenziali sono considerate alla stregua di qualità personali riservate, identificatrici della persona e viene, quindi, punito colui il quale si procuri in modo illecito tali credenziali di autenticazione e d’accreditamento atte a rendere inefficaci le misure di sicurezza, rischiando di pregiudicare con ciò stesso integrità, riservatezza e disponibilità dei dati. Tale ipotesi di reato si configura nel momento in cui il phisher abusivamente detiene o diffonde le credenziali di accesso al servizio di home banking della vittima e da tale detenzione o diffusione ne derivi un profitto per sé o per altri con l’altrui danno.

2.3.5 **Furto di identità attraverso il phishing**

Nel sistema penale non esiste un reato denominato “*furto di identità*” e l' unica fattispecie criminosa che se ne occupa è costituita dall'art. 494 c.p., che contempla tanto la sostituzione della propria ad altrui persona, quanto l'attribuzione a sé o ad altri

di un falso nome, di un falso stato ovvero una qualità cui la legge attribuisce effetti giuridici così da indurre in errore altri, il tutto al fine di procurare un profitto o arrecare un danno.

A causa della estensione della nozione di "*qualità cui la legge attribuisce effetti giuridici*", il concetto di identità ai fini dell'art. 494 c.p. è tale da ricomprendere tutti quei dati personali in grado di identificarla, quali ad esempio la casella di posta elettronica e gli estremi del conto corrente. Di converso, nel concetto di "*sostituzione all'altrui persona*" rientra anche l'attribuzione a sé di una immagine o di un video che ritraggono altri.

Il fatto è punito non solo perché lesivo della fede pubblica, ma soprattutto perché funzionale a frodi di vario tipo. Il reato di cui all'art. 494 c.p. ha natura sussidiaria, come si evince dalla formula di chiusura «*se il fatto non costituisce altro reato contro la fede pubblica*» ed è ammesso il concorso di tale delitto e quelli di cui agli artt. 640 c.p. e 640 *ter* c.p., in quanto lesivi di un bene giuridico diverso, il patrimonio, nonché dell'art. 615 *ter* c.p..

Una possibile qualificazione giuridica delle condotte che integrano il phishing, in particolare la prima fase di esso, è proprio il reato di sostituzione di persona, disciplinato dall'art. 494 c.p.. Infatti, nella fase iniziale di un phishing attack, il phisher, per "*pescare*" le sue vittime, molto spesso forma ed invia messaggi di posta elettronica apparentemente provenienti da mittenti "*reali*", utilizzando gli estremi identificativi di un mittente realmente esistente ed attribuendosi un falso nome. Tale

attività è stata considerata dalla giurisprudenza della Suprema Corte come integrante gli estremi del delitto di sostituzione di persona[124].

La condotta dell'art. 494 c.p. integra tutti gli elementi costitutivi richiesti, sia dal punto di vista oggettivo, e cioè l'induzione in errore della persona offesa tramite la sostituzione illegittima della propria all'altrui persona, sia dal punto di vista soggettivo, e cioè del dolo specifico, essendo l'invio dell'e-mail finalizzato a procurarsi un vantaggio con altrui danno. La Cassazione ha affermato in una recente sentenza[125] che "*integra il reato di sostituzione di persona, di cui all'articolo 494 c.p., la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet, nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese*". Qualora, invece, il phisher assuma l'identità di una persona assolutamente indeterminata, ad esempio nel caso in cui come mittente appaia un organismo, un'istituzione, una società, sembrerebbe da escludere l'applicazione della norma di cui all'art. 494 c.p.[126]. Non mancano, però, pronunce giurisprudenziali, quale quella del Tribunale di Milano del 2011[127], in cui il phisher è stato ritenuto responsabile del delitto di cui all'art. 494 c.p. anche con l'invio di false email, con le quali venivano messi in guardia gli utenti in merito a problemi di sicurezza relativi all'istituto di credito e la creazione di false pagine web, del tutto simili a quelle di istituti di credito di cui la vittima era cliente, pur essendo, pertanto, la persona sostituita indeterminata.

[124] Cass. Pen., Sez. V, 14 dicembre 2007, n. 46674.
[125] Cass. Pen., Sez. III, 15 dicembre 2011- 3 aprile 2012, n. 12479.
[126] Flor, R., *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, p. 903.
[127] Trib. Milano, Sez. 8, 7 ottobre 2011, n. 11696.

L'ordinamento si occupa dell'identità personale anche al di fuori del sistema penale. In particolare il d.lgs. 30 giugno 2003, n. 196, all'art. 2 afferma che il codice medesimo «*garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*». Ed, in effetti, l'utilizzo non autorizzato di dati personali o documenti di un soggetto incide sulla genuinità, integrità e correttezza dei dati personali.

Capitolo III. Casi pratici di phishing

3.1 **Il caso "*Phish&Chip*"**

L'operazione "*Phish&Chip*", condotta nel corso del 2007 dalla Procura di Milano e dal Gruppo Pronto Impiego della Guardia di Finanza di Milano, costituisce una delle prime indagini, in Italia, relative al fenomeno delle organizzazioni criminali dedite sistematicamente all'attività di phishing. Tale complessa operazione ha, dunque, consentito di identificare due diverse associazioni a delinquere operanti sul territorio milanese, che potrebbero anche appartenere ad un'unica realtà criminale tenuto conto del medesimo modus operandi utilizzato, le quali, nel corso del 2007, avevano posto in essere frodi legate ad un precedente furto di identità tramite phishing, relative alle carte prepagate ed, in particolare, alle carte c.d. postepay emesse da Poste Italiane.

Le indagini sono iniziate nel febbraio 2007, a seguito di una segnalazione da parte della sezione antifrode di Poste italiane agli operanti di polizia giudiziaria di un massiccio attacco di phishing ai danni dei clienti di Poste Italiane. In particolare, venivano indicate quarantanove transazioni fraudolente verso due carte postepay attivate il giorno precedente ed intestate ad un cittadino romeno. In tale segnalazione venivano, inoltre, forniti i relativi indirizzi IP, tutti assegnati ad un Internet Service Provider italiano, tramite i quali è stato possibile acquisire le informazioni relative al soggetto intestatario della connessione internet ed evincere che le connessioni erano tutte partite da una stessa utenza cellulare, sottoposta quindi ad intercettazione. Le intercettazioni hanno portato all'identificazione dell'effettivo utilizzatore, rivelatosi il capo di una delle due organizzazioni criminali: un altro cittadino romeno, che

adoperava numerosi alias con la speranza di non riuscire ad essere identificato. Egli era, inoltre, in stretto contatto con connazionali in Romania, i quali si occupavano della creazione delle e-mail da inviare ai vari utenti intestatari di una carta postepay. Ulteriori indagini avevano portato ad individuare una seconda associazione a delinquere, anch'essa composta da cittadini romeni residenti in Italia, dedita a porre in essere frodi a danno dei correntisti di Banca Intesa. Entrambi i sodalizi criminosi, secondo quanto rivelano le conversazioni intercettate, si avvalevano di strumenti e competenze tecniche atte ad inviare e-mail di phishing, creare siti fasulli riproducenti fedelmente quello di Poste Italiane e quello di Banca Intesa da utilizzare come esche per l'acquisizione delle credenziali di home banking dei correntisti utilizzatori dello specifico servizio, utilizzare le credenziali fraudolentemente acquisite per prelevare illegittimamente fondi dai conti correnti postali tramite operazioni di trasferimento, che potevano avvenire da postepay a postepay[128] oppure da conto corrente a postepay[129], reclutare soggetti sul territorio italiano che si prestavano ad attivare carte postepay da utilizzare per scopi illeciti.

I soggetti facenti parte delle associazioni a delinquere, per realizzare la loro attività criminosa, hanno, innanzitutto, ottenuto da Poste Italiane e Banca Intesa l'attivazione di carte di credito e di pagamento, anche intestate a persone fittizie, su cui erano destinati a confluire i fondi illeciti. Successivamente, i phisher, per procurarsi le credenziali di autenticazione dei correntisti, hanno inviato loro una e-mail, simulandone la provenienza da parte di Poste Italiane o Banca Intesa, in cui veniva

[128] In tale tipologia di truffa si aveva l'acquisizione in frode delle credenziali della carta postepay c.d. "*ricaricante*" dalla quale, successivamente, venivano trasferiti fraudolentemente i fondi presenti ed accreditati su altra postepay nella disponibilità dell'organizzazione criminale.

[129] In questa fattispecie di truffa l'organizzazione criminale, una volta acquisite in frode le credenziali di accesso ai servizi di home banking, disponeva veri e propri bonifici dal conto corrente della vittima sulle carte postepay in suo possesso.

richiesto di cliccare un link con la dizione "*accedi ai servizi online di Poste.it (o Banca Intesa.it) e diventa utente verificato*". Acquisite in tal modo le credenziali, i phisher hanno effettuato un preliminare accesso ai conti correnti al fine di verificarne la capienza: in caso positivo, ovvero con saldo superiore a cinquanta euro, venivano immediatamente operate le disposizioni in frode, con trasferimento di denaro sulle carte che essi avevano precedentemente attivato; in caso contrario, le credenziali venivano salvate su una MiniSD, su cui venivano anche raccolte altre importanti informazioni, con riserva di accessi e trasferimenti in periodi successivi. Il metodo utilizzato per prelevare il denaro trasferito sulle carte all'uopo attivate venne chiamato "*Casinò mon amour*": alcuni membri dell'organizzazione si recavano nei Casinò italiani e stranieri, in particolare in Germania, Austria e Grecia, ed acquistavano fiches di valore pari al massimo importo ricaricabile, e cioè tre mila euro, eludendo il limite giornaliero di duecentocinquanta euro per il prelievo agli ATM. L'errore dei soggetti agenti, che ha condotto, poi, al loro arresto è stato l'uso della stessa Sim card sia per la connessione internet utilizzata per porre in essere le operazioni illecite, sia per le conversazioni telefoniche tra coloro che avevano preso parte al crimine. In questo modo è stato possibile intercettare i soci e continuare le investigazioni con successo. Proprio per questo motivo l'operazione è stata denominata "*Phish&Chip*": "*phish*", in riferimento al fenomeno illecito del phishing e "*chip*", in riferimento all'interno della scheda Sim che raccoglie di volta in volta le informazioni aggiornate dal gestore telefonico, dalle chiamate alla connessione internet. Dalle indagini è risultato, quindi, che i capi delle due organizzazioni criminali erano romeni residenti in Italia ed erano coadiuvati l'uno da un phisher all'estero, l'altro da un giovane connazionale residente

nella periferia di Milano. Il giovane phisher ha ammesso, durante il lungo interrogatorio a cui è stato sottoposto, di aver effettuato, da uno dei suoi portatili, connessi tramite bluetooth al suo Nokia E61 e, per esso, ad Internet, gli accessi abusivi ai sistemi di home banking dei correntisti frodati. L'analisi forense del computer ha confermato la sua confessione. In seguito, nell'aprile del 2007 gli investigatori avevano scoperto che il maggiore responsabile della seconda organizzazione stava ritornando a casa sua a Craiova, in Romania. A questo punto, era necessaria un'eccellente collaborazione tra le autorità giudiziarie di Milano, Bucarest e Craiova e, proprio grazie alla collaborazione della polizia rumena, è stato possibile localizzare il capo della seconda organizzazione criminale, condurlo in Italia tramite un mandato di arresto europeo, arrestare un altro membro dell'organizzazione dedito alla materiale riscossione dei proventi illeciti ed intercettare varie conversazioni avvenute in Romania. La Guardia di Finanza di Milano, poi, nel luglio 2007, ha eseguito ventisei mandati di arresto nei confronti di coloro che erano risultati appartenenti alle due associazioni criminali che avevano effettuato gli accessi abusivi ai sistemi di home banking dei clienti di Poste Italiane e Banca Intesa. Dopo la conclusione delle indagini, nel dicembre 2007, venne celebrata l'udienza preliminare davanti al GUP presso il Tribunale di Milano Piero Gamacchio, con sentenza di condanna[130] a seguito di giudizio abbreviato per i capi e per altri soggetti ritenuti appartenenti alle associazioni criminali transnazionali che avevano commesso attività di phishing. Il successo dell'operazione "*Phish&chip*", significativo per numero degli indagati e per i reati contestati, nonché per la definizione e configurazione dell'attività di phishing, vi è stato soprattutto grazie alla cooperazione transnazionale tra le autorità italiane e le

[130] **T**rib. di Milano, Ufficio GUP, Sent. 10 dicembre 2007 n. 888 .

autorità romene e grazie alle nuove tecniche di indagine ed investigazione, necessarie quando si tratta di cyber crime, ed, in particolare, le analisi dei dati contenuti nei computers.

3.1.1 **Profili penali**

La sentenza emessa nel dicembre 2007 dal GUP di Milano, a seguito dell'operazione "*Phish&chip*", costituisce una delle prime e più importanti sentenze della giurisprudenza italiana riguardante gli attacchi di phishing. La pronuncia del GUP Gamacchio ha affrontato le questioni di fatto e di diritto connesse al caso, dopo un esame del fenomeno del phishing e delle sue modalità di manifestazione ed ha sottolineato il carattere sovranazionale della vicenda, dovuto principalmente al suo manifestarsi in rete attraverso la raccolta illecita di dati personali degli utenti, il loro successivo utilizzo abusivo e la realizzazione di un evento materiale, il trasferimento di denaro, quale conseguenza dei fatti criminosi realizzati on-line. I reati contestati ai soggetti facenti parte delle due associazioni criminose, oltre all'associazione a delinquere di cui all'art. 416 c.p., sono stati la falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche di cui all'art. 617 *sexies* c.p., la truffa di cui all'art. 640 c.p., l'accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 *ter* c.p., l'utilizzo indebito di carte di credito e di pagamento di cui all'art. 12[131] della legge 5 luglio 1991, n. 197. Sono state

[131] Articolo 12 l. 197/1991- Carte di credito, di pagamento e documenti che abilitano al prelievo di denaro contante: "*Chiunque, al fine di trarre profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni. Alla stessa pena soggiace chi, al fine di trarre profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi*."

considerate applicabili anche le aggravanti previste dai numeri 2 e 7 dell'art. 61 c.p., ossia rispettivamente: aver commesso il reato per eseguirne od occultarne un altro o per conseguire o assicurare a sé o ad altri il prodotto, profitto o prezzo, ovvero l'impunità; aver cagionato un danno patrimoniale di rilevante gravità nei delitti contro il patrimonio o che offendono il patrimonio o nei delitti determinati da fini di lucro, nel caso di specie il danno sia del correntista che degli istituti bancari. Infine, il delitto di associazione per delinquere nonché i reati previsti dagli artt. 615 *ter* c.p. e 12 della legge 5 luglio 1991, n. 197 sono stati ricondotti alla definizione di "*reato transnazionale*", essendo la relativa preparazione e pianificazione avvenuta , per una parte sostanziale, in Romania. L'art. 3, comma 1, lettera "*b*", della legge 16 marzo 2006, n. 146[132], infatti, definisce "*reato transnazionale*" quello in cui sia coinvolto un gruppo criminale organizzato, nonché sia commesso in uno Stato, mentre una parte sostanziale della sua preparazione, pianificazione, direzione o controllo sia avvenuta in un altro Stato. Il giudice di merito, dopo aver ripercorso dettagliatamente le fasi delle indagini preliminari ed averne riportato gli esiti, ha dedicato attenzione alla verifica degli elementi strutturali della fattispecie prevista dall'art. 416 c.p., concludendo per la sussistenza della "*formazione e permanenza di un vincolo associativo continuativo tra tre o più persone allo scopo di commettere una serie indeterminata di delitti, con la predisposizione comune dei mezzi occorrenti per la realizzazione del programma e con la permanente consapevolezza di ciascun associato di far parte del sodalizio criminoso*". Tale esito positivo riguarda anche l'aggravante contestata e connessa alla

[132] Si tratta della legge di "*Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea Generale il 15 dicembre 2000 ed il 31 maggio 2001*", pubblicata nella *Gazzetta Ufficiale* n. 85 dell' 11 aprile 2006 - Supplemento ordinario n. 91.

categoria del "*reato transnazionale*". In particolare, l'art. 4 della legge 16 marzo 2006, n. 146 prevede che "*per i reati puniti con la pena della reclusione non inferiore nel massimo a quattro anni nella commissione dei quali abbia dato il suo contributo un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato la pena è aumentata da un terzo alla metà*". Nel caso di specie, l'associazione per delinquere rientra, a parere del giudice, tra i reati cui la Convenzione[133] si riferisce e l'aggravante di cui all'art. 4 si applica tenendo presenti i parametri dell'art. 3[134] della stessa legge 16 marzo 2006, n. 146. La difesa degli imputati aveva sostenuto la configurazione del solo reato, assorbente tutte le altre ipotesi contestate, di frode informatica previsto dall'art. 640 *te*r c.p.. Il giudice, invece, ha ritenuto, riportando le tesi dottrinali riguardanti tale fattispecie di reato[135], che l'elemento oggettivo di tale ultima fattispecie richieda la necessaria realizzazione di una delle condotte tipiche, cioè l'alterazione del funzionamento di un sistema informatico o intervento senza diritto su dati, informazioni o programmi ivi contenuti, di fatto non sussistenti.

In verità, il comportamento criminoso del phisher riproduce lo schema dell'induzione in errore del soggetto passivo, che rappresenta il modus operandi tipico della fattispecie prevista dal reato di truffa. Il giudice ha ritenuto evidenti gli artifici e raggiri posti in essere da chi utilizza una e-mail in cui vengono riprodotti colori, marchi ed altre caratteristiche, compresi i segni distintivi, di enti esistenti e reali. Il giudice ha, inoltre, considerato realizzati gli altri elementi costitutivi della fattispecie di truffa, compresi il danno e l'ingiusto profitto, oltre che la disposizione patrimoniale.

[133] "*Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale*", sottoscritta nel corso della Conferenza di Palermo (12 - 15 dicembre 2000).
[134] Si tratta dei parametri per la definizione di reato transnazionale- art. 3
[135] Flor R., *Phishing, identity theft* e *identity abuse*: *le prospettive applicative del diritto penale vigente*, in *Riv. It. dir. proc. pen*., 2007,p. 899 e ss.; Cajani F., *Profili penali del phishing*, in *Cass. pen*., 2007, p. 2294 e ss..

Il danno, in particolare, è risultato evidente e di rilevante gravità, sia per i due enti, di cui sono stati clonati i siti e i loghi, sia per gli stessi correntisti. Pertanto, a parere del giudice, si sono configurate le aggravanti contestate[136].

Il GUP, per quanto attiene gli elementi costitutivi del delitto di accesso abusivo ad un sistema informatico o telematico in riferimento all'accesso ai sistemi dei titolari delle carte di credito e di pagamento e di *home banking* finalizzato ad effettuare operazioni di ricarica sulle carte acquistate dall'organizzazione criminale, ha ritenuto sussistente il reato, dopo aver ripercorso l'evoluzione dell'interpretazione giurisprudenziale[137] relativa alle condotte tipiche di "*introduzione*" e di "*mantenimento*", al bene giuridico protetto dalla norma ed all'ammissibilità del concorso con il reato di truffa[138]. In particolare, il giudice ha sottolineato la natura di "*misure di sicurezza*" , necessarie per la protezione del sistema informatico o telematico, dei nomi utenti e delle passwords di accesso al sistema di home banking. Egli ha specificato, inoltre, che si tratta di accesso abusivo al sistema di home banking del correntista e non di un'introduzione senza diritto nel sistema informatico della banca, "*non violabile, nella sua interezza, con la semplice disponibilità delle credenziali di alcuni utenti*". Permangono, però, alcuni dubbi interpretativi[139] circa la titolarità dello spazio informatico in questo caso violato. La concezione tradizionale di "*domicilio informatico*", quale spazio ideale e fisico in cui sono contenuti i dati informatici di pertinenza della persona, a cui estendere la tutela della riservatezza della sfera individuale quale bene anche costituzionalmente

[136] Si tratta delle aggravanti di cui all'articolo 61 n. 2 e 7 c.p..
[137] Cass. Pen., sez. V, 7 novembre 2000, Zara, in *Giust. Pen.*, 2001, p. 548; Cass. Pen., sez. II, 4 maggio 2006, in *Dir. Pen. Proc*., 2007, fasc. 3, p. 373; Cass. Pen., sez. V, 6 febbraio 2007, su *Mass. Pen*., n. 236221.
[138] Flor R., *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. pen. proc*., 2008, p. 106 e ss.; Flor R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo jus excludendi alios,* in *Dir. Pen. Proc*., 2005, p. 85 e ss..
[139] Flor R., *Commento a G.I.P., Tribunale di Milano, sentenza 10 dicembre 2007, n. 888*, in *Riv. Giur. Ec. d'Az*., n. 4/2088.

protetto[140], non coglie totalmente il contenuto dell'interesse all'esclusione di terzi dalla sfera di disponibilità del titolare dello spazio informatico. Tale spazio deve essere inteso non tanto quale area riservata ed esclusiva in senso fisico, ma bensì come una zona virtuale delimitata rispetto alla quale il "*detentore qualificato*" può esercitare uno *jus excludendi alios* che si estende fino a quei soggetti che, in base al suo legittimo consenso, egli abilita ad accedere. E' necessario, dunque, valutare caso per caso, sulla base degli accordi tra la banca e il correntista, se esista o meno uno spazio virtuale esclusivo concesso all'utente per svolgere determinate operazioni on-line. Il giudice ha ritenuto che vi sia uno spazio esclusivo del correntista e, per questo, ha affermato l'insussistenza di un'aggressione al sistema informatico degli istituti "*nella sua interezza*", non violabile con la disponibilità dei dati personali di soltanto alcuni utenti. Però, non rileva il fatto che l'accesso non sia avvenuto al sistema della banca nella sua interezza, ma che sussista la violazione dello *jus excludendi alios* che, nel caso di specie, può essere la "*titolarità*" del cliente, al quale gli enti di credito hanno fornito le credenziali per l'uso di uno spazio informatico esclusivo. Un sistema informatico può ospitare, al proprio interno, una pluralità di spazi riservati di pertinenza esclusiva di diversi soggetti, anche se individuati o collocati fisicamente in un unico macro-sistema, il cui titolare concede una limitata autonomia operativa e gestionale a soggetti terzi. Dunque, secondo questo ragionamento, potrebbe ritenersi che il titolare del sistema informatico sia l'istituto di credito, il quale ha concesso ad altri soggetti terzi, i clienti, degli spazi esclusivi per la gestione di alcune risorse, fra cui il conto corrente.

[140] Cass. Pen., sez. VI, 4 ottobre 1999, causa Piersanti, in *Foro it.*, 2000, II, p. 133.

Il giudice ha, poi, verificato la sussistenza dei requisiti previsti dall'art. 12 della legge 5 luglio 1991, n. 197, per la configurazione del reato di indebito utilizzo di carte di credito o di pagamento. Egli non ha avuto alcun dubbio che le carte che permettevano al phisher il trasferimento di fondi da "*postepay a postepay*" potessero essere considerate "*documenti abilitanti al prelievo di denaro contante o all'acquisto di beni o servizi*". Inoltre, ha ritenuto integrato il reato di indebito utilizzo di carte di credito o di pagamento e non quello di frode informatica, in quanto la condotta dell'agente, nel caso concreto, è risultata diretta a ricaricare le citate carte attraverso l'uso indebito delle credenziali del legittimo titolare, a cui sono state fraudolentemente sottratte[141]. Per quanto attiene, invece, il rapporto tra il reato di indebito utilizzo di carte di credito o di pagamento ed il reato di truffa, la diversità dell'elemento oggettivo e del bene giuridico protetto ha portato il giudice a sostenere che si possa configurare il concorso formale dei due reati.

Sul piano oggettivo l'art. 12, diversamente da quanto prevede l'art. 640 c.p., sanziona la condotta di uso indebito della carta di credito o di pagamento indipendentemente dal conseguimento di un profitto e dal verificarsi di un danno e tale condotta prescinde dal necessario uso di artifici o raggiri che inducano taluno in errore. Riguardo al bene protetto, mentre la truffa è un delitto contro il patrimonio, il reato di indebito utilizzo di carte di credito o di pagamento prevede la tutela dell'interesse pubblico a che il sistema di pagamento venga utilizzato in modo corretto, a garanzia della fede pubblica e a prevenzione del riciclaggio.

[141] Flor R., *Phishing, identity theft* e *identity abuse*: *le prospettive applicative del diritto penale vigente*, in *Riv. It. dir. proc. pen*., 2007, p. 935 e ss..

Il giudice ha poi affrontato anche la problematica questione del concorso di reati fra le disposizioni in questione. Da un lato, gli artifici o raggiri costituiscono uno dei modi tramite cui si manifesta l'uso indebito della carte di credito e di pagamento, dall'altro lato, si ammette il concorso di reati quando la condotta del reo non si limiti a tale uso, ma sia connotata da un *quid pluris* di attività ingannatoria. In sostanza, la truffa non è assorbita nel più grave reato di uso di indebito di carte di credito o di pagamento, mancando l'identità del bene alla cui tutela sono finalizzate le disposizioni in esame[142].

Il GUP, nel caso di specie, ha ritenuto, inoltre, sussistente anche il reato previsto dall'art. 617 *sexies* c.p., con riferimento alla condotta di formazione del contenuto non veritiero di un'e-mail, apparentemente proveniente da enti o istituzioni realmente esistenti. Infatti, i soggetti agenti, al fine di procurarsi il vantaggio di acquisire indebitamente le credenziali dei correntisti, avevano formato falsamente, simulandone la provenienza da Poste Italiane o da Banca Intesa, il contenuto di un'e-mail, contenente il link di reindirizzamento ad un sito non autentico, ma del tutto simile a quello istituzionale. Anche in questo caso, è stato utilizzato il criterio della "*diversità del bene giuridico*" per affermare il possibile concorso con la truffa, ritenendo che l'art. 617 *sexies* c.p. tuteli "*l'integrità della comunicazione telematica nelle forme di autenticità della comunicazione, della conformità del contenuto originale e della esistenza stessa della comunicazione*". L'e-mail con contenuto falso può ritenersi una "*comunicazione relativa ad un sistema informatico o telematico o intercorrente fra più sistemi*" solo nella fase dinamica della trasmissione[143], e cioè tra il momento di effettuato invio del messaggio di posta elettronica e prima della sua ricezione da parte

[142] Cass. Pen., sez. I, 23 aprile 2004, n. 26300.
[143] Pecorella C., *Diritto penale dell'informatica*, Padova, 2006, p. 292 e ss..

del destinatario. Una volta ricevuta dal destinatario, l'e-mail diviene "*corrispondenza informatica o telematica*", secondo la definizione dell'art. 616 cpv. c.p.. Dunque, per una corretta applicazione dell'art. 617 *sexies* c.p. al caso di specie[144], è necessario considerare che la formazione falsa o l'alterazione del contenuto delle comunicazioni tra sistemi, quello del phisher che finge di essere l'istituto di credito e quello del cliente, riguardi la fase di trasmissione.

E' necessario precisare, inoltre, che la riproduzione di loghi e simboli di un istituto bancario in una e-mail non può considerarsi come reato di sostituzione di persona, previsto dall'art. 494 c.p., in quanto non può parlarsi propriamente di sostituzione materiale della propria all'altrui "*persona*".

Diversamente, potrebbe trovare applicazione la norma in esame se il mittente fosse una persona fisica e sostituisse illegittimamente la propria all'altrui persona oppure si attribuisse qualità personali non veritiere. Infatti, la giurisprudenza si è pronunciata in un caso simile[145] sostenendo che è configurabile il reato di cui all'art. 494 c.p. nel caso di apertura di accounts di posta elettronica intestati ad altri soggetti, da cui derivi l'induzione in errore dei "*corrispondenti che si trovano ad interloquire con una persona diversa da quella che ad essi viene fatta credere*".

La sentenza che ha fatto seguito all'operazione "*Phish&Chip*", quindi, giungendo in un periodo di riforme sostanziali del diritto penale dell'informatica, ha fornito un grande contributo per la definizione del fenomeno del phishing, delle modalità con cui esso viene posto in essere, nonché delle norme penali in tali casi applicabili.

[144] Flor R., *Commento a G.I.P., Tribunale di Milano, sentenza 10 dicembre 2007, n. 888*, in *Riv. Giur. Ec. d'Az.*, n. 4/2088.
[145] Cass. Pen., sez. V, 14 dicembre 2007, n. 46674.

3.2 **Il caso "*Carta Si*": phishing via sms**

L'evoluzione della tecnologia e delle forme di comunicazione ha comportato l'aumento delle possibilità e delle modalità di azione illecita. Un esempio può essere il caso relativo alla truffa "*SMS Carta Si*", realizzata attraverso la tecnica del phishing via sms, ossia il c.d. "*smshishing*", di cui si è occupato il Tribunale di Milano nell'ottobre 2007[146].

Nel febbraio del 2006 il responsabile dell'Ufficio Investigazioni e Sicurezza ha denunciato alla Polizia Postale di Milano che nel corso del mese precedente alcuni titolari di carte di credito Carta Si avevano segnalato la ricezione di messaggi SMS, tutti aventi come mittente "*Carta Si*", riportanti il testo: "*Chiami il numero 02/xxxxxxxx di Servizi Interbancari per verificare la transazione con la sua carta di credito, al fine di verificarne gli usi fraudolenti*". Il primo passo investigativo è stato quello di accertare a chi fossero intestate le utenze telefoniche indicate nel testo del messaggio: esse risultavano fornite per un servizio VoIP e gestite dalla società Eutelia.

Nel frattempo, l'amministratore della società Linkas S.r.l., che offre servizi per l'invio di sms tramite internet, ha denunciato di aver ricevuto una telefonata da un utente che disconosceva l'acquisto di sms dal sito subitosms.it: a seguito di ciò è stata appurata la dicrasia tra i dati lasciati in sede di registrazione del servizio e i dati della carta di credito utilizzata per il pagamento.

A questo punto, essendoci tale dicrasia, è stato doveroso verificare l'attività dell'utente registratosi in maniera fittizia al servizio di invio sms ed è emerso che, effettivamente, risultavano molti messaggi con mittente Carta Si. Da ulteriori indagini è poi emerso

[146] Trib. di Milano, Ufficio GUP, 15 ottobre 2007 (depositata 7 novembre 2007).

che questa stessa persona aveva, nel tempo, effettuato più volte l'acquisto di sms utilizzando un determinato indirizzo di posta elettronica. Con l'analisi di altri dati attinenti al traffico telematico, si è riusciti ad arrivare ad un intestatario di un'utenza telefonica fissa, che era stato, altresì, già indagato nel 2005 dalla Polizia Postale di Varese e poi anche condannato per fatti inerenti all'utilizzo indebito di carte di credito a mezzo di internet.

La Polizia Postale di Milano, a seguito del sequestro del computer, di foglietti di carta su cui erano riportati numeri di carte di credito e relativi CVV, nonché del cellulare dell'indagato, aveva analizzato gli stessi e individuato, sul computer, software capaci di effettuare e ricevere telefonate VoIP tramite un risponditore automatico in grado di acquisire i dati della carta di credito, la sua scadenza e il CVV a seguito della digitazione degli stessi sulla tastiera del telefono del soggetto chiamante. Tramite, poi, un'analisi incrociata dei dati forniti dalla Linkas S.r.l. hanno trovato ulteriore riscontro gli invii di sms ai numeri di cellulare intestati a soggetti che avevano successivamente fornito i dati della propria carta di credito. Inoltre, tramite un ulteriore incrocio con i dati forniti da Carta Si, è stato accertato che, dopo la fraudolenta acquisizione dei dati delle carte, esse erano state utilizzate per acquisti su internet[147].

Il GUP presso il Tribunale di Milano, nella sentenza del 15 ottobre 2007, ha condannato, con rito abbreviato, a due anni e otto mesi di reclusione e mille euro di multa il soggetto che ha posto in essere l'smshishing. Per il GUP, nel caso di specie, sono ravvisabili sia il reato di sostituzione di persona, di cui all'art. 494 c.p., in quanto l'imputato, per procurarsi un vantaggio economico, tramite l'invio degli sms, ha

[147] Cajani F., Costabile G., Mazzaraco G., *Phishing e furto di identità digitale*. *Indagini informatiche e sicurezza bancaria,* Milano, Giuffrè, 2008, pgg. 179 ss..

indotto in errore i destinatari degli stessi sostituendo illegittimamente il nome dell'istituto emittente la carta al proprio, sia il reato di truffa, di cui all'art. 640 c.p., perpetrata attraverso tale meccanismo unitamente al servizio telefonico apparentemente riconducibile all'istituto emittente le carte di credito, con il quale induceva gli ascoltatori del messaggio vocale a fornire i dati delle carte di credito, poi utilizzati per effettuare o tentare di effettuare acquisti via internet.

Il GUP ha, altresì, affermato la sussistenza del reato di indebito utilizzo di carta di credito previsto all' art. 12 della legge 5 luglio 1991, n. 197, in quanto, in alcuni casi, vi è stato un effettivo utilizzo indebito delle carte di credito da parte del phisher, perfezionatosi nell'acquisto di beni su internet. Per la sussistenza del reato, comunque, è sufficiente l'utilizzo indebito anche quando non si pervenga al perfezionamento dell'acquisto e all'impossessamento della merce o al godimento del servizio, bastando persino l'illecita acquisizione o il solo possesso di numeri di carte di credito di provenienza illecita al fine di trarne profitto.

Esaminando in modo più specifico le singole fattispecie di reato rintracciabili nel caso in esame, possiamo, innanzitutto, ravvisare gli estremi del delitto di cui all'art. 494 c.p., ossia la sostituzione di persona. La sostituzione di persona potrebbe essere considerata il punto di partenza della tecnica di phishing, nel nostro caso smshishing, in quanto tale tecnica si realizza, la maggior parte delle volte, con l'invio di una e-mail, nel nostro caso sms, nella quale un soggetto si attribuisce un falso nome o un falso stato, ovvero una qualità per indurre in errore un gran numero di soggetti, al fine di sottrarre loro dati personali, credenziali d'accesso, ecc[148]. Come rilevato dalla

[148] Cass. Pen., Sez. V, 14 dicembre 2007, n. 46674.

dottrina[149], però, non si può dare per scontata l'applicazione dell'art. 494 c.p. al caso del phishing via sms, in quanto alcune peculiarità proprie del mondo virtuale non coincidono perfettamente con gli elementi tipici del reato, creando quindi alcune difficoltà interpretative. In primo luogo, rileva il problema di definire quale sostituzione di persona l'invio di una e-mail, anche se corredata dai segni distintivi di un determinato sito, istituto di credito o azienda. In tali casi, non è possibile individuare un riferimento indicativo o distintivo di un soggetto persona fisica, così come, invece, dovrebbe avvenire nel delitto in esame.

In secundis, l'utilizzo sui siti web di dati personali o credenziali d'autenticazione di un determinato soggetto per l'accesso a determinati servizi, quali ad esempio la gestione online del conto corrente bancario, non configurerebbe né la materiale sostituzione di una persona né l'attribuzione di un falso nome, di un falso stato o di una qualità cui la legge attribuisce effetti giuridici. Ed infine, pur ammettendo un'interpretazione estensiva e forzata dei requisiti della norma, ritenendola idonea a ricomprendere fra ciò che rappresenta un mezzo essenziale e necessario negli scambi interpersonali anche gli username, le passwords o i numeri di conto corrente in quanto connotazioni identificative, rimane l'ostacolo, difficile da superare, costituito dall'evento consumativo del reato, e cioè l'induzione in errore di taluno, che non è in alcun modo compatibile o applicabile all'esecuzione automatizzata di richieste inoltrate ai sistemi informatici[150].

[149] Flor R., Phishing, *Identity Theft e Identity Abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2007, 2-3, p. 907 ss..

[150] Flor R., Phishing, *Identity Theft e Identity Abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2007, 2-3, p. 908 ss..

Date tali premesse, potrebbe apparire poco felice la scelta del giudice che, nella sentenza in esame, ritiene provato il reato di cui all'art. 494 c.p. in quanto il phisher, con gli sms, allo scopo di procurarsi un vantaggio economico, ha indotto in errore i destinatari degli stessi sostituendo illegittimamente il nome di CartaSi al proprio. Anche la successiva comunicazione verso un numero VoIP non rientrerebbe, a stretto rigore, nel reato di sostituzione di persona, in quanto la risposta è avvenuta tramite una casella vocale a cui rispondeva una voce elettronica preregistrata. Si verserebbe, invece, nel delitto di sostituzione di persona qualora al numero VoIP rispondesse un soggetto che, dichiarando una falsa identità o una falsa qualità, induca in errore la vittima al fine di sottrarle dati e informazioni riservate.

Il secondo reato riscontrato dal GUP nella sentenza in esame è quello di truffa, anche se potrebbe individuarsi una frode informatica, soprattutto tenuto conto dell'ampiezza della formula usata dal legislatore per cui ricade in questa fattispecie pure chi interviene senza diritto su dati, informazioni o programmi anche solo "*pertinenti*" ad un sistema informatico o telematico[151]. Le difficoltà definitorie a proposito del phishing, e dello smshishing, si traducono, infatti, spesso, in dubbi interpretativi circa la fattispecie da applicare, in quanto questo tipo di illecito sicuramente può ricadere nel reato di truffa *ex* art. 640 c.p., ma ben potrebbe, altresì, integrare il delitto di frode informatica di cui all'art. 640 *ter* c.p., in quanto essi hanno la medesima struttura, e quindi i medesimi elementi costitutivi, differenziandosi soltanto per l'attività fraudolenta dell'agente che, nella frode informatica, investe il sistema informatico[152].

[151] Perri P., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia, in Dir. Internet,* n. 3/2008, p. 265 ss..
[152] Cass. Pen., Sez. IV, 4 ottobre 1999, n. 3056.

Il giudice che ha emesso la sentenza in esame ha affermato che sia la sostituzione di persona che la truffa risultano teleologicamente connesse all'utilizzo indebito di carte di credito per conseguire un ingiusto profitto. Emerge, quindi, come aspetto rilevante della sentenza, l'elemento dell'ingiusto profitto con l'altrui danno, che nel caso di specie è stato integrato mediante l'utilizzo, al fine di acquistare beni su internet, dei numeri di carte di credito e dei codici di verifica di queste ultime illecitamente sottratti.

A questo punto, è necessario sottolineare la distinzione tra l'ipotesi di frode informatica pura e semplice e quella commessa mediante l'utilizzo indebito di una carta di credito. Tale delitto, infatti, è previsto dall'art. 12 della legge 5 luglio 1991, n. 197, a norma del quale "*chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi*". In realtà, il delitto di uso indebito di carta di credito o di pagamento e la frode informatica differiscono sia da un punto di vista oggettivo che da un punto di vista soggettivo. Per quanto riguarda la differenza da un punto di vista oggettivo, infatti, mentre nel caso di indebito utilizzo di

carta di credito o di pagamento si è dinanzi ad un reato di pura condotta, consistente, appunto, nell'indebito utilizzo, nel secondo caso è necessario che vi sia un evento, ossia l'ingiusto profitto con altrui danno. Sotto l'aspetto soggettivo, invece, mentre per l'uso indebito di una carta di credito è richiesto il dolo specifico del "*trarne profitto per se o per altri*", per il delitto di frode informatica è sufficiente il dolo generico[153].

Enucleate le principali differenze sostanziali tra le due fattispecie, bisogna rilevare anche le differenze procedurali, che risultano essere abbastanza sensibili. La fattispecie prevista dall'art. 12 della legge n. 197/1991, infatti, prevede la procedibilità d'ufficio e la sanzione della reclusione da 1 a 5 anni e la multa da euro 309 a euro 1.549, mentre nel caso della frode informatica la procedibilità è a querela della persona offesa e le sanzioni prevedono la reclusione da sei mesi a tre anni e la multa da euro 51 a euro 1.032, fatte salve le circostanze aggravanti.

Dal dato letterale della sentenza in esame[154], nulla osta a rilevare, nel caso di specie, la corretta individuazione del delitto di utilizzo indebito di carta di credito o di pagamento. Infatti, lo strumento utilizzato sicuramente rientra tra i documenti idonei ad abilitare "*al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi*", nonché sussiste l'ingiusto profitto, sebbene, come sottolineato dal giudice, fosse sufficiente, ai fini dell'esistenza della fattispecie, anche il mero possesso dei dati della carta, non essendo necessario il possesso della carta di credito vera e propria, in quanto i dati sono già idonei ad abilitare l'acquisto di beni e non essendo necessario nemmeno che gli acquisti si perfezionino, bastando solamente l'utilizzo indebito del

[153] Scopinaro L., *Internet e reati contro il patrimonio*, Torino, 2007, p. 70.
[154] Perri P., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia, in Dir. Internet*, n. 3/2008, p. 265 ss..

numero di carta e del codice di verifica della stessa[155]. La sentenza del GUP di Milano consente, dunque, di riflettere su un fenomeno che conosce sempre maggiore diffusione e che trova in Internet il suo luogo di elezione anzitutto per via delle caratteristiche intrinseche della comunicazione telematica, che si basa su un'elevata rapidità delle comunicazioni a costi irrisori e garantisce, tra l'altro, il facile raggiungimento di un buon grado di anonimizzazione o di mascheramento della propria identità. La forte componente tecnologica che caratterizza questo tipo di attività e la continua evoluzione dei metodi con cui porla in essere ha comportato da sempre difficoltà di adeguamento da parte del diritto positivo, che mai come in questo caso è costretto ad inseguire le sempre nuove modalità di commissione del reato[156].

3.3 **Indagini sul "*money laundering*"**

Le indagini, sul c.d. "*money laundering*"[157], che hanno portato alla prima vera e propria condanna[158] per phishing in Italia, hanno preso il via dall'attività investigativa della Direzione Centrale Tutela Aziendale delle Poste Italiane nel settore del riciclaggio di denaro illecitamente derivato dalla perpetrazione di frodi telematiche. Tale attività segnalava un trasferimento di fondi, non autorizzato dal titolare del conto, verso un differente conto Bancoposta, intestato ad un ignaro cittadino, il quale, raggirato da due soggetti con la scusa di permettere ai loro genitori di versare un importo di denaro al fine di proseguire gli studi in Italia, aveva consentito tale

[155] Borsari R., *Utilizzo indebito di carte di credito, sostituzione di persona e truffa* (nota a GUP Milano, 15 ottobre 2007), http://www.penale.it/page.asp?mode=1&IDPag=566 .
[156] Flor R., *Phishing, Identity Theft e Identity Abuse. Le prospettive applicative del diritto penale vigente, in Riv. it. dir. e proc. pen*., 2007, 2-3, p. 901-902.
[157] Il nome attribuito alle indagini, "*money laundering*", che in italiano significa "*riciclaggio di denaro*", è dovuto al reato di riciclaggio di denaro proveniente da reato susseguente alle attività di phishing.
[158] Trib. di Milano, Ufficio del GUP, 28 luglio 2006, in *Dir. dell'Internet*, n. 1/2007, p. 62 ss..

trasferimento. Le indagini, svolte dalla Guarda di Finanza di Milano tra la fine del 2005 e i primi mesi del 2006, hanno permesso di appurare che i due soggetti, entrambi provenienti dall'Europa dell'Est, precisamente dalla Lettonia, erano giunti in Italia nel dicembre del 2005 per riscuotere i fondi illecitamente raccolti grazie all'attività di phishing a danno, in particolare, dei correntisti di Poste Italiane, Banca Intesa e Fineco Bank, e accumulati su conti accesi in Italia, con l'intento successivo di versarli, mediante trasferimenti di denaro attraverso il servizio Western Union, ai propri complici residenti in Russia e Lettonia. Dalle indagini sono emersi, dunque, i contorni di una complessa attività internazionale fondata su truffe e frodi informatiche, condotte anche tramite phishing, spesso via e-mail, perpetrate ai danni degli utenti internet meno esperti. La strategia attuata dai phisher si basava sull'invio di due tipi di e-mail, l'uno finalizzato ad ingannare il ricevente con l'intento di ottenere i dati del conto corrente on-line, l'altro finalizzato al reclutamento di "*financial manager*" per il trasferimento delle somme di denaro all'estero. Le indagini della Guardia di Finanza di Milano hanno portato all'individuazione ed identificazione di oltre settanta persone implicate nell'attività illecita e hanno consentito il blocco di trasferimenti per 220 mila euro, denaro che sarebbe stato stornato su conti all'estero con bonifici internazionali. A seguito della conclusione delle indagini, nel luglio del 2006, il GUP del Tribunale di Milano[159] ha emanato una sentenza di condanna, a conclusione del giudizio abbreviato, nei confronti dei due soggetti che erano giunti in Italia per continuare a porre in essere la loro attività illecita. Una successiva sentenza di condanna, poi, è

[159] Trib. di Milano, Ufficio del Giudice per le Indagini preliminari, 28 luglio 2006.

stata emanata dal giudice del Tribunale di Milano, nell'ottobre del 2011[160], anche nei confronti di alcuni dei soggetti reclutati quali "*financial manager*". L'attività truffaldina posta in essere dai due soggetti provenienti dall'est Europa, coadiuvati anche da altri soggetti facenti parte dell'organizzazione costituita per porre in essere tale attività illecita, aveva preso avvio con l'invio di due tipi di e-mails. I phisher, che solitamente agivano dall'estero, e nel caso in esame dall'est Europa, in modo da essere più difficilmente identificabili, avevano inviato in modo casuale migliaia di e-mails[161] in lingua inglese, molto spesso sgrammaticato, con veste grafica e logo degli istituti di credito, quali in particolare BancoPosta, Fineco Bank e Banca Intesa, che figuravano come mittenti[162], in cui il destinatario veniva invitato a compilare una scheda anagrafica e a fornire i dati personali e i codici di accesso ai conti correnti on-line per una presunta verifica dei dati stessi, ovvero per motivi di sicurezza, blocco del conto corrente, falsa comunicazione di una vincita. Dato l'elevato numero di e-mails che venivano inviate, una percentuale limitata di destinatari rispondeva ed inseriva le proprie credenziali. A questo punto, il phisher poteva accedere al conto corrente della vittima e sottrarre il denaro. Nasceva, però, il problema di come incassare le relative somme, dal momento che il sistema dell'home banking italiano non consentiva bonifici verso l'estero, se non tramite ulteriori controlli da parte degli istituti bancari. Dunque, quasi contemporaneamente all'invio delle e-mail di phishing, venivano inviate a migliaia di utenti, cittadini italiani o comunque residenti in Italia, altre e-mail da parte di false società, nel caso di specie si trattava della "*Europe Sells LTD*",

[160] Trib. di Milano, Sez. 8, 7 ottobre 2011, n. 11696 del, rv. 00313, Pres. Pellegrino A., Est. Corbetta S., Impp. P. ed altri.
[161] Tecnica c.d. "*spamming*".
[162] C.d. mail "*spoofing*".

contenenti allettanti offerte di lavoro. Per tale lavoro non venivano richieste né specifiche competenze, né precedenti esperienze professionali, ma era sufficiente la disponibilità di un computer collegato alla rete e di un conto corrente bancario. Infatti, se l'offerta di lavoro veniva accettata, ai collaboratori, cosiddetti "*financial manager*", veniva richiesto di trasferire all'estero, in brevissimo tempo, delle somme di denaro, che erano quelle sottratte dai conti correnti delle vittime, fatte pervenire su un conto corrente che essi avrebbero dovuto accendere presso la stessa banca presa di mira, in modo da velocizzare i tempi di valuta, eludendo i sistemi antifrode, con un compenso oscillante tra il 5 e il 10% della somma. Tuttavia, l'invio di e-mail non costituiva l'unico modo utilizzato dai phisher per instaurare un primo contatto con i soggetti destinatari dell'offerta, in quanto le stesse fantomatiche società si avvalevano anche di contatti via ICQ o altri canali di chat, nonché di inserzioni su siti Internet specializzati in offerte di lavoro. Molte di queste fantomatiche società avevano anche allestito un sito Internet, con sezioni in italiano, per rendere ancora più credibile, sotto il profilo della liceità di quanto offerto, la loro azione. Tramite tali siti era altresì possibile stampare la documentazione relativa a contratti di collaborazione, nonché ricevere ulteriori informazioni, sintetizzate in alcune FAQ[163]. Si noti come, dopo aver allettato l'utente con un lavoro semplice e redditizio, i truffatori cerchino di convincerlo anche della serietà e validità della relativa società. La prospettata attività di "*financial manager*" costituisce, dunque, l'anello per far pervenire agli autori della truffa i relativi proventi.

[163] Si tratta delle c.d. "*risposte alle domande più frequenti*".

Ottenuta la disponibilità attiva di soggetti italiani o comunque residenti in Italia, la seconda fase della truffa era volta a sottrarre i soldi dal conto corrente di cui erano state fraudolentemente acquisite le credenziali di accesso, attraverso bonifici disposti a favore del conto corrente comunicato ai phishers dal "*financial manager*". Tali bonifici on-line venivano materialmente effettuati tramite operazioni partite principalmente da computer allocati all'estero, ma anche in Italia, quasi certamente appartenenti a una rete di computers infettati da virus, in danno degli ignari titolari dei rispettivi conti ordinanti.

A questo punto, i phishers inviavano un sms o una e-mail ai "*financial manager*" per avvertirli che sui loro conti vi erano somme disponibili e per dar loro istruzioni circa il prelievo e riversamento delle stesse. Per portare a compimento il disegno criminoso, i "*financial manager*" dovevano, quindi, trasferire, secondo le modalità indicate, le relative somme, tramite servizi di money transfer, e cioè Western Union o Money Gram, previa trattenuta di un compenso per l'attività svolta. Proprio per questa ragione, avendo i phisher, nel caso di specie, richiesto ai "*financial manager*" l'utilizzo del servizio Western Union per il trasferimento del denaro, l'autorità giudiziaria italiana aveva stilato un accordo con la società Western Union, il cosiddetto "*International Seizure Warrant*", per far sì che quest'ultima, in casi sospetti, ritardasse il pagamento di 48 ore, dando il tempo sufficiente per verificarne la liceità. Grazie alla collaborazione con la Western Union, infatti, l'autorità giudiziaria è riuscita a rintracciare il denaro e a sequestrarlo, senza che esso potesse pervenire ai phishers.

3.1.2 **Profili giuridici**

In seguito alla conclusione dell'attività investigativa sul c.d. "*money laundering*", come anticipato, sono state pronunciate due importanti sentenze[164], con le quali si è arrivati a delineare il corretto inquadramento giuridico dei comportamenti illeciti integranti l'attività di phishing e le fattispecie penali applicabili nei confronti dei soggetti reclutati come "*financial manager*".

Il GUP del Tribunale di Milano[165], nel 2006, ha dovuto, seppur incidentalmente, nella stesura della sentenza emessa a seguito degli eventi narrati, tener conto dei fatti presupposti all'attività di riciclaggio di denaro proveniente da delitto e dare ad essi una precisa connotazione giuridica, interpretandoli come " *phishing a danno di correntisti Bancoposta nonché di altri istituti di credito italiani*" ed inquadrandoli come "*delitti previsti e puniti dagli articoli 640 ter, 615 quater e 615 quinquies c.p.*".

Il giudice ha, quindi, considerato il phishing come attività integrante il reato di frode informatica, accompagnata alla detenzione abusiva di codici di accesso a sistemi informatici e telematici ed alla diffusione di programmi diretti a danneggiare un sistema informatico. Lo schema operativo del phishing prevede, infatti, che vi sia un intervento senza diritto o un'alterazione del sistema informatico o telematico, condotte tipiche del reato di frode informatica, con vantaggio dei phishers e danno dei correntisti e dell'istituto di credito.

I soggetti legittimati alla proposizione della querela sono, appunto, sia la vittima dell'illecita acquisizione di dati che l'istituto di credito, poiché entrambi subiscono i danni, tanto materiali quanto dovuti alla lesione d'immagine, originati dal reato. Infatti, l'istituto di credito i cui clienti siano stati vittima di phishers dovrà aumentare i

[164] Trib. di Milano, Ufficio del Giudice per le Indagini preliminari, 28 luglio 2006; Trib. di Milano, Sez. 8, 7 ottobre 2011, n. 11696.
[165] Trib. di Milano, Ufficio del Giudice per le Indagini preliminari, 28 luglio 2006.

sistemi di sicurezza, avvisare tutti i suoi utenti, in modo riservato per evitare ulteriori eventuali danni d'immagine, predisporre, fintantoché sia possibile, mezzi idonei a scongiurare l'eventualità che l'accaduto si ripeta, nonché mettere in conto la consequenziale diminuzione di fiducia da parte del cliente truffato. E' anche possibile, volendo inquadrare in precise fattispecie penali la commissione di illeciti attraverso l'attività di phishing, dividere l'elemento materiale del reato in due distinti segmenti temporali, mantenendo applicabili differenti fattispecie incriminatorie quali ascrivibili ai phishers: un primo inquadramento del reato di detenzione abusiva di codici di accesso a sistemi informatici e telematici e diffusione di programmi diretti a danneggiare un sistema informatico, ai sensi degli artt. 615 *quater* e 615 *quinquies* c.p., ai danni del titolare dei dati personali illecitamente acquisiti mediante lo stratagemma delle e-mails fintamente provenienti dagli istituti di credito, ed una susseguente imputazione ai sensi dell'art. 640 *ter* c.p., qualora il phisher, o un soggetto terzo, riesca, mediante tali dati, a penetrare nel server della banca e, di fatto, disporre bonifici in favore di conti terzi senza averne effettivamente la facoltà. Solo nel secondo caso, dunque, si potrebbe parlare correttamente di frode informatica, poiché soggetto passivo del reato non sarebbe una persona, come nel caso dell'illecita acquisizione dei dati, bensì un sistema informatico, nello specifico quello sul quale risiede il server dell'istituto di credito[166].

Il GUP ha, quindi, qualificato il phishing come un'attività che prevede, in primo luogo, un comportamento necessariamente dannoso per il titolare dei dati, finalizzato all'illecita introduzione nel sistema dell'istituto di credito, e, successivamente,

[166] Cass. Pen., Sez. VI, 14 dicembre 1999, n. 3065.

l'induzione in errore del sistema suddetto, ai fini della distrazione di fondi o, comunque, del perseguimento di un illecito profitto con altrui danno.

Il giudice del Tribunale di Milano, nel 2011, ha emesso un'altra sentenza[167] in cui, dopo aver descritto sinteticamente il fenomeno del phishing, ha cercato di individuare le fattispecie penali applicabili sia nei confronti dei phishers che dei "*financial manager*".

I phishers, in primo luogo, si sono resi responsabili del delitto di sostituzione di persona *ex* art. 494 c.p., che è integrato con l'invio di false e-mails e la creazione di false pagine web, in tutto simili a quelle di istituti di credito di cui la vittima è cliente.

In secondo luogo, l'illecita introduzione nel sistema informatico delle banche attraverso i dati, illecitamente acquisti, relativi al conto corrente delle vittime che cadono nella trappola, integra il delitto di accesso abusivo ad un sistema informatico o telematico *ex* art. 615 *ter* c.p..

In terzo luogo, i phishers si sono resi responsabili anche del delitto di truffa *ex* art. 640 c.p., di cui ricorrono tutti gli elementi costitutivi: l'artificio o il raggiro, consistente, appunto, nell'invio di false e-mail e nella creazione di false pagine web; l'errore in cui cade il destinatario della mail, il quale ritiene che il mittente sia la banca di cui è cliente, così fornendo inconsapevolmente i dati di accesso del proprio conto corrente; l'ingiusto profitto con correlativo altrui danno, rappresentato dalle somme di denaro illecitamente sottratte dal conto corrente della vittima.

Nel caso in esame, in cui agli imputati si contesta il ruolo di "*financial manager*", il delitto presupposto delle imputazioni di ricettazione e di riciclaggio è stato individuato nella truffa. Con riferimento alla posizione del "*financial manager*" il tribunale ha

[167] Trib. di Milano, Sez. 8, 7 ottobre 2011, n. 11696.

distinto due ipotesi. Se il "*financial manager*" agisce essendo consapevole della complessiva attività truffaldina posta in essere dal phisher, egli dovrebbe rispondere a titolo di concorso dei medesimi delitti realizzati dal phisher. Viceversa, nell'ipotesi in cui il "*financial manager*" abbia agito rimanendo all'oscuro dei fatti commessi in danno dei correntisti, ma si presti a mettere a disposizione il proprio conto corrente e poi a trasferire il denaro, può configurarsi il delitto di riciclaggio ovvero il delitto di ricettazione. Nel caso di specie, agli imputati è stato contestato il fatto di avere dato la disponibilità a soggetti entrati in contatto con loro via posta elettronica a ricevere su propri conti correnti bancari o postali degli accrediti di somme provenienti da terzi, di averli poi effettivamente ricevuti, di aver prelevato in contanti la somma accreditata e, previa decurtazione delle spese e delle provvigioni, di averla trasferita all'estero al soggetto indicato dal phishers.

Dunque, agli imputati non è stata mossa l'accusa di essere stati consapevoli della complessiva attività fraudolenta dei phishers, bensì è stato contestato loro il ruolo ora di ricettatori, ora di riciclatori, a seconda che si siano limitati a ricevere il denaro, nella consapevolezza che fosse provento di attività delittuosa, ovvero l'abbiano anche trasferito all'estero con modalità idonee ad ostacolarne l'identificazione della provenienza.

La prima ipotesi è integrata dalla mera ricezione di denaro provento di delitto: è il caso di chi abbia acconsentito di accreditare somme sui propri conti correnti, ma poi, consapevole della provenienza delittuosa del denaro, non l'abbia ritrasferito, vuoi perché, a sua volta, abbia "*truffato*" i phishers, vuoi perché l'azione sia stata interrotta prima di essere portata a termine grazie all'intervento della polizia giudiziaria, che, nel

corso delle indagini, è riuscita a predisporre una black list dei destinatari finali delle somme inviate tramite le società di money tranfer.

La seconda ipotesi viene realizzata con il prelievo delle somme in contanti e con il successivo trasferimento all'estero di quelle somme mediante le società di money transfer: ciò integra la condotta di trasferimento di denaro provento di delitto con modalità idonee ad ostacolare l'identificazione della provenienza delittuosa. Non vi è dubbio, infatti, che il prelievo di somme in contanti da un istituto di credito ed il successivo invio all'estero mediante altra forma interrompe la tracciabilità dei trasferimenti e permette al phisher di ricevere in modo sicuro il profitto del reato. Questa è, inoltre, la linea interpretativa della giurisprudenza di legittimità[168], secondo cui integra il delitto di riciclaggio il compimento di operazioni volte non solo ad impedire in modo definitivo, ma anche a rendere difficile l'accertamento della provenienza del denaro, dei beni o delle altre utilità, attraverso un qualsiasi espediente idoneo.

Gli accertamenti di polizia giudiziaria e l'acquisizione di informazioni e documenti sia presso gli istituti di credito di cui le persone offese erano correntisti, sia presso le società di money transfer, sia presso le stesse abitazioni degli imputati e i loro computer, hanno dimostrato la materialità dei fatti descritti nelle imputazioni e, dunque, sul piano oggettivo, a parere del giudice, nulla quaestio. Maggiori problemi sono sorti, invece, riguardo all'elemento soggettivo dei delitti di ricettazione e riciclaggio. Va premesso che sulla controversa questione concernente l'elemento soggettivo richiesto dall'art. 648 c.p. e dell'art. 648 *bis* c.p. è intervenuta, nel 2009, la

[168] Cass. Pen., Sez. II, 12 gennaio 2006, Caione, in *Ced. Cass*., n. 232869; Cass. Pen., Sez. VI, 18 dicembre 2007, Gocini, in *Ced Cass*., n. 239844.

Corte di Cassazione a Sezioni Unite[169], stabilendo che "*l'elemento psicologico della ricettazione può essere integrato anche dal dolo eventuale, che è configurabile in presenza della rappresentazione da parte dell'agente della concreta possibilità della provenienza della cosa da delitto e della relativa accettazione del rischio, non potendosi desumere da semplici motivi di sospetto, né potendo consistere in un mero sospetto"*. In motivazione, le Sezioni Unite hanno chiarito che, con riguardo alla configurazione del dolo eventuale, "*occorrono circostanze più consistenti di quelle che danno semplicemente motivo di sospettare che la cosa provenga da delitto, sicché un ragionevole convincimento che l'agente ha consapevolmente accettato il rischio della provenienza delittuosa può trarsi solo dalla presenza di dati di fatto inequivoci, che rendano palese la concreta possibilità di una tale provenienza*".

Il giudice di merito nel caso de quo, estendendo tali considerazioni anche al delitto di riciclaggio, ha ritenuto sussistente il dolo quando, sulla base di precisi elementi di fatto, si possa affermare che l'imputato si sia seriamente rappresentato l'eventualità della provenienza delittuosa del denaro e l'abbia comunque trasferito all'estero. Il giudice ha richiamato, peraltro, anche un'altra decisione della Corte di cassazione[170] riguardante un caso analogo, la quale aveva affermato che non concorrono nel reato di riciclaggio coloro che abbiano svolto operazioni di trasferimento di denaro con il mero sospetto dell'illecita provenienza di esso.

In altri termini, il dolo eventuale nel delitto di riciclaggio richiede un atteggiamento psicologico che, pur non attingendo il livello di certezza, si deve collocare ad un livello superiore rispetto a quello del sospetto. Il giudice, inoltre, con riferimento alla

[169] Cass. Pen., Sez. Un., 26 novembre 2009, Nocera, in *Ced Cass*., n. 246324.
[170] Cass. Pen., Sez. II, 17 giugno 2011, n. 25960, in *Guida dir*., 2011.

provenienza illecita della res, ha esteso l'interpretazione della giurisprudenza di legittimità[171] in materia di prova dell'elemento soggettivo nel reato di ricettazione, giungendo alla conclusione che anche nel delitto di riciclaggio la prova dell'elemento soggettivo può essere raggiunta sulla base dell'omessa o non attendibile indicazione della provenienza della cosa ricevuta.

Nel caso in esame, tutti i soggetti imputati sono stati reclutati come collaboratori, c.d. "*financial manager*", da sedicenti società straniere, mediante l'invio di e-mails spesso scritte in un inglese scorretto e sgrammaticato, che promettevano ingenti guadagni in cambio di prelievi di denaro contante ricevuto sul proprio conto corrente senza una causale evidente, che doveva poi essere immediatamente trasferito all'estero tramite società di money transfert.

Tali elementi indubbiamente potrebbero far sorgere il sospetto, in capo al "*financial manager*", circa l'illiceità della provenienza del denaro accreditato, ma ad avviso del tribunale, essi non rappresentavano una "*una situazione fattuale di significato inequivoco"* che potesse far ritenere sussistente il dolo, anche nella forma del dolo eventuale.

Le caratteristiche intrinseche dell'operazione potevano certamente rappresentare un motivo di sospetto, rispetto al quale l'agente avrebbe potuto avere un atteggiamento psicologico di disattenzione, di noncuranza o di mero disinteresse, ma non paiono di per sé decisive per dimostrare, oltre ogni ragionevole dubbio, il dolo richiesto dall'art. 648 c.p. o dell'art. 648 *bis* c.p. in capo al "*financial manager*". Per contro, il dolo potrà ritenersi sussistente quando, sulla base di precisi elementi di fatto, quali potrebbero

[171] Cass. Pen., Sez. II, 27 febbraio 2003, Crevena, in *Ced Cass.*, n. 224634; Cass. Pen., Sez. II, 11 giugno 2008, Nardino, in *Ced Cass*., n. 241458; Cass. Pen., Sez. II, 25 maggio 2010, Fontanella, in *Ced Cass*., n. 248265.

essere lo scambio di e-mail fra "*financial managers*" e phishers da cui emergano il suggerimento di mentire al personale dell'istituto di credito o le spiegazioni di tutti i dettagli o le modalità dell'operazione o, ancora, l'omessa indicazione della provenienza del denaro avente il palese obiettivo di occultarla, si possa affermare che l'imputato si sia seriamente rappresentato l'eventualità della provenienza delittuosa del denaro e, nondimeno, si sia comunque determinato a trasferirlo all'estero.

Conclusioni

Alla luce delle considerazioni svolte nella presente tesi, possiamo affermare che, ad oggi, i c.d. computer crimes rappresentano, al pari di qualsiasi altro tipo di reato, una concreta minaccia per la nostra società. Sempre più persone, dai più piccoli agli anziani, utilizzano quotidianamente il computer, spesso senza avere la consapevolezza dei rischi legati ad esso e ad internet e si espongono alla possibilità di attacchi da parte di altri utenti, più o meno esperti, che fanno leva, appunto, sull'ingenuità e l'inesperienza dei più.

Sarebbe, quindi, opportuno che l'ordinamento giuridico italiano, dato il continuo evolversi delle tecnologie e il loro utilizzo costante e quasi, ormai, necessario nella vita di ogni giorno, predisponga una normativa che sappia impedire, con adeguate barriere di protezione, gli attacchi informatici e, se nel caso, intervenire tempestivamente con misure tecniche quando siano scoperti i primi segnali di violazioni massicce.

Quanto predisposto con le leggi n. 547/ 1993 e, poi, n. 48/ 2008 non è più sufficiente. E' ormai necessaria una normativa che sia in grado di rispettare e valorizzare la libertà di utilizzo dei dispositivi informatici e delle reti telematiche e, allo stesso tempo, di tutelare al meglio i soggetti offesi dai cybercrimes.

Per raggiungere tale scopo sarebbe quindi utile, da un lato, una maggiore sensibilizzazione ed informazione, in modo da fornire un'adeguata conoscenza dei rischi che possono correrси con l'uso degli strumenti tecnologici, dall'altro, una maggiore asprezza delle pene, in modo da disincentivare i pirati informatici dal porre in essere le condotte criminose.

Data la rilevanza che ormai hanno assunto gli strumenti tecnologici, divenuti un ulteriore mezzo per porre in essere attività illecite, come dimostra l'analisi fin qui svolta in merito, è compito del legislatore fornire un'adeguata tutela a tali nuove situazioni e nuove problematiche.

Sarebbe, dunque, auspicabile che il legislatore revisionasse la normativa in materia di reati informatici, prevedendo ulteriori specifiche disposizioni, l'aumento delle pene per questi reati che fanno ormai parte della nuova società net-centrica e l'inserimento di un nuovo titolo nel codice penale ad essi dedicato.

Bibliografia

Agnino F., commento a Sentenza 29/10/2008 Tribunale di Milano, *Computer crime e fattispecie penali tradizionali: quando il phishing integra il delitto di truffa*, Il Corriere del Merito n. 3/2009.

Alesiani V., *Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione*, in *Cass. pen*., 2001.

Amore S., Stanca V., Staro S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Massa Carrara, 2006.

Bartoli R., *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma***,** Dir. informatica, fasc. 3, 2011.

Bianchi D., *Phishing, Primo grande processo in Italia. Ordinanza tribunale di Milano. Attenzione adesso agli escrow truffa. Normativa di riferimento*, in www.personaedanno.it , 2008.

Blaiotta R., *I reati commessi con le carte di pagamento nel sistema penale*, in *Critica del dir.*, 1996.

Borruso R., Buonomo G., Corasaniti G., D'Aietti G., *Profili penali dell'informatica*, Giuffrè, Milano, 1994.

Borsari R., *Utilizzo indebito di carte di credito, sostituzione di persona e truffa* (nota a GUP di Milano - 15 ottobre 2007, est. Interlandi), febbraio 2008, in www.penale.it.

Bovino L., *Phishing come illecito civile*, in www.anti-phishing.it.

Bovino L., *Phishing come accesso abusivo ad un sistema informatico*, in www.anti-phishing.it.

Cajani F., Costabile G., Mazzaraco G., *Phishing e furto di identità digitale*. *Indagini informatiche e sicurezza bancaria,* Milano, Giuffrè, 2008.

Cajani F., *La tutela penale dell'identità digitale alla luce delle novità introdotto dal d. l. 14 agosto 2013 n. 93 (convertito con modificazioni dalla legge 15 ottobre 2013 n. 119),* Cassazione Penale, fasc. 3, 2014.

Cajani F., *Profili penali del phishing*, in CP, 2007.

Campeis C., *Frode informatica*,in AA.VV. (a cura di), *Reato e danno*, Milano, Giuffrè, 2014.

Campeis C., *La frode informatica*, in AA.VV. (a cura di), *Trattato dei nuovi danni*, Padova, CEDAM, 2011.

Cipolla P., *E-commerce e truffa*, Giur. merito, fasc. 12, 2013.

Cipolla P., *Social network,furto di identità e reati contro il patrimonio*, Giur. merito, fasc.12, 2012.

Citarella G., *Informatica e danni esistenziali,Persona e danno,* IV, Cendon P. (a cura di), Giuffrè, Milano, 2004.

Cocco G., *Trattato breve di diritto penale - Parte speciale - II - I reati contro i beni economici 2015 > Frode informatica (640ter, 640quinquies)*, CEDAM, 2015.

Corbetta S., *Creazione e utilizzo di un account di posta elettronica con un falso nome*, in *Dir. Pen. e Processo*, 3, 2008.

Corrias Lucente G., *I reati in materia di carte di credito nella legge 5 luglio 1991 n. 197*, in *Dir. informaz. informat*., 1991, 3.

Corrias Lucente G., *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in *Diritto dell'informazione e dell'informatica*, 1987.

Crisafi M., Trunfio E., *Il phishing*, in AA.VV. (a cura di), *Trattato dei nuovi danni*, Padova, CEDAM, 2011.

Cuniberti M., Gallus G., Micozzi F., *I nuovi reati informatici*, Giappichelli, Torino, 2009.

Cuomo L., Razzante R., *La nuova disciplina dei reati informatici*, Giappichelli, Torino,2009.

Delogu T., *Il momento consumativo della truffa*, in *Giur. Cass. pen.*, 1944.

De Marsico A., *Delitti contro il patrimonio*, Napoli, 1951.

Destito V. S. , Dezzani G., Santoriello C., *Il diritto penale delle nuove tecnologie*, Padova, 2007.

De Robbio C., *Giurisdizione e competenza in materia penale*,Giur. merito, fasc. 12, 2013.

Dello Iacono A., *Articolo 640 ter: truffa o furto? La Frode informatica e il «modello 640»*, in *Temi Romana*, 1996.

Di Ciommo F., *La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in *Danno e Resp*., 2005.

Falcone V., *I diritti della personalità*, in *Il quantum nel danno esistenziale*, Cendon P.(a cura di), Giuffrè, Milano, 2010.

Fanelli A., *La truffa*, Giuffrè, 1998.

Fanelli A., *Sub art. 640 ter*, in *Codice penale*, Lattanzi G., Lupo L., Giuffrè, Milano, 2004.

Fanelli A., *Telefonate abusive e frode informatica*, in *Foro italiano*, 1999.

Fiandaca G. – Musco E., *Diritto penale, parte speciale, II, Delitti contro il patrimonio*, Bologna, 2002.

Flor R., *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. pen. proc*., 2008.

Flor R., *Commento a G.I.P., Tribunale di Milano, sentenza 10 dicembre 2007, n. 888*, in *Riv. Giur. Ec. d'Az*., n. 4/2088.

Flor R., *Frodi identitarie e diritto penale*, in www.penale.it , 2008.

Flor R., *Phishing, identity theft e identity abuse:le prospettive applicative del diritto penale vigente*, in RIDPP, 2007.

Flor R., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo jus excludendi alios*, in *Dir. Pen. Proc*., 2005.

Fondaroli D., *Osservazioni intorno ad alcune delle norme contenute nella recente normativa italiana sui computer crimes*, in *La nuova normativa in tema di criminalità informatica: alcune riflessioni*, Sola L., Fondaroli D., CLUEB, Bologna 1995.

Frosini V., *Introduzione*, in Borruso R., Buonomo G., Corasaniti G., D'Aietti G., *Profili penali dell'informatica*, Milano, 1994.

Iurilli C., *Il furto di identità nel settore bancario. Tutela normativa e profili risarcitori*, in RC, 2009.

Lagroscino S., *La frode informatica quale autonoma figura di reato rispetto al delitto di truffa*, articolo pubblicato su www.altalex.it in data 05/01/2012.

Landi S., *Rapporto 2010- Il furto di identità nell'esperienza dei consumatori*, ADICONSUM, in www.furtoidentita.com , 2010.

Librando V., *La tutela della riservatezza nello sviluppo tecnologico*, in *Dir. inf. e informatica*, 1987.

Lorusso S., *L'insicurezza dell'era digitale, Tra cybercrimes e nuove frontiere dell'investigazione*, Milano, 2011.

Lucarino A., *Responsabilità e risarcimento dei danni in seguito al trattamento dei dati personali*, in www.privacy.it , 2000.

Mantovani F., *Diritto penale, Parte speciale, II, Delitti contro il patrimonio*, III ed., Padova, 2009.

Manzini V., T*rattato di diritto penale italiano*, Vol. IX, Torino, 1952.

Maraffino, *Falso profilo su Facebook, un reato che può costare caro*, in www.ilsole24ore.com.

Marini G., *Condotte in alterazione del reale aventi ad oggetto nastri ed altri supporti magnetici e diritto penale*, in *Riv. it. dir. proc. pen.*, 1986.

Marini G., (Voce) *Truffa* (frode informatica) in *Digesto delle discipline penalistiche*, Torino, 2006.

Masi A., *Frodi informatiche e attività bancarie*, in *Riv. Pen. econ.*,1995.

Massa R. G., *Il phishing*, in www.pmi.it , 2008.

Militello V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ.*, 1992.

Mucciarelli F.,*Commento all'art. 10 della legge n. 547 del 1993*, in *Legislazione penale*, 1996.

Padovani T., *Sub art. 640 ter*, in *Codice penale*, Giuffrè, Milano, 2007.

Pagliaro A., *Principi di diritto penale, parte speciale*, III, Milano, 2003.

Parodi C., *Detenzione abusiva di codici d'accesso a sistemi e illecito impedimento di comunicazioni telematiche*, in *Dir. pen. proc.*, 1998.

Parodi C., *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in *Criminalità informatica*, Sarzana Di S. Ippolito F. (a cura di), in *Diritto e procedura penale*, 1997.

Pecorella C., *Commento Art. 640 ter c.p.*, in *Codice penale commentato, Artt. 575-734 bis*, a cura di Dolcini E. e Marinucci G., III ed., Milano, 2011.

Pecorella C., *Il diritto penale dell'informatica*, Cedam, Padova, 2000.

Pecorella C., *Il nuovo diritto penale della carte di pagamento*, in *Riv. it. dir. proc. pen.*, 1993.

Pecorella C., *L'abuso dei distributori automatici di banconote*, in *Riv. it. dir. proc. pen*, 1990.

Pecorella C., *Truffe on-line:momento consumativo e competenza territoriale*, Riv. it. dir. e proc. pen., fasc. 1, 2012.

Perri P., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia, in Dir. Internet*, n. 3/2008.

Pica G., *Computer crimes e uso fraudolento delle nuove tecnologie, Seminario di studi*, Roma 15 dicembre 2000.

Pica G., *Diritto penale delle tecnologie informatiche*, Torino, 1999.

Pica G., *Internet*, in *Dig. pen.*, Aggiornamento, I, Torino, 2007.

Pica G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Rivista penale dell'economia*, 1995.

Picotti L., *Commento all'art. 5 della legge n. 547 del 1993*, in *Legislazione penale*, 1996.

Picotti L., *I diritti fondamentali nell'uso e abuso dei social network. Aspetti penali*, *Giur. merito*, fasc. 12, 2012.

Putzu G., *Art. 640 ter c.p.*, in Ronco M., Ardizzone S. (a cura di) *Codice penale ipertestuale. Commentario con banca dati di giurisprudenza e legislazione*, II Ed., Torino, 2007.

Resta F., *Banche dati on line . I limiti della tutela penale*, in GM, 2007.

Resta F., *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, GM, 2008.

Salcuni G., *La frode e il danneggiamento informatico tra prassi applicativa, note di diritto comparato ed esigenze di riforma*, in Plantamura V. e Manna A. (a cura di), *Diritto penale e informatica*, Caccucci, Bari, 2007.

Sambucci L., *Falsi call center sul VoIP: la nuova truffa si chiama Vishing*, in www.anti-phishing.it , 2006.

Scognamiglio P., *Criminalità informatica*, Simone, Napoli, 2008.

Scopinaro L., *Internet e reati contro il patrimonio*, Torino, 2007.

Sieber V., *La tutela penale dell'informazione*, in *Rivista trimestrale di diritto penale dell'economia*, 1992.

Stalla G., *L'accesso abusivo ad un sistema informatico o telematico*, febbraio 2003, in www.penale.it . http://www.penale.it/commenti/stalla_01.htm

Surace C., *Dal Phishing al Vishing: l'evoluzione della truffa come conseguenza dell'evoluzione tecnologica*, 18 febbraio 2007, Ricerca svolta presso l'Osservatorio CSIG (Centro Studi Informatica Giuridica) di Reggio Calabria, in www.filodiritto.com.

Valastro A., La *tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. e proc. pen.*, 1999.

Riferimenti giurisprudenziali

Cass. Pen., Sez. III, 15 dicembre 2011- 3 aprile 2012, n. 12479.

Cass. Pen., Sez. II, 17 giugno 2011, in *Guida dir*., 2011, n. 25960.

Cass. pen., Sez. II, 24 febbraio 2011, in *DeJure*, n. 9891.

Cass. Pen., Sez. II, 25 maggio 2010, Fontanella, in *Ced Cass*., n. 248265.

Cass. Pen., Sez. Un., 26 novembre 2009, Nocera, in *Ced Cass*., n. 246324.

Cass. Pen., Sez. II, 11 novembre 2009, n. 44720.

Cass. Pen., Sez. II, 11 giugno 2008, Nardino, in *Ced Cass*., n. 241458.

Cass. Pen., Sez. VI, 18 dicembre 2007, Gocini, in *Ced Cass*., n. 239844.

Cass. pen., Sez. V, 14 dicembre 2007, n. 46674.

Cass. Pen., Sez. V, 8 novembre 2007, n. 46674, in *Ced Cass*., n. 238504.

Cass. Pen., Sez. V, 6 febbraio 2007, su *Mass. Pen*., n. 236221.

Cass. Pen., Sez. II, 12 gennaio 2006, Caione, in *Ced. Cass*., n. 232869.

Cass. Pen., Sez. II, 4 maggio 2006, in *Dir. Pen. Proc*., 2007, fasc. 3.

Cass. Pen., Sez. V, 1 ottobre 2004, n. 2672.

Cass. Pen., Sez. I, 23 aprile 2004, n. 26300.

Cass. Pen., Sez. II, 27 febbraio 2003, Crevena, in *Ced Cass*., n. 224634.

Cass. Pen., Sez. V, 24 novembre 2003, in *Giur. It.*, 2004, n. 4576.

Cass. Pen., Sez. V, 7 novembre 2000, Zara, in *Giust. Pen.*, 2001.

Cass. Pen., Sez. VI, 14 dicembre 1999, n. 3065.

Cass. Pen., Sez. VI, 4 ottobre 1999, in *Dir. Inf.*, 2001, n. 214945.

Cass. Pen., Sez. Un., 16 dicembre 1998, n. 24 , Messina, m. 212076.

Cass. Pen., Sez Un., 9 ottobre- 13 dicembre 1996, n. 1282.

Cass. Pen., Sez. II, 24 novembre 1986, n.13166.

Trib. di Como, Sez. Pen., 21-25 settembre 1995, n. 611.

Trib. di Firenze, 27 gennaio 1986, in *Foro it.*, 1986.

Trib. di Milano, Ufficio del GUP, 28 luglio 2006, in *Dir. dell'Internet*, n. 1/2007.

Trib. di Milano, 10 dicembre 2007, n. 888.

Trib. di Milano, Ufficio GUP, 15 ottobre 2007 (depositata 7 novembre 2007- est. Interlandi).

Trib. di Milano, Sez. 8, 7 ottobre 2011, n. 11696.

Trib. di Nola, 11 dicembre 2007, n. 488.

Trib. di Roma, 20 giugno 1984, "*Testa ed altri*", in *Dir. Inf.*,1986.

Trib. di Roma, 14 dicembre 1985, "*Manenti ed altri*", in *Dir. Inf.*,1988.

Trib. di Torino, 12 dicembre 1983, in *Giur. it.*, 1984.

Trib. di Torino 4 dicembre 1997, *Zara e altro*, in *Dir. informazione e informatica*, 1998.