ENRICO DI PAOLO

Cyber crime. Il *Phishing*: prospettive di un delitto

SOMMARIO: 1. Introduzione. – 2. Le responsabilità del *phisher*. – 3. Le responsabilità del *financial manager*. – 4. Conclusioni.

1. Introduzione

Accedere alla propria casella di posta elettronica e cestinare le *email* inviate nelle ore precedenti da una serie di seccatori o truffatori informatici ha, ormai per molti, assunto i contorni di un vero e proprio "rito mattutino".

Ciononostante, accade, sempre con maggior frequenza, che l'automatismo del gesto si interrompa e l'occhio venga catturato da una *email* in particolare, che parrebbe essere stata inviata da un istituto di credito, ovvero da enti impositori, società finanziarie, Poste Italiane[1]: è in questo istante che i meno accorti, o forse i più apprensivi, finiscono con l'assecondare il loro istinto, cadendo così nella rete del *phisher*, ossia un *hacker* che persegue l'intento di consumare illeciti bancari attraverso la rete.

Il *Phishing*[2] è una tecnica fraudolenta di *social engineering*,[3] volta ad adescare l'utente tramite il confezionamento di un messaggio quanto più credibile – perché somigliante a quello che potrebbe inviare il mittente ufficiale – e a carpire le informazioni personali del destinatario (quali *user id*, *password* di carte di credito, conti correnti, ecc.). In un secondo momento, irretito il destinatario e acquisite le sue credenziali, il *phisher* può liberamente accedere al conto corrente della vittima.

Eppure, manca ancora qualcosa perché l'*iter criminis* possa essere portato a compimento e il *phisher* godere degli effetti di un piano così ben congegnato. Il *phisher*, che generalmente risiede oltreconfine, non può eseguire bonifici dall'Italia verso l'estero senza un'ulteriore autorizzazione bancaria, necessitando di una collaborazione sul territorio. Entra così in gioco il *financial ma-*

[1] Il "Caso Poste Italiane e Banca Intesa", deciso con sentenza del Trib. Milano, Sez. G.I.P., 10 dicembre 2007, n. 888, Braditeanu ed altri, in *www.penalecontemporaneo.it*, confermata in Cassazione nel 2011, rappresenta la prima condanna pronunciata da un giudice italiano ad una associazione transnazionale dedita alla commissione di reati di *Phishing*.

[2] Il termine evoca l'immagine della pesca e parrebbe essere stato coniato attraverso la crasi di tre vocaboli inglesi: "*password*", "*harvesting*" e "*fishing*", associato al "*phreaking*" (*hacking* telefonico).

[3] Tale locuzione si riferisce allo studio del comportamento di una persona, finalizzato a catturare le informazioni necessarie per un successivo attacco vero e proprio.

nager.
Quest'ultimo è un prestaconto che consente al *phisher*, operante all'estero, di appropriarsi delle somme presenti nei conti correnti delle vittime che hanno 'abboccato' alla *email* 'esca', rivelando avventatamente le proprie credenziali.
Il *financial manager* può essere reclutato, a sua volta, con un inganno, ossia con una *email* nella quale si propone un'offerta di lavoro molto allettante, consistente nel mettere a disposizione il proprio conto corrente per ricevere somme di denaro, che dovranno poi essere girate verso un altro conto, tramite canali come *Western Union* o *Money Gram*. Ricevuto l'accredito da parte del *phisher*, che *medio tempore* si è introdotto nel conto della vittima avvalendosi dei codici d'accesso trafugati con le modalità sopra descritte, il prestaconto ha il compito – in ciò consisterebbe il suo "lavoro" – di prelevare la somma in contanti e, dopo aver detratto il suo compenso calcolato in percentuale, trasferire gli importi al *phisher*.
Una digressione, cursoria quanto essenziale, relativa alle modalità concrete con cui il "*Phishing attack"* può inverarsi, fornisce un abbrivio funzionale ad una successiva e più puntuale disamina circa i risvolti penali della fattispecie.
Il *Phishing* è un fenomeno ontologicamente in evoluzione, grazie alla sua caratteristica di giovarsi di uno sviluppo delle tecnologie sempre più teso a favorire una completa simbiosi digitale, a parziale detrimento della sicurezza e della *privacy*.
La più comune tecnica di attacco informatico è quella del "*deceptive phishing"* – ossia la condotta poc'anzi descritta – ove tramite una *email*, che si propone di riprodurre in maniera realistica il "*look and feel*" di siti e mittenti reali, si cerca di impressionare la vittima, che è indotta a cliccare su di un *link* che la reindirizza su di un sito in tutto e per tutto simile a quello ufficiale, ove le verrà richiesto, con un pretesto, di inserire i suoi codici bancari.
L'apprensione dei codici di accesso o dei dati sensibili di un individuo può avvenire in forma ancor più invasiva, attraverso l'installazione sul *computer* dell'utente di un *malware*, ossia un codice o un *software* maligno, naturalmente a sua insaputa. Il cybernauta poco avveduto si fa persuadere ad aprire un allegato oppure a scaricare un *file* da un sito *web*, al cui interno è celato un *malware* o un *trojan* capace di monitorare le attività dell'utente: la concreta captazione delle credenziali può avvenire anche mediante i c.d. "*keylogger*", traducibile in "registratore di tasti". La portata offensiva di un simile attacco è notevole, tanto da evocare le potenzialità[4] intrusive di quel "captatore infor-

[4] TESTAGUZZA, Exitus acta probat *"Trojan di Stato": La composizione di un conflitto*, in *questa Rivista* online, 2016, n. 2; ABBAGNALE, *In tema di captatore informatico*, in *questa Rivista*., 2016, n. 2.

matico" adoperato dalle procure per fini di indagine.
Un'ulteriore e più subdola modalità di aggressione è quella chiamata "*Man in the middle*", in cui il *phisher* si interpone tra l'utente ed il sito ufficiale – come uno spettatore invisibile ma operoso – e si avvantaggia della comunicazione tra l'utente ed il legittimo destinatario dell'informazione, intercettandone i messaggi ed usufruendo del relativo contenuto.
Meritano ancora di essere menzionati lo *Smshishing*, in cui l'approccio fraudolento avviene attraverso l'invio di *sms* o di applicazioni "malevoli" sugli *smartphone*, e il più sofisticato di tutti – almeno sinora – ossia il *Pharming*. Quest'ultimo consiste nella manipolazione degli indirizzi di DNS (*Domain Name Server*) che impiega l'utente. Senza voler risultare eccessivamente tecnici, il *phisher*, attraverso un *malware* o infettando direttamente i *router* casalinghi, aggredisce i *server* DNS, mutandone la corrispondenza numerica, di guisa che tali *server* decodifichino un indirizzo IP distinto dall'originale. Sicché l'ignaro utente, intenzionato a connettersi ad un determinato sito *web*, viene dirottato su di un altro sito che replica in tutto e per tutto quello ufficiale[5], ove, senza alcuna inibizione, riverserà le sue chiavi di accesso bancarie, di fatto depositandole nelle mani tese del *phisher*.
Dalla carrellata appena tratteggiata, che non vanta alcuna pretesa di esaustività, traspare come le diverse declinazioni del *Phishing* appaiano tutte accumunate da due caratteri generali: l'influenza sulla psicologia del destinatario e l'utilizzo dell'identità virtuale di un soggetto[6] al fine di trarne un profitto.
Si tratta, pertanto, di un'attività criminosa camaleontica e liquida, capace di suggere nuova linfa dal continuo progresso tecnologico e, ciò che è forse più significativo, suscettibile di attingere da un bacino di potenziali vittime pressoché illimitato. La *vis persuasiva* del messaggio, più o meno abilmente adornato, è in grado di colpire non solo l'utente seduto alla scrivania di casa, ma anche le imprese, gli istituti di credito, assicurazioni, financo enti pubblici. Anche in virtù di tali considerazioni, si è rivelato arduo il tentativo di collocare il *Phishing* all'interno di una astratta fattispecie di reato[7].

---

[5] CAJANI, COSTABILE, MAZZARACO, Phishing *e furto di identità digitale. Indagini informatiche e sicurezza bancaria*. Milano, 2008, 14 ss.; CAPUTO, Computer crimes*: frode informatica e* phishing, LUISS Guido Carli, A.A. 2014-2015, 64 ss.
[6] Siffatto concetto verrà parzialmente approfondito più avanti.
[7] VICENTINI, *La frode informatica nel quadro della disciplina nazionale e comparata. Prospettive* de iure condendo, Università degli studi di Trento, A.A. 2014-2015, 149 ss.; ARONICA, *Il "fishing" tra nuove esigenze di tutela ed acrobazie interpretative della giurisprudenza*, in *Riv. di giurispr. ed econ. d'azienda*, 4, 2008, 83 ss.; CAJANI, *Profili penali del* Phishing, in *Cass. pen., 2007*, 2294 ss; PERRI, *Lo* smishing *e il* vishing*, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. int., 3*, 2008, 265 ss.

Ad una platea tanto folta di prede si giustappone, sotto la lente della criminologia, una categoria di criminale non facilmente identificabile – se non solo per le capacità informatiche del soggetto attivo, ormai sempre più diffuse – favorita dall'usbergo della realtà virtuale, che accentua la mancata percezione del disvalore della condotta. In tal modo si finisce col rendere vani gli sforzi generalpreventivi delle norme penali, acuendo quell'incremento della criminalità che gli affanni del legislatore nazionale non sono in grado di mitigare, e che, almeno nella fattispecie oggetto di analisi, sarebbero certamente favoriti da una uniformità normativa a livello europeo e internazionale.
Del resto, a stimolare gli impulsi del *phisher* depongono un investimento criminale iniziale tutt'altro che ingente – se posto in raffronto con le prospettive di profitto – e la possibilità di aggredire il patrimonio di soggetti sparsi per il globo, restando sempre adagiati dietro la propria postazione PC. Ciò contribuisce ad attutire la percezione della natura delittuosa del proprio agire, con la conseguenza che si sono avvicinati al crimine soggetti prima avulsi dalla area dell'illegalità[8].
Delle potenzialità di guadagno insite nel *Phishing* si è presto avveduta anche la criminalità organizzata, che ha iniziato ad impiegarlo come strumento di finanziamento[9].
In tale cornice si innesta una iniziale difficoltà delle procure, tanto che, in buona parte dei casi, gli unici elementi che riescono ad essere acquisiti nel fascicolo processuale sono la querela della persona offesa ed i successivi rilievi investigativi utili ad identificare il solo *financial manager*[10].
L'Italia è stato uno dei primi Paesi europei a dotarsi di una legge organica in materia di illeciti informatici. Con la L. 23 dicembre 1993, n. 547, sedotto dall'eco dei primi "*computer crimes*", il legislatore introdusse una serie di nuove fattispecie criminose, disseminandole all'interno del codice e delle leggi speciali; a differenza di quanto avvenne nel *code penàl* francese, entrato in vigore il 1° marzo 1994, che reca un capo specifico sui reati informatici.
Affezionati al ricordo di tale primato, più volte celebrato nel testo e nei lavori preparatori della L. 18 marzo 2008, n. 48 – con cui l'Italia ha ratificato la Convenzione di Budapest sul *cyber crime* del 2001 – l'intervento sul crimine

[8] BATTAGLIA, *Criminalità informatica al tempo di internet: rapporti tra* phishing *e riciclaggio*, in *www.altalex.com*, 2014.
[9] Trib. Milano, Sez. G.I.P., 10 dicembre 2007, n. 888, Braditeanu ed altri, in *www.penalecontemporaneo.it*.
[10] PIANCASTELLI, *La ricezione di somme di denaro provento di* phishing*: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, in *www.dirittopenalecontemporaneo.it*, 2015; Direttive per la Polizia Giudiziaria del Distretto di Milano, *Sui primi accertamenti investigativi in materia di reati informatici* (in vigore dal 1 luglio 2011).

informatico in quella sede fu piuttosto modesto e poco preconizzante.
Tanto che già nel 2013[11] il Governo, proponendosi di far fronte proprio alle condotte di sottrazione di dati sensibili sulla rete *internet*, volte a conseguire un indebito profitto, aggiunse un'aggravante all'art. 640-*ter* c.p., rubricato «*Frode informatica*», nel terzo comma, a mente della quale «*La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*»: aggravante che incide sul delitto anche in punto di procedibilità ed i cui effetti, sul versante della sussunzione del *Phishing,* sono stati subito colti dalla giurisprudenza, con i risultati che ci si appresta ad analizzare.

2. Le responsabilità del *phisher*

È giunto il momento di inerpicarsi lungo l'irto sentiero della sussunzione, partendo dal *phisher*.
L'assenza di una disposizione *ad hoc* che sanzioni e definisca la pratica illecita del *Phishing*, ha indotto la dottrina prima e la giurisprudenza poi ad interrogarsi in merito, con il risultato che i "*Phishing attacks*" sono stati, di volta in volta, ricondotti nell'alveo di una vasta congerie di fattispecie di natura penale.
In tale prospettiva, si è pensato sin da subito di sezionare il fenomeno in più fasi, al fine di meglio discernere quali di queste abbiano autonoma rilevanza penale[12]: una scomposizione sicuramente utile in un momento di primo avvicinamento alla faccenda, che si presentava allora come adesso piuttosto spinosa, ma che, con il tempo, ha finito per acuirne gli angoli.
L'operazione del *Phishing* si snoderebbe in tre passaggi.
Dapprima il *phisher*, situato solitamente all'estero e difficilmente identificabile, ordito l'inganno, lo mette in pratica: invia le *email*, invitando il destinatario a cliccare su di un *link* o a rispondere con i propri codici di accesso, adducendo dei pretesti, quali ad esempio: motivi di sicurezza, un carico pendente, un asserito blocco del conto corrente, la comunicazione di una vincita, una offerta invitante per l'acquisto di un determinato prodotto.
Una volta che la vittima è caduta nella rete, la seconda fase consiste nell'assoldare il collaboratore esterno, cosicché il *phisher* potrà adoperare le chiavi di accesso bancarie per entrare nel conto corrente dell'individuo frodato e sottrarre somme di denaro, per poi accreditarle in favore del prestaconto

[11] Art. 9, co. 1, lettera a), della legge di conversione 15 ottobre 2013, n. 119, del d.l. 14 agosto 2013, n. 93.
[12] CAJANI, *Profili penali del* phishing, cit.; FLOR, Phishing*,* identity theft *e* identity abuse*. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. Pen.*, 2007, 899 ss.; Trib. Milano, 7 ottobre 2011, Sez. XI, P.G.E. ed altri, in *www.dirittopenalecontemporaneo.it.*

situato sul territorio.
Il terzo ed ultimo momento è quello in cui il *financial manager* – appellativo che suggerisce una certa dignità professionale – realizza lo scopo criminale del *phisher*, consentendogli di entrare in possesso degli importi trafugati dai risparmi della vittima.
Pregio primario di una simile schematizzazione è quello di lasciar emergere *ictu oculi* come ad essere immediatamente aggredito non è il patrimonio del soggetto passivo, bensì la sua "identità digitale", *lato sensu* intesa, ossia come quell'insieme di dati riservati che consentono di identificare uno specifico soggetto all'interno della rete.
I primi commentatori, nonché i primi giudici che sono stati chiamati a confrontarsi con la questione, hanno ritenuto anzitutto integrato il delitto di sostituzione di persona, di cui all'art. 494 c.p., che, secondo la giurisprudenza di legittimità, può venire in considerazione anche quando il fatto di reato viene perpetrato sulla rete[13].
Nonostante la tendenza giurisprudenziale ad un costante approdo sulle confortanti rive delle fattispecie più tradizionali, parte della dottrina ha avuto modo di evidenziare come vi sia un limite applicativo alla fattispecie *de qua*, ossia l'assenza di un mittente persona fisica e, quindi, l'impossibilità che si configuri una effettiva sostituzione materiale della propria all'altrui persona. Situazione, tale ultima, che si verificherebbe, per converso, ove una persona fisica sostituisse illegittimamente se stesso all'altrui persona oppure si attribuisse qualità personali non veritiere (si pensi alle piattaforme di "*social network*").
Non è mancato, tuttavia, chi ha aggirato il problema, sulla scorta di una lettura esegetica più attenta ai risultati dell'attività criminosa. É stato rilevato, in particolare, come l'evento consumativo del reato di sostituzione di persona sia a tutti gli effetti sussistente, giacché l'utente che riceve il messaggio di posta elettronica è, di fatto, tratto in inganno dal *phisher*, che sostituisce illegittimamente se stesso a qualcun altro.
Le perplessità permangono, specie ove si consideri che la condotta del *phisher* è finalisticamente proiettata non a frodare la vittima, ma ad ottenere un vantaggio patrimoniale attraverso l'uso delle sue credenziali, sul modello del

[13] Cass., Sez. V, 16 giugno 2014, Sarlo, in *Mass. Uff.*, n. 259303; Id., Sez. V, 08 novembre 2007, A.A.M., *ivi*, n. 238504; In tale ultimo arresto, la Suprema Corte ha precisato che la pubblica fede può essere messa a repentaglio anche attraverso inganni relativi alla vera essenza di una persona perpetrati sulla rete *internet*, in quanto le informazioni così diffuse sono in grado di raggiungere una pluralità di soggetti molto vasta, chiarendo come «*... nel caso in esame il soggetto indotto in errore non è tanto l'ente fornitore del servizio di posta elettronica, quanto piuttosto gli utenti della rete, i quali, ritenendo di interloquire con una determinata persona (la T.), in realtà inconsapevolmente si sono trovati ad avere a che fare con una persona diversa*».

furto aggravato dall'uso di un mezzo fraudolento.
Le false *email* e i falsi siti *web* sono stati interpretati *ab initio* anche quali artifici e raggiri propri della truffa *ex* art. 640 c.p[14]. Ad avvalorare tale ipotesi delittuosa vi sarebbero anche l'induzione in errore, la rivelazione da parte dell'utente delle proprie credenziali bancarie e l'ingiusto profitto con l'altrui danno[15].
Le prime pronunce, probabilmente anche a causa di una scarsa conoscenza informatica del fenomeno, ritenevano preferibile l'applicazione del reato di truffa, addirittura in concorso con la sostituzione di persona, piuttosto che del delitto di frode informatica, di cui all'art. 640-*ter* c.p., non rinvenendo nella condotta del *phisher* alcuna «*alterazione del funzionamento di un sistema informatico*» né un intervento «*senza diritto con qualsiasi modalità su dati informazioni o programmi contenuti in un sistema informatico o telematico*».
In tal modo, si finiva col punire l'invio di *email* ingannevoli o la creazione di false pagine *web*, sia a titolo di sostituzione di persona, sia come artifici e raggiri propri della truffa. Qualche giudice, avvedutosi della non opportunità di irrogare una duplice sanzione ad una medesima condotta materiale, ha optato per la contestazione della sola truffa[16]; sicché, il disvalore dell'adescamento rimarrebbe interamente assorbito negli artifici e raggiri con i quali l'internauta è stato indotto a cadere in errore[17].
La giurisprudenza recente, più sensibile alle modalità tecniche in cui si concretizzano gli attacchi di *Phishing*, ha compreso che spesso questi consistono in una vera e propria "alterazione" del funzionamento del sistema informatico, ad esempio tramite l'inoculazione sul PC o su uno *smartphone* di *trojan* o *malware*, nonché tramite un «*intervento non autorizzato su dati o informazioni*» dell'utente, nell'ipotesi di trasferimenti *home banking* di fondi[18].
Depone in tal senso la considerazione per cui ad essere assente nei "*Phishing attacks"* è l'atto di disposizione patrimoniale ad opera del soggetto passivo, requisito implicito ma indefettibile del delitto di cui all'art. 640 c.p[19]. In altri termini, nella truffa il soggetto è indotto, con artifici e raggiri, ad autodanneg-

[14] Trib. Milano, 7 ottobre 2011, Sez. XI, P.G.E. ed altri, in *www.dirittopenalecontemporaneo.it*.
[15] AMORE, STANCA, STARO, *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Massa Carrara, 2006, 73.
[16] Trib. Milano, Sez. G.I.P., 10 dicembre 2007, n. 888, Braditeanu ed altri, in *www.penalecontemporaneo.it*.
[17] Sebbene si tratti di fattispecie di reato che ben possono concorrere, attesa la diversità del bene giuridico tutelato. In tal senso, *ex multis*: Cass., Sez. VI, 10 dicembre 2009, L.M., in *red. Giuffré*, 2010; Id., Sez. II, 06 luglio 2007, Ferraloro, in *Cass. pen.*, 2008, 4189.
[18] Cass., Sez. II, 24 febbraio 2011, D.L.P.M.C., in *Mass. Uff.*, n. 249675.
[19] Cass., Sez. II, 04 maggio 2012, G.M., in *Mass. Uff.*, n. 252818.

giarsi; quella del *phisher*, differentemente, una volta ottenuti i dati di accesso, è un'aggressione unilaterale del reo al patrimonio della persona offesa. La contrapposizione è, allora, quella fra il concetto di "farsi dare" e quello di "prendere".

La frode informatica si rivela, al dunque, non più come una «*versione tecnologicamente avanzata della truffa*»[20] o una «*forma qualificata di truffa*»[21], come era stata sbrigativamente liquidata agli inizi della sua entrata in vigore, bensì come una figura di reato dotata di una autonoma dignità, la quale sanziona condotte che, in sua assenza, non sarebbero ricadute nel perimetro applicativo della truffa : ove così non fosse, l'intera fattispecie di cui all'art. 640-*ter* c.p. si rivelerebbe una sterile superfetazione.

L'intervento normativo del 2013 ha guarnito la frode informatica di una nuova aggravante indipendente, che sembrerebbe cucita su misura per la responsabilità del *phisher*[22].

Trattasi pur sempre di una frode informatica, ma la lesione alla riservatezza informatica e alla sicurezza della dimensione virtuale della propria identità, strumentali all'ingiusto profitto con l'altrui danno – difatti si legge «*se il fatto è commesso con*» – accrescono il disvalore penale della condotta in ottica offensività, rendendola meritevole di una sanzione più marcata.

Il legislatore, tuttavia, non si è profuso in una definizione universale di identità digitale, con tutti i pericoli che un'interpretazione eccessivamente lata della locuzione *de qua* potrebbe celare. Lo sforzo del legislatore è stato in ogni caso quello di conferire un sostrato di materialità all'identità personale in rete, intesa come le forme con cui taluno proietta se stesso nell'universo digitale[23]. Un'identità digitale che, così come quella reale ed interiore, è cangiante, mutevole, con confini sempre nuovi e mobili, suscettibile di essere scomposta in una serie di frammenti e capace, se ricomposta, di delineare, in una realtà virtuale, il profilo di una e una sola persona, dietro alla maschera del cyberspazio. Un processo di identificazione informatica[24] che riecheggia il relativismo pirandelliano[25], di talché «*Ciascuno di noi si crede uno ma non è vero: è*

---

[20] BORRUSO, BUONOMO, CORASANTI, D'AIETTI, *Profili penali dell'informatica*, Milano, 1994, 9.

[21] PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 141.

[22] Il terzo comma dell'art- 640-*ter* c.p. dispone che «*la pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*».

[23] MALGIERI, *La nuova fattispecie di "indebito utilizzo d'identità digitale", un problema interpretativo*, in *Dir. Pen. Cont.,* 2015, n. 2, 143 ss.

[24] GUARDA, P*er la difesa del crimine informatico serve un cambiamento culturale*, in *Resp. e risarc. (Sole24ore)*, 2008.

[25] La poetica di Pirandello presenta come motivo ricorrente la crisi di identità dell'uomo e l'empito,

tanti, signore, tanti, secondo tutte le possibilità d'essere che sono in noi: uno con questo, uno con quello diversissimi! E con l'illusione, intanto, d'esser sempre uno per tutti, e sempre quest'uno che ci crediamo, in ogni nostro atto. Non è vero!»[26].

Sarebbe allora il caso di affrancarsi, seppure solo per un istante, dalle strette paratie categoriali, per attardarsi in una indagine che abbia precipuo riguardo ai beni giuridici lesi dalla condotta del *phisher*.

Nulla di più complesso, perché la sensazione è quella di trovarsi in un terreno minato, dove il rischio di una violazione del *ne bis idem* sostanziale è palpabile. A renderlo tanto concreto è la molteplicità di fattispecie introdotte senza una visione organica, a tutela di beni giuridici disparati, in un'epoca di ipertrofia del diritto penale.

Senza troppo "astrologare", potrebbe tentarsi un approccio olistico, inteso a configurare la frode informatica, integrata ai sensi del terzo comma dell'art. 640-*ter* c.p., come un'autonoma fattispecie delittuosa. Di tal guisa, si avrebbe un'ipotesi di reato plurioffensiva, a presidio non solo del patrimonio economico dell'individuo, ma anche della sua identità digitale, proiezione di quella personale e che, nell'ipotesi del *Phishing*, consta delle credenziali di accesso ad un patrimonio materiale e finanziario. Eppure, anche tale soluzione non persuade, perché quella di cui al terzo comma dell'art. 640-*ter* c.p. appare proprio una circostanza aggravante indipendente: a definirla come tale ci pensa già il quarto comma della medesima norma, nella parte in cui statuisce la punibilità a querela della frode informatica «*salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante*».

Alla continua ricerca di un equilibrio tra le varie disposizioni normative, dal combinato disposto degli artt. 167 e 23[27] del codice della *privacy* risulta che sono puniti con la reclusione da sei a diciotto mesi quei privati o enti che, al fine di procurare per se o per altri un profitto o di recare ad altri un danno, procedano al trattamento dei dati personali senza il consenso dell'interessato, espresso liberamente e per iscritto per un trattamento chiaramente individuato, sempre che il fatto non costituisca un più grave reato. Tale ultima clausola di riserva, parrebbe escludere un concorso di reati – in particolare con la frode informatica – ogniqualvolta la violazione della norma si pone come un *modus procedendi* di un altro e più grave reato. La giurisprudenza, neanche a

---

vano e illusorio, di ciascuno di rintracciare la propria identità anche nello sguardo degli altri, al fine di conferire un senso alla propria esistenza.

[26] PIRANDELLO, *Sei personaggi in cerca di autore*, Milano, 2007.

[27] Per il vero, l'art. 167 richiama una gran quantità di disposizioni la cui violazione costituisce reato, di cui quella contenuta nell'art. 23 è solo la più generica e di più ampio respiro.

dirlo, richiede, per l'assorbimento della violazione nel reato più grave, la medesimezza del bene giuridico, con la conseguenza che sarebbe da escludersi nel caso di specie un'ipotesi di consunzione, dovendosi propendere, piuttosto, per un rapporto di specialità bilaterale.

E ancora, non può trascurarsi, anche in ragione dei più recenti sviluppi interpretativi[28], la possibilità che la condotta successiva alla indebita captazione dei dati possa assumere le fogge dell'indebito utilizzo di carte di credito o pagamento, allorquando l'agente dovesse porre in essere una delle condotte di cui all'art. 55, co. 9, D.Lgs. 21 novembre 2007, n. 231[29]. Siffatta fattispecie tutela l'interesse pubblico a che il sistema di pagamento venga utilizzato in modo corretto, a garanzia della fede pubblica e a prevenzione del riciclaggio. In effetti, già *prima facie*, sembrerebbe doversi escludere la configurabilità dell'ipotesi criminosa in questione, non essendovi alcuna carta di credito «*o altro documento analogo*» di cui il *phisher* si avvalga indebitamente, ovvero falsifichi o alteri. E difatti, parte della giurisprudenza di legittimità ha ritenuto che integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, «*il fatto di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua*»[30]. Nel *Phishing*, del resto, il soggetto attivo del reato non entra mai in possesso della carta di credito della vittima, limitandosi a carpirne a distanza le chiavi di accesso, tramite il ricorso a tecniche di hackeraggio.

La giurisprudenza unanime, sulla scia della "frode identitaria", continua a ritenere integrato anche il delitto di accesso abusivo al sistema informatico, di cui all'art. 615-*ter* c.p.; delitto posto a presidio del domicilio informatico, inteso come proiezione digitale del domicilio *ex* art. 14 Cost., sotto l'angolo visuale del titolare dello *ius excludendi alios*. Al di là delle problematiche concer-

[28] Cass., Sez. II, 14 febbraio 2017, P.C.V., in *D&G*, con nota di LAROTONDA, *Uso indebito di supporto magnetico clonato: l'illecito c'è... ma qual è?*, 8.

[29] Il nono comma dell'art. 55, d.lgs. 231 del 2007 punisce «*Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi*».

[30] Cass., Sez. II, 15 aprile 2011, F.M.I. ed altri, in *Mass. Uff.*, n. 250113; Id., Sez. II, 28 marzo 2012, P.V., *ivi*, n. 252797.

nenti, anche qui, la mancanza nel diritto positivo di una definizione di "domicilio informatico", considerata la diversità del bene giuridico tutelato dalle due norme (art. 615-*ter* e art. 640-*ter* c.p.), potrebbe ipotizzarsi un caso di concorso di reati[31].

E allora, laddove l'accesso abusivo riesca, ma la frode non venga perpetrata, per via di un impedimento esterno ad arginarla, potrebbe dirsi configurabile un concorso tra l'accesso abusivo ed il tentativo di frode informatica. Così come sarà configurabile il concorso nei casi in cui l'accesso vada a buon fine e, in virtù di esso, anche la frode informatica.

La circostanza che l'effettivo titolare dello spazio informatico non sia invero il correntista, bensì la banca – fautrice di un sistema informatico che ospita al suo interno una moltitudine di spazi riservati, di pertinenza esclusiva di diversi soggetti, comunque collocati in un'unica ed esclusiva struttura tecnica informatica[32] – non sembra aggiungere alcunché, anche in ordine alla corretta identificazione della persona offesa, poiché, di fatto, l'unico che può legittimamente far valere il suo diritto di opporsi a qualsivoglia ingerenza altrui è sempre e solo il correntista.

Potrebbe potenzialmente concretizzarsi financo l'ipotesi di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, prevista e disciplinata dall'art. 615-*quater* c.p. Da escludersi, invece, la configurabilità della fattispecie criminosa di cui all'art. 617-*sexies* c.p., rubricato «*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*», che punisce chi agisce sul contenuto «*anche occasionalmente intercettato*» di comunicazioni relative ad un sistema informatico ovvero intercorrenti tra più sistemi, avendo riguardo, dunque, ad una corrispondenza telematica, così come definita dall'art. 616 c.p., già intercorsa (fase statica) o intercorrente tra sistemi informatici. Diversamente, l'invio di una *email* con contenuti decettivi, che riproducono loghi e simboli di enti o istituzioni reali, si innerva nella fase dinamica di trasmissione, non configurando, di per sé, la fattispecie *ex* art. 617-*sexies* c.p[33]. Tale ultima ipotesi delittuosa potrebbe essere più validamente divisata nel caso, sopra cennato, del "*Man in the middle*", allorché il *phisher*, ad esempio, oltre ad avvalersi del contenuto del-

[31] Cass., Sez. VI, 14 dicembre 1999, P.N., in *Dir. inform.*, con nota di LUCENTE, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, 2011, 485.

[32] FLOR, *Frodi identitarie e diritto penale, un ampio contributo in tema di* phishing *e condotte correlate*, in *www.penale.it.*

[33] FLOR, *Frodi identitarie e diritto penale, un ampio contributo in tema di* phishing *e condotte correlate*, ult. cit.; sulla distinzione tra "fase di trasmissione" e "fase statica", PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, 292 ss.

le *email* intercettate, le sopprima o le falsifichi.
La circostanza per cui il *phisher* opera il più delle volte nell'ambito di un'organizzazione criminale, ha portato i giudici, almeno quelli che hanno avuto la possibilità di vagliare direttamente la responsabilità penale del *phisher*[34], a contestare anche il delitto di associazione a delinquere *ex* art. 416 c.p.
La giurisprudenza più recente pare ormai assestata nel sussumere la condotta del *phisher*, all'interno della latitudine applicativa della frode informatica, nella forma aggravata, e dell'accesso abusivo ad un sistema telematico ed informatico, nella forma semplice, avvinte dal vincolo della continuazione *ex* art. 81 c.p.[35].
La prima pertanto sarebbe procedibile *ex officio*, mentre l'accesso abusivo semplice necessita della querela. A tal proposito, è interessante segnalare come in almeno un caso[36] sia stata ritenuta sussistente l'aggravante di cui al terzo comma dell'art. 615-*ter* c.p., che rende il delitto procedibile d'ufficio, sulla scorta della considerazione che il sistema informatico di Poste Italiane S.p.a. sia da considerarsi un sistema di interesse pubblico, perché preposto alla gestione ed alla tutela del credito in ambito nazionale ed internazionale, alla stregua dei sistemi informatici degli istituti di credito.
La frode informatica si perfeziona, stando alla lettera dell'art. 640-*ter* c.p., allorquando il reo, mediante la condotta fraudolenta, procuri a sé o ad altri l'ingiusto profitto con altrui danno, secondo il tipico schema dei reati contro il patrimonio; mentre l'accesso abusivo è un reato di mera condotta e di pericolo, che si compie con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, a nulla rilevando che si verifichi o meno un'effettiva lesione della riservatezza degli utenti[37].
Quanto al *locus commissi delicti*, questo potrebbe finire col coincidere, sebbene solo in taluni casi, per entrambi i reati con il luogo in cui si trova il *phisher*. Ciò poiché l'accesso abusivo, com'è noto, si consuma nel luogo in cui si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente[38]; sull'altro versante, la frode informatica si consuma nel luogo in cui si è cristallizzato il conseguimento del profitto ingiusto, rispetto al quale si pongono in alternativa le strumentali condotte di alterazione del sistema informa-

[34] Trib. Milano, Sez. G.I.P., 10 dicembre 2007, n. 888, Braditeanu ed altri, in *www.penalecontemporaneo.it*.
[35] Cass., Sez. II, 09 febbraio 2017, P.C. ed altri, in *Guida dir.*, 2017, 49; Id., Sez. II, 04 novembre 2016, in *www.italgiure.giustizia.it*.
[36] Trib. Milano, Sez. VI, 28 maggio 2013, Trozzola, in *www.penalecontemporaneo.it*.
[37] Cass., Sez. V, 06 febbraio 2007, Cerbone, in *D&G* online, 2007.
[38] Cass., Sez. Un., 26 marzo 2015, Rocco ed altri, in *Mass. Uff.*, n. 263020.

tico e di intervento, o accesso, abusivi, «*senza diritto con qualsiasi modalità*»[39].
Quella appena prospettata è una soluzione che forse non è in grado di vestire compiutamente la condotta del *phisher* e di cogliere tutti i suoi possibili addentellati. Non è difficile intravedere dei lembi scoperti, di cui, uno dei più vistosi è certamente quello della tutela dell'identità digitale della vittima.
Le incertezze sono lontane dall'esaurirsi, perché porsi nella direzione di tale filone ermeneutico – e quindi ritenere il *phisher* sanzionabile *ex* artt. 615-*ter* e 640-*ter* c.p. – significherebbe escludere la responsabilità penale dell'intera fase di adescamento della vittima. Difatti, tale prima fase dell'agire del *phisher* non può dirsi ricompresa nel cono d'ombra della frode *ex* art. 640-*ter* c.p.
Entrando nuovamente nelle pieghe della frode informatica, essa, come già anticipato, consta di due condotte alternative: la prima si sostanzia nell'alterazione, in qualsiasi modo, del «*funzionamento di un sistema informatico o telematico*», che potrebbe essere ottenuta, ad esempio, inoculando nel PC o in uno *smartphone* un *malware* o un *trojan horse* – il sistema continua a funzionare ma in modo alterato da quello programmato – la seconda condotta è costituita dall'intervento «*senza diritto su ... informazioni ... contenute in un sistema informatico*», che si concretizza in un'illecita condotta intensiva ma non alterativa del sistema informatico, realizzata, nell'ipotesi in interesse, tramite operazioni di *home banking* o acquisti *on-line*[40].
Cionondimeno tale impostazione, che parrebbe quella più aderente alla fenomenologia del delitto in esame, non convince appieno. A ben voler guardare, anche laddove il *phisher* si innesti nel PC della vittima facendo uso di un *software* malevolo, per poi poter effettivamente dirottare i fondi dell'utente a suo vantaggio, ricorrerà in ogni caso ad operazioni di *home banking*: di guisa che le due condotte (quella di infettare il PC del frodato e quella trafugare i suoi conti) non appaiono alternative, come da molti sostenuto, bensì l'una prodromica all'altra.
Anche a voler prendere per buona la ricostruzione sopra prospettata, non si può fare a meno di considerare come la fattispecie di frode informatica non presuppone un'induzione in errore di un soggetto con artifici e raggiri, con la conseguenza per cui il disvalore dell'inganno con cui il *phisher* ha circuito l'internauta non può dirsi ricompreso nella frode informatica, la quale non richiede una cooperazione artificiosa del soggetto passivo. Con altre parole, nella frode informatica è assente il passaggio intermedio dell'induzione in er-

[39] Cass., Sez. I, 07 novembre 2014, Curca, in *www.frattallone.it*.
[40] Cass., Sez. II, 24 febbraio 2011, D.L.P.M.C., in *Mass. Uff.*, n. 249675; VICENTINI, *La frode informatica nel quadro della disciplina nazionale e comparata. Prospettive* de iure condendo, cit., 162 ss.

rore e degli artifici e raggiri. La dinamica dell'induzione in errore non ricorre nella frode *ex* art. 640-*ter* c.p. per la semplice ragione che la condotta dell'autore del reato è indirizzata direttamente ed esclusivamente al sistema informatico o telematico[41]. Differentemente, la condotta del *phisher* si rivolge in prima battuta alla vittima persona fisica, che è tratta in inganno: inganno che, stando alla sussunzione operata dalle interpretazioni più recenti, non sarebbe meritevole di rilievi penalistici e che, invece, potrebbe essere recuperato in chiave sanzionatoria andando a rispolverare il delitto di sostituzione di persona, di cui all'art. 494 c.p., pur con tutte le esitazioni espresse in merito.
Pertanto, e in definitiva, la lettura proposta dalla ultima giurisprudenza è forse meno ragionevole di quanto possa apparire ad un primo sguardo. Va rilevato che l'esercizio ermeneutico è tutt'altro che agevole per chi è chiamato a confrontarsi con un panorama normativo così frastagliato, perché solcato da interventi poco organici del legislatore ed in cui il pericolo è quello di conferire all'interprete una discrezionalità eccessiva, stante la specialità reciproca che connota le diverse disposizioni astrattamente configurabili.

3. Le responsabilità del *financial manager*

L'urgenza criminale di entrare materialmente in possesso delle somme depredate dai conti delle ignare vittime, specialmente per il *phisher* che opera dall'estero, si coniuga con quella di ripulire le tracce della *scena criminis* informatica e, soprattutto, quelle del denaro sottratto. Il contributo di un collaboratore indigeno è dunque essenziale.
La figura del *financial manager* assume una centralità insperata non solo nel complessivo dipanarsi degli avvenimenti, ma anche in sede processuale. L'esperienza delle procure distrettuali ha dimostrato, finora, come sovente le indagini prendano le mosse e si concludano proprio con l'identificazione del solo prestaconto, che, di fatto, altri non è se non un componente intermedio di una più sinuosa filiera criminale.
Si tratta, concisamente, di soggetti compiacenti che mettono a disposizione dei conti correnti, spesso accesi per l'occasione con carte prepagate ricaricabili, dei cui dati identificativi viene previamente reso edotto il *phisher*, il quale impingua il conto con trasferimenti *online* di somme provenienti dai conti delle vittime. Il *financial manager*, detrae una percentuale a titolo di corrispettivo e rigira il restante importo all'estero, tramite i canali di società di *money*

[41] Cass., Sez. VI, 14 dicembre 1999, F.D.V., in *Giur. it.*, 2001, 583; LOGROSCINO, *Analisi e considerazioni sul delitto di Frode informatica quale autonoma figura di reato rispetto al delitto di Truffa*, 2012, in *www.penale.it*.

transfer, quali *Western Union* e *Money Gram*, che consentono di interrompere la tracciabilità dei flussi monetari, portando a compimento il disegno criminoso del *phisher*.

Come è facilmente intuibile, il dibattito giurisprudenziale destatosi in questi ultimi tempi verte sulla possibilità di ascrivere in capo a tali soggetti una responsabilità a titolo di concorso nei reati perpetrati dal *phisher* ovvero una responsabilità per i delitti di ricettazione o riciclaggio.

La soluzione preferita dalla giurisprudenza, almeno sino a poco tempo fa, sembrava quella di valorizzare il dato gnoseologico del collaboratore. Il criterio discretivo veniva individuato nel *quantum* di conoscenza che il *financial manager* avrebbe potuto avere della sua funzione all'interno del piano criminoso orchestrato dal *phisher*.

Il confine è labile e scivoloso, in particolare sotto la lente dell'accertamento probatorio, anche perché il propendere per l'una o l'altra determinazione implica conseguenze non certo di poco momento dal punto di vista edittale della sanzione irrogabile.

In buona sostanza, solo laddove il prestaconto sia ben consapevole dell'attività truffaldina e assicuri comunque la propria collaborazione, sarà chiamato a rispondere dell'attività delittuosa a titolo di concorso nel reato presupposto: nella maggior parte dei casi «*in concorso con ignoti e previo accordo*»[42]. È qui richiesto che il *financial manager* abbia la piena contezza che è solo in virtù del proprio contributo se il *phisher* può entrare materialmente in possesso del maltolto, ripulendo nel contempo il denaro illecitamente sottratto dal suo collegamento con i delitti commessi.

Qualora, per converso, il collaboratore fosse all'oscuro dell'intero *modus operandi* e si prestasse comunque a mettere a disposizione un proprio conto corrente, o ad accenderne uno allo scopo, e poi a ritrasferire il denaro, nella generica consapevolezza dell'illiceità della operazione a monte, potrebbe configurarsi il delitto di ricettazione o al più di riciclaggio. Il primo è il caso di chi ha prestato il proprio consenso per accreditare le somme sui propri conti correnti, ma, pur consapevole della provenienza delittuosa del denaro, non l'abbia ritrasferito, o perché è stato impedito dall'intervento della p.g., oppure perché a sua volta ha "gabbato" il *phisher*. La seconda ipotesi è quella più sopra rappresentata, in cui il *financial manager*, rivolgendosi a società di *money transfer* impedisce o in ogni caso ostacola l'identificazione della prove-

[42] Trib. Milano, Sez. G.I.P., 10 aprile 2013, Ciavarella, in *www.penalecontemporaneo.it*; Trib. Milano, 7 ottobre 2011, Sez. XI, P.G.E. ed altri, in *www.dirittopenalecontemporaneo.it*; PIANCASTELLI, *La ricezione di somme di denaro provento di* phishing*: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, cit.

nienza delittuosa del denaro[43].
Questa pareva essere l'impostazione esegetica condivisa dalla giurisprudenza, almeno fino al 02 marzo scorso, giorno in cui sono state depositate le motivazioni della sentenza pronunciata il 02 febbraio 2017 dalla Sezione II della Suprema Corte[44]. In tale sede i giudici di legittimità parrebbero aver escluso la possibilità che il prestaconto possa rispondere a titolo di concorso nei delitti perpetrati dal *phisher*. Ciò sulla scorta della considerazione per cui il comportamento del collaboratore si colloca inevitabilmente in una fase successiva alla consumazione del delitto presupposto, essendosi la frode informatica ormai perfezionata e avendo esaurito le sue conseguenze. L'agire dell'imputato non potrebbe essere ricondotto a titolo concorsuale all'art. 640-*ter* c.p., avendo di fatto realizzato condotte «*volte ad ostacolare la provenienza delittuosa delle somme depositate nei conti correnti e successivamente utilizzate per prelievi in contanti, ricariche di carte di credito o ricariche telefoniche, realizzando in tal modo gli elementi costitutivi del delitto previsto dall'art. 648-bis c.p. ...*». In presenza di siffatti presupposti, dunque, il collaboratore non può che rispondere di riciclaggio, non potendosi configurare l'assorbimento di tale fattispecie nella sfera della precedente azione criminosa del *phisher*. Come a dire che il *Phishing* si è già perfezionato e quello del *financial manager* è un contegno che, per quanto essenziale, si trova ad essere successivo e autonomo.
Si tratta di una prospettiva gravida di perplessità, per vari motivi.
Uno di questi è certamente quello per cui nelle ipotesi – rare a dire il vero sino a questo momento, ma non così immaginifiche da potersi trascurare *a priori* – in cui il prestaconto fosse complice, magari addirittura *ab initio*, del *phisher*, non si vede come possa escludersi in via definitiva che la sua condotta possa atteggiarsi come un contributo, persino necessario, o al limite solo come un contributo a livello morale, che comunque possa aver rafforzato un proposito criminoso già esistente, o anche agevolato il *Phishing* nella fase esecutiva: in breve, una responsabilità a titolo di concorso, che, pertanto, escluderebbe in radice il riciclaggio.

---

[43] Cass., Sez. II, 21 novembre 2014, B., in *Mass. Uff.*, n. 263155, «*Integra di per sè un autonomo atto di riciclaggio qualsiasi prelievo o trasferimento di fondi successivo a precedenti versamenti, ed anche il mero trasferimento di denaro di provenienza delittuosa da un conto corrente bancario ad un altro diversamente intestato, ed acceso presso un differente istituto di credito, e ciò pur in presenza di una completa tracciabilità dei flussi finanziari, atteso che, stante la natura fungibile del bene, per il solo fatto dell'avvenuto deposito, il denaro viene automaticamente sostituito, essendo l'istituto di credito obbligato a restituire al depositante il mero* tantundem. *Infatti, in tale fattispecie delittuosa non è necessario che sia efficacemente impedita la tracciabilità del percorso dei beni, essendo sufficiente che essa sia anche solo ostacolata*».
[44] Cass., Sez. II, 02 marzo 2017, Prili, in *www.quotidianogiuridico.it*.

I giudici di legittimità hanno focalizzato l'attenzione sul compendio storico, ossia sulle concrete modalità con sui sono susseguiti i fatti, giungendo a conclusioni probabilmente troppo "tranchanti"; perché, se è vero che la condotta oggettiva del collaboratore si estrinseca in un intralcio alla individuazione della provenienza delittuosa dei beni, è altrettanto vero che il programma del *phisher* è ben lungi dall'essere portato a compimento e che il momento in cui il *financial manager* interviene è sì successivo, ma non sempre autonomo.
La Corte non si limita alla considerazione sopra prospettata, fa un'aggiunta, fugace ma rimarchevole, esprimendosi con i seguenti termini: «*peraltro, quand'anche si ritenesse (*omissis*) complice del delitto presupposto, questo andrebbe considerato proprio l'illecito ex art. 648-bis cod.pen. e non anche ex artt. 615 ter e 640 ter c.p., dal momento che il contegno di (*omissis*) si innesterebbe, quale prosecuzione, sulla già avvenuta frode informatica*».
Una valutazione di non immediata intelligibilità: si fatica, difatti, a comprendere se i giudici intendano significare che il riciclaggio sia da considerarsi quale delitto presupposto di se stesso e, in ogni caso, chi avrebbe commesso il delitto presupposto di cui il prestaconto si rende complice.
D'altro canto, l'attività dell'interprete nel caso di specie è resa ancor più gravosa dall'assenza di una norma che definisca e stigmatizzi il *Phishing* interamente considerato – il che non significa necessariamente che ve ne sia il bisogno – e dalla tendenza a modulare l'*iter criminis* in più fasi, che, se pure ha i suoi pregi, finisce con l'ostacolare una visione omogenea del fenomeno criminoso.
Potrebbe anche considerarsi l'ipotesi per cui, in caso di concorso con il reato presupposto, il prestaconto sia chiamato a rispondere di autoriciclaggio *ex* art. 648-*ter* 1 c.p., introdotto dalla L. 15 dicembre 2014, n. 186, del quale potrebbe rispondere in concorso anche il *phisher*, sebbene la giurisprudenza non sembra al momento propendere con decisione per una simile soluzione ermeneutica[45].
Anche ammesso che il *financial manager* sia perseguibile squisitamente a titolo di ricettazione o riciclaggio, ad essere controversa è, difatti, l'esatta determinazione dell'elemento psicologico che anima l'agire del soggetto attivo del reato. Tanto più che l'affermazione della responsabilità per il delitto di ricettazione non richiede l'accertamento giudiziale del delitto che ne costituisce il presupposto, né dei suoi autori, né dell'esatta tipologia del reato, potendo il

[45] Cass., Sez. II, 28 luglio 2016, Babuleac ed altri, in *Guida dir.*, 2016, 40, sul significato da attribuire alle espressioni «*attività economiche, finanziarie*».

giudice affermarne l'esistenza persino attraverso prove logiche[46] – anche se l'affermazione può suscitare non poche riserve, rischiando di risolversi in un'utilizzazione di meccanismi probatori sostanzialmente presuntivi.
Il dolo di ricettazione o riciclaggio può dirsi sussistente in capo al *financial manager* solo allorquando, in forza di precisi elementi di fatto, si possa affermare che questi si sia seriamente rappresentato l'eventualità della provenienza delittuosa del denaro e, nondimeno, si sia comunque determinato a riceverlo e, se del caso, trasferirlo all'estero con le modalità indicate dal *phisher*. In termini soggettivi, occorre qualcosa di più del mero sospetto della provenienza illecita del denaro: un atteggiamento della psiche inequivoco, un impulso cosciente della volontà che implica una scelta consapevole tra l'agire, rappresentandosi la concreta possibilità della provenienza della cosa da delitto, e il non agire. Collocandosi nel solco tracciato dalle Sezioni Unite nel 2009, per quanto attiene alla ricettazione, ma pacificamente ritenuto valido anche per il riciclaggio, deve escludersi il mero sospetto dalla latitudine del dolo eventuale. Il prestaconto verrà chiamato a rispondere del delitto contestatogli solo laddove vi sia la prova che non avrebbe agito diversamente se anche avesse avuto la certezza della provenienza illecita del denaro: dovrà, allora, essersi rappresentato l'eventualità della fonte criminosa delle somme accreditate in suo favore, con un atteggiamento psicologico che «*seppur non attingendo al livello della certezza, si colloca un gradino immediatamente più in alto del mero sospetto*»[47], e aver voluto agire lo stesso.
Trattasi di un accertamento che investe l'atteggiarsi della volontà dell'agente e che, anche solo per questo, corre su di un crinale probatorio piuttosto sottile.
È bene considerare che, sovente i collaboratori vengono reclutati con le stesse modalità con cui viene raggirata la vittima di *Phishing*, con la differenza che in tal caso viene sempre prospettato un tornaconto personale. Ora, se è pur vero che il sospetto dovrebbe sorgere spontaneo, la volontà di agire nonostante gli scrupoli e di vincere la propria diffidenza, accettando il rischio di ricevere e trasferire somme di provenienza illecita, deve in ogni caso essere oggetto di prova e, a tal fine, sono occorrenti elementi gravi ed univoci non sempre rintracciabili – nonostante non possa più parlarsi di un fenomeno che si affaccia per la prima volta sullo scenario italiano, facendo così perno sulla "dabbenaggine" degli imputati.
Precipitato logico dell'analisi sopra spiegata è l'ammissione di una "zona fran-

[46] Cass, Sez. II, 05 luglio 2011, Tartari, in *Mass. Uff.*, n. 251028.
[47] Cass., Sez. Un., 26 novembre 2009, Nocera, in *Mass. Uff.*, n. 246323; Id., Sez. II, 01 luglio 2011, O.F. ed altri, in *Guida dir.*, con nota di CISTERNA, 2011,76.

ca" a vantaggio degli intermediari nei cui confronti non si possa raggiungere la piena prova della sussistenza del c.d. "dolo di partecipazione" nell'attività illecita del *phisher* – almeno nella sua dimensione di dolo eventuale[48] – il che contribuisce ad alimentare quella sensazione di impunità che aleggia intorno al *Phishing*.

4. Conclusioni

È il caso di tirare le fila. Il *Phishing* è un fenomeno diffuso e in forte espansione, la cui carica offensiva non si esaurisce solo in un'aggressione verso il patrimonio altrui, bensì anche, ed *in primis*, in una violazione dell'identità digitale e del domicilio digitale di coloro che cadono vittime di un imbroglio, nascosto sì, ma assai "baluginante".

L'interprete è chiamato a destreggiarsi all'interno una normativa disorganica e dispersiva, trovandosi di fronte, tra l'altro, all'esigenza di riempire di contenuti una serie di beni giuridici, che si trovano ad essere particolarmente esposti perché sguarniti di una definizione al livello normativo: beni la cui tutela si rivela ancor più precaria, proprio perché lasciata inevitabilmente in balìa degli umori della giurisprudenza. A mancare sono, in particolare, le definizioni.

Il sentiero della sussunzione è, dunque, tortuoso e cosparso di spine, reso ancor meno agevole dalla necessità di dover costringere all'interno degli steccati delle norme penali una condotta, quella del *phisher*, che è ricca di possibili declinazioni ed in continua evoluzione, capace di assumere tante forme quanti sono i potenziali sviluppi della tecnologia.

L'esigenza di dover sanzionare un'aggressione così tentacolare ha colto di sorpresa la giurisprudenza che ancora, a svariati anni dalla manifestazione del fenomeno in Italia, non è stata in grado di fornire una risposta credibile in ottica sussuntiva.

In tal senso, come si è constatato, ritenere che il *phisher* risponda dei reati di accesso abusivo e di frode informatica, seppure nella forma aggravata perché commessa con furto di identità digitale, non sembra cogliere tutte le sfumature cromatiche del *Phishing*, nel suo concreto dispiegarsi. In tal modo, difatti, si finisce col lasciare sprovvisto di presidio penale il momento in cui il *phisher* si sostituisce ad un altro soggetto – di solito un ente pubblico – e raggira l'ignaro internauta, che viene indotto a rivelare le proprie chiavi di accesso

[48] SCIRE', *In tema di riciclaggio, dolo eventuale e frode informatica mediante 'Phishing', Nota a Cass. pen., Sez. II, 17.6.2011 (dep. 1.7.2011), n. 25960, Pres. Fiandanese, Est. Gallo*, in *www.penalecontemporaneo.it*, 2011.

bancarie, nonché, se del caso, si insinua nel PC della vittima tramite un *maleware* o un *trojan horse*. Si tralascia la componente umana del "*Phishing attack*", che, in principio, si invera in una costrizione psicologica probabilmente meritevole di stigma penale.
Sarebbe il caso di eludere gli automatismi e domandarsi, tornando così alle primissime battute della presente disamina – e quindi a quelle *email* che ormai tutti riceviamo anche più volte al giorno da finti indirizzi di posta elettronica, presuntivamente riconducibili ad enti impositori o ad istituti di credito ecc. – se e in che modo queste siano inquadrabili dal punto di vista giuridico e, per quel che ci compete, sotto il profilo penale.
Si è osservato che, ove il *phisher* acceda al conto corrente della persona offesa tramite sistemi *home banking*, senza però portare a compimento il suo intento, si realizzerebbe un tentativo di frode informatica. *Quid iuris*, tuttavia, in tutte quelle ipotesi in cui il *phisher* si limiti a carpire le *password* senza poi farne alcunché? Anche in tal caso si concretizzerà un tentativo di frode informatica? Il rischio è, evidentemente, quello di dilatare eccessivamente l'area del tentativo, attese le differenze, più sopra descritte, tra truffa e frode informatica, la quale è rivolta unicamente al sistema informatico e telematico, parrebbe potersi affermare financo nella forma aggravata di cui al terzo comma.
Di certo, se si vuole conferire una qualche rilevanza penale ai primi approcci del *phisher*, questi non potranno venire in considerazione come un tentativo di frode informatica e neppure come tentativo di truffa – giacché la truffa non può consumarsi – ma al più, sembrerebbe, come un tentativo di sostituzione di persona[49].
La direzione intrapresa dalla giurisprudenza, potrebbe, invece, condurre l'interprete a sanzionare le condotte sopra delineate come dei tentativi di frode informatica. Ciò significherebbe tornare a considerare la frode informatica quale *species* della truffa[50], trascurando le massicce differenze che segnano le due disposizioni, di cui la più immediatamente percepibile è l'assenza nella frode informatica dell'induzione in errore della vittima[51]. Una china pericolo-

[49] Sulla configurabilità della sostituzione di persona nella forma di tentativo, *ex multis*: Cass., Sez. V, 06 marzo 2009, Liberti, in *Mass. Uff.*, n. 242771, Id., Sez. V, 22 aprile 2010, Righi, in *Foro it.*, 2010, n. 2, 514.
[50] In tal senso, Cass., Sez. VI, 26 febbraio 2009, Giambertone, in *Mass. Uff.*, n. 243238, ove *expressis verbis* si sostiene che «*il reato di frode informatica altro non è che una ipotesi specifica di quella di truffa*»; e ancora, in Id., Sez. II, 30 aprile 2013, T.L., *ivi*, n. 255551, si parla espressamente di «*truffa informatica*».
[51] Non è un caso se non tutti gli ordinamenti hanno scelto di introdurre una fattispecie *ad hoc* per le frodi informatiche. In Francia, ad esempio, si continua a ritenere applicabile la disposizione tradizionale in materia di truffa.

sa, stante la palese volontà del legislatore di separare la frode informatica dall'alveo applicativo della truffa[52], foriera di una inevitabile collisione con il divieto di analogia *in malam partem*. Né, può intervenire, a scongiurare tale evenienza, l'aggravante di cui al terzo comma dell'art. 640-*ter* c.p., nonostante la novità del concetto di "furto di identità" (nella sua accezione di "identità digitale"), in quanto la stessa non fa che specificare le modalità che possono portare al perfezionamento del fatto tipico dell'«*ingiusto profitto con altrui danno*»[53].

Stando agli ultimi approdi giurisprudenziali, poi, il *financial manager*, sovente unico imputato nei processi penali che originano dal *Phishing*, finirebbe per essere perseguibile esclusivamente per il più grave delitto di riciclaggio. In buona sostanza, il *phisher* non solo non si espone, perché trincerato dietro allo schermo di un PC, situato per lo più all'estero, ma sacrifica agli organi requirenti un facile bersaglio di indagine: il prestaconto che opera sul territorio.

Siffatte difficoltà non possono che aggravare la percezione di immunità di cui si ammanta l'agire del *phisher*. Lo stesso potrebbe dirsi anche del *financial manager*, considerate le difficoltà in ordine al raggiungimento della prova del suo coinvolgimento psicologico, e quindi del *Phishing* nel suo insieme.

Le conseguenze sul crinale della generalprevenzione sono presto disvelate e, senza dubbio, necessitano di un incisivo sforzo collaborativo e armonizzante a livello internazionale; del resto, ormai la prevenzione o è internazionale o non può definirsi realmente prevenzione. A tal proposito, con l'entrata in vigore del Trattato di Lisbona, la "criminalità informatica" è stata inserita nell'art. 83 TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale. Trattasi di una previsione che ha già prodotto i primi risultati a livello europeo[54], dove è particolarmente sentita l'esigenza di una maggiore cooperazione internazionale tra le autorità giudiziarie e le forze di polizia *in subiecta materia*.

Al fine di tamponare le antinomie sopra riscontrate si potrebbe reclamare un

---

[52] Nella frode informatica l'attenzione si concentra sugli interventi e sulle alterazioni di un sistema informatico, indice di un'espressività criminale più elevata e di più semplice e diverso accertamento rispetto agli "artifici e raggiri" propri della truffa. ROMANI, LIAKOPOULOS, *La globalizzazione telematica*, 2009, 232.

[53] La disposizione, difatti, si esprime con un significativo «*se il fatto è commesso con*» e non con un «*se il fatto consiste in*».

[54] Segnatamente: la Direttiva 2011/93/UE del 13 dicembre 2011, che sostituisce la decisione quadro 2004/68/GAI del Consiglio, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e la Direttiva 2013/40/UE del 12 agosto 2013, che sostituisce la decisione quadro 2005/222/GAI del Consiglio, inerente agli attacchi contro i sistemi di informazione.

intervento sostanziale del nomopoieta nostrano in tema di *Phishing*, ma, considerati i recenti risultati, è un rischio che forse è meglio evitare: «*I would prefer not to*» direbbe Bartelby[55].

Nel maneggiare la materia, difatti, il legislatore – animato dal timore di lasciare senza tutela penale condotte complesse da esprimere in termini esaustivi – ha impropriamente ecceduto nella formulazione di talune fattispecie[56]. É stata seguita, in tale sede, una logica di "omnicomprensività", tesa a fronteggiare il continuo sviluppo delle tecnologie, in grado di rendere rapidamente obsolete le disposizioni che il legislatore medesimo si prefigurava di introdurre. Il risultato di siffatta preoccupazione è stato quello di dare vita ad un quadro d'insieme poco organico e definito, espressione di un grave *vulnus* alla prioritaria esigenza di tassatività.

In tal senso, il *Phishing,* come si ha avuto modo di appurare, è una realtà liquida, sfumata, proteiforme, troppo mutevole per mantenersi immobile come il diritto vorrebbe, per cui sarebbe probabilmente preferibile una soluzione sincretica, che prediliga come prospettiva angolare quella dei differenti beni giuridici da tutelare. Nel compiere una simile operazione di sussunzione, non può essere trascurata la tutela dell'integrità e della riservatezza dei dati e degli "spazi informatici", in modo da assicurare l'affidabilità dei rapporti giuridici che si stabiliscono nel cyberspazio[57]: interesse di fronte al quale altri diritti, pur meritevoli di tutela, non possono che cedere il passo – stando anche agli ultimi indirizzi della Corte di Giustizia[58] – e che può essere valorizzato

---

[55] MELVILLE, *Bartleby lo scrivano: una storia di Wall Street*, Milano, 2006.

[56] Il riferimento è, in particolare, alla frode informatica, ove il legislatore si è prodigato in una descrizione sovrabbondante del fatto tipico, con l'intento di ricomprendervi tutte le condotte latamente manipolative che possono colpire un elaboratore con fini di profitto. In tal senso, VICENTINI, *La frode informatica nel quadro della disciplina nazionale e comparata. Prospettive* de iure condendo, cit., 38; ROMANI, LIAKOPOULOS, *La globalizzazione telematica*, cit., 248.

[57] FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali e nuovi diritti fondamentali nell'era di internet*, in www.penalecontemporaneo.it, 2012.

[58] Corte di Giustizia, Grande Sezione, sent. 8 aprile 2014, *Digital Rights Ireland v. Seitlinger*, cause riunite C-293/12 e C-594/12, ove la Corte ha dichiarato invalida la direttiva sulla conservazione dei dati di traffico, c.d. "*data reunion*", per violazione del principio di proporzionalità nel bilanciamento tra il diritto alla protezione dei dati personali e le esigenze di pubblica sicurezza; Corte di Giustizia, Grande Sezione, sent. 13 maggio 2014, *Google Spain SL, Google Inc.* v. *Agencia Española de Protección de Datos*, causa C-131/12, in cui la Corte ha riconosciuto il diritto all'oblio a fronte dell'ingerenza dei motori di ricerca, chiarendo come non sia sufficiente invocare un interesse economico per comprimere il diritto alla riservatezza; Corte di Giustizia, Sezione III, sent. 16 febbraio 2012, *Belgische Verening van Auteurs, Componisten ed Uitgevers CVBA - SABAM* v. *Netlog NV*, causa C 360/10, alla cui stregua il gestore di un s*ocial network* non può essere costretto a predisporre un sistema di filtraggio generale, esteso a tutti i suoi utenti, per prevenire l'utilizzo illecito di opere musicali e audiovisive. Un simile obbligo comporterebbe una invasione sproporzionata nel diritto alla riservatezza degli utenti ed alla libertà di impresa.

non solo sul piano sostanziale, rivalutando il momento del furto di identità ad opera del *phisher*[59], ma anche, eventualmente, tramite misure processuali e pre-processuali di contrasto, nel rispetto del nucleo essenziale dei diritti fondamentali.

[59] Che, come si ha avuto modo di osservare, non esaurisce il suo disvalore penale nella frode informatica.