G.U.P. TRIBUNALE MILANO
15 OTTOBRE 2007
ESTENSORE: **INTERLANDI**
IMPUTATO: **XXX**

Informatica • Phishing • Configurabilità dei delitti di: sostituzione di persona • Truffa • Utilizzo non autorizzato di carte di credito

La condotta di chi allo scopo di procurarsi vantaggio economico, invii sms inducendo i destinatari in errore sul mittente facendo credere che si tratti del gestore del servizio di carta di credito, al fine di ottenere dati riservati e poi utilizzare le carte di credito configura i delitti di sostituzione di persona, truffa ed indebito utilizzo di carte di credito.

SVOLGIMENTO DEL PROCESSO. — In data 14 febbraio 2007 è pervenuta richiesta di rinvio a giudizio nei confronti di XXX in ordine all'imputazione sopra enunciata.

All'udienza del 17 maggio 2007, dichiarata, la contumacia dell'imputato, è stato disposto rinvio su richiesta della difesa dell'imputato al fine di valutare l'ipotesi di definizione del procedimento con applicazione della pena.

All'udienza del 9 luglio 2007 producendo procura speciale il difensore di XXX, in assenza di un accordo con il pubblico ministero per il patteggiamento, ha chiesto la definizione del procedimento con rito abbreviato.

Il processo è stato rinviato per la discussione al 15 ottobre quando, comparso l'imputato e revocata la dichiarazione di contumacia, CartaSi s.p.a. si è costituita parte civile.

Il pubblico ministero ha concluso chiedendo la condanna dell'imputato per i reati a lui ascritti, unificati i fatti nel vincolo della continuazione, alla pena di tre anni e due mesi di reclusione e 700 euro di multa.

L'imputato ha poi reso dichiarazioni spontanee, dichiarandosi dispiaciuto e sostanzialmente ammettendo i fatti, affermando di avere trovato su Internet, su un blog che non ha peraltro indicato, le informazioni per realizzare quanto contestategli, da lui realizzato senza aiuto di terzi, che gli ha consentito di lucrare complessivamente, considerato quanto contestatogli anche in altro procedimento, circa 20.000 euro.

Sul sito della ZZZ s.r.L., acquistando un pacchetto di messaggi da inviare a terzi, aveva avuto modo di accedere ad un programma che consente di estrapolare numeri telefonici da siti Internet che raccolgono annunci privati di compravendita di beni (autoveicoli ed immobili), indicati dagli stessi privati che avevano inserito l'annuncio.

Inviato un Sms dal testo indicato nel capo d'imputazione *sub A*) ai telefoni cellulari così acquisiti, alla chiamata dei titolari di carte di credito allarmati dall'Sms ricevuto rispondeva non XXX personalmente, ma, sotto le apparenze di un numero telefonico al quale corrispondeva in realtà l'indirizzo elettronico del suo personal computer, una voce sintetica che forniva una risposta automatica e richiedeva i dati della carta di credito a colui che stava chiamando.

Proseguendo nelle conclusioni la parte civile associandosi alle richieste del pubblico ministero ha chiesto la condanna dell'imputato al risarcimento del danno morale nella misura di 10.000 euro, ed ha depositato conclusioni scritte e nota spese.

Il difensore dell'imputato ha depositato sentenza pronunciata dal g.i.p. presso il Tribunale di Varese il 29 marzo 2007 nei confronti dello stesso XXX ed ha chiesto l'assoluzione dell'imputato dai reati a lui ascritti ai

sensi del 2º comma dell'art. 530 c.p.p., ed in subordine condanna a pena minima, con circostanze attenuanti generiche, per il solo reato contestato sub E), ritenendo i fatti di cui al capo *A*) in esso assorbiti; in ulteriore subordine ha chiesto la condanna dell'imputato, con circostanze attenuanti generiche ed unificati i fatti nel vincolo della continuazione, a pena contenuta nel minimo.

Dopo le repliche del pubblico ministero e del difensore è stato pronunciato il dispositivo della presente sentenza.

MOTIVI DELLA DECISIONE. — I fatti, sostanzialmente ammessi dall'imputato al processo, sono stati ricostruiti grazie all'attività d'indagine del compartimento della polizia postale e delle comunicazioni di Milano e della polizia tributaria di Catania.

La tecnica utilizzata dall'imputato è quella del phishing (che suona come fishing, dall'inglese pescare), cioè dell'acquisizione dei dati di utenti di un servizio di carta di credito, i quali volontariamente rispondono ad una richiesta di dati, inviata a un grande numero di persone, contattate grazie all'acquisizione dei loro recapiti, nel caso di specie per mezzo di programmi informatici che estrapolano i numeri dei telefoni cellulari da siti che raccolgono inserzioni private.

Il meccanismo comporta l'utilizzo di plurimi mezzi fraudolenti: in primo luogo l'alterazione dell'identità di chi chiede di essere chiamato (fatto che costituisce un autonomo reato) fingendo di essere emissario di una società emittente carte di credito — nel caso di specie CartaSi, BNL, Consum Credito, Visa —, la falsa segnalazione di un allarme-esca che induca l'utente a rispondere al messaggio, e la predisposizione di un servizio automatico di risposta che sia simile a quello effettivamente corrispondente alla società di gestione delle carte di credito, ed induca l'interlocutore ad indicare i dati relativi alla propria carta di credito e al codice segreto, che verranno quindi utilizzati da chi ha predisposto la truffa.

Dall'annotazione riassuntiva della polizia tributaria servizi di polizia giudiziaria aliquota web della guardia di finanza di Catania del 22 giugno 2006, dalla comunicazione di notizia di reato del 31 agosto 2006 e dall'allegata annotazione del 29 agosto, si evince che erano state iniziate indagini a seguito della denuncia sporta da Tizio Gaetano il 6 febbraio 2006: questi aveva riferito di avere ricevuto un Sms, apparentemente proveniente da CartaSi, che lo invitava a chiamare un numero per verificare una transazione con la sua carta di credito. Alla telefonata di Tizio Gaetano aveva risposto una voce automatica che gli aveva richiesto i dati relativi alla carta di credito, che Tizio Gaetano non aveva fornito. Informatosi presso i servizi interbancari CartaSi, aveva poi appreso che il numero indicato sull'Sms non corrispondeva ai servizi interbancari, e che la società di gestione delle carte di credito aveva ricevuto analoghe segnalazioni da altri clienti.

La conseguente analisi da parte della guardia di finanza di Catania dei dati relativi al traffico telefonico del denunciante e quindi del numero da cui era partito il messaggio a lui diretto aveva consentito di verificare che il messaggio, identico, era stato spedito a ventuno diversi numeri, grazie ad un pacchetto di Sms acquistati dalla ZZZ s.r.l.

Il messaggio appariva come spedito dal mittente CartaSi con il testo: « Attenzione: chiami il numero 02 40707505 di servizi interbancari per

verificare la transazione con la sua carta di credito, al fine di evitarne usi fraudolenti ».

In realtà il numero indicato nel corpo del messaggio, che l'interlocutore era invitato a chiamare, non corrisponde ai servizi interbancari ma costituisce una numerazione VOIP intestato a « eia lee », cui corrisponde l'indicato indirizzo e-mail « manager@thevoicemedia.com », e l'indicazione dell'utenza fissa 02 67086XXX intestata a Digital Broadcast BPM, di cui è legale rappresentante AAA Gabriele.

L'utente che aveva il messaggio, presso la ZZZ s.r.l. ove era stato acquistato il pacchetto, risultava però avere un nominativo diverso, BBB Veronica, risultato inesistente così come il codice fiscale indicato. Anche alla ZZZ s.r.l. l'indirizzo di posta elettronica indicato era « manager@thevoice.media.com »; tuttavia questo indirizzo e-mail era stato creato negli Stati uniti e non costituiva un utile filone di indagine.

AAA Gabriele sentito a sommarie informazioni il 18 dicembre 2006 ha dichiarato di non conoscere XXX, ne sono emersi ulteriori elementi nella presente indagine che lo coinvolgano.

Appare quindi evidente che chi spediva gli Sms si nascondeva dietro identità altrui o fittizie.

Contemporaneamente alle indagini svolte dall'autorità giudiziaria di Catania, altre indagini venivano svolte dall'autorità giudiziaria di Milano (cfr. comunicazione di notizia di reato della polizia postale e delle comunicazioni per la Lombardia del 14 aprile 2006), su denuncia sporta da CartaSi in persona del responsabile dell'ufficio investigazioni e sicurezza Andrea Fontanella il 1º febbraio 2006, a seguito di segnalazioni da parte di utenti del servizio CartaSi del gennaio 2006.

Anche in questi casi il numero che i destinatari degli Sms erano invitati a contattare era lo 02 40707505, al quale rispondeva una voce automatica che chiedeva al titolare della carta di credito di digitare il numero, la data di scadenza e il codice segreto, comunicando poi che gli operatori del servizio interbancario erano occupati e avrebbero richiamato; cosa che naturalmente non accadeva. Ne il numero corrispondeva a CartaSi, e nemmeno risultava registrato negli elenchi telefonici pubblici.

Dalla denuncia emerge anche che Cartasì fornisce un servizio denominato.: « Sms alert », che consenta al cliente il quale fornisce il proprio numero di telefono cellulare di ricevere un messaggio per ogni spesa effettuata con la carta di credito; tuttavia non tutti i clienti contattati dagli Sms fraudolenti avevano aderito al servizio Sms alert, ed anzi alcuni non erano titolari di CartaSi ed alcuni non erano titolari di alcuna carta di credito.

L'8 e il 23 marzo 2006 CartaSi integrava la denuncia a seguito di ulteriori segnalazioni da parte di clienti di Sms che invitavano a chiamare i diversi numeri 02 40707XXX, 02 40707XXX, 02 39198XXX.

Nella denuncia dell'8 marzo 2006 si specifica che CartaSi aveva verificato che in alcuni casi i dati delle carte di credito comunicati nelle telefonate effettuate a seguito della ricezione dell'Sms fraudolento erano stati utilizzati per acquisti.

Le indagini hanno consentito di accertare che anche gli ultimi tre numeri corrispondono ad un servizio VOIP, e sono state registrate a nome di A. Sandro, B. Alessandra, C. Rocco, con i rispettivi indirizzi e-mail e, in un caso, di nuovo al nome « manager@thevoicemedia.com », di dominio straniero.

Ulteriore integrazione di denuncia è stata presentata da CartaSi il 16 maggio 2006; in questo caso il numero indicato da contattare era lo 02 45073XXX, anche questo VOIP, registrato al nome già emerso di B Alessandra.

Il 23 febbraio 2006 anche QQQ Julien, amministratore unico di ZZZ s.r.L., società che offre servizi per l'invio di Sms presso cui era stato acquistato il pacchetto di Sms emerso nel Corso delle indagini di Catania, ha a sua volta sporto denuncia a seguito del disconoscimento da parte di un cliente di un acquisto di un altro pacchetto di Sms risultante a suo notte e addebitatogli. Anche in questo caso l'account di registrazione presso il venditore ZZZ corrispondeva non al nome del cliente della società ma al nome di A. Veronica

QQQ Julien si era insospettito anche perché alcuni degli Sms del pacchetto erano stati inviati a nome CartaSi (e non CartaSi come nel logo della società).

Dall'annotazione del 23 giugno 2006 della polizia postale emerge che l'acquisizione dei files di log comprensivi dei caller ID dei messaggi del pacchetto oggetto della denuncia di QQQ Julien ha consentito di accertare che le connessioni per la spedizione dei messaggi avvenivano attraverso l'utenza fissa intestata alla madre dell'attuale imputato 0332 237XXX, presso l'abitazione di XXX, fornendo però I.P vari e falsi.

Lo stesso nominativo, di XXX Giuseppe, corrisponde altresì al titolare dell'utenza cellulare 338 1639XXX alla quale era stato inviato uno degli Sms del medesimo pacchetto.

Nel frattempo l'acquisizione da parte dell'autorità giudiziaria di Catania dei dati relativi al traffico (della numerazione VOIP e di tutti gli Sms del pacchetto acquistato presso la Linkas comprensivo dei Sms inviati a Cormaci), nonché degli IP di registrazione per l'utenza 02 40707XXX, dei mittenti degli Sms presso la Linkas nonché di A Veronica che aveva tra l'altro inviato Sms con IP simili tra loro, hanno consentito di accertare che i primi messaggi del pacchetto, di prova del sistema di adescamento delle vittime, erano stati trasmessi tra l'altro ad una utenza cellulare (338 1639XXX) intestata a XXX, il quale era anche stato il primo a chiamare il numero VOIP 02 40707XXX.

Sempre a XXX, e precisamente alla linea Adsl intestata a XXX, sono risultati riconducibili gli. indirizzi IP utilizzati per la registrazione: al servizio Sms della ZZZ S.r.l., per la trasmissione del messaggio oggetto della denuncia sporta da Tizio Gaetano e per la registrazione del numero VOIP.

Le indagini svolte a Catania erano cioè giunte ai medesimi risultati delle indagini svolte a Milano, dove gli atti sono stati trasmessi.

È anche stato accertato che l'invio degli Sms non tramite cellulare ma tramite web era funzionale a consentire l'apparizione sullo schermo dei cellulari che ricevevano gli Sms, come mittente dei messaggi, non un numero telefonico ma una stringa di testo, appunto CartaSi, che ha indotto i destinatari a credere di ricevere il messaggio da parte della società di gestione delle carte di credito.

Risultando XXX già indagato per lo stesso tipo di reato dall'autorità giudiziaria di Varese, è stata disposta perquisizione domiciliare.

Al momento della perquisizione effettuata il 30 giugno 2006 l'indagato insieme a alla madre, ha atteso circa quindici minuti prima di aprire la porta dell'abitazione, affermando di non avere sentito il campanello benché un cane continuasse ad abbaiare, e la madre ha cercato di apprendere

e gettare via i fogli sui quali erano stati annotati circa quindici numeri di carte di credito, rinvenuti nella tasca di un giubbotto nella stanza da letto dell'attuale imputato, dagli operanti posti in salotto e poi rinvenuti tra altra spazzatura sul balcone.

Nel corso della perquisizione è stato tra l'altro rinvenuto un telefono cellulare sul quale erano memorizzati anche numeri di telefono emersi nel corso della pregressa analisi del traffico telefonico che ha condotto a XXX; sono state inoltre sequestrate numerose fotocopie di assegni esteri.

L'analisi della documentazione sequestrata presso l'abitazione di XXX ha fatto emergere che diverse carte di credito erano state bloccate dai rispettivi titolari ma senza segnalare quanto qui accertato al servizio antifrode della società di gestione; altre erano invece state denunciate in questo contesto e sono emersi tentativi di utilizzazione successivi al blocco, e ciò dimostra dello scopo dell'attività criminosa; talvolta anche quando gli utenti non avevano comunicato di avere ricevuto Sms truffaldini: la circostanza è emersa dalle successive indagini interne di CartaSi.

Anche l'analisi della memoria del personal computer di XXX ha confermato la fondatezza dell'ipotesi accusatoria: è stato rinvenuto il software che consente di effettuare telefonate Voice over: IP, la registrazione di tali telefonate e il collegamento ad un risponditore automatico che attraverso passaggi successivi presenta il servizio a nome della centrale di allarme dei servizi interbancari ed invita l'ascoltatore a tenere presso di sé la carta, di credito, attribuendo un codice: di chiamata, invitando poi a digitare il numero della carta di credito, la sua scadenza e il cvv, rimandando alle fasi precedenti o interrompendo la chiamata se non vengono comunicati i dati via via richiesti, ed infine invitando l'ascoltatore a rimanere in linea per essere collegato con un operatore che peraltro non viene contattato, in quanto il risponditore comunica che gli operatori non sono disponibili, suggerendo di chiamare di nuovo.

Nel personal computer era installato anche un programma per la verifica delle numerazioni delle carte di credito.

Decine sono i numeri di carte di credito rinvenuti nella memoria del personal computer di XXX e ivi inseriti a partire dal 30 gennaio 2006.

Parecchi di questi sono stati oggetto di denuncia da parte di CartaSi, e quattro sono stati rinvenuti anche annotati su foglietti scritti a mano sequestrati in occasione, della perquisizione.

In occasione della perquisizione sono peraltro stati rinvenuti segnati su foglietti anche numerosi numeri memorizzati nel computer ma non denunciati da CartaSi.

È stato accertato, prendendo in considerazione solo cinque dei numeri che i destinatari degli Sms erano invitati a chiamare, che XXX ha inviato oltre 870 Sms, sotto il falso nome CartaSi e anche a nome Visa. L'analisi dei dati relativi alle carte di credito i cui numeri sono stati rinvenuti nella memoria del computer dell'imputato ha confermato che gli stessi sono stati utilizzati per acquisti (per circa 800 euro complessivamente) e tentativi di acquisti.

W. Mario e E. Stefano, i cui numeri di telefono sono stati memorizzati nel personal computer di XXX hanno confermato di essere stati destinatari di un Sms apparentemente proveniente da CartaSi; XXX Mario, che aveva fornito i dati richiesti a differenza di E. Stefano si è visto poi addebitare spese su siti Internet, da lui non effettuate, per 600 euro circa, che aveva denunciato l'8 marzo 2006 alla questura di Milano.

Anche M. Cristina ha confermato di. avere telefonato al numero indicato su un Sms ricevuto, e che in seguito le erano state addebitate spese per pochi euro mensili.

C. Antonino ha confermato di avere subito il medesimo meccanismo truffaldino, e che il suo conto, in precedenza attivo per 116 euro, era poi risultato in rosso, per 92 euro.

Yahoo ha confermato che tramite l'indirizzo elaleo che era emerso nel corso dell'analisi del traffico telefonico che ha portato all'identificazione di XXX, sono stati effettuati numerosi acquisti presso siti italiani ed esteri, però non quantificati ne specificamente indicati,

Anche gli accertamenti effettuati sui dati emersi dall'analisi della memoria del personal computer sequestrato hanno confermato che non tutti coloro che avevano bloccato le proprie carte di credito, a seguito del meccanismo qui evidenziato, avevano denunciato il meccanismo truffaldino di cui erano state vittime.

L'imputato non ha reso nel corso delle indagini preliminari dichiarazioni sui fatti contestatigli.

Solo all'udienza di discussione del processo con rito abbreviato dopo le conclusioni del pubblico ministero, XXX ha infatti ammesso, attraverso dichiarazioni spontanee, sia di avere ottenuto i numeri di telefono cellulare di un ampio numero di persone estrapolandoli da siti che raccolgono annunci privati di compravendita, sia di avere inviato gli Sms a tali utenti, sia di avere predisposto un sistema automatico di risposta che si attivava alla chiamata di uni numero telefonico fittizio, corrispondente al suo indirizzo informatico su personal computer, ed apparentemente riconducibile a CartaSì.

Sono quindi provati tanto il reato di cui all'art. 494 c.p., avendo XXX con gli Sms, allo scopo di procurarsi un vantaggio economico, indotto in errore i destinatari degli Sms sostituendo illegittimamente il nome di CartaSi (e Visa) al proprio, quanto la truffa perpetrata attraverso tale meccanismo unitamente al servizio telefonico apparentemente riconducibile a Servizi interbancari con il quale induceva gli ascoltatori del messaggio vocale a fornire i dati delle carte di credito, che venivano poi utilizzati da XXX per effettuare e tentare di effettuare acquisti via Internet. Anche tale artificio è, come la sostituzione di persona, connessa teleologicamente all'utilizzo indebito delle carte di credito con relativo profitto ingiusto per XXX.

Il danno per i destinatari degli Sms corrisponde talora ai prelievi effettuati sui rispettivi conti correnti, talora alle spese/per quanto modeste, comunque sostenute per bloccare le carte di credito, per ottenere il rimborso dei prelievi illegittimi, è comunque gli accertamenti relativi e il rilascio di nuove carte di credito.

Analogamente è provato il reato di cui al capo *b*): è stato provato che in alcuni casi XXX ha utilizzato indebitamente le carte di credito di cui non era titolare, talora riuscendovi; ma per la prova del reato è sufficiente l'utilizzo indebito anche quando non pervenga al perfezionamento dell'acquisto e dell'impossessamento della merce o al godimento del servizio, ai sensi dell'art. 12 D.L. 143/91, e persino il solo possesso o l'acquisizione di carte di credito di provenienza illecita al fine di trarne profitto.

Certamente l'acquisizione dei numeri delle carte di credito con i codici segreti (dati la cui apprensione integra il reato a prescindere dal possesso del supporto magnetico relativo, consentendo l'utilizzo della carta come

mezzo di pagamento) è avvenuta mediante la pregressa sostituzione di persona sopra descritta, che integra l'illecita provenienza della carta, ben nota a XXX che ne è l'autore.

Lungi dall'essere assorbiti in quelli contestati al capo *B*), che non richiedono alcun artificio, i fatti-reato di cui al capo *A*) nella concreta attuazione del piano criminoso qui valutato concorrono con il reato di cui al capo *B*) integrando i rispettivi elementi costitutivi, posti in essere contestualmente nell'unica azione criminosa, da intendere come condotta finalizzata al perseguimento dello scopo illecito anche se costituita di una serie di azioni materiali succedentisi in un tempo ravvicinato e collegate funzionalmente.

XXX deve quindi essere dichiarato penalmente responsabile di tutti i reati contestatigli.

Il danno economico arrecato nel caso di specie ai titolari delle carte di credito ed alle società di gestione è modesto (complessivamente meno di 900 euro come si evince dall'annotazione della polizia postale del 14 marzo 2007 e dagli elementi sopra esposti).

Assai grave è invece il danno arrecato al bene protetto dalla norma incriminatrice della sicurezza nelle transazioni economiche, come elevata è la capacità a delinquere dimostrata dall'imputato, il quale ha sfruttato il servizio Sms alert fornito da CartaSi per carpire fraudolentemente dati relativi a carte di credito che poi ha in numerosi casi cercato di utilizzare, come risulta dall'incrocio dei dati memorizzati sul personal computer di XXX con i dati relativi alle carte di credito oggetto della denuncia sporta da CartaSi.

Ulteriore elemento d'inganno, strettamente collegato alla fiducia riposta dal titolare della carta di credito nella società di gestione, è stata la disponibilità da parte di XXX dei numeri di cellulare dei titolari della carte di credito, in quanto i numeri di telefono cellulari allo stato non sono pubblici per cui, salvo estrapolazioni abusive come nel caso di specie, i numeri sono noti solo a coloro ai quali vengano forniti direttamente dall'intestatario o su suo incarico.

Quanto al trattamento sanzionatorio si osserva inoltre quanto segue.

Il comportamento tenuto dall'imputato al momento della perquisizione è indicativo del tentativo di occultare le prove della attività illecita.

Le dichiarazioni ammissive rese dall'imputato sono inoltre tardive, e non hanno in alcun modo contribuito a ricostruire i fatti commessi.

Ne l'imputato ha risarcito il danno.

Nessun elemento consente quindi di considerare in suo favore circostanze attenuanti generiche.

Infine XXX è già stato giudicato dal Tribunale di Varese per un fatto analogo commesso tra il febbraio 2004 e l'ottobre 2005, per avere abusivamente utilizzato numerose carte di credito di cui si era procurato i codici segreti assumendo false generalità inducendo in errore altro soggetto presso il quale aveva effettuato acquisti pagando con le carte di credito di cui non era titolare.

La pena non può peraltro essere calcolata in continuazione, sulla pena inflitta dal Tribunale di Varese in quanto quella sentenza non risulta irrevocabile.

Del resto i fatti là contestati riguardano una diversa tecnica di acquisizione dei dati relativi alle carte di credito, allora tratti dai dati relativi ai clienti della società I A viaggi di Vattelapesca presso, cui XXX aveva lavorato.

Infatti dal verbale di sommarie informazioni rese da L. Paolo, amministratore delegato di A viaggi s.p.a., del 22 settembre 2006, si evince che i numeri di telefono oggetto della presente indagine non sono ricompresi tra i numeri presenti nell'archivio clienti di quella società.

Inoltre quei fatti sono cessati prima dell'inizio della condotta oggetto del presente procedimento, che è proseguita certamente fino a fine giugno 2006, quando è stata effettuata la perquisizione nell'abitazione dell'imputato, dove sono stati rinvenuti i codici di diverse carte di credito: annotati su fogli.

La pena viene calcolata come segue: partendo dalla pena base di tre anni di reclusione e 700 euro di multa per il più grave reato di cui al capo *B*), per le considerazioni di cui sopra, si aumenta la pena, per il concorso e la contestuale continuazione nel medesimo disegno criminoso prolungato per diversi mesi, con riferimento al reato di cui all'art. 494 c.p., di un mese di reclusione è di 100 euro di multa, e quindi per il reato di cui all'art. 640 c.p. di undici: mesi di reclusione e 700 euro, fino a quattro anni di reclusione e: 1.500 euro di multa.

La pena viene quindi ridotta per la scelta del rito abbreviato a due anni e otto mesi di reclusione e 1.000 euro di multa.

La condanna dell'imputato per i reati ascrittigli comporta la sua condanna al pagamento delle spese processuali.

L'imputato deve inoltre essere condannato al risarcimento in favore di CartaSi, costituitasi parte civile, del danno morale che si liquida in 10.000 euro come richiesto.

Quanto in sequestro, corpo del reato, può essere distrutto.

L'imputato viene infine condannato alla rifusione in favore della parte civile delle spese di costituzione e rappresentanza nel: presente procedimento, che si liquidano come da dispositivo.

USO NON AUTORIZZATO DI CARTE DI CREDITO E CONCORSO DI REATI NEL « PHISHING »

1. La recente sentenza che si annota offre lo spunto per una riflessione su un fenomeno ormai invalso di uso non autorizzato di carte di credito.

Si tratta del c.d. phishing, tecnica finalizzata ad ottenere dati riservati[1], attraverso l'utilizzo di sistemi di comunicazione od informatici.

La fattispecie concreta affrontata dalla sentenza in commento si profila articolata e complessa.

[1] Sull'etimologia del termine « phishing », Flor, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2007, 903 ss.: « Il phishing può essere definito come una tecnica di social engineering in quanto è una metodologia di comportamento sociale indirizzata a carpire informazioni personali, oppure abitudini e stili di vita. L'etimologia del termine ne indica un'origine dubbia, derivante dall'unione delle parole ''harvesting'' con ''password'', ovvero, ''password'' con ''fishing'' o, ancora, quest'ultima con ''phreaking'' ».

I titolari di carte di credito erano stati contattati dal phisher che si presentava loro quale rappresentante dell'Istituto di credito, gestore del servizio e segnalava il rischio che la loro carta potesse essere stata utilizzata senza la loro autorizzazione (c.d. « allarme-esca »); i fruitori legittimi, per consentire la palesata (ma non reale) necessità di verificare le operazioni eseguite, comunicavano il numero PIN della carta al phisher (celato sotto le mentite spoglie di soggetto appartenente alla società che gestisce il servizio di carta di credito); questi, ottenuto il dato riservato, accedeva al servizio e prelevava, in tal modo, contanti dai conti correnti collegati alle carte di credito, ovvero, ne disponeva, operando acquisti via internet, con conseguente proprio illecito profitto e danno del fruitore legittimo ed ingannato.

L'analisi dei numerosi passaggi del complesso meccanismo illecito induce a ritenere integrate una pluralità di fattispecie.

Tale il *modus operandi* descritto nella pronuncia in esame, infatti, il Tribunale ha ravvisato, nei fatti oggetto del giudizio, la sussistenza di un concorso di reati: il delitto di truffa, con riferimento alla fase di raccolta (o « pesca ») dei dati riservati attraverso l'induzione in errore del titolare e, successivamente, con l'utilizzo da parta del phisher delle informazioni così ottenute, il reato di indebita utilizzazione di carte di credito (fattispecie prevista dal D.Lgs. del 21 novembre 2007, n. 231 il cui art. 55 ha riprodotto nell'ordinamento la norma contenuta nell'art. 12, della Legge 5 luglio 1991, n. 197), nonché il reato di sostituzione di persona, in relazione all'invio del messaggio apparentemente proveniente dalla società emittente le carta di credito, attraverso il quale il titolare della carta è indotto a contattare il phisher, credendolo dipendente di tale società.

In particolare, l'individuazione delle norme che si assumono violate discende dall'esame degli strumenti utilizzati per indurre in errore il legittimo titolare della carta di credito: « Il meccanismo *del c.d. phishing* » — si legge nella sentenza — « comporta l'utilizzo di plurimi mezzi fraudolenti: in primo luogo l'alterazione dell'identità di chi chiede di essere chiamato (fatto che costituisce un autonomo reato) fingendo di essere emissario di una società emittente carte di credito — nel caso di specie CartaSì, BNL, Consum Credit, Visa —, la falsa segnalazione di un allarme-esca che induca l'utente a rispondere al messaggio, e la predisposizione di un servizio automatico di risposta che sia simile a quello effettivamente corrispondente alla società di gestione delle carte di credito, ed induca l'interlocutore ad indicare i dati relativi alla propria carta di credito e al codice segreto, che verranno quindi utilizzati da chi ha predisposto la truffa ».

Esaurita la ricostruzione del fatto alla luce di tali rilievi, il Tribunale ne definisce la cornice giuridica: « sono quindi provati tanto il reato di cui all'art. 494 c.p., avendo XXX con gli Sms, allo scopo di procurarsi un vantaggio economico, indotto in errore i destinatari degli Sms sostituendo illegittimamente il nome di CartaSì (e Visa) al proprio, quanto la truffa perpetrata attraverso tale meccanismo unitamente al servizio telefonico apparentemente riconducibile a Servizi Interbancari con il quale induceva gli ascoltatori del messaggio vocale a fornire i dati delle carte di credito, che venivano poi utilizzati da XXX per effettuare e tentare di effettuare acquisti via internet. Anche tale artificio è, come la sostituzione di persona, connesso teleologicamente all'utilizzo indebito delle carte di credito con relativo profitto ingiusto per XXX (…) Analogamente (…) è stato provato che in alcuni casi XXX ha utilizzato indebitamente le carte di cre-

dito di cui non era titolare, talora riuscendovi; ma per la prova del reato è sufficiente l'utilizzo indebito anche quando non pervenga al perfezionamento dell'acquisto e dell'impossessamento della merce o al godimento del servizio, ai sensi dell'art. 12 D.L. 143/91 e persino il solo possesso o l'acquisizione di carte di credito di provenienza illecita al fine di trarne profitto ».

2. Traendo alcune conclusioni dall'analisi sin qui condotta, si può rilevare che sono da condividersi le ragioni adottate dal Tribunale per inquadrare la sostituzione del phisher con il soggetto erogante il servizio di carta di credito nella fattispecie di reato descritta dall'art. 494 c.p.

Invero, il fatto costitutivo di tale delitto consiste nell'indurre taluno in errore, sostituendo la propria all'altrui persona, segue l'errore, ovvero l'affidamento mal riposto della vittima che, nel caso di specie, produce l'effetto di indurla a comunicare il numero della carta di credito.

Parimenti corretta l'argomentazione del Tribunale che ravvisa la sussistenza del reato previsto dall'art. 55, D.Lgs. n. 231 del 2007 nella utilizzazione non autorizzata della carta di credito da parte del phisher, dal momento che l'elemento oggettivo del delitto in esame è costituito proprio dall'uso indebito, in sé considerato, della carta (ed anche della sua alterazione/falsificazione)[2] e, dunque, prescinde dal conseguimento del profitto con altrui danno.

Resta da interrogarsi se la fattispecie prevista dall'art. 640 c.p. possa coesistere con i delitti configurati; in altri termini, se ogni elemento, integrante la truffa, sopravvive nella ricostruzione dei fatti contenuta nella sentenza.

Come è noto tale reato richiede che la vittima, a seguito dell'errore cagionato dagli artifici o dai raggiri realizzati dall'agente, ponga in essere un atto di disposizione patrimoniale per se dannoso.

Sul punto, autorevole dottrina[3] — attraverso un'espressione particolarmente eloquente — ha sottolineato tale peculiarità: « nella truffa … l'agente mediante artifici o raggiri, riesce ad ottenere che la vittima si danneggi da sé: consegni una cosa, assuma un'obbligazione, rinunzi ad un suo diritto, ecc., compia insomma un atto di disposizione pregiudizievole per il suo patrimonio e vantaggioso per altri ».

Orbene, il c.d. phishing (nella ricostruzione fattuale sottoposta al Tribunale) presuppone la cooperazione del soggetto passivo soltanto nella parte in cui questi, ingannato, rivela il numero della carta di credito necessario per accedere al servizio, ma, al contempo, tale meccanismo si discosta dal modello della truffa poiché il phisher, ottenuto, con l'inganno, il dato riservato, esegue direttamente l'operazione per ottenere il profitto personale[4].

---

[2] L'art. 55, D.Lgs. n. 231 del 2007 punisce « chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito … falsifica o altera carte di credito … possiede, cede o acquisisce tali carte … ».

[3] Antolisei, *Manuale di diritto penale - Parte speciale*, I vol., 1999, 348 ss.

[4] Sul punto Flor, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, cit. 916, ha acutamente osservato: « L'evento della disposizione patrimoniale costituisce dunque un limite all'applicazione della norma de quo nei casi di phishing attaks in cui non vi sia alcun atto, negoziale o meno,

Difetta, pertanto, nel caso che ci occupa, l'atto di disposizione patrimoniale da parte del titolare della carta di credito, requisito tacito, ma essenziale per la consumazione della truffa.

È proprio dal contrasto irrisolto tra fattispecie astratta (della truffa) ed il fenomeno (quello del phishing), che il ragionamento del Tribunale sembra essere viziato nel punto in cui configura il reato di truffa per ricondurre il fatto nell'ambito di applicazione delle fattispecie penali esistenti e dimostrare con ciò la capacità del nostro ordinamento penale di adattarsi a situazioni sempre nuove venutesi a creare con l'evoluzione tecnologica.

Occorre, infatti, sottolineare che quando il Tribunale riconosce l'integrazione della condotta del phisher nel delitto di truffa, esamina soltanto un aspetto della fattispecie astratta e, segnatamente, il ricorso, ad opera del phisher agli artifici od ai raggiri idonei ad indurre in errore la vittima (che ingannata comunica il dato riservato: PIN), senza affrontare l'analisi della figura di reato nella sua globalità e, dunque, trascurando di accertare la sussistenza dell'atto dispositivo ad opera del truffato che, come rilevato, deve verificarsi perché possa dirsi integrata la fattispecie in esame.

3. Alla luce delle riflessioni sin qui svolte, l'iter esecutivo del c.d. phishing non realizza la fattispecie prevista dall'art. 640 c.p. perché non ne sostanzia l'intera serie causale: all'attuazione del raggiro ed alla conseguente induzione in errore del titolare che comunica il dato riservato, segue, ad opera del solo phisher « ingannatore » e non del titolare ingannato, l'accesso abusivo al sistema bancario con le conseguenze in termini di contestuale ottenimento di profitto e produzione di danno.

Tuttavia, la questione merita di essere affrontata anche per un diverso profilo. Posto che non si condivida la conclusione esposta, ossia l'insussistenza del delitto di truffa, occorre verificare se questo può concorrere con il delitto di indebito utilizzo di carte di credito, oppure — per il principio di specialità — si possa determinare l'assorbimento, in questa fattispecie, del delitto di truffa.

La verificazione di tale ipotesi, passa inevitabilmente attraverso l'inquadramento sistematico della fattispecie prevista dall'art. 55, D.Lgs. n. 231 del 2007 e ha implicazioni pratiche di non scarso rilievo.

È stato osservato[5] che la fattispecie di indebita utilizzazione di carte di credito è reato plurioffensivo, nel quale i beni tutelati e, segnatamente,

---

commissivo o omissivo, realizzato dallo stesso soggetto ingannato, che provochi gli eventi di danno e di profitto. La condotta ingannatoria del phisher può essere la causa del compimento dell'atto di disposizione patrimoniale se il soggetto ingannato, ad esempio, rinuncia ad un credito o esegue direttamente un bonifico a favore del phisher. Al contrario tale effetto non si verifica, non realizzandosi quindi il citato requisito tacito ed essenziale della fattispecie, se il phisher, ottenuti i dati riservati tramite la falsa rappresentazione della realtà, accede egli stesso abusivamente al sistema bancario dell'istituto di credito, eseguendo direttamente operazioni bancarie e finanziarie, a favore suo o di altri ».

[5] In giurisprudenza v. Cass., Sez. V penale, 1 ottobre-17 novembre 1999, n. 13164, Melluccio, in *Guida al diritto*, 2000, n. 2, 177. L'assenza di un orientamento giurisprudenziale univoco ha indotto la dottrina ad interrogarsi sulla questione, cfr.: Blaiotta, *I reati commessi con le carte di pagamento nel sistema penale*, in *Crit. Dir.*, 1996, 198, Pecorella, *Il diritto*

l'interesse pubblico alla salvaguardia dell'integrità del sistema finanziario (con riferimento all'ipotesi di utilizzo indebito delle carte di credito) e la pubblica fede (con riferimento all'ipotesi di falsificazione o alterazione delle carte di credito) coesistono con la tutela del patrimonio del danneggiato, bene protetto già nella fattispecie prevista dall'art. 640 c.p.

In virtù di tale sovrapponibile oggettività giuridica, il reato di indebita utilizzazione delle carte di credito assorbe, dunque, quello delle truffa.

L'orientamento de quo — pur movendo dall'esigenza di limitare il ricorso ad un modello più generale, quale quello delineato nell'art. 640 c.p. — non sembra, però, meritevole di adesione.

Si consideri, in via preliminare, che, sebbene l'entrata in vigore del D.Lgs. n. 231 del 2007 non abbia modificato alcunché sul piano della struttura del reato, dal momento che l'art. 55 riproduce pedissequamente la norma contenuta nell'art. 12 della Legge n. 197 del 1991 (richiamata nella sentenza che si annota, emessa prima dell'entrata in vigore della nuova normativa), tuttavia non può sottacersi la scelta del legislatore in termini di collocazione sistematica.

Ed è proprio dall'aver inserito tale reato nell'ambito della normativa volta a salvaguardare l'integrità del sistema finanziario che si comprende come il patrimonio del soggetto passivo, soltanto in via mediata, sia il bene protetto dal reato di indebita utilizzazione delle carte di credito.

Orbene, traslando dall'analisi del bene giuridico tutelato, all'individuazione degli elementi costitutivi della fattispecie in esame, il reato previsto dall'art. 55 del D.Lgs. n. 231 del 2007 si distingue dalla figura comune della truffa dal momento che non sono richiesti gli artifici e i raggiri, né l'induzione in errore, essendo sufficiente una mera attività materiale di utilizzo non autorizzato della carta di credito.

È interessante a questo punto soffermarsi su un altro aspetto problematico che emerge dall'analisi della fattispecie: l'uso indebito, in sé considerato, delle carte di credito prescinde, pure, dal profitto e dal danno che possono derivarne; in altri termini, il momento consumativo del reato non richiede il conseguimento del profitto e del relativo danno, necessari per l'integrazione del delitto di truffa.

Per le evidenziate diversità, il reato di indebito utilizzo delle carte di credito (e di pagamento) rappresenta senza alcun dubbio un'autonoma figura di reato che si contrappone, senza assorbirla, alla fattispecie della truffa.

La distinzione attiene, dunque, al modo in cui l'agente è venuto in possesso della carta di credito: vi è truffa tutte le volte in cui il soggetto agente si sia procurato fraudolentemente, con artifici e raggiri, la disponibilità del bene oggetto della sua illecita condotta; mentre l'uso indebito della carta di credito (o di pagamento) si sostanzia nell'impossessamento unilaterale del bene in cui l'uso del mezzo fraudolento costituisce soltanto l'eventuale strumento, estraneo alla figura tipica, per agevolare la commissione del reato[6].

---

penale dell'informatica, CEDAM, 1996, p. 162, Borruso, *Gli aspetti legali della sicurezza nell'uso delle carte di credito e di pagamento*, in *Giust. civ.* 1992, 1223.

[6] Coerente con le argomentazioni esposte l'aver ravvisato nell'utilizzo di tessera Viacard smarrita dal titolare, la fattispecie prevista dall'art. 12, D.L. n. 143 del 1991, cfr. Cass., 9 aprile 1999, Sorgente, in *Guida al diritto*, 1999, n. 7, 108.

Le considerazioni formulate con riferimento al rapporto tra la truffa ed il reato di uso indebito delle carte di credito, sembrano essere valide anche nell'ipotesi di phishing attacks, in tutti i casi in cui — come quello che si annota — il titolare comunica il numero della carta di credito al phisher e la disposizione patrimoniale si realizza attraverso l'utilizzo indebito della carta ad opera del phisher stesso.

Se, alla luce di tali rilievi, l'interpretazione dell'art. 640 c.p., adottata dal Tribunale, ci può apparire non condivisibile, tuttavia riteniamo che la sentenza annotata vada segnalata per aver offerto l'occasione per sollevare le problematiche sottese alla qualificazione giuridica del c.d. phishing ed auspicare così l'intervento del legislatore rispetto a tali nuove situazioni venutesi a creare con l'evoluzione tecnologica.

Agnese Di Ronzo