Il Phishing

Le massime

Il phishing è quell'attività illecita in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici ed malwere) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (user e password) di un utente, codici che, poi, utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancali o postali che vengono rapidamente svuotati.

La suddetta truffa presuppone, poi, anche un terzo "collaboratore", ed finacial manager, ossia colui che si presta a che le somme che l'hacker trafuga dal conto corrente nel quale è entrato abusivamente, vengano accreditate sul proprio conto corrente al fine poi di essere definitivamente trasferite all'estero con operazioni di money transfert.

Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.

Per alterazione, ai sensi dell'art. 640 ter c.p., deve intendersi ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul software. In altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato: il che consente di differenziare la frode informatica dai delitti di danneggiamento informatico (artt. 635 bis - ter - quater - quinquies c.p.) non solo perchè in quest'ultimi è assente ogni riferimento all'ingiusto profitto ma anche perchè l'elemento materiale dei suddetti reati è costituito dal mero danneggiamento dei sistemi

informatici o telematici e, quindi, da una condotta finalizzata ad impedire che il sistema funzioni o perchè il medesimo è reso inservibile (attraverso la distruzione o danneggiamento) o perchè se ne ostacola gravemente il funzionamento (cfr. sul punto, in particolare, l'art. 635 quater c.p.).

Il testo integrale

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

LA CORTE SUPREMA DI CASSAZIONE

SEZIONE SECONDA PENALE

Sentenza 13 marzo 2011, n. 9891

1. Con sentenza del 18/01/2010, la Corte di Appello di Lecce confermava, in punto di responsabilità, la sentenza del 14/03/2008 con la quale il Tribunale della medesima città aveva ritenuto D.L. P.M.C. responsabile del delitto di frode informatica aggravata "perchè, al fine di procurarsi un ingiusto profitto, introducendosi abusivamente nel sistema informatico delle Poste Italiane spa, contro la volontà tacita di chi ha diritto ad escluderlo, interveniva senza diritto sui dati informatici del conto corrente postale n. (OMISSIS) di C.V., utilizzando la postazione informatica avente indirizzo IP (OMISSIS) mediante inserimento dei codici di accesso personali della predetta C., e trasferiva fraudolentemente sul proprio conto corrente n (OMISSIS) mediante bonifico la somma di Euro 9.037,00; in tal modo cagionava alla persona offesa un danno patrimoniale di rilevante gravità. In (OMISSIS)".

2. Avverso la suddetta sentenza, l'imputato, a mezzo del proprio difensore, ha proposto ricorso per Cassazione deducendo i seguenti motivi:

1. Violazione dell'art. 640 ter c.p.: sostiene il ricorrente che il fatto addebitatogli (consistente nell'impiego abusivo dei dati personali di accesso) non è configurabile come frode informatica in presenza di un normale funzionamento del sistema ed in assenza di un'alterazione, atteso che "l'oggetto della contestazione non sono fatti di c.d. hackeraggio,

ma l'utilizzo di codici di accesso personali che non costituisce certamente l'alterazione del sistema necessaria alla sussistenza del reato contestato".

2. violazione dell'art. 192 c.p.p.: ad avviso del ricorrente la Corte non avrebbe congruamente motivato, sotto il profilo logico giuridico, in ordine alla sua responsabilità. Infatti, dalla mera presenza del denaro sul conto di esso ricorrente e dal fatto storico dell'avvenuta esecuzione del bonifico non potrebbe dedursi che esso ricorrente aveva commesso il reato contestatogli, atteso che non vi era alcuna prova che era stato lui ad inserire, tramite un computer nella sua disponibilità o connesso alla sua linea telefonica, i codici di accesso personali della parte offesa, non essendovi alcun collegamento fra la persona di esso ricorrente e la postazione informatica avente indirizzo IP (OMISSIS).

Ne la motivazione poteva dirsi soddisfacente nella parte in cui, per giustificare la suddetta carenza probatoria era ricorsa all'escamotage di ritenere la responsabilità di esso ricorrente come concorrente "eventualmente" con terze persone. La suddetta ipotesi, però, non solo era rimasta priva di alcun riscontro probatorio, ma doveva ritenersi anche effettuata in violazione dell'art. 521 c.p.p. non risultando che fosse stata mai contestata.

3. violazione dell'art. 61 c.p., n. 7: ad avviso del ricorrente, il mero fatto dell'avvenuta ricezione di un bonifico sul conto, non consentirebbe, in assenza di partecipazione ad altre condotte, di imputargli la circostanza aggravante, alla stregua della previsione di cui all'art. 59 c.p. in quanto non era stata provata la conoscenza, la previsione o la prevedibilità della menzionata aggravante. L'aggravante in questione, poi, non avrebbe potuto essere ritenuta perchè la medesima tutela esclusivamente la persona offesa dal reato e tale non poteva ritenersi la C. ma le Poste Italiane ossia il titolare del sistema informatico violato.

Infatti, nei confronti della C., parte danneggiata, la suddetta aggravante avrebbe potuto, al più, essere contestata in relazione al reato di cui all'art. 615 ter c.p. per il quale, però, esso ricorrente era stato prosciolto. Di conseguenza, l'insussistenza dell'aggravante, avrebbe dovuto indurre la Corte territoriale a dichiarare l'improcedibilità per mancanza di querela.

Motivi della decisione

3. Violazione dell'art. 640 ter c.p..

L'incontestato fatto materiale è quello esattamente indicato nel capo d'imputazione (cfr. supra in parte narrativa).

Il ricorrente sostiene che quel fatto non è configurabile come frode informatica (art. 640 ter c.p.) bensì, al più, come accesso abusivo ad un sistema informatico (art. 615 ter c.p.).

La doglianza è infondata.

Come questa Corte ha reiteratamente stabilito, il reato di frode informatica si differenzia dal reato di truffa perchè l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema: ex plurimis Cass. 44720/2009 Rv. 245696 - Cass. 3065/1999 riv 214942. Anche nel reato di frode informatica, quindi, l'ingiusto profitto costituisce elemento costitutivo.

E' evidente, pertanto, l'inconfigurabilità dell'ipotesi delittuosa di cui all'art. 615 ter c.p., atteso che il fatto contestato prevede un'attività fraudolenta finalizzata all'appropriazione di una somma di denaro e, quindi, a procurarsi un ingiusto profitto ossia l'elemento materiale del tutto assente nell'ipotesi criminosa di cui all'art. 615 ter c.p. che, non a caso, si trova inserito fra i delitti contro l'inviolabilità del domicilio. Va, peraltro, osservato che, nel fatto così come contestato, ben avrebbe potuto essere contestato - in concorso con l'art. 640 ter c.p. - anche il reato di cui all'art. 615 ter c.p. atteso che i suddetti reati hanno diversi presupposti giuridici e, quindi, ben possono concorrere (in terminis Cass. 2672/2003 riv 227816; Cass. 1727/2008 riv 242938): non a caso, secondo quanto riferito dallo stesso ricorrente (pag. 3 ricorso), il reato di accesso abusivo al sistema informatico fu contestato ma dichiarato improcedibile per mancanza di querela.

Il reato di cui all'art. 640 ter c.p., prevede, poi, due distinte condotte.

La prima, consiste nell'alterazione, in qualsiasi modo, del "funzionamento di un sistema informatico o telematico": in tale fattispecie vanno fatte rientrare tutte le ipotesi in cui viene alterato, in qualsiasi modo, il regolare svolgimento di un sistema informatico o telematico.

Per sistema informatico o telematico deve intendersi "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" Cass. 3067/1999 riv 214945.

Per alterazione deve intendersi ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul software. In altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato: il che consente di differenziare la frode informatica dai delitti di danneggiamento informatico (artt. 635 bis - ter - quater - quinquies c.p.) non solo perchè in quest'ultimi è assente ogni riferimento all'ingiusto profitto ma anche perchè l'elemento materiale dei suddetti reati è costituito dal mero danneggiamento dei sistemi informatici o telematici e, quindi, da una condotta finalizzata ad impedire che il sistema funzioni o perchè il medesimo è reso inservibile (attraverso la distruzione o danneggiamento) o perchè se ne ostacola gravemente il funzionamento (cfr. sul punto, in particolare, l'art. 635 quater c.p.).

La seconda condotta prevista dall'art. 640 ter c.p. è costituita dall'intervento "senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico (...)": si tratta di un reato a forma libera che, finalizzato pur sempre all'ottenimento di un ingiusto profitto con altrui danno, si concretizza in una illecita condotta intensiva ma non alterativa del sistema informatico o telematico.

Ora, applicando i suddetti principi al caso di specie, deve ritenersi che, correttamente è stato ritenuta la configurabilità del reato di cui all'art. 640 ter c.p., in quanto la condotta contestata è sussumibile nell'ipotesi "dell'intervento senza diritto su (...) informazioni (...) contenute in un sistema informatico" di cui alla seconda parte dell'art. 640 ter c.p., comma 1.

Infatti, anche l'abusivo utilizzo di codici informatici di terzi ("intervento senza diritto") - comunque ottenuti e dei quali si è entrati in possesso all'insaputa o contro la volontà del legittimo possessore ("con qualsiasi modalità") - è idoneo ad integrare la fattispecie di cui all'art. 640 ter c.p. ove quei codici siano utilizzati per intervenire senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico, al fine di procurare a sè od altri un ingiusto profitto.

Nella fattispecie in esame, l'utilizzazione della password - illecitamente ottenuta - per entrare nel sistema informatico di home banking del correntista (protetto da misure di sicurezza costituite, appunto, dai dati di accesso personali) e messo a sua disposizione dalle Poste Italiane, servì per stornare fondi dal conto corrente della C.: con il che si è verificata l'ipotesi di intervento (nella specie: ordine di bonifico dal conto corrente della C. a quello dell'imputato) senza diritto sui dati e/o informazioni (nella specie: sul saldo attivo del conto corrente) contenuti nel suddetto sistema informatico. Si può quindi concludere

per l'infondatezza della prima censura atteso che la fattispecie, così come contestata, rientra nell'ipotesi criminosa di cui all'art. 640 ter c.p..

4. Violazione dell'art. 192 c.p.p.: la tesi del ricorrente, in pratica, è la seguente: non vi è alcuna prova che sia stato lui a perpetrare la truffa informatica perchè, a ben vedere, si trattò di un caso di ed phiscing nel quale egli stesso rimase incolpevolmente coinvolto in quanto lo sconosciuto hacker avrebbe utilizzato il conto corrente di esso ricorrente a sua insaputa. Anche la suddetta censura è infondata alla stregua delle seguenti considerazioni.

Il phishing è quell'attività illecita in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici ed malwere) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (user e password) di un utente, codici che, poi, utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancali o postali che vengono rapidamente svuotati.

La suddetta truffa presuppone, poi, **anche un terzo "collaboratore", ed finacial manager, ossia colui che si presta a che le somme che l'hacker trafuga dal conto corrente nel quale è entrato abusivamente, vengano accreditate sul proprio conto corrente al fine poi di essere definitivamente trasferite all'estero con operazioni di money transfert. Orbene, la tesi del ricorrente è proprio questa**;

ossia che, a sua insaputa, il suo conto corrente fu utilizzato dall'ignoto hacker. da qui la doglianza secondo la quale la Corte lo avrebbe ritenuto responsabile sulla base di un insufficiente compendio probatorio. Sennonchè va replicato che la Corte territoriale si è fatta carico della suddetta censura e l'ha disattesa rilevando che se fosse stata vera la tesi prospettata dal ricorrente "il reale autore del prelievo abusivo ai danni della C. non avrebbe mai lasciato la somma illecitamente carpita a giacere per un lungo periodo (quasi sette giorni) sul conto di un soggetto ignaro correndo il rischio, serio e concreto, che quest'ultimo, in virtù della titolarità esclusiva del conto, la utilizzasse in qualsiasi forma. D'Altra parte appare difficile che a pochi giorni dall'apertura del conto da parte del D.L.P. M. altre persone siano state in grado di carpire allo stesso i dati personali necessari per potervi accedere on line".

Orbene, a fronte di tale motivazione, il ricorrente, in questa sede nulla ha, in pratica obiettato, limitandosi a ribadire la propria tesi. Sennonchè va replicato che il ricorrente, in modo surrettizio, tenta di introdurre, in modo inammissibile, in questa sede di legittimità, una nuova valutazione di quegli elementi fattuali già ampiamente presi in esame dalla

Corte di merito la quale, con motivazione accurata, logica, priva di aporie e del tutto coerente con gli indicati elementi probatori, ha puntualmente disatteso la tesi difensiva del prevenuto. Pertanto, non avendo il ricorrente evidenziato incongruità, carenze o contraddittorietà motivazionali, la censura, essendo incentrata tutta su una nuova rivalutazione di elementi fattuali e, quindi, mero merito, va dichiarata inammissibile. Del tutto irrilevante, infine, ai fini processuali, è l'ipotesi prospettata dalla Corte in ordine ad un eventuale concorso del ricorrente con altri soggetti rimasti sconosciuti: infatti, la suddetta ipotesi non sposta minimamente la posizione processuale del ricorrente nè è ipotizzabile la lamentata violazione dell'art. 521 c.p.p. (in terminis Cass. 24438/2005 riv 231855).

5. violazione dell'art. 61 c.p., n. 7: in ordine alla sussistenza della suddetta aggravante, la Corte, in fatto, ha motivato in modo ampio, congruo ed adeguato agli evidenziati elementi fattuali.

Il ricorrente ha sostenuto che: a) la Corte avrebbe violato l'art. 59 c.p.;

b) l'aggravante non avrebbe potuto essere ritenuta perchè la medesima tutela esclusivamente la persona offesa dal reato e tale non poteva ritenersi la C. ma le Poste Italiane ossia il titolare del sistema informatico violato.

In ordine alla censura sub a) va replicato che, secondo entrambi i giudici di merito, essendo il ricorrente responsabile dell'episodio di frode informatica contestatogli, egli, nel momento in cui si appropriava della somma di Euro 9.000,00 non poteva non sapere che arrecava alla vittima un danno di rilevante gravità essendo la suddetta somma, di per sè, di notevole importo: si tratta di una conclusione che, essendo coerente ed adeguata rispetto agli evidenziati elementi fattuali e logici, non si presta ad alcuna censura di legittimità.

In ordine alla censura sub b), va obiettato che parte offesa del reato di frode informatica, contrariamente a quanto ritenuto dal ricorrente, è proprio la C. sotto un duplice profilo: 1) perchè l'intrusione abusiva fu effettuata nel suo sistema informatico, ossia nel sistema informatico di home banking (protetto da misure di sicurezza costituite, appunto, dai dati di accesso personali) messo a sua disposizione dalle Poste Italiane; 2) perchè fu la C. che subì il danno dell'illegittimo prelievo.

6. In conclusione, l'impugnazione deve rigettarsi con conseguente condanna del ricorrente al pagamento delle spese processuali, nonchè alla rifusione delle spese a favore della costituita parte civile come da dispositivo.

P.Q.M.

Rigetta il ricorso e condanna il ricorrente al pagamento delle spese processuali nonchè alla rifusione delle spese sostenute nel grado dalla parte civile C.V. che liquida in complessivi Euro 3.000,00 oltre spese generali, I.v.a. e c.p.a..