



## ASPETTI LEGALI

a cura dell'**Avv. Salvatore Frattallone**

911-PLE Triveneto

<http://www.frattallone.it>

[salvatore@frattallone.it](mailto:salvatore@frattallone.it)

### **PHISHING, FENOMENOLOGIA E PROFILI PENALI: DALLA NUOVA FRODE TELEMATICA AL CYBER-RICICLAGGIO**

---

**IL FENOMENO «PHISHING»** - Sembra che, nei modi davvero più disparati, da poco più d'un anno ai lestofanti tecnologici non sia stato mai così facile poter carpire le altrui informazioni bancarie. Non passa giorno in cui, attraverso lo *spamming*, non vengano lanciati, nel mare telematico che non conosce frontiere, gran quantità di ami aspettando che, in ossequio alla legge dei grandi numeri, qualche utente di *internet* abocchi. Ma di cosa si tratta, in concreto? E, soprattutto, quali i risvolti giudiziari?

**LE CONDOTTE FRAUDOLENTE** - Il neologismo *phishing* compare per la prima volta in un *newsgroup* del 1996 e l'anno successivo viene già utilizzato dai media. Per alcuni si tratterebbe del gergale *fishing* (pescare) scritto in grafia stile *hacker*, mentre per altri sarebbe una crasi, un *collage* di tre parole anglosassoni, *password+harvesting+fishing*, ad indicare la raccolta, attuata pescando, di parole chiave e di codici d'accesso a servizi economico/finanziari; infine, la «f» («*ph*») del vocabolo potrebbe trarre origine da una variante del *phone phreaking*, il fenomeno delle truffe attuate ai danni delle compagnie telefoniche negli anni '70, mediante allacciamenti abusivi, con mezzi meccanici (non informatici), direttamente alle linee del telefono per effettuare chiamate senza pagarle.

Le prime vere e proprie *e-mail* di *phishing*, però, stando a quanto presente negli archivi,<sup>[1]</sup> risalirebbero solo al 2003, anno in cui nella penisola iberica vennero sferrati i primi efferati colpi a noti istituti di credito, a società di *e-commerce* e ad istituti specializzati in strumenti di pagamento e credito al consumo.

---

<sup>[1]</sup> Si vedano le utili pagine reperibili ai link [http://www.antiphishing.org/phishing\\_archive.html](http://www.antiphishing.org/phishing_archive.html) e <http://www.millersmiles.co.uk/archives.php>.

Nel *report* di maggio 2005 redatto dall'*Anti-Phishing Working Group* si legge che sarebbero stati sinora individuati oltre 3 mila siti creati a scopo di frode, di cui il 2% ospitati in Italia. Oggi, il *phishing* si è differenziato, tanto che taluni siti «specializzati»<sup>[2]</sup> mettono a disposizione degli utenti informazioni ed archivi, in cui sono classificati i vari tipi di messaggi finora utilizzati dagli *scammers* o elenchi delle diverse metodologie d'attacco.

Siffatte frodi vengono poste in atto con effetti devastanti per la fiducia riposta dagli utenti nell'affidabilità delle transazioni effettuate con l'ausilio di sistemi telematici.

Dal punto di vista prettamente tecnico-informatico, l'inganno è ordito mediante l'invio di una c.d. *spoof e-mail* fraudolenta, oppure è attuato facendo apparire sul *monitor* dell'utente, mentre questi procede ad una regolare connessione e consultazione del sito d'interesse, una finestra c.d. di *pop-up*, che invita al collegamento con un altro sito, apparentemente autentico, di banche o di società di *e-commerce* (tra cui: *Barclays iBank, Citibank, Nat West Bank U.S. Bank, Unicredit, Banca Intesa, Yahoo, ebay, Paypal*; ma la lista si allunga di giorno in giorno). Attivando il link e proseguendo nella connessione, l'ignaro navigatore viene indotto in errore, finendo col comunicare ai *phishers* i propri dati personali. Da lì, il passo è breve: l'abilitazione diretta del titolare consente loro di operare sui conti correnti, attivando prelievi, disponendo bonifici o, comunque, usufruendo di altre funzioni altrimenti riservatissime.

Spesso, l'utente viene abbagliato dal tenore della comunicazione pervenutagli, poiché viene attirato dalla seducente promessa di ricevere un premio fedeltà.<sup>[3]</sup> Altre volte, invece, gli viene paventato un danno (quale la perdita dei dati, un guasto tecnico al sistema informatico della banca, la possibile chiusura anticipata dei suoi conti correnti *online*, la disattivazione temporanea dei servizi di *home banking*). In altre occasioni, viene fatta leva sulla ...sicurezza, suggestionandolo con l'asserita necessità che, per ovviare ad asserite falle riscontrate nel sistema di protezione del gruppo creditizio o della società di *e-commerce*, egli provveda ad inviare nuovamente – e, per giunta, subito! – gli estremi della carta di credito (numero, periodo di validità), la password o i codici per l'*home banking*.<sup>[4]</sup>

---

<sup>[2]</sup> Sul tema, in particolare, <http://www.antiphishing.org> e <http://www.millersmiles.co.uk>, benché i siti che affrontano seriamente la questione del *phishing* siano numerosi: ad esempio, <http://www.aessenet.org> oppure <http://www.telemar.it>.

<sup>[3]</sup> Questo il testo d'una delle *e-mail* di *spoofing*.

«Caro cliente, Banca Intesa vi rimborsa per la vostra fedeltà con 100 Euro. Prima di usare questo importo, dovete seguire il collegamento e usare il vostro Codice cliente e Codice segreto. Un operatore si metterà in **contacto** con voi per confermare l'importo. [Http://www.bancaintesa.it](http://www.bancaintesa.it)».

Cliccando sul link lì indicato, si viene invero trasferiti alla pagina: <http://free.hostdepartment.com/j/jpxcnnq2> in cui appare perfettamente riprodotta l'*home-page* di Banca Intesa, attivata per l'atteso inserimento dei codici riservati.

<sup>[4]</sup> I clienti di *ebay* furono invero tra i primi ad essere colpiti dalle *e-mail phished*; proprio in questi giorni peraltro (l'*e-mail* è difatti giunta in data 01.08.2005), *ebay* è stata nuovamente presa di mira dagli *scammers*, che questa volta hanno inteso astutamente puntare sull'aspetto sicurezza, avvertendo l'utente della minaccia di una frode e della conseguente irrefragabile necessità che siano comunicato il proprio *account* ad un sito sicuro, raggiungibile cliccando sull'indirizzo indicato nell'*e-mail* intitolata «*eBay Fraud Mediation Request*», all'apparenza inviata da [support@ebay.com](mailto:support@ebay.com). L'invito *de quo*, avente ad oggetto «\*\*\*Urgent Safeharbor Department Notice\*\*\*», recita così:

«You have recieved this email because you or someone had used your account to make fake bids at eBay. For security purposes, we are required to open an investigation into this matter. THE FRAUD ALERT ID CODE CONTAINED IN THIS MESSAGE WILL BE ATTACHED IN OUR FRAUD MEDIATION REQUEST FORM, IN ORDER TO VERIFY YOUR EBAY

Per rendere più credibile la contraffazione, l'e-mail o il *pop-up* vengono callidamente progettati in modo da far presupporre la navigazione in un'area familiare, secondo metodiche che paiono, allo stato, purtroppo «collaudate»:

i) con l'utilizzo d'immagini di noti marchi e loghi; ii) con la fedele riproduzione dei *form* d'inserimento dati solitamente in uso sui siti «legittimi»; iii) con la strutturazione del sito *web spoofed* in modo tale che compaiano quelle tipiche finestre con le stringhe d'inserimento e conferma dati che l'utente ha imparato ad adoperare;<sup>[5]</sup> iv) addirittura in alcuni casi generando un browser apparente, grazie ad un *worm* (*virus* del tipo *mimail worm*) presente sulle *e-mail*; v) oppure persino attivando siti *web* (cui si accede cliccando sull'indirizzo indicato nella corrispondenza) di cui una parte è stata *tout court* copiata mentre un'altra parte non è dinamica, cioè risulta disattivata; vi) in altri più subdoli casi s'è persino verificato che il sito «vero», che «si apre» all'atto della connessione, contenga un messaggio ad apertura automatica (*pop-up*) «falso» che, interponendosi tra il *client* dell'utente e il *server* dell'istituto di credito, impone all'utente di comunicare, in una sorta di cieca obbedienza, i suoi dati ad un fantomatico nuovo *server* aziendale o a un sito *web* dall'apparente origine legittima; vi) ancora, prelevando all'interno di un'area a *Ftp* alcuni *file* contenenti informazioni ottenute mediante l'utilizzo di programmi cc.dd. *key-logger*, camuffati e posti in circolazione durante sessioni di «P2P» ed installati abusivamente dopo il *download*.

E le tecniche criminali del dilagante fenomeno *de quo* sembrano destinate ad una continua «evoluzione»: non ultima, la «trovata» d'inoltrare *e-mail* di *phishing* con testo

---

ACCOUNT REGISTRATION INFORMATION. Fraud Alert ID CODE: 00937614 (Please save this Fraud Alert ID Code for your reference. To help speed up this process, please access the following form to complete the verification of your eBay account registration informations: [http://scgi.ebay.com/verify\\_id=ebay fraud alert id code=00937614](http://scgi.ebay.com/verify_id=ebay%20fraud%20alert%20id%20code=00937614). Please Note: If we do not receive the appropriate eBay account verification within 48 hours, then we will assume this eBay account is fraudulent and will be suspended. The purpose of this verification is to ensure that your eBay account has not been fraudulently used and to combat the fraud from our community. We appreciate your support and understanding, as we work together to keep eBay a safe place to trade. Thank you for your patience in this matter. Regards, Safeharbor Department (Trust and Safety Department) eBay Inc. Please do not reply to this e-mail, as this is only a notification. Mail sent to this address cannot be answered. Copyright © 2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. eBay and the eBay logo are trademarks of eBay Inc. eBay is located at 2145 Hamilton Avenue, San Jose, CA 95125 ».

Senonché, visualizzando i codici HTML di tale *e-mail*, è stato possibile scoprire che il sito a cui si viene dirottati, pur apparendo come riferibile alla società di e-commerce *ebay* («[http://scgi.ebay.com/verify\\_id=ebay fraud alert id code=00937614](http://scgi.ebay.com/verify_id=ebay%20fraud%20alert%20id%20code=00937614)»), in sostanza è ben altro (<http://ns.beshtau.ru/beshtau.html>).

<sup>[5]</sup> In queste ultime settimane sono stati colpiti anche utenti italiani, con *e-mail* di *spoofing* apparentemente trasmesse da *UniCredit*, *Banca Intesa* e *Poste.it*. Di tali messaggi, talvolta infarciti d'errori grammaticali, si ne riportano un paio:

a. «Egredi clienti della banca UniCredit Banca via Internet Imprese, Vi informiamo che in relazione al sovraccarico del nostro generale server <http://www.unicreditbanca.it> la nostra zona **tecniche e** allargata con l'aggiunta di nuovo server attualmente nella fase di test. L'indirizzo fisso del nuovo web server del servizio online banking è [www.unicreditsbanca.com](http://www.unicreditsbanca.com). Tutti i clienti devono essere soggetti alla procedura obbligatoria d'autenticazione al nuovo server per far **transferire** i Vostri dati d'utente con successo alla base dei dati del nuovo più protetto server del servizio online banking. 1. Aprite la web pagina <http://www.unicreditsbanca.com>, 2. Entrate nel Vostro conto online usando la combinazione Codice i Pin; 3. Per evitare la perdita dei Vostri dati personali e per la protezione contro assalti di «Phishing» si prega di sempre chiudere la finestra del Vostro Internet Browser al termine di lavori con la banca online. Distinti saluti, il servizio d'assistenza tecnica della banca **online** UniCredit».

b. «Dear UniCredit Banca Member, this email was sent by the UniCredit Banca server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your UniCredit Banca online access details. This is done for your protection – because some of our members no longer have access to their email addresses and we must verify it. to verify your e-mail address click on the link below: <http://www.unicreditbanca.it/hhICEVzkHnIZQFD5zw2Lbg10JuSChOTzEHBf0QWYVqywYs9EnSp8645a0>».

fraudolento stavolta con testo della missiva non «in chiaro», ma inserito all'interno d'una serie d'immagini (*file* con estensione *.gif* o *.bmp*), verosimilmente per aggirare gli appositi filtri *anti-spamming* oggi diffusi in commercio.<sup>[6]</sup>

**LA QUALIFICAZIONE GIURIDICA** – Un misurato approccio con la recente fattispecie impone di valutare quale norma incriminatrice meglio sembri attagliarsi al caso concreto, sì da delineare i contorni del fatto-reato di *phishing*. È certo, però, che il fenomeno delinquenziale in esame, talvolta classificato con l'accattivante epìteto di «furto d'identità»,<sup>[7]</sup> non abbia in realtà nulla a che spartire con la tradizionale figura della «sottrazione di cose mobili altrui» prevista e punita dall'art. 624 C.P.<sup>[8]</sup>

1. Innanzitutto, pare possa fondatamente sostenersi la ricorrenza della violazione dell'**art. 617-sexies C.P.**, che punisce la **falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche**.

Infatti, tale norma è diretta a reprimere la condotta di colui che, ledendo i diritti della persona e l'inviolabilità dei segreti, formi in tutto o in parte una comunicazione telematica, o la alteri o sopprima. Il delitto, inserito nel Codice Penale con L. n. 547/1993, è perseguito d'ufficio, a condizione che il colpevole faccia uso dell'atto falso oppure lasci che altri nel faccia uso.

La struttura della norma è sostanzialmente identica a quella di cui all'art. 485 C.P. (falsità in scrittura privata), con il necessario adeguamento dell'oggetto materiale attinto dalla condotta del reo, che deve consistere nel contenuto di talune delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti fra più sistemi. Il fatto, peraltro, può venir aggravato dalla circostanza speciale di cui al quarto comma dell'art. 617-*quater* C.P., nell'ipotesi in cui ricorra un danno ad un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente un servizio di pubblica necessità.

Orbene, non v'è chi non veda come il comportamento del falsificare comunicazioni

---

<sup>[6]</sup> La novità di posta elettronica con immagini fuse assieme al testo ingannevole ha fatto ora la sua comparsa, con un'*e-mail* rivolta al «Dear Banca Intesa Member», che invita al *link* ad un certo indirizzo, da cui promanano altri collegamenti con l'usuale *sistema a cascata* (da *google.dk*, *.cg*, *.fi*, *.fr*, etc.) e il cui messaggio così esordisce: «This email was sent by the Banca Intesa server to verify your e-mail address. You must complete this process by...».

<sup>[7]</sup> «*Phishing is a form of online identity theft...*», esordisce, ad esempio, il *Phishing Activity Trend Report* dell'aprile 2005, reperibile in rete all'indirizzo ; così pure, usa l'appellativo suggestivo di «furto d'identità», ne «*La nostra breve guida al phishing*», <http://www.millersmiles.co.uk>, uno dei tanti siti apparsi per diffondere servizi e notizie anti-*phishing*.

<sup>[8]</sup> Si potrebbe, in ipotesi, pensare che «cosa mobile altrui» possa essere anche la *passwords*, i codici e i dati occorrenti per l'operazione di *login* (in riferimento al concetto di «ogni altra energia che abbia un valore economico» presente nel capoverso della norma a commento; ma dottrina e giurisprudenza concordemente ritengono – e una diversa interpretazione, allo stato, è difficilmente sostenibile – che «cosa» sia ogni entità materiale, di qualunque specie essa sia, idonea a soddisfare un bisogno: deve cioè trattarsi di una parte del mondo esterno avente una dimensione fisica, talché cose sono tutti gli oggetti che possono essere sottratti dal ladro. De iure condendo, peraltro, sarebbe forse necessario sostanziare tale definizione adeguandola ad un'accezione più ampia, tale da poter ritenere cose anche quelle entità non aventi solamente una dimensione strettamente fisica, proprio come avviene, oggi su scala mondiale, con i furti di dati che si traducono in impossessamenti di denaro portati a termine attraverso internet.

telematiche attraverso la formazione *ex novo* di un contenuto mendace<sup>[9]</sup> (oltrech  alterando o sopprimendo le notizie o le informazioni oggetto della comunicazione), serbando un contegno che   stato definito «il clone telematico» dell'art. 617-ter C.P. (in tema di falsit  di comunicazioni telegrafiche o telefoniche), ben costituisca il prodromo dell'agire degli *scammer*: il *phishing* prende avvio (solitamente) proprio da una *e-mail* falsa, mascherata per apparire, agli utenti cui   spedita, come se provenisse dall'organizzazione legittima che la sottoscrive. La punibilit  del reato, pertanto, appare indubbia.

2. Qualora, invece, la condotta iniziale del *phisher* consista nel far apparire una finestra di *pop-up* sul monitor dell'utente che si connetta al sito legittimo, invitandolo tramite tale «esca» a convogliare i suoi dati su altro sito «mascherato», allora si verifica una diversa situazione, quella peculiare della violazione dell'**art. 615-ter C.P.**, ovvero sia **l'accesso abusivo ad un sistema informatico o telematico**.

L'abusiva intrusione o l'indebita permanenza nel collegamento con i sistemi informatici, contro la volont  espressa dell'avente diritto – per tale dovendosi intendere anche una persona giuridica, cio  una societ  di capitali, non solo una persona fisica – comporta la lesione dell'interesse specificamente tutelato da questa norma, la riservatezza del domicilio informatico, inteso come «luogo informatico» in cui la persona (o l'ente) agisce ed estrinseca la sua personalit .<sup>[10]</sup>

La fattispecie ricorre, dunque, nel caso in cui il tipo di *phishing* posto in essere sia quello, particolarmente insidioso, che viene attuato servendosi del sito «vero» della societ  (banca, etc.), accedendo al quale s'interponga il *pop-up* «fasullo» (in corrispondenza della connessione operata dagli utenti): attraverso l'espedito del «reindirizzamento» l'*hacker* pu  cercare, per perpetrare la frode, d'adescare il cliente del sito «legittimo» e d'impossessarsi dei suoi dati.

3. Si constata, in terzo luogo, che il *phisher* ottiene con l'inganno *password*, codici cliente, numeri di carte di credito e quant'altro gli consente d'accedere al conto corrente della vittima e di ...ripulirlo: **la detenzione** (come pure la diffusione) **abusiva di codici di accesso a sistemi informatici o telematici**   peraltro espressamente sanzionata dall'art. 615-quater C.P., che appresta un non irrilevante tutela penale proprio alla riservatezza delle «chiavi di accesso».

---

<sup>[9]</sup> In materia, L. Picotti, Legislazione penale, 96, p. 122, in *Crespi-Stella-Zuccal *, Commentario breve al Codice Penale, CEDAM, 2003, p. 2047.

<sup>[10]</sup> Secondo la Suprema Corte, il legislatore, con la previsione di questa norma, «ha assicurato la protezione del domicilio informatico quale spazio ideale (ma anche fisico) in cui sono contenuti i dati informatici, di pertinenza della sfera individuale, quale bene costituzionalmente protetto», e poi ha precisato che «la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che il titolare dello jus escludendi sia persona fisica, sia che sia persona giuridica, privata o pubblica, o altro ente»: cfr. Cass. Pen., Sez. VI, 04.10.1999, n. 3067, con note di S. Aterno, Sull'accesso abusivo a un sistema informatico o telematico, e di L. Cuomo, La tutela penale del domicilio informatico, in *Juris data*, Cass. Pen. 2000, p. 2990A e 2990B, Giuffr  ed., DvD 2005.

Esse, difatti, sono state considerate dal legislatore alla stregua di «qualità personali riservate, in quanto identificatrici della persona»,<sup>[11]</sup> nella duplice considerazione che le misure di sicurezza costituiscano il presupposto irrinunciabile del nostro moderno operare per via telematica e, inoltre, che la condotta del cercare di varcare abusivamente la soglia di protezione d'un sistema informatico o telematico – possedendone indebitamente le chiavi, appunto – sia fonte di pericolo da reprimere nella misura più drastica, quindi in via anticipata.

Viene punito, perciò, colui che si procuri in modo illecito le credenziali di autenticazione e d'accreditamento atte a rendere inefficaci quelle misure di sicurezza, rischiando di pregiudicare con ciò stesso integrità, riservatezza e disponibilità dei dati. Peraltro, tale contegno detentivo (serbato acquisendo chiavi d'accesso, codici e *login* tramite un'e-mail di *spoofing* o un sito «mascherato») si rivelerà quale prodromo di altro delitto, quello punito dall'art. 615-ter C.P., relativo all'accesso al sistema da parte di persone non autorizzate.<sup>[12]</sup>

4. Sfruttato l'artificio dell'e-mail ingannatoria o il raggiro del messaggio *pop-up*, misteriosamente attivatosi all'atto dell'accesso al sito «vero», così da indurre in errore in ambedue i casi l'utente sino a determinarne la connessione ad un sito «mascherato» o ad una suggestiva casella di posta elettronica, e procuratesi in tal modo abusivo le chiavi d'accesso al sistema, il *phisher* giunge ad arrecare pregiudizio economico al titolare delle credenziali di autenticazione comunicategli, portando a compimento l'inganno.

La fattispecie, al di là dell'innovazione insita nel mezzo tecnologico adoperato, è quella della **truffa**, delitto commesso mediante frode, con la quale viene aggredito il patrimonio, alla cui tutela l'ordinamento ha apprestato l'**art. 640 C.P.**

L'elemento oggettivo è perfettamente integrato dalla condotta del reo, che fa credere alla persona offesa d'essere «chi non è» (la banca di fiducia, piuttosto che la nota società di *e-commerce*), allo scopo d'ottenere un ingiusto profitto con altrui danno (l'illegittimo esborso che il raggirato sempre subisce, qualunque sia il tipo di *phishing* attuato), di modo che la vittima viene indotta in errore, comunicando i propri dati (poiché crede d'interloquire con soggetto autorizzato) mentre gli consegna «le chiavi di casa», senza prevedere che questi si accinge a svaligiargliela.<sup>[13]</sup>

---

<sup>[11]</sup> Sul punto: *Pica*, Diritto penale delle tecnologie informatiche, UTET, 1999, p. 80 e ss.

<sup>[12]</sup> Addirittura, nel caso della frode consumata a danno di alcune società di *e-commerce* (come *ebay*), il *phisher* si intromise nella procedura di compravendita dei beni, facendo sì che il pagamento venisse accreditato a lui, anziché all'ignaro venditore.

<sup>[13]</sup> Risale al 10 agosto 2005 l'inoltro agli internauti dell'ennesima e-mail di *spoofing*, che stavolta (al di là dei soliti errori grammaticali cui, prima o dopo, gli *scammer* stranieri impareranno a porre rimedio!) è volta ad attuare un'aggressione ai clienti *Banco Posta*, con un *link* a un fantomatico sito riprodotto colori, font e composizione del sito delle *Poste Italiane*, contenente un *form* che richiede di digitare *nome utente* e *password* «per accedere al servizio *Banco Posta online*». Ecco il testo della missiva:

«Caro ... @....it, Recentemente abbiamo notato uno o più tentativi di entrare al vostro conto di *BancoPostaonline* da un IP indirizzo differente.

L'atto di disposizione patrimoniale da parte dell'ingannato (anche nei casi in cui l'intervento del *phisher* ha riguardato le sole procedure di *home banking*) è effetto dell'errore in cui è stato indotto e è, nel contempo, 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:<sup>[14]</sup> ciò senza dubbio realizza la condotta e l'evento propri della truffa commessa dall'*hacker*.

5. La configurazione del reato di **frode informatica** presenta invece qualche aspetto critico. *Prima facie* difatti sembrerebbe che l'agire del *phisher* sia riconducibile ad una frode abilmente compiuta con mezzi informatici, anche in considerazione dei beni giuridici tutelati da tale norma, costituiti – e qui v'è affinità con la truffa ex art. 640 C.P. – dal patrimonio del danneggiato, oltreché dall'interesse alla regolarità di funzionamento dei sistemi informatici ed alla riservatezza che ne deve accompagnare l'utilizzazione. Ma l'**Art. 640-ter C.P.** attiene in senso stretto ad un'altra condotta.

L'elemento oggettivo della speciale figura di raggio *de qua* richiede infatti la necessaria realizzazione di una delle due condotte alternative<sup>[15]</sup> prefigurate dalla norma, l'alterazione del funzionamento d'un sistema informatico oppure l'intervento su dati, informazioni o programmi contenuti nel sistema.<sup>[16]</sup>

Si tratta peraltro di un reato a forma libera, tanto che la norma punisce qualsivoglia l'intervento senza diritto e con qualsiasi modalità su dati, informazioni e programmi contenuti in un sistema informatico o telematico o ad esso pertinenti.

Ebbene, se è vero che nel caso di invio di mere *e-mail* ingannatorie, siffatto delitto non pare configurabile, ricorrendo altre situazioni la sussistenza di tale ulteriore fattispecie di reato ben difficilmente potrà escludersi: così, ad esempio, se l'*hacker* – oltre a limitarsi a sfruttare in modo illecito talune caratteristiche del codice *html* (tipico della struttura delle pagine web) ed alcuni *bug* dei *browser* (è noto, ad esempio, quello della falla di *Microsoft Internet Explorer*, che permetteva l'indicazione di *URL* fasulli nella «barra degli indirizzi» di versioni non

---

Se recentemente **accedeste** al vostro conto **mentre viaggiate**, i tentativi insoliti di accedere a vostro Conto BancoPosta possono essere iniziati da voi. Tuttavia, visiti prego appena possibile BancoPostaonline per controllare le vostre informazioni di conto: <https://bancopostaonline.poste.it/bpol/bancoposta/formslogin.asp>.

Invece, superando le apparenze, ed a dispetto del rassicurante messaggio sottostante («BancoPostaonline è sicuro, l'accesso a BancoPostaonline avviene attraverso il protocollo HTTPs che garantisce la protezione delle informazioni scambiate tra il cliente e Poste Italiane criptandole in modo che nessuno possa intercettarle e comprenderle»), il link è diretto al sito truffaldino «<http://www.withwith.or.kr/zboard/icon/formslogin.php>», dal quale l'*hacker* è pronto a carpire ogni informazione riservata ed a cagionare il danno patrimoniale trasferendo altrove i fondi del cliente Banco Posta, il cui sito è stato illegalmente così clonato.

<sup>[14]</sup> Si veda: A. Fanelli, commento all'art. 640 C.P., in Lattanzi-Lupo, Codice Penale, Rassegna di giurisprudenza e di dottrina, Giuffrè, 2005, p. 157, il quale ritiene che: «nella truffa il possesso viene conseguito con l'atto di disposizione dello stesso soggetto passivo il cui consenso è viziato da artifici e raggiri posti in essere dall'agente».

<sup>[15]</sup> Secondo A. Manna, Artifici e raggiri *on line*: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici, in Dir. Inform., 2002, p. 961 «l'alternatività di tali condotte sarebbe solo apparente, poiché l'intervento senza diritto su dati, informazioni o programmi comporta già un'alterazione del funzionamento del sistema informatico o telematico, e dunque la prima previsione non è altro che un'inutile specificazione della seconda».

<sup>[16]</sup> Cfr. Trib. Torino, 30.09.2002, in Dir. Inform., 2003, p. 322.

aggiornate del *browser*<sup>[17]</sup>) – giunga o ad alterare il funzionamento del sistema informatico o telematico del c.d. sito *web spoofed*, determinando la contemporanea visualizzazione sullo schermo dell'utente (appena connessosi al sito «legittimo») delle finestre di *pop-up*, con messaggi fraudolenti verosimilmente attendibili); così, per altro verso, in quei casi in cui vengano utilizzati i cc.dd. programmi *key-logger*, per l'intrusione nei p.c. degli utenti e l'estrazione abusiva di dati e informazioni sulle operazioni compiute attraverso quei sistemi informatici.<sup>[18]</sup>

Corre l'obbligo di precisare inoltre che, come per la tradizionale figura della truffa, la prevalente dottrina accoglie anche per il reato di frode telematica la concezione «economico-patrimoniale del danno». Conseguentemente, si afferma che esso si consuma nel momento stesso in cui l'agente consegue la disponibilità concreta del bene, piuttosto che in quello (temporalmente anteriore) in cui si realizza l'evento informatico (ad es., l'ordine d'eseguire il bonifico di una somma di denaro sul conto corrente del *phisher*).<sup>[19]</sup> Inoltre, secondo la Cassazione «l'evento nella fattispecie della frode informatica consiste nel conseguimento da parte del soggetto attivo di un ingiusto profitto con altrui danno»: <sup>[20]</sup> 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.

6. Ci si può infine domandare se nel comportamento del *phisher* sia ravvisabile il delitto previsto dall'**art. 12 del D.L. n. 143/1991, convertito in L. n. 197/1991** (recante «Provvedimenti urgenti per limitare l'uso del contante e titoli al portatore nelle transazioni e prevenire l'utilizzo del sistema finanziario a scopo di riciclaggio»).

La citata disposizione di parte speciale – sulla cui peculiare specialità rispetto alla ricettazione di cui all'art. 648 C.P. si è ampiamente dibattuto, in dottrina ed in giurisprudenza – punisce aspramente (con la reclusione da uno a cinque anni e con una corposa multa) «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». Inoltre, è previsto anche che "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

---

<sup>[17]</sup> Si veda il link <http://www.microsoft.com/italy/athome/security/email/phishing.msp>.

<sup>[18]</sup> Al riguardo, è recente la notizia («Truffe a clienti di home banking: 9 denunce a Torino») apparsa sul web ([http://www.repubblica.it/news/ired/ultimora/rep\\_nazionale\\_n\\_1014435.html](http://www.repubblica.it/news/ired/ultimora/rep_nazionale_n_1014435.html)) d'una serrata indagine condotta dalla Polizia Postale di Torino, nel cui ambito sono stati contestati i reati di accesso abusivo e frode informatica.

<sup>[19]</sup> *Contra*, A. Manna, cit., per cui «in un caso del genere» (cioè nel caso in cui l'agente ottenga la disposizione «elettronica» di somme senza incassarle, ma soltanto provocandone l'accredito sul proprio conto corrente, il reato deve ritenersi già consumato, perché da tale momento le somme entrano nella disponibilità dell'agente, n.d.r) «il momento consumativo del reato si ha nel momento in cui la banca dà la disposizione per l'accreditamento e non quando la somma perviene sul conto del beneficiario, in quanto il primo dei due eventi è il vero e proprio risultato della condotta criminosa, mentre il secondo è determinato dallo svolgimento di una procedura automatica su cui l'agente non è più in grado di intervenire».

<sup>[20]</sup> Cfr. Cass. Pen., Sez V, 24.11.2003, n. 4576, in Giur. It., 2004, p. 2363; nel caso di specie, l'imputato aveva sottratto € 30.000,00 da un conto corrente, accedendovi tramite *internet* ed operando immediati bonifici in favore del proprio conto corrente.

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».

Come emerge dalla lettura della norma, nell'unica disposizione sono individuabili tre diverse fattispecie:

I) «l'utilizzo indebito» di carte di credito o di pagamento o di altro documento che consenta di prelevare del denaro in contanti ovvero permetta di acquisire beni o servizi;<sup>[21]</sup>

II) la falsificazione o l'alterazione di quegli stessi documenti;

III) il possesso, la cessione, l'acquisizione dei medesimi documenti laddove essi siano già stati alterati, falsificati o, comunque, risultino – genericamente – di «illecita provenienza».<sup>22</sup>

Per quanto può rilevare nell'ambito della presente disamina, va osservato come la condotta del *phisher* possa costituire violazione dell'art. 12 L. n. 197/1991, nel caso in cui – previamente riuscito ad impadronirsi per via telematica *ut supra* dei dati concernenti una carta di credito altrui – egli «utilizzi indebitamente» la carta di credito o di pagamento o un altro documento che consenta di prelevare del denaro in contanti ovvero permetta di acquisire beni o servizi (cioè la adoperi contro la volontà del legittimo titolare della medesima).

In riferimento quindi alla condotta dianzi menzionata sub I), dovrà concludersi che l'abusivo e clandestino prelievo, attuato dall'*hacker*, di denaro dal conto del titolare della carta, non potendo certo definirsi «utilizzo lecito» della stessa (giacché l'usurpazione dei dati *de quibus* è nient'affatto conforme alla volontà del titolare), comporta il perfezionarsi del delitto ex art. 12 L. cit.

Oggi giorno, del resto, si effettuano prenotazioni alberghiere mediante invio di fax riprodotte la carta di credito, cosicché nessuna obiezione può seriamente sollevarsi in ordine al fatto che l'indebito utilizzo per via telematica delle potenzialità dispositive economico/finanziarie della carta, insite nella «conoscenza e gestione» dei dati di siffatto strumento creditizio, costituisca tale reato.

---

<sup>[21]</sup> In tale ipotesi, la condotta ha ad oggetto solo carte di credito e gli altri equipollenti strumenti di pagamento, avendo previsto il legislatore un'ipotesi di specialità c.d. per specificazione, rispetto all'art. 648 C.P., norma di carattere generale (cfr. Cass., Sez. II, 30.01.1998, n. 30, imp. *Scandinaro*); peraltro, l'indebito utilizzo rileva penalmente qualunque sia la provenienza lecita o illecita della carta di credito e degli altri strumenti di pagamento o simili.

<sup>[22]</sup> Non occorre, cioè, la provenienza «da delitto», cosicché vi rientra anche la c.d. illiceità contrattuale, quale mero inadempimento d'una obbligazione, laddove il legittimo titolare di una carta di credito ne sia rimasto in possesso in violazione del contratto concluso con l'emittente e l'abbia poi ceduta al terzo senza essere legittimato a disporne (cfr. Cass., Sez. II, 08.08.1994, n. 8911, imp. *Marrero Mieres*); a conferma di ciò, si sono pronunciate anche le Sezioni Unite della S.C., secondo le quali con il reato di cui all'art. 12 L. cit. si sanziona la medesima condotta di ricettazione allorché essa concerna uno dei detti documenti proveniente da illecito civile, contrattuale o extracontrattuale, o amministrativo o anche penale se trattasi di violazione contravvenzionale, così venendo incriminati comportamenti in precedenza penalmente irrilevanti, diversamente tali condotte dovendosi perseguire ex art. 648 C.P. (Cass. SS.UU. 07.06.2001, n. 22902, imp. *Tiezzi*).

7. Un ragionamento a parte va abbozzato per quanto attiene alla trasgressione delle regole della *privacy*, *rectius* della normativa vigente in Italia a tutela della libera circolazione e della protezione dei dati personali, così come disciplinata dal D.L.vo n. 196/2004 e successive modificazioni: infatti, la violazione delle disposizioni sul consenso costituisce fattispecie di reato ai sensi dell'**art. 167 del Codice Privacy** – norma da considerarsi come «cardine» della tutela penale nel settore *privacy* – che punisce il **trattamento illecito di dati**. Dunque, posto:

- che il «consenso» è valido solo se è stato espresso liberamente, specificatamente, per un determinato trattamento, se è documentato per iscritto e se fa seguito all'informativa di cui all'art. 13 (e, inoltre, che se il trattamento riguarda dati sensibili, deve essere pure prestato per iscritto), e che l'apprensione dei codici di *home banking* e/o di quelli inerenti alla carta di credito avviene, col *phishing*, in difetto di valida autorizzazione al relativo trattamento, e

- che «dato personale» è qualunque informazione relativa a persona fisica, a persona giuridica, a ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione ivi compreso un numero di identificazione personale, talché anche *account* e *password* e gli altri estremi necessari per eseguire transazioni telematiche sono riservati al loro titolare e allo stesso riferibili in via esclusiva,

se ne trae la logica conseguenza che la condotta dell'eseguire un trattamento di dati personali in carenza di consenso (cioè in violazione dell'art. 23 *T.U. Privacy*), è espressamente prevista come delitto.

Tale comportamento, se tenuto con il dolo specifico di voler trarne profitto o di recare danno ad altri, costituisce infatti delitto e se dal trattamento derivi nocimento è punito con la reclusione da sei a diciotto mesi oppure se si proceda al trattamento mediante comunicazione o diffusione di dati personali (in tali casi: a prescindere dal fatto di causare un danno, poiché il reato diventa di pura condotta) si applica la pena della reclusione da sei a ventiquattro mesi, oltre in ogni caso alla sanzione accessoria della pubblicazione della sentenza (ex art. 172 *T.U. Privacy*).

Nel caso del *phishing*, la raccolta, l'acquisizione, l'utilizzo e la comunicazione dei dati personali usurpati all'utente rientrano nelle condotte di trattamento senza consenso dell'interessato e, in quanto finalizzate all'uso d'effettuare prelievi dai conti correnti con conseguente depauperamento patrimoniale del *deceptus*, paiono perseguibili penalmente, ex art. 167, comma primo, D.L.vo n. 196/2004.<sup>[23]</sup>

---

<sup>[23]</sup> Né può valere, a scriminare il trattamento di dati personali compiuto senza consenso dell'interessato, il semplicistico riferimento all'art. 5 D.L.vo n. 196/2004, che contempla l'uso «personale» (l'art. 5, comma terzo, D.L.vo cit. dispone che «Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione»). Altrimenti, ogni sanzione – civile, amministrativa o penale – comminata dal T.U. in argomento diverrebbe *sempre* inapplicabile, poiché ogni illecito potrebbe sempre venire inopinatamente ricondotto all'uso personale dei dati fattone dal reo. Del resto, ben diversa è la *ratio* della norma, che esenta l'uso personale (si pensi alla gestione della rubrica con gli indirizzi e i numeri telefonici degli amici o della fidanzata) dalla stringente normativa sulla riservatezza,

Casomai, una questione procedurale si pone a causa della clausola di riserva posta dalla norma *de qua*, che prevede che essa si applichi «salvo che il fatto non costituisca più grave reato»: pertanto, la tutela sanzionatoria apprestata in sede penale dal *Codice Privacy* finirà con l'essere del tutto residuale e, segnatamente, priva di valenza pratica ogniqualvolta il fatto-reato del trattamento illecito appartenga alla struttura di altra e più grave norma incriminatrice (ad esempio, si pensi al trattamento dei dati svolto senza consenso in conseguenza d'un accesso abusivo ex art. 615-ter C.P., norma che prevarrà sull'art. 167, comma primo, D.L.vo n. 196/2004).

8. Da ultimo, ma non per importanza, va posta nell'esatto rilievo l'eventuale responsabilità penale di coloro che si prestino all'operazione di "ripulitura" del denaro trafugato con le varie tecniche di *phishing*.

Tale attività sarà autonomamente incriminabile in forza dell'**art. 648-bis C.P.**, norma che punisce **il riciclaggio**, o dell'**art. 648-ter C.P.**, il delitto di **impiego di denaro, beni o utilità di provenienza illecita**, in tema di incriminazione dell'illecito utilizzo di proventi illeciti in attività economiche «oneste» (così come innovati con L. n. 55/90).

Come si evince dalle notizie trapelate dalle indagini in corso, v'è chi ha acconsentito, in cambio di percentuali variabili (fino al 20%, nei casi sinora emersi), da un lato, a far transitare sui propri conti correnti delle somme frutto delle altrui attività di *phishing*<sup>[24]</sup> e, dall'altro, ad effettuarne successivi trasferimenti fuori dal territorio nazionale, magari tramite innocenti agenzie di *money transfer*.

9. Aggiungasi, per completezza, che si può ipotizzare peraltro il concorso formale di reati fra alcune delle suddette norme incriminatrici, ove due o più delle stesse risultino applicabili alla fattispecie.

Ciò potrà accadere, ad esempio, tra l'art. 615-ter C.P. e l'art. 640-ter: infatti, si tratta di reati totalmente diversi, il secondo dei quali, che tutela interessi di natura strettamente economico-patrimoniale, postula necessariamente la manipolazione del sistema, mentre la norma che sanziona l'accesso abusivo, che tutela la lesione del bene della riservatezza informatica e telematica ed al diritto di «libertà domiciliare/informatica» di qualsiasi soggetto, non richiede necessariamente per la sua consumazione, detta manipolazione.

E così via, ben potendosi ipotizzare il concorso tra il falso nella creazione della posta

---

eccezion fatta per l'applicazione d'un minimo delle misure di sicurezza, quale ad esempio l'uso del *pin* sul telefonino (come stigmatizza il secondo periodo del cennato terzo comma: «Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31»).

<sup>[24]</sup> «Perfect way to earn extra money - Our company offers you money transfer manager job. You must have ability to work two hours a day and a credit card, you will be receiving money transfers to it. Your salary is 4% of transferred amount. We are glad to answer all your questions. email us at johnq@2d.com. We will be glad to cooperate with you. Best regards.»: questa una delle moltissime *e-mail* simili giunte allo scrivente ed avente ad oggetto: *un modo perfetto di guadagnare denaro extra*, relativa alle ben remunerate operazioni di trasferimento di denaro per via telematica.

elettronica ingannatoria ex art. 617-sexies C.P. e l'indebito utilizzo di carta di credito ex art. 12 L. n. 197/1991, etc.

**CONCLUDENDO, UNA PRECISAZIONE** - Il *phishing* si presenta come violazione di norme diverse, spesso in concorso tra loro, a seconda sia del tipo di condotta di falso utilizzata, sia dell'interesse che di volta in volta viene tutelato/violato (quello della società/istituto di credito, il cui sito sia stato utilizzato dagli *scammer* per attuare la frode, o quello del privato che ha subito nolente il «prelievo»).

Inoltre, tranne pochi casi sporadici, sembra si tratti sempre più di atti orditi da «organizzazioni criminali», come riportato dalle cronache di stampa e sul *web*,<sup>[25]</sup> con ovvie ripercussioni anche su aspetti procedurali molto singolari, inerenti al piano delle indagini preliminari, alle misure cautelari in concreto applicabili, alla procedibilità non meno che alla competenza per territorio.

Sta quindi emergendo, con sempre maggior prepotenza, una nuova forma di criminalità, adusa alle nuove tecnologie telematiche, che si sta rendendo responsabile di fatti di *cyber-riciclaggio* d'imponenti dimensioni.

Per smascherare tali attività di reimpiego di capitali illecitamente accumulati occorre che gli istituti di credito, *in primis*, oltre a dotarsi d'innovativi sistemi di contrasto alle più diffuse frodi contro l'*e-banking*,<sup>[26]</sup> prestino la loro più ampia collaborazione alle autorità investigative di controllo.

Le perniciose condotte di sistematico mendacio telematico e di frode, al di là dell'indubbia valenza criminosa delle singole condotte di *phishing*, altro infatti non sono che il presupposto del più grave fenomeno del reimpiego illecito dei proventi di attività criminose.

08 Settembre 2005

**Avv. Salvatore Frattalone**  
**Foro di Padova**

©Avv. S. Frattalone 2005

---

<sup>[25]</sup> Si consulti, fra gli altri, l'aggiornato sito <http://punto-informatico.it>, in cui v'è menzione di una maxioperazione della polizia spagnola, che proprio in questi giorni ha messo a segno 15 arresti e centinaia di perquisizioni con il sequestro di p.c., telefoni cellulari e supporti ottici, scoprendo oltre a tutto che gli *hacker* si erano organizzati al punto da assumere «lavoratori esterni», reclutati attraverso annunci/offerte di telelavoro, sui p.c. dei quali «collaboratori» erano stati installati dei *software* atti a permettere agli *scammer* d'usarli per l'invio di *spam* infetta, per l'inoltro di *e-mail* di *spoofing*.

Un cenno merita, altresì, un recentissimo fatto di cronaca, oggetto di altrettanti articoli di stampa di *Repubblica.it* e *Reuters.it* (apparsi il 04.08.05 su [http://www.repubblica.it/news/ired/ultimora/rep\\_nazionale\\_n\\_1052130.html](http://www.repubblica.it/news/ired/ultimora/rep_nazionale_n_1052130.html) e, rispettivamente, il 03.08.05 su <http://today.reuters.it/news/newsArticleSearch.aspx?storyID=109711+03-Aug-2005+RTRS&srch=phishing>), dai quali traspare che la maxi-frode informatica scoperta dagli abili investigatori delle Fiamme Gialle della Lombardia è stata perpetrata ai danni di 4 istituti di credito nazionali nonché di ben 400 cittadini italiani, di cui gli inquirenti sono riusciti a bloccare € 1,3 milioni indebitamente sottratti ai correntisti, abituati a gestire i propri conti bancari mediante servizi di *banking on line*: le accuse elevate dal P.M., nei riguardi di quasi una trentina di correi, sarebbero, nella fattispecie, quelle di riciclaggio e di frode informatica.

<sup>[26]</sup> Per evitare accessi non autorizzati ai conti *on line* dei clienti si stanno invero mettendo a punto taluni sistemi atti a garantire una duplice autenticazione, cliente<-->banca: non solo abbinamenti di codici riservati (*account* e *password*), ma sequenze di domande/risposte e/o d'immagini da visualizzare da parte del cliente (riposte sul server protetto del sito «legittimo»), affinché vi sia un riscontro previamente concordato *de visu* col cliente; sull'argomento, a mero titolo esemplificativo, vedasi il bollettino pubblicato il 15.07.05 sul n. 2348 di <http://www.punto-informatico.it>.