ELIANA RECCIA

La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un *focus* sull'attività bancaria

L'attuale emergenza pandemica ha avuto molteplici ripercussioni sul nostro ordinamento giuridico, non da ultimo sui cybercrimes e in modo particolare sulle frodi informatiche perpetrate in ambito bancario. Un ambito, questo, in cui il proliferare di tali fattispecie di reato ha reso ancor più evidente l'innato deficit di tipicità di cui le stesse si connotano.

The typicality of the latest types of cyber fraud: need for a rethink? A focus on banking

The current pandemic emergency has had multiple repercussions on our legal system, not least on cybercrimes and, in particular, on cyber fraud perpetrated in the banking sector. This is an area in which the proliferation of these types of crime has made even more evident the innate lack of typicality with which they are characterised.

1. *Le frodi informatiche: una breve analisi ai tempi del Covid.* L'attuale emergenza pandemica ha avuto molteplici ripercussioni sull'ordinamento giuridico; non da ultimo in materia di frodi informatiche[1], particolarmente mutevoli al mutare della realtà.

[1] I *cybercrimes* sono definiti dalla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 23.11.2001 (ratificata dall'Italia con l. n. 48/08) come "ogni tipo di violazione penale commessa per mezzo, con l'ausilio e/o avente ad oggetto un sistema o programma informatico". Per tutti, si veda PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, 10 ss. La distinzione tra *computer crime* e *cybercrime* nel passaggio all'"*epoca di Internet",* in cui il *cyber space* è diventato l'ambiente ideale e privilegiato per la realizzazione di molteplici reati, è descritta da PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di Picotti, Padova, 2004, 21 ss. e 29. Per una precedente panoramica sui reati informatici si veda PICOTTI, voce *Reati informatici*, in *Enc. Giur.*, Treccani, Roma, VIII agg., 2000, 1 ss.; SALVADORI, *I reati contro la riservatezza informatica*, in *Cybercrime,* a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2019, 656 ss.

In proposito, di estremo interesse risulta il report dell'Interpol[2], pubblicato nell'agosto 2020, che ha analizzato proprio l'impatto dell'emergenza sanitaria sui *cybercrimes*, evidenziando come tra gennaio e aprile 2020, siano stati identificati circa 907.000 messaggi *spam*, 737 incidenti dovuti all'impiego di *malware* e 48.000 URL dannosi, tutti correlati alla pandemia in corso. Il *report* mette in evidenza una significativa modifica nella selezione dei destinatari "elettivi" di tali attività criminose – non più individui e piccole aziende ma soprattutto grandi aziende, governi e infrastrutture –, sottolineando, altresì, come l'impiego generalizzato dello *smart working* abbia favorito la sottrazione di moltissimi dati sensibili.

D'altronde, l'utilizzo dei sistemi informatici è diventato indispensabile per quasi ogni attività economica, ancor più alla luce della necessità di ridimensionare gli incontri *de visu* e il lavoro in presenza. Diviene allora necessario domandarsi se il quadro normativo di riferimento, a ben 29 anni dalla sua introduzione, risulti in grado di contrastare adeguatamente tutte le "mutazioni" cui sono andate incontro le differenti attività ingannatorie o predatorie via web, o se sia invece necessario un tempestivo intervento del legislatore. Il discorso verterà in particolare sull'ambito bancario, sede "privilegiata" dell'incremento delle frodi informatiche.

---

[2] Cfr. Interpol Cybercrime, Covid-19 Impact, in *www.sistemapenale.it*, 11 settembre 2020. Al pari interessante anche rispetto alle relative ripercussioni del Covid-19 è il ENISA Threat Landscape – 2020, reperibile all'indirizzo *www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.* Si veda anche Relazione sulla politica dell'informazione per la sicurezza per il 2020, a cura del Comparto Intelligence (DIS, AISE e AISI) e mediante la quale il Governo riferisce al Parlamento sulla politica dell'informazione per la sicurezza, dell'1 marzo 2021, in *www.sistemapenale.it/it/scheda/cybercrime-rassegna-novita-marzo-aprile-2021.* Tra i *focus* trattati dalla relazione vi è la minaccia cibernetica**,** per cui viene delineato, in connessione all'emergenza pandemica, un significativo incremento. In particolare, gli attacchi censiti rilevano progettualità ostili (di matrice statuale, *hacktivista* o criminale), miranti a sfruttare il massiccio ricorso al lavoro agile in danno di operatori pubblici e privati, ovvero tese a carpire dati sensibili da strutture ospedaliere, centri di ricerca e realtà impegnate nello sviluppo di vaccini e terapie contro il Covid-19. I soggetti pubblici presi di mira sono stati soprattutto enti/operatori afferenti al settore della sanità e della ricerca e dicasteri ed altre Amministrazioni dello Stato, nei cui confronti si è registrata una intensa campagna di diffusione di malware e attacchi ransomware. Le azioni digitali ostili perpetrate nei confronti dei soggetti privati hanno, invece, interessato prevalentemente, oltre il settore farmaceutico/sanitario, quello bancario, i servizi IT e l'industria del Made in Italy. Sono state, in particolare, individuate attività di phishing, nonché la registrazione di domini malevoli allo scopo di ingannare gli utenti nel corso delle procedure di erogazione dei contributi economici per far fronte alla crisi economica generata dalla pandemia.

Per quanto attiene al quadro normativo, va detto che il legislatore italiano solo nel 1993, e dunque tardivamente rispetto alle sollecitazioni sovranazionali[3], ha conferito una - seppur "problematica" - autonomia a tali fattispecie, immaginando tuttavia la *dimensione* "*informatico-virtuale*" *in termini strumentali e accessori rispetto ad altre esigenze di tutela*[4]: collocate tra i reati contro il patrimonio, in costante oscillazione ermeneutica tra la macro categoria della truffa e quella del furto, avrebbero dovuto dar conto di condotte poliformi e plurioffensive, in costante evoluzione modale, peculiarmente insidiose in ragione dell'elevato grado di spersonalizzazione che tipicamente le connota. Ma procediamo con ordine. La frode informatica è prevista dall'art. 640 *ter* c.p.[5], che incrimina il fatto di «chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032».

La frode informatica – reato di evento a dolo generico – costituisce una «fattispecie decisamente problematica, dai tratti molto ambigui»[6] e «priva di una vera e propria identità tipologica»[7]. Si pensi, per tutti, all'inciso "senza diritto", che potrebbe, in astratto, leggersi in termini sia di totale sia di parziale assenza

---

[3] Cfr. Consiglio d'Europa, Comitato dei Ministri, Racc. n. R (89) 9, *Sulla criminalità connessa agli elaboratori elettronici*, 13 settembre 1989, in *Riv. trim. dir. pen. econ.*, 1992, 378.

[4] BARTOLI, *La frode informatica tra "modellistica", diritto vigente, diritto vivente, e prospettive di riforma*, in *Dir. inf.*, 2011, 3, 383 e ss.

[5] Nella norma è confluito l'originario disposto dell'art. 10, l. n. 547 del 23 dicembre 1993. Tra i primi commenti alla novella introdotta si veda MUCCIARELLI, *Commento all'art. 10 della L. n. 547 del 1993*, in *Leg. pen.*, 1996, 136 ss. Successivamente, con la Legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001, è stata integrata la definizione di cyber crimes, ai quali certamente appartiene la fattispecie di phishing, come "ogni tipo di violazione penale commessa per mezzo, con l'ausilio e/o avente ad oggetto un sistema o programma informatico". Per completezza, ai reati di cui alla Legge 547, sono peraltro stati aggiunti i nuovi articoli 167, 167-bis e 167-ter del D.lgs. n. 196/2003, così come novellato dal D.lgs. 10 agosto 2018, n. 101, e relativi al trattamento illecito di dati, comunicazione e diffusione illecita di dati personali ed acquisizione fraudolenta di dati personali trattati su larga scala.

[6] PECORELLA, *Diritto penale dell'informatica*, cit., 67 ss.; ID., *Art. 640-ter*, in *Codice penale commentato*[3], a cura di Marinucci-Dolcini, Milano, 2006, 4640; SCOPINARO, *Internet e reati contro il patrimonio*, Torino, 2007, 44 ss.

[7] BARTOLI, *La frode informatica*, cit., 392.

di autorizzazione[8]. Al riguardo, si è notato come questa dicotomia tra "illegittimità in astratto" e "in concreto" indurrebbe, nel primo caso, a includere la frode informatica nell'ambito tipologico della truffa, nel secondo in quello del furto[9]. Più nello specifico, secondo la prima opzione l'illecito costituirebbe un'ipotesi di truffa speciale per specificazione[10], in ragione del peculiare disvalore che connota l'alterazione del sistema informatico[11] – e quanti, ponendo l'attenzione più sull'esito che sulla struttura modale, l'hanno ritenuta invece riconducibile al paradigma del furto[12]. Dei due modelli ricostruttivi, il primo risulta, allo stato, ampiamente prevalente[13], pur nella diffusa consapevolezza

[8] Sul punto si veda BARTOLI, *La frode informatica,* cit., 388: «Si tratta infatti di un'espressione alquanto ambigua perché non solo non distingue tra manipolazione (al di là dell'autorizzazione) e uso (connesso a questioni di autorizzazione), ma addirittura la fattispecie fa riferimento soltanto alla manipolazione (intervento su) e non anche all'uso. Inoltre, e soprattutto, la manipolazione, che di per sé dovrebbe essere del tutto indipendente dalla questione dell'autorizzazione, deve avvenire "senza diritto", in presenza cioè di una caratteristica che è coerente con la condotta di uso dei dati che invece non è prevista».

[9] BARTOLI, *La frode informatica,* cit., 390, che puntualizza: «classica ipotesi problematica è quella del dipendente di banca che s'impossessa mediante movimentazioni effettuate con i terminali dell'ufficio di somme di danaro di clienti depositate in conti correnti. Ebbene, se si ricostruisce la frode informatica sul modello della truffa, l'espressione "senza diritto" non può che essere interpretata nei termini più ampi possibili, talmente ampi da perdere nella sostanza di significato, con la conseguenza che possono integrare la fattispecie sia i soggetti del tutto estranei, sia quelli che avrebbero una autorizzazione in astratto, ma assente in concreto. Se invece si asseconda la formulazione ambigua del legislatore e quindi si attribuisce un significato all'espressione "senza diritto" tale da dare rilevanza soltanto alle ipotesi in cui il soggetto agisce in totale assenza di un'autorizzazione, le ipotesi di manipolazione di dati in presenza di una illegittimità parziale finiscono per essere ricondotte alla fattispecie di furto»

[10] In dottrina sostengono questa posizione PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 141 ss.; in giurisprudenza cfr. Cass., Sez. VI, 5 febbraio 2009, n. 8755, Giambertone, Rv. 243238, secondo cui: «la fattispecie tracciata *ex* art. 640-*ter* c.p. ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il "sistema informatico" di pertinenza alla medesima, attraverso la manipolazione di detta persona»

[11] BARTOLI, *La frode informatica*, cit., 390, che ha puntualizzato al riguardo: «si tratta di una soluzione che non ci sentiamo di condividere, perché il disvalore della frode informatica non può incentrarsi sulla mera alterazione di un sistema informatico, richiedendo necessariamente anche la conseguente manipolazione dei dati o interferenza sulla attività del programma. In buona sostanza, ogni condotta della frode informatica deve essere diretta in termini più o meno immediati alla manipolazione dei dati e alla interferenza sul programma. Con la conseguenza che se a séguito della condotta di interferenza il software o la sua attività restano inalterati, non si può parlare di vera e propria frode informatica, potendo il fatto eventualmente integrare altre ipotesi di reato».

[12] Cfr. *ex multis* Cass., Sez. VI, 10 maggio 2007, n. 32543, Varriano, Rv. 237175.

[13] Cfr. Cass., Sez. II, 10 febbraio 2020, n. 10534, Gerbino, Rv. 278518, dove è precisato che: «Il delitto di frode informatica di cui all'art. 640-*ter* cod. pen. ha la medesima struttura ed i medesimi elementi costitutivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza di quest'ultima attraverso la sua manipolazione, onde, come la truffa, si consuma nel momento e nel luogo

che «la legge penale vigente [...] non – sia comunque – adeguata a perseguire [...] tutte le diverse fasi e forme del furto di identità»[14].

2. *Le diverse tipologie di frodi informatiche in ambito bancario e la relativa copertura normativa.* Alla luce di un quadro normativo comunque incerto, andranno analizzate le diverse tipologie di frodi informatiche – che in questa sede saranno approfondite con riferimento all'ambito bancario –: *Phishing* – basato sul *malware*[15] o "man in the middle"[16] –, *Pharming*[17], *Vishing*[18], *Smishing*, *Sim swap fraud*.

Il *Phishing*[19], peculiare forma di furto d'identità digitale, consiste in una captazione di dati, *username* e *password*, mediante la quale viene ottenuto un in-

in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui (in motivazione la Corte ha precisato che la manipolazione del sistema informatico, in quanto modalità "speciale" e tipizzata di espressione dei comportamenti fraudolenti necessari per integrare la truffa "semplice", non esaurisce e perfeziona l'illecito che, pertanto, si consuma nel momento dell'ottenimento del profitto)».

[14] CRESCIOLI, *La tutela penale dell'identità digitale*, in *www.dirittopenalecontemporaneo,* 25 maggio 2018, 274.

[15] Ipotesi in cui il *phisher* intercetta i messaggi indirizzati ad un sito scelto da qualsiasi utilizzatore, salva le informazioni che gli interessano, poi trasmette i messaggi al sito scelto dalla vittima ed infine inoltra le risposte di ritorno. Per un approfondimento si veda CAJANI-COSTABILE-MAZZARACO, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria,* Milano, 2008, 188.

[16] Caso in cui l'*e-mail* di *phishing* contiene un *link* c.d. "maligno" che una volta scaricato danneggia o altera i dati informatici presenti nel computer. Sul punto si veda OECD, *Scoping Paper on Online Identity Theft*, OECD, *Scoping Paper on Online Identity Theft*, Seul, 2008, disponibile *online* all'indirizzo *www.oecd.org/dataoecd/35/24/40644196.pdf*, 16.

[17] Si veda CRESCIOLI, *La tutela penale*, cit., 273 e 275. Si veda anche OECD, *Scoping Paper on Online Identity Theft*, cit., 19, in cui si puntualizza che: nel *computer* del malcapitato viene inserito un *virus* che modifica la lista dei siti contrassegnati come preferiti nel *browser* utilizzato dalla vittima, che viene quindi reindirizzata su un sito "clone" di quello dell'istituto di credito o dell'istituzione, ed attraverso il *login* a quest'ultimo vengono intercettate le sue credenziali.

[18] In tema si veda al riguardo 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, 266.

[19] Etimologicamente derivante dal verto inglese *To fish* (pescare). In tema *ex pluris* si veda ARONICA, *Il* "fishing" *tra nuove esigenze di tutela ed acrobazie interpretative della giurisprudenza*, in *Riv. di giur. ed econ. d'azienda*, 4, 2008, 83 ss.; BARTOLI, *La frode informatica,* cit., 383; CAJANI, *Profili penali del* Phishing, in *Cass. pen.*, 2007, 2294 ss.; CERQUA, *Accesso abusivo e frode informatica: l'orientamento della Cassazione*, in *Dir. prat. soc.*, 2000, 51; DI PALO, Cyber crime. *Il* Phishing: *prospettive di un delitto*, in *Arch. pen.*, 2017, 2, 1 ss.; FLOR, Phishing, Identity theft e Identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 899 ss.; PARODI, *Profili di rilevanza penale dei* dialer, in *Dir. pen. proc.*, 2003, 1426; ID., *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del* software, in *Criminalità informatica*, a cura di Sarzana di Sant'Ippolito, in *Diritto e proc. pen*, 1997, 12, 1539; PECORELLA, *Il diritto penale dell'informatica*, cit., 11 ss.; ID., *Commento Art. 640*ter *c.p.*, in *Codice penale commentato*[3]*, Artt. 575-734*bis, a cura di Marinucci-Dolcini, Milano, 2011, 6417; PERRI, *Lo* smishing *e il* vishing, *ovvero quando l'unico limite all'utilizzo criminale delle*

debito profitto ai danni del titolare degli stessi. Si tratta di un fenomeno che viene realizzato attraverso l'invio di messaggi di posta elettronica ingannevoli, così che le vittime vengono indotte a fornire volontariamente informazioni sensibili come, ad esempio, *password* di accesso all'*home banking*, o modalità di c.d. *social engineering*[20]. Più in particolare, di regola l'utente riceve messaggi che indicano l'esistenza di presunti problemi sul server della banca, provenienti, peraltro, da un indirizzo associato a quello messo a disposizione per la tutela dei clienti dell'istituto di credito di appartenenza, o che indicano insoliti tentativi di accesso al conto, se non procedure di aggiornamento del sistema di identificazione. L'utente viene così indotto, per risolvere il problema di volta in volta prospettato, a fornire i propri codici identificativi e operativi, accedendo a una pagina web raggiungibile da un *link* contenuto nella stessa e-*mail*. La richiesta, spesso di carattere urgente, allerta il cliente circa il rischio del blocco del conto corrente. A quel punto il truffatore, entrato nel pieno possesso delle credenziali del cliente, effettua tutte le operazioni finanziarie che desidera a mezzo dell'*home banking*.

Il *Pharming* è un'evoluzione più sofisticata del *phishing*. Qui la vittima è invitata a fornire le proprie generalità su un sito "clone" di quello ufficiale; il traffico di rete tra un cliente e un *web server* viene infatti dirottato verso siti In-

nuove tecnologie è la fantasia, in *Dir. int.*, 3, 2008, 265 ss.; PICA, voce Internet, in *Dig. disc. pen.*, Torino, 2004, 425; PICOTTI, voce *Reati Informatici*, in *Enc. giur.*, Roma, 1999, 1 ss.; RESTA, *Banche di dati on-line. I limiti della tutela penale*, in *Giur. mer.*, 2007, 2052; SCOPINARO, *Furto di dati e frode informatica*, in *Dir. pen. proc.*, 2007, 364; ID., *Internet e reati contro il patrimonio*, Torino, 2007, 10 ss.

[20] Per un approfondimento si veda CAJANI, *Profili penali*, cit., 2225, che così sintetizza: «Questa tecnica è anche un metodo (improprio) di crittoanalisi quando è usata su una persona che conosce la chiave crittografica di un sistema. Similmente al metodo del tubo di gomma può essere un modo sorprendentemente efficiente per ottenere la chiave, soprattutto se comparato ad altri metodi crittoanalitici. Con l'evoluzione del software, l'uomo ha migliorato i programmi a tal punto che essi presentano pochi bug (errori che i programmatori generalmente commettono quando creano un software). Per un hacker sarebbe impossibile attaccare un sistema informatico in cui non riesce a trovare bug. Quando ciò accade l'unico modo che l'hacker ha per procurarsi le informazioni di cui necessita è quello di attuare un attacco di ingegneria sociale. Un ingegnere sociale (*social engineer*) per definirsi tale deve saper fingere, sapere ingannare gli altri, in una parola saper mentire. Un *social engineer* è molto bravo a nascondere la propria identità, fingendosi un'altra persona: in tal modo egli riesce a ricavare informazioni che non potrebbe mai ottenere con la sua identità reale. Nel caso sia un hacker può ricavare informazioni attinenti ad un sistema informatico. Il *social engineering* è quindi una tecnica per ricavare informazioni molto usata dagli hacker esperti e dalle spie, e dato che comporta (nell'ultima fase dell'attacco) il rapporto più diretto con la vittima, questa tecnica è una delle più importanti per carpire informazioni. In molti casi il cosiddetto ingegnere potrà riuscire a ricavare tutto ciò che gli serve dalla vittima ignara».

ternet fraudolenti costruiti *ad hoc*, con lo scopo di carpire dati sensibili o di fungere da "teste" di ponte per ulteriori tipologie di frodi.

Si ha, invece, *Vishing* quando la condotta di *phishing* ha inizio con una telefonata in cui un finto operatore chiama al telefono le possibili vittime dell'attacco mediante un sistema vocale automatizzato (utilizzando ad esempio un sistema VoIP), spacciandolo per il *call center* di una banca o di un istituto di credito.

Lo *Smishing* è una peculiare forma di *phishing* che ha inizio con un sms sui telefonini per attirare le vittime nella trappola ed estorcere informazioni personali, numeri di carte di credito ad altri dati riservati.

La *Sim swap fraud* è una tecnica di attacco che consente di avere accesso al numero di telefono del legittimo proprietario e violare determinate tipologie di servizi online che usano il numero di telefono come sistema di autenticazione.

Per contrastare queste peculiari forme predatorie, oltre all'applicabilità dell'art. 494 c.p.[21] – che sconta tuttavia il limite di un evidente deficit di determinatezza[22] –, sono stati introdotti, nel 1993, la fattispecie di cui all'art. 640-*ter* c.p. e, nel 2013 – *ex* l. n. 119/2013[23] –, un terzo comma all'art. 640-*ter*

[21] Cfr. Cass., Sez. II, 2 luglio 2020, n. 23760, Moscatiello, Rv. 279585, secondo cui: «Integra il delitto di sostituzione di persona di cui all'art. 494 c.p., la condotta di colui che si inserisce nel sistema operativo di un servizio di home banking servendosi dei codici personali identificativi di altra persona inconsapevole, al fine di procurarsi un ingiusto profitto con danno del titolare dell'identità abusivamente utilizzata, mediante operazioni di trasferimento di denaro».

[22] Si veda al riguardo e per il necessario approfondimento FLOR, Phishing, Identity Theft *e* Identity Abuse, cit., 901 e ss., che puntualizza: «è utile premettere che la natura "informatica" , o "non fisica" , del "profilo" personale ed il suo utilizzo in Internet evidenziano come l'ipotetica lesione della affidabilità e certezza dei rapporti interpersonali si realizzi con peculiari metodi tecnici, riconducibili all'uso (e abuso) della c.d. "identità virtuale", non del tutto corrispondenti agli elementi tipici del reato in esame, che è chiaramente a forma vincolata commissiva e comporta la necessità di "indurre taluno in errore" con le modalità tassativamente previste dalla norma stessa». In tema di tipicità dell'art. 494 c.p. *ex multis* DE FELICE, *Le falsità personali. Profili generali*, Napoli, 1983, 175 e ss.; si veda, altresì, ampiamente, CRISTIANI, *Il delitto di sostituzione di persona*, Padova, 1985, 10 e ss.; ID., voce *Falsità personale*, in *Dig. disc. pen.*, Torino, 1991, V, 105 ss. Per riferimenti anche giurisprudenziali si veda CAPPITELLI, *La sostituzione di persona nel diritto penale italiano* (nota a Cass. Sez. V, 11 dicembre 2003, n. 8670), in *Cass. pen.*, 2005, 2994 e ss.; cfr. anche Cass., Sez. V, 21 gennaio 1999, in *Riv. it. dir. proc. pen.*, 2000, 1274 e ss. In prospettiva storica si veda, infine, JACOVONE, *Il delitto di sostituzione di persona*, Napoli, 1974, 15 ss.

[23] Recante "*Disposizioni urgenti in materia di sicurezza per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province*", un decreto "omnibus" in cui il Governo è intervenuto sulla disciplina delle fattispecie di maltrattamenti in famiglia, atti persecutori e

c.p., che prevede un aggravamento della pena quando il «il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti». Tale circostanza sintetizza in modo significativo, a ben vedere, l'identità incerta conferita a questa tipologia di illeciti, laddove furto e frode continuano a incrociare in modo incerto le loro strade[24].

D'altronde, all'art. 640-*ter* c.p., quantomeno fino all'introduzione del terzo comma, non veniva riconosciuta neanche la natura di autonoma ipotesi di reato[25].

Lo scotto pagato da questa fattispecie è la convinzione, da parte del legislatore, che essa possa disciplinare efficacemente tutte le tipologie di frode operate a mezzo di strumenti informatici, nonostante le condotte di riferimento siano molteplici e in continuo mutamento. L'art. 640-*ter* c.p. è, infatti, sicuramente tipizzato sul modello della truffa, anche se quest'ultima è innegabilmente modulata, anche sul piano semantico, sulle dinamiche di un rapporto interpersonale che, nelle frodi informatiche, può risultare quantomai sfuggente. La giurisprudenza, soprattutto di merito[26], risolve il problema, sostanzialmente, evitando di porselo, ad esempio ritenendo non necessaria l'induzione in erro-

violenza sessuale, sia agendo sulla cornice edittale sia prevedendo nuove circostanze aggravanti e nuove misure pre-cautelari; vengono poi introdotte nuove aggravanti dei reati di furto, rapina, ricettazione a tutela di attività di particolare rilievo strategico nonché per garantire soggetti deboli come anziani e minori. Si veda Rel. Cass. n. III/01/2013, Roma, 22/08/2013.

[24] *Contra* la sussumibilità di tali fattispecie nel furto si sostiene che l'identità è un'entità immateriale, pertanto non è elevabile a "cosa" suscettibile di furto (*ex* art. 624 c.p.) o anche di essere materialmente "utilizzata": al riguardo si veda MALGIERI, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo,* in *Dir. pen. cont.,* 2015, 2, 149 ss.; ZICCARDI, voce *Furto d'identità*, in *Dig. disc. pen.*, Torino,VI, agg., 2001, 253 ss.

[25] Si veda MANTOVANI, *Diritto penale, Parte speciale, I delitti contro il patrimonio*[4], II, Padova, 2016, 226; MARGIOCCO, *Frode informatica*, in *Diritto dell'informatica*, a cura di Finocchiaro-Delfini, Milano, 2014, 1107 e 1110.

[26] Cfr. Tribunale di Napoli, Sez. VI, 25 gennaio, n. 205, in *www.dejure.it*, ha evidenziato che: «L'art 640-*ter* c.p. sanziona chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. In tal modo si vuole tutelare il patrimonio individuale, ma più specificatamente il regolare funzionamento dei sistemi informatici e la riservatezza dei dati ivi contenuti. Per la configurabilità del reato in questione, a differenza di quanto previsto per il reato di cui all'art 640 c.p., non è richiesta l'induzione in errore della vittima, in quanto l'attività fraudolenta investe il sistema informatico della stessa e consiste nell'alterazione, comunque realizzata, del sistema informatico e dell'intervento, senza averne diritto, con qualsiasi modalità, su dati, informazioni, programmi di un sistema informatico».

re, surrogabile dalla compresenza di una forte pressione psicologica sulla vittima e dell'utilizzo dell'altrui identità virtuale con il fine di trarne profitto[27].
L'incerta tipicità è probabilmente la causa per cui il *phishing*, e le sue diverse tipologie, vengono ricondotte, in dottrina[28], ora all'art. 640 c.p., ora all'art. 640-*ter* c.p.
La giurisprudenza di legittimità[29], invece, sembra ormai orientata a ritenere il *phishing* tipico *ex* art. 640-*ter* c.p., pur riconducendolo a volte all'art. 615-*ter* c.p., sulla base del presupposto che l'ultima fase dei *phishing attacks* è comunque diretta all'utilizzo delle informazioni raccolte, per accedere abusivamente ad aree informatiche riservate o a servizi *online*.
Ma il progressivo moltiplicarsi delle opzioni modali, a fronte di un quadro normativo incerto, solleva forti dubbi sulla effettiva adeguatezza della disciplina legale.

3. *Il Phishing nell'attività bancaria*. L'ambito che è stato maggiormente esposto al binomio Covid/frodi informatiche è probabilmente quello bancario. Qui, peraltro, l'art. 640-*ter* c.p. – quale strumento di contrasto – appare in particolare difficoltà.
I primi problemi attengono già alla «individuazione del soggetto passivo singolo» e alla «distinzione fra soggetto passivo della condotta e soggetto passivo del danno. Infatti, nel fenomeno sinora descritto non è coinvolto solo l'utente, ma anche l'istituto bancario, l'ente o la società finanziaria che "subisce" la

[27] DI PALO, Cyber crime, cit., 2, 3 ss.
[28] Per una più ampia analisi si veda BARTOLI, *La frode informatica*, cit., 385 e ss. Ritiene inapplicabile alcuna delle due norme: FLOR, Phishing, Identity theft *e* identity abuse, cit., 910 ss. Per un approfondimento si vedano: MINICUCCI, *Le frodi informatiche*, in *Cybercrime*, a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2019, 827 ss.; PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, cit., 21 ss.
[29] Cfr. *ex multis* Cass., Sez. II, 24 febbraio 2011, n. 9891, De La Parra, Rv. 249675, secondo cui: «Nella fattispecie in esame, l'utilizzazione della password – illecitamente ottenuta – per entrare nel sistema informatico di *home banking* del correntista (protetto da misure di sicurezza costituite, appunto, dai dati di accesso personali) e messo a sua disposizione dalle Poste Italiane, servì per stornare fondi dal conto corrente della C.: con il che si è verificata l'ipotesi di intervento (nella specie: ordine di bonifico dal conto corrente della C. a quello dell'imputato) senza diritto sui dati e/o informazioni (nella specie: sul saldo attivo del conto corrente) contenuti nel suddetto sistema informatico. Si può quindi concludere [...] che la fattispecie, così come contestata, rientra nell'ipotesi criminosa di cui all'art. 640-*ter* c.p.»

"clonazione" dei propri siti, loghi o simboli e le successive operazioni effettuate loro tramite dal *phisher*»[30].

Facciamo un esempio. Qualora taluno induca in errore la vittima per poter accederne all'*home banking*, e in tal modo disponga direttamente operazioni finanziare a proprio vantaggio, non sembrano sorgere particolari problemi: il fatto andrà ritenuto integrato. D'altronde, «l'eventuale negligenza del soggetto passivo nella verifica della genuinità ed autenticità dell'*e-mail* o della veridicità dei suoi contenuti appare irrilevante»[31] ai fini della configurabilità della frode informatica, così come accade, peraltro, nel delitto di truffa[32]. Più delicata, al contrario, l'ipotesi in cui il *phisher* determini un soggetto, inducendolo in errore, a effettuare un'operazione finanziaria a vantaggio del *phisher* stesso – magari adducendone il carattere meramente fittizio. Qui, infatti, sembra esistere una significativa discrasia tra la fattispecie astratta e quella concreta, tale da escludere la riconducibilità di quest'ultima al paradigma normativo della frode informatica.

Nell'ambito della tipologia di illeciti qui osservata, merita sicura attenzione l'art. 615 *ter* c.p., per la cui configurabilità è sufficiente che l'agente entri nell'*home banking* di altri, senza necessità che disponga operazioni finanziarie.

Tale norma, seguendo lo schema "fisico" dell'art. 614 c.p., tutela infatti l'inviolabilità del domicilio e della c.d. riservatezza informatica. Si tratta tuttavia di beni non facilmente "afferrabili": lo spazio informatico e quello cibernetico non sono, infatti, suscettibili di chiara delimitazione. L'impressione è

[30] R. FLOR, Phishing, Identity Theft *e* Identity Abuse, cit., 903.

[31] *Ibid.*

[32] Va precisato, al riguardo, che la più recente giurisprudenza, cfr. Tribunale di Napoli, Sez. VI, 25 gennaio 2021, n. 205, in *DeJure*, anche di merito non ha ritenuto necessaria la sussistenza dell'induzione in errore quale requisito propedeutico alla configurabilità della frode informatica, precisando che: «L'art 640-*ter* c.p. sanziona chi, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. In tal modo si vuole tutelare il patrimonio individuale, ma più specificatamente il regolare funzionamento dei sistemi informatici e la riservatezza dei dati ivi contenuti. Per la configurabilità del reato in questione, a differenza di quanto previsto per il reato di cui all'art 640 c.p., non è richiesta l'induzione in errore della vittima, in quanto l'attività fraudolenta investe il sistema informatico della stessa e consiste nell'alterazione, comunque realizzata, del sistema informatico e dell'intervento, senza averne diritto, con qualsiasi modalità, su dati, informazioni, programmi di un sistema informatico».

che il legislatore muova da una ritenuta sintonia tra la privacy del privato domicilio e quella del proprio spazio informatico, che però è tutt'altro che reale, perché soltanto il primo ha limiti predeterminati e davvero riconoscibili. Tali perplessità si concretizzano in modo chiaro nelle applicazioni giurisprudenziali[33] in cui il bene giuridico tutelato viene individuato nel c.d. domicilio informatico, inteso come spazio fisico in cui sono contenuti dati informatici personali, ma anche come spazio virtuale di pertinenza della sfera individuale e privata. Fatto sta, tornando così alla "ipotesi critica" con cui ci siamo confrontati, che la stessa non appare riconducibile neanche allo specifico dell'art. 615 *ter*. Insomma, il rapporto tra la realtà empirica e il dato normativo chiamato a regolarla si mostra decisamente problematico.

Il *Phishing* presuppone, poi, la violazione delle regole di sicurezza predisposte dal titolare dello spazio informatico. Regole non oggetto di tipizzazione normativa né fissate dalla PSD2[34]: un *vacuum* inquietante perché, al di là dell'applicazione da parte del singolo cliente delle misure predisposte dalla banca a sua tutela (attivazione *secure code*, certificazione numero cellulare, *sms alert*, cambio PIN periodico, etc.), dovrebbe essere l'istituto di credito a tutelare in prima istanza i propri correntisti da invasioni nel loro *home banking* da parte di terzi. Al netto delle statuizioni dell'ABF[35] – organo di natura ibrida che deve essere adito prima di rivolgersi all'Autorità Giudiziaria –, non

[33] Cfr. Cass., Sez. VI, 4 ottobre 1999, in *Dir. inf.*, 2001, 485 ss.; ID., Sez. V, 6 dicembre 2000, in *Guida dir.*, 2001, 8, 78; Corte di Appello di Bologna, Sez. II, 30 gennaio 2008, in *Riv. it. dir. proc. pen.*, 2010, 1, 456, con nota di FOTI, *Accesso abusivo a sistema informatico o telematico. Un "pericoloso" reato di pericolo.*

[34] Payment Services Directive 2**,** Direttiva europea n. 2366/2015, entrata in vigore il 13 gennaio 2016.

[35] *Ex multis* ABF, Collegio di Torino, Decisione n. 10880, del 21 aprile 2021, in *www.arbitrobancariofinanziario.it*, che ha puntualizzato: «Al fine di dimostrare di avere ottemperato alla normativa vigente, l'intermediario ha fornito evidenza di avere adottato un sistema di autenticazione multifattoriale consistente nell'inserimento delle credenziali statiche di accesso al canale di home banking, di un codice OTP inviato tramite notifica push, e una ulteriore password – cd. codice OTS – inviata tramite sms sul cellulare della ricorrente; nonché di avere correttamente registrato e contabilizzato l'operazione per cui è controversia»; nello stesso senso ABF, Collegio di Coordinamento, Decisione n. 4171, del 20 maggio 2015, in *www.arbitrobancariofinanziario.it*; ma anche ABF, Collegio di Milano, Decisione n. 5727/2014, in *www.arbitrobancariofinanziario.it*; e, da ultimo, ABF, Collegio di Roma, Decisione n. 6581, del 22 marzo 2018, in *www.arbitrobancariofinanziario.it* , che ha espressamente esonerato la banca da responsabilità per avere la stessa adottato un sistema di sicurezza a due fattori; ABF, Collegio di Milano, Decisione n. 46, del 15 febbraio 2010, in *www.arbitrobancariofinanziario.it*.

è dato però ritrovare precise opzioni ordinamentali in tal senso, neanche in termini di qualità e contenuto delle prescrizioni.

La giurisprudenza civile non è di grande supporto al riguardo, ritenendo, con una indubbia petizione di principio, che la banca debba operare secondo il modello dell'"accorto banchiere"[36], finendo così per individuare a carico dell'istituto di credito una possibile responsabilità di posizione, ma dai confini incerti, una forma di responsabilità oggettiva[37] legata al c.d. rischio di impresa[38], una responsabilità "prevedibile ed evitabile" con appropriate misure destinate a verificare la genuinità delle operazioni. Il che potrebbe anche andare se esistesse un parametro alla luce del quale poter conoscere *ex ante* lo specifico di tali obblighi. Tra questi, secondo alcune decisioni dell'ABF[39], vi sarebbe anche l'approfondito monitoraggio delle operazioni disposte su internet dalla clientela, per verificare il regolare andamento delle operazioni e segnala-

[36] *Ex pluris* cfr. Cass., Sez. VI, 12 aprile 2018, n. 9158, in *Resp. civ. e prev.*, 2019, 2, 622, con nota di Frau, *Home Bannkig, Phishing e responsabilità civile della banca*.

[37] In termini generali sulla responsabilità oggettiva e senza pretesa di completezza di richiami, si vedano, per tutti, ALPA, *Responsabilità civile e danno*, Bologna, 1991, 10 ss.; ID., *Responsabilità oggettiva*, in *Contratto impr.*, 2005, 959 ss.; CASTRONOVO, *Responsabilità oggettiva. II. Disciplina privatistica - dir. comp. e stran.*, in *Enc. giur.*, Roma, 1991, XXVII, 2 ss.; RODOTÀ, *Modelli e funzioni della responsabilità civile*, in *Riv. crit. dir. priv.*, 1984, 595 ss.; SCOGNAMIGLIO, *Responsabilità per colpa e responsabilità oggettiva*, in *Studi in Onore di Andrea Torrente*, a cura di Aa.Vv., Milano, 1968, 1113 ss.; TRIMARCHI, *Rischio e responsabilità oggettiva*, *Atti illeciti rischio e danni*, Milano, 2019, 20 ss.

[38] Con specifico riguardo alla trattazione del rischio di impresa in ambito bancario si veda VIVANTE, *Trattato di diritto commerciale*[5], Milano, 1916, III, 145. In tempi più recenti ASCARELLI, *Pagamento di assegni falsi e diligenza del traente*, in *Banca borsa tit. cred.*, 1954, II, 170; BENATTI, *Le clausole di esonero da responsabilità nella prassi bancaria*, in *Le operazioni bancarie*, a cura di Portale, Milano, 1978, 137; DE SEMO, *Diritto cambiario*, Padova, 1963, 689; DI LAURO, *Colpa, rischio e responsabilità obiettiva di impresa bancaria*, in *Banca borsa tit. cred.*, 1968, II, 606; FRAU, Home banking, phishing, cit., 636, precisa, proprio in merito alle posizioni in tema dell'ABF, che: «Al riguardo, infatti, l'Autorità ha avuto modo di osservare che la responsabilità più stringente addossata all'intermediario troverebbe una giustificazione espressamente definita «social-commerciale», ispirata al principio del rischio d'impresa, secondo il quale è razionale far gravare i rischi statisticamente prevedibili, legati ad attività oggettivamente pericolose e che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ripartire sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi. Si tende, in altri termini, a diluire sulla moltitudine degli utilizzatori il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento, in modo da evitare che esso gravi esclusivamente e direttamente sul singolo»; GRAZIANI, *Manuale di diritto commerciale*, Napoli, 1955, 301; GUALTIERI, *Titoli di credito*, Torino, 1953, 311.

[39] *Ex multis* ABF, Collegio di Torino, Decisione n. 10880, del 27 aprile 2021, in *www.arbitrobancariofinanziario.it*; ID., Collegio di Torino, Decisione n. 10578, del 22 aprile 2021, in *www.arbitrobancariofinanziario.it*; ID., Collegio di Bologna, Decisione n. 9506, dell'8 aprile 2021, in *www.arbitrobancariofinanziario.it*.

re quelle anomale rispetto all'usuale operatività del conto, specie se emergano numerose transazioni effettuate in un ristretto spazio temporale e nei confronti del medesimo beneficiario.
Resta però un ineludibile quesito di fondo: che valore hanno le statuizioni di un organo stragiudiziale come l'ABF sull'individuazione degli obblighi pendenti in capo alla banca, e come si pongono gli stessi a fronte di quelli, non sempre coincidenti, individuati dalla giurisprudenza? Il tema, come appare evidente, è particolarmente rilevante in sede sia stragiudiziale, sia civile sia penale[40].
Al riguardo, non può non evidenziarsi come il d.l. 93/2013, oltre a introdurre il comma tre all'art. 640 *ter* c.p., avesse anche inserito, all'art. 24-*bis* D.lgs. n. 231/2001, il reato di frode informatica aggravato dalla sostituzione dell'identità digitale nel catalogo dei reati presupposto della responsabilità degli enti[41], norma poi eliminata in sede di conversione, ma che – al contrario – avrebbe potuto rafforzare la tutela predisposta nei confronti delle frodi informatiche realizzate a danno dei clienti degli istituti di credito.

3.2 *Il ruolo del financial manager e* il tempus e locus commissi delicti *del phishing.* Nell'ambito delle frodi informatiche, assume un ruolo peculiare, e particolarmente discusso, il c.d. financial manager. Tale figura è da identifi-

[40] Per un approfondimento del tema si veda FALDUTI, *Frode informatica e utilizzo indebito di carte di credito: variabili interpretative*, in *Giur. pen.*, 2017, 1 ss.; PREVITALI, *Il reato di frode informatica ai sensi del d.lgs. 231/2001: standard di controllo e procedure per la* compliance *del Modello Organizzativo*, in *www.rivista231.it*, che evidenzia a proposito della frode informatica commessa dall'ente: «La condotta incriminata, dunque, consiste nell'alterare il funzionamento di un sistema informatico o nell'intervenire senza diritto su dati, informazioni o programmi contenuti in un sistema informatico. Ai sensi del decreto 231 la frode informatica rileva se commessa in danno dello Stato o di altro ente pubblico: tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato o ad altro ente pubblico. L'ipotesi di reato si potrebbe inoltre ricondurre all'alterazione di registri informatici della Pubblica Amministrazione per far risultare esistenti condizioni essenziali per la partecipazione a gare (iscrizione in albi, ecc.) ovvero per la successiva produzione di documenti attestanti fatti e circostanze inesistenti o, ancora, per modificare dati fiscali/previdenziali di interesse dell'azienda (ad esempio, Modello 770), già trasmessi all'Amministrazione. Il reato in esame potrebbe anche configurarsi qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico della Pubblica Amministrazione al fine di inserire un importo superiore a quello legittimamente ottenuto»

[41] GUERNELLI, *Frodi informatiche e responsabilità delle persone giuridiche alla luce del d.lgs. 8 giugno 2001, n. 231,* in *Riv. trim. dir. pen. econ.*, 2002, 292.

carsi con colui che, in accordo con il phisher – consapevole, quindi, della natura criminosa dallo stesso posta in essere – riceva le somme indebitamente sottratte, le ponga all'incasso e successivamente le trasferisca a terzi.
Il *financial manager*, dunque, è incaricato di far transitare sui propri conti, spesso accesi attraverso l'utilizzo di carte prepagate, dietro pagamento di una commissione, il denaro provento della condotta di phishing, che sarà, a sua volta, trasferito all'estero su altri conti correnti. Dopo aver sottratto il proprio "corrispettivo", il *financial manager*, infatti, attraverso l'utilizzo di piattaforme quali Money Transfer, o Western Union, trasferisce il restante su conti di terzi, così da interromperne il flusso di tracciabilità.
Si discute sulla natura di tale contributo; *in primis* quanto alla sussistenza di un potenziale concorso di reati tra phishing e riciclaggio; risulta, poi, problematico individuare, nella condotta di tale soggetto, una partecipazione in termini di concorso nella frode informatica o, quale titolo autonomo, il reato di riciclaggio, *ex* art. 648 *bis* c.p, ovvero di ricettazione, *ex* art. 648 c.p.
Nel phishing, infatti, si assiste spesso al concorso tra phisher, *financial manager* e terzo destinatario delle somme sottratte, il quale può anche coincidere con una delle due prime figure.
Se, però, per il phisher, date le condivise debolezze della relativa fattispecie tipica, la natura della sua condotta risulta già piuttosto difficile da inquadrare, per il *financial manager,* tali difficoltà si acuiscono.
Presupposto indefettibile per la rilevanza penale della sua condotta è il dolo che deve connotare un simile contributo, ormai esteso dalla giurisprudenza di legittimità[42], per quanto concerne il riciclaggio, anche alla forma eventuale – consapevolezza della natura illecita del provento o accettazione del relativo rischio[43]. In particolare, sussiste il concorso laddove il *financial manager* sia

[42] *Ex multis,* Cfr. Cass., Sez. II, 28 maggio 2018, n. 36893, Franchini, Rv. 274457.
[43] Risponderà pertanto, secondo tale ragionamento, colui che, con più azioni in esecuzione del medesimo disegno criminoso, senza essere concorso nel reato presupposto, accetta il rischio — ovvero agisce nella piena consapevolezza — della probabile origine delittuosa di denaro, che si impegna a fare transitare sul proprio conto corrente bancario e, quindi, a trasferire verso soggetti terzi e ciò anche con riferimento alla possibilità che la propria condotta sia idonea ad ostacolare l'attività di accertamento della provenienza delittuosa delle somme ricevute. Cfr. Uff. Ind. Prel. Palermo, 21 aprile 2009, in *Giur. merito*, 2009, 2825. Nella fattispecie, il dolo del delitto di riciclaggio, nella forma del dolo eventuale, è stato ritenuto sussistente in considerazione della natura dell'operazione complessivamente effettuata dall'imputato principale e dal compartecipe suo genitore, operazione originata dall'accettazione di una

ben consapevole dell'attività truffaldina del phisher e assicuri comunque la propria collaborazione[44]; qualora, invece, ne sia all'oscuro, ma comunque metta a disposizione un proprio conto corrente, o ne accenda uno a tal fine, e poi trasferisca il denaro, nella generica consapevolezza dell'illiceità della operazione a monte, ne risponderà, a seconda dei casi, di ricettazione o di riciclaggio[45].

Alcune pronunce di legittimità[46], al riguardo, hanno negato la possibilità di un concorso di reati tra phishing e riciclaggio, di fatto optando per la configurabilità dell'art. 648 *bis* c.p. in capo al *financial manager*, sul presupposto che l'intervento di quest'ultimo sarebbe avvenuto in una fase successiva alla consumazione del phishing, così elevandosi a fattispecie autonoma. Altre[47] hanno

---

proposta di prestazione lavorativa inviata tramite e-mail, contenente la prospettazione di facili guadagni in relazione alla semplice attività, richiesta da una società straniera non meglio identificata, di porre all'incasso e successivamente trasferire verso l'estero somme di denaro. Si veda, peraltro, Trib. Milano, 7 ottobre 2011, in *Guida dir.*, 2013, dossier 5, 60, la cui massima è riportata come segue: «Chi utilizza tecniche di "phishing" per ottenere, tramite artifici e raggiri e inducendo in errore l'utente, le credenziali di autenticazione necessarie ad accedere abusivamente a spazi informatici esclusivi del titolare (ad esempio relativi alla gestione dei conti correnti on line) e a svolgere, senza autorizzazione, operazioni bancarie o finanziarie, può rispondere dei delitti di cui agli art. 494 (sostituzione di persona), 615-ter (accesso abusivo a sistemi informatici o telematici) e 640 c.p. (truffa). Sono penalmente responsabili coloro che, senza essere concorsi nel reato presupposto, nella piena consapevolezza della provenienza illecita o, comunque, accettandone il rischio — purché non desunto da semplici motivi di sospetto, bensì da una situazione fattuale inequivoca — a seguito di proposte di collaborazione in internet, tramite e-mail, contatti in chat o messaggi allocati su pagine web, e la prospettazione di facili guadagni in relazione alla semplice attività richiesta ai cosiddetti "financial manager", pongono all'incasso e successivamente trasferiscono somme di denaro, tutte provenienti da delitti non colposi ».

[44] Cfr. Trib. Milano, Sez. G.I.P., 10 aprile 2013, Ciavarella, *in www.penalecontemporaneo.it,* 3 marzo 2015, con nota di PIANCASTELLI, *La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*; Trib. Milano, 7 ottobre 2011, Sez. XI, P.G.E. ed altri, in *www.dirittopenalecontemporaneo.it*, 5 dicembre 2011.

[45] Cfr. Cass., Sez. II, 21 novembre 2014, n. 10746, Bassini, Rv. 263155, che ha precisato: «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».

[46] Cfr. Cass, Sez. II, 9 febbraio 2017, n. 10060, Prili, Rv. 275263. In questa occasione la Cassazione ha puntualizzato che: «Il reato di riciclaggio non concorre con quello di frode informatica realizzata attraverso il cd. phishing, ovvero l'invio di mail riportanti il logo contraffatto di un istituto di credito o di una società di commercio elettronico con cui il destinatario viene invitato a fornire dati bancari riservati»

47 Cfr. Cass., Sez. II, 17 giugno 2011, n. 25960, in *Guida dir.*, 2011, 44, 76, secondo cui sussiste il delit-

poi introdotto una distinzione, sostenendo, da un lato, che, ove il riciclatore sia consapevole dell'attività illecita del phisher ed assicuri a questi il proprio apporto, lo stesso risponde di concorso nell'attività delittuosa del secondo; nel caso in cui, invece, il *financial manager* sia inconsapevole del disegno criminoso complessivo, non sussisterebbe il concorso doloso nel reato presupposto, bensì la sua responsabilità per il reato di riciclaggio, a titolo di dolo eventuale.

Di recente è intervenuta una interessante pronuncia di legittimità in cui la Cassazione[48] ha risolto una questione inerente all'inquadramento della condotta di intestazione di carte prepagate, al fine di consentire il trasferimento su di esse di denaro indebitamente sottratto, attraverso l'operazione di clonazione delle carte. La peculiarità si sostanziava nel chiarire se, data la contestualità tra prelievo e ricarica, tale condotta potesse integrare il reato di riciclaggio o il reato presupposto di frode informatica *ex* art 640 *ter* c.p. ovvero di indebito utilizzo e falsificazione di carte di credito di cui all'art. 55 d.lgs. 231/2007 (ora 493 *ter* c.p.), in concorso con gli altri partecipanti

---

to di riciclaggio nel caso di ricezione sul proprio conto corrente, e di successivo trasferimento ad altro beneficiario all'estero con il sistema del money transfer, di somme di denaro prelevate fraudolentemente dal conto di un ignaro cliente di banca con il sistema del c.d. phishing. Si veda anche Uff. Ind. Prel. Milano, 29 ottobre 2008, in *Foro ambrosiano*, 2008, 406. In dottrina, sul punto BARBIERI, *I difficili rapporti tra dolo e presupposti della condotta: l'accertamento del dolo nel delitto di riciclaggio*, in *Cass. pen.*, 2014, 2520.

[48] Cfr. Cass., Sez. II, 11 marzo 2021, n. 9787, in *DeJure*. In questo caso, infatti, rileva la Corte: «al momento del passaggio di denaro, era già stato commesso, ab origine, quale presupposto logico del reato di frode informatica, il reato di cui all'art. 55 co. 9 *ex* d.lgs. 231/2007 (ora 483 *ter* c.p.), ovvero, il reato di indebito utilizzo e falsificazione di carte di credito e di pagamento, non contestato nei confronti dei ricorrenti. Più in particolare, era stata sicuramente commessa una o più tra le tante condotte descritte nella seconda parte di quest'ultima norma e consistenti nel fatto di 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"». La Corte si pone, sul punto, in linea con i suoi orientamenti consolidati, secondo cui in tema di riciclaggio di carte di credito rubate o clonate, l'indebita utilizzazione delle carte stesse non costituisce reato presupposto del riciclaggio, ma reato strumentale alla commissione del riciclaggio medesimo (Cass., Sez. II, 24 ottobre 2013, n. 47147, Tumbarello, Rv. 257821).

Viene peraltro negata la possibilità che il reato di cui all'art 55 sia da ritenere assorbito nel reato di frode informatica, cui i ricorrenti avevano concorso: fa, infatti, luogo assorbimento in relazione all'ipotesi prevista nella prima parte dell'art. 55, comma 9 d.lgs. 231/2007, consistente nel fatto di chi «utilizza, non essendone titolare carte di credito o di pagamento...». Fattispecie del tutto diversa da quella, prevista nella prima parte della norma e contestata nel caso di specie, di chi, a monte, "falsifica" detti strumenti di pagamento.

all'associazione per delinquere. Un aspetto, questo, dirimente ai fini del giudizio di responsabilità dei ricorrenti, in virtù della clausola di salvaguardia contenuta nell'art. 648 *bis* c.p. La Cassazione è giunta alla conclusione che in simili ipotesi venga il rilievo il reato di riciclaggio, sul presupposto che, in caso di contestualità del passaggio di denaro dalla carta clonata alla carta prepagata, la condotta contestata agli imputati effettivamente costituisce una delle modalità esecutive della frode informatica, di tal ché la frode non si consuma se non nel momento in cui avviene il contestuale trasferimento dei fondi dai conti correnti, delle ignare vittime della clonazione delle carte bancomat, alle carte prepagate intestate agli imputati. In questa chiave di lettura, la condotta di questi ultimi si strutturava come strumentale al raggiungimento dello scopo finale cui tutta l'operazione illecita era preordinata, acquistando una sua autonoma rilevanza quale fattispecie penale, proprio in virtù del fatto, incontestato, che detti imputati non avevano partecipato al reato di cui all'art. 55, comma 9 d.lgs. 231/2007, nella modalità prima indicata.

L'esclusione *a priori* di un contributo del *financial manager* in termini di concorso nel reato di phishing, in realtà, lascia perplessi in quanto occorrerebbe valutare caso per caso quando ha inizio l'attività criminosa di quest'ultimo rispetto alla genesi del reato di phishing. Il problema però è più ampio.

La diversa identificazione della fattispecie imputabile al *financial manager*, nei casi in esame, infatti, è inevitabilmente correlata al *tempus commissi delicti* del reato di phishing – e relativo *locus*. Sul punto l'orientamento consolidato della Cassazione opta per quello in cui il soggetto agente consegua l'ingiusto profitto[49]; alcune pronunce[50] di legittimità, però, individuano il *tempus com-*

[49] Cfr. *ex multis* Cass., Sez. II, 5 febbraio 2020, n. 10534, Gerbino, Rv. 278518, secondo cui: «il reato di frode informatica, che ha la medesima struttura ed elementi costitutivi della truffa, si differenzia da quest'ultima in quanto l'attività fraudolenta investe non il soggetto passivo (rispetto al quale manca l'induzione in errore), bensì il sistema informatico di pertinenza del medesimo. Il momento consumativo del reato di cui all'art. 640-ter c.p. coincide quindi con quello in cui il soggetto agente consegue l'ingiusto profitto». Tale orientamento, elaborato in tema di truffa, si è affermato a partire da una sentenza delle Sezioni unite della fine degli anni '60, secondo la quale il reato di truffa può dirsi perfezionato «soltanto con l'effettivo conseguimento del bene economico o di altro bene che sia idoneo ad una valutazione patrimoniale, con la definitiva perdita di esso da parte del soggetto passivo». Cfr. Cass., Sez. un., 22 marzo 1969, in *Foro it.*, 1970, II, 5 ss.; Cass., Sez. II, 30 novembre 1974, Forneris, in *Cass. pen.*, 1975, 751 ss. In tale occasione fu risolto un contrasto interpretativo sorto in seno a due diverse concezioni del patrimonio: una concezione c.d. giuridica, in base alla quale sarebbe sufficiente, per la consumazione del reato, che l'atto di disposizione della vittima abbia inciso negativa-

missi delicti nel momento in cui il soggetto agente sia intervenuto sui dati del sistema informatico, in modo da modificarne il funzionamento rispetto a quanto in precedenza possibile, non essendo necessaria una effettiva alterazione dei programmi inseriti nel "server", così anticipando il momento consumativo alla fase dell'intervento "senza diritto".

La prima opzione interpretativa, dunque, si basa sulla individuazione della natura di reato di danno della truffa – e pertanto della derivata ipotesi di phishing – che si consuma con la effettiva *deminutio patrimonii* della persona offesa; la seconda, invece, presuppone che tale reato sia di mera condotta. D'altronde l'individuazione del momento consumativo, già nell'atto di disposizione, è stata anche autorevolmente sostenuta sul presupposto che «se in materia di truffa la determinazione della competenza territoriale offre delle difficoltà, ciò è dovuto alla qualità dell'evento consumativo (...), che non è a prima vista individuabile e circoscrivibile come, poniamo nell'omicidio o nel danneggiamento. L'evento della truffa non intacca la sostanza fisica dei beni: incide solo sui rapporti patrimoniali (rapporti fra soggetto e beni, rapporti fra soggetto e altri soggetti), alterando in peggio, o estinguendo, rapporti preesistenti, oppure facendo sorgere nuovi rapporti sfavorevoli al soggetto»[51]. Partendo da simili premesse in tema di frode[52], e focalizzando l'attenzione sulla peculiarità di tale tipologia di reato rispetto altre forme di aggressione patrimoniale contemplate nel nostro ordinamento, si è valorizzato il nesso causale sussistente tra l'errore nel quale è stata indotta la vittima del raggiro e le conseguenze patrimoniali (il profitto ingiusto con altrui danno) nelle quali si sostanzia l'offesa, il che comporta necessariamente la cooperazione della vittima

---

mente sul "complesso dei rapporti giuridici che attengono ad una persona o ad un ente", e una concezione c.d. economica, secondo la quale quell'effetto potrebbe prodursi solo in presenza di un "danno concreto ed effettivo del patrimonio", che si realizzerebbe allorquando il reo sia giunto effettivamente in possesso del bene altrui. Per un approfondimento in tema si veda PECORELLA, *Truffe on-line: momento consumativo e competenza territoriale*, in *Riv. it. dir. proc. pen.,* 2012, 113 ss.

[50] *Ex multis* cfr. Cass., Sez. II, 10 maggio 2019, n. 36359, T. N., Rv. 268252; Cass., Sez. V, 19 febbraio 2015, n. 32283, C. P., Rv. 264349; Cass., Sez. III, 24 aprile 2012, n. 23798, Casalini, Rv. 2353633, che ha puntualizzato: «Nel reato di frode informatica il momento consumativo va individuato nel luogo di esecuzione della attività manipolatoria del sistema di elaborazione dei dati, che può coincidere con il conseguimento del profitto anche non economico».

[51] PEDRAZZI, *Postilla circa la competenza per territorio in materia di truffa*, in *Riv. it. dir. proc. pen.*, 1958, ora in PEDRAZZI, *Diritto penale*, vol. II, *Scritti di parte speciale*, Milano, 2003, 361.

[52] *Ibid.*

nella produzione del danno; una cooperazione, in particolare, in grado di produrre direttamente quelle conseguenze patrimoniali senza la necessità di un'ulteriore attività del reo, perché altrimenti sussisterebbe un altro tipo di offesa al patrimonio, contraddistinta da un'aggressione diretta, a usurpazione unilaterale.

La soluzione non è così agevole; anche perché, come detto, tali problemi in materia di phishing si acuiscono, data la debolezza della fattispecie tipica.

Ne consegue che qualora si acceda alla tesi tradizione di reato di danno, il contributo del *financial manager* debba integrare il concorso nella frode informatica, diversamente dal secondo caso in cui dovrebbe elevarsi a fattispecie autonoma di riciclaggio, come di recente confermato in giurisprudenza[53]. Nel primo caso, però, occorrerà provare che lo stesso abbia contribuito personalmente e direttamente all'attività fraudolenta, o che abbia apportato un contributo morale in termini di istigazione o rafforzamento del proposito criminoso altrui. Così che il momento consumativo coinciderà con l'effettivo conseguimento del profitto ingiusto. Nel secondo caso, invece, occorrerà la consapevolezza della provenienza delittuosa del denaro ricevuto, o la concreta possibilità di rappresentarselo, accettandone il rischio[54], unitamente allo scopo ulteriore di far perdere le tracce della relativa origine illecita. In tale ipotesi, pertanto, il *tempus commissi delicti*[55] andrà individuato nel momento in cui venga posta in essere una singola operazione idonea a ostacolare l'identificazione del bene, la quale può determinarsi in modo progressivo sino ad arrivare alla realizzazione di un ostacolo così pregnante da integrare un vero e proprio impedimento.

Di certo, gli evidenziati e più attuali approdi interpretativi, anche quanto al contributo del *financial manager*, confermano l'esigenza di un intervento legi-

[53] Cfr. Corte di Appello di Ancona, 23 febbraio 2021, n. 1607, in *DeJure*, secondo cui: «il solo accreditamento sul proprio conto corrente ed il conseguente prelievo del denaro proveniente da prelievi e bonifici online non autorizzati (phishing) pur attuati da terzi (senza certezza di poter ricondurre l'imputato anche a tale attività criminosa), integra il solo reato di riciclaggio; per il quale, ai fini dell'elemento soggettivo è sufficiente che ricorra il dolo eventuale, e cioè l'accettare il rischio che le somme siano di provenienza delittuosa».

[54] Cass., Sez. II, n. 36893, 28 maggio 2018, Franchini, Rv. 274457.

[55] Cfr. Tribunale di Milano, Sez. I, 27 ottobre 2021, n. 43315, Rv. 282314; Cass., Sez. II, 21 settembre 2016, n. 46321, M. C., Rv. 268401.

slativo in materia. Il concorso di persone nel reato per sua natura nasce dal combinato disposto dell'art. 110 c.p. con la fattispecie tipica di riferimento, ma se questa, già carente di tipicità, viene oltremodo estesa, i problemi in termini di garanzie – che geneticamente connotano il concorso di persone, soprattutto nel minato terreno del dolo di partecipazione[56] – diventano irrisolvibili.

3.3. *Le decisioni ABF quale indirizzo "disorientante".* È giunto il momento di dedicare all'ABF una maggiore attenzione con una dovuta premessa. Il presente *focus* è unicamente finalizzato a dimostrare – o tentare di dimostrare – che la carente tipizzazione delle ipotesi di phishing, unitamente al silenzio del legislatore e all'altalenante giurisprudenza, determina delle invasioni in materia da parte dell'ABF che, in quanto organo mediatore, stragiudiziale, di natura prettamente civilistica, non dovrebbe avere alcuna competenza – legittimità – in materia penale e per questo non dovrebbe nemmeno provare a "orientare" in detta materia. Il diritto penale, però, entra ormai nelle decisioni dell'ABF, e non più solo indirettamente.

L'Arbitro Bancario Finanziario (ABF) è un sistema di risoluzione alternativa delle controversie (in inglese ADR – *Alternative Dispute Resolution*) che possono sorgere tra i clienti e le banche o gli altri intermediari in materia di operazioni e servizi bancari e finanziari. È un organismo indipendente e imparziale nei compiti e nelle decisioni, sostenuto nel suo funzionamento dalla Banca d'Italia. Le decisioni dell'ABF non sono vincolanti ma, qualora non rispettate dall'intermediario, la notizia del loro inadempimento è resa pubblica su un sito internet dedicato per un periodo di 5 anni ed evidenziato sulla *home page* del sito internet dell'intermediario per la durata di 6 mesi.

Recentemente si è assistito a casi di conflittualità interpretativa, soprattutto in tema di onere della prova da parte della banca e di oneri di sicurezza da predisporre per evitare casi di frodi informatiche ai danni di clienti, tra giurisprudenza e ABF. Conflittualità che desta non poche perplessità visto che: «pro-

[56] Per un recente approfondimento del tema, si veda SEMINARA, *Sul "dogma" dell'unità del reato concorsuale*, in *Riv. it. dir. proc. pen.*, 3, 789, 2021; ID., *Accessorietà e fattispecie plurisoggettiva eventuale nel concorso di persone nel reato. Considerazioni sul senso di una disputa dottrinale*, in *Riv. it. dit. proc. pen.*, 2, 2021, 421.

prio l'obiettivo di assicurare una tutela effettiva dei clienti rende ineludibile il confronto e il raccordo con l'Autorità Giudiziaria e con i suoi precedenti, soprattutto di legittimità, non potendo l'Arbitro "isolarsi" dal sistema della tutela giurisdizionale dei diritti, se non rinunciando alla sua funzione (anche "prognostica") e alla sua autorevolezza»[57].

Per meglio comprendere il problema, appare opportuno seguire "il cammino" di una vittima di *phishing*. Per prima cosa andrà in un posto di Polizia per denunciare l'accaduto, per poi recarsi presso l'istituto di credito per disconoscere le operazioni oggetto di frode. Qualora la banca non riconosca la presenza di elementi tali da fondare la propria responsabilità, individuandone la causa esclusiva nella negligente condotta tenuta dal cliente, il soggetto potrà rivolgersi all'ABF e, qualora questa non accolga il ricorso, alla giustizia civile. Parallelamente, viene esercitata l'azione penale a seguito della denuncia sporta.

Torniamo, però, alle pronunce dell'ABF, nel cui ambito sono frequentemente individuate, sebbene non vi sia alcun fondamento normativo a sostegno, due distinte tipologie di *phishing* da cui dipenderebbe un differente standard di diligenza doverosa: «in particolare, il Collegio di Coordinamento (decisioni nn. 3498/2012 e 1820/2013) ha distinto: a) le ipotesi di *phishing* tradizionale caratterizzate dall'invio di un semplice messaggio *email*, telefonico (c.d. *vishing*) o SMS (c.d. *smishing*) con il quale si invita il cliente a digitare le proprie credenziali di accesso; molti dei tentativi di truffa posti in essere in materia di servizi di pagamento si svolgono secondo tale schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, email, sms o altri strumenti di comunicazione, a comunicare e/o ad inserire su dispositivi (Decisione N. 10070 del 15 aprile 2021 Pag. 5/6) o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza; b) la forma, più insidiosa, consistente in un "subdolo meccanismo di aggressione [che] ha luogo attraverso un sofisticato metodo di intru-

[57] TUCCI, *L'Arbitro bancario finanziario tra trasparenza bancaria e giurisdizione*, in *Banca borsa tit. cred.*, 2019, 625.

sione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino". Tra le due fattispecie vi è una differenza tale da indurre a ritenere che solamente nella seconda, consistente in una sofisticata intrusione nell'autentico sito dell'intermediario nel momento in cui l'utente vi accede per compiere un'operazione, debba escludersi la sussistenza di una colpa grave del cliente»[58]. In questa decisione l'ABF entra a gamba tesa nel merito della tipizzazione e dei limiti alla meritevolezza di tutela[59].

Diciamo che quello che avrebbe dovuto fare il legislatore sul piano della tipicità, ma anche la giurisprudenza nel suo confronto con un precetto sfuggente e inadeguato, viene "risolto" dall'ABF – "giurisprudenza dottrinale"[60], si è detto – efficace sintesi post-moderna non solo di tutti i formanti, ma soprattutto dei poteri giudiziario e legislativo. Senza alcuna legittimazione, evidentemente, né sotto l'uno né sotto l'altro aspetto.

4. *Legalità e nuove tipologie di frodi informatiche: una prospettiva di riforma.* A fronte di rilievi che risalgono già all'introduzione della fattispecie di frode informatica, l'unica risposta del legislatore, evidentemente del tutto inadegua-

[58] Cfr. ABF, Collegio di Napoli, Decisione n. 10070 del 15 aprile 2021, in *www.arbitrobancariofinanziario.it*.

[59] Ulteriori esempi di intromissioni illegittime da parte dell'ABF si possono individuare in materia di furto del Bancocard sottratto alla vittima con una peculiare modalità: questa, di solito in macchina, viene distratta dal soggetto che carpisce la sua attenzione indicandole oggetti o monetine in terra, in prossimità dell'auto, così che la stessa si determina a scendere, lasciando l'auto aperta e all'interno, incustodita, la borsa. Nel frattempo, il ladro le sottrae la borsa con all'interno il BancoCard con cui poi vengono effettuate operazioni fraudolente. Nelle più recenti decisioni, l'ABF, (cfr. Collegio di Torino, Decisione n. 22593, del 3 novembre 2021) ha ricondotto tali ipotesi nella fattispecie di furto con destrezza. Tale organo avrebbe dovuto solo riportare la dinamica e occuparsi di temi afferenti alla responsabilità civile sussistente nei casi esaminati, ma così non è stato. Dette ipotesi, infatti, non vengono ricondotte dalla giurisprudenza di legittimità al furto con destrezza, bensì al furto aggravato dal mezzo fraudolento (*ex multis* cfr. Cass., Sez. V, 22 luglio 2019, n. 32847, Lazzari, Rv. 276924), ma l'ABF, addirittura arriva a puntualizzare: «tuttavia, il Collegio rileva che, in base al più recente orientamento dello stesso, la custodia congiunta non costituisce di per sé colpa grave del titolare dello strumento di pagamento nelle ipotesi di furto con destrezza, cui va assimilato il furto tramite l'artificio delle "chiavi smarrite"(cfr. Collegio di Torino, Decisione n. 22593, del 3 novembre 2021)». E nel ricondurre tali ipotesi al furto con destrezza, il conciliatore non cita pronunce della giurisprudenza penale, ma proprie decisioni.

[60] TUCCI, *L'Arbitro bancario finanziario*, cit., 643.

ta, è stata l'introduzione della circostanza aggravante di cui all'art. 640-*ter*, comma 3, c.p.

Sia dunque consentita qualche riflessione sul tema, nella prospettiva di un possibile approccio di riforma.

Accanto a una descrizione rigorosa delle condotte cui si intenda attribuire rilevanza, sarebbe innanzitutto opportuna l'introduzione nel Libro II del Codice penale di un titolo XIV, "*Dei delitti contro la sicurezza e la riservatezza informatica*", in cui far confluire anche le ipotesi già oggi previste (artt. 612 *ter*, 615 *bis*, *ter*, *quater*, *quinquies*, 616, 617 *bis*, *ter*, *quater*, *quinquies*, *sexies*, 618, 619, 620, 623 *bis* c.p.) – con eventuale ridefinizione strumentale ad innalzarne i coefficienti di determinatezza –, eventualmente enucleando capi autonomi cui ricondurre fattispecie peculiarmente eterogenee. D'altronde, individuare l'ambito di offensività di questa tipologia di illeciti nel solo patrimonio è sicuramente riduttivo. Vengono infatti in gioco, a titolo esemplificativo, il domicilio informatico inteso come *ius excludendi alios*, la "segretezza dei dati e dei programmi"[61], l'"intangibilità informatica", da intendersi come il diritto del titolare dei dati informatici a non subire uso e/o alterazione da parte di terzi non autorizzati, e così via. Nel contempo, la polarizzazione sul bene della sicurezza informatica consentirebbe di tutelare, in modo sinergico ma differenziato, sia l'interesse del singolo sia i suoi risvolti pubblicistici.

Una nuova tipizzazione della frode informatica, rispondente ai canoni di determinatezza e offensività, dovrebbe essere plausibilmente modulata su uno schema del tipo: «chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, anche attraverso l'induzione in errore del titolare di tali dati, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito [...]», formulazione adeguata a ricomprendere anche le diver-

[61] Al riguardo, la Cassazione – cfr. Cass., Sez. II, n. 26604, 29 maggio 2019, Fragasso, Rv. 276427 – nel ribadire l'impossibilità che le due ipotesi di cui agli artt. 615 ter e quater c.p. possano concorrere ha precisato che: «L'art 615-*ter* c.p., ovvero l'accesso abusivo al sistema informatico, serve a contrastare il fenomeno degli hacker, e protegge in maniera più incisiva il domicilio informatico tout court(inteso come spazio ideale di esclusiva pertinenza di una persona fisica o giuridica); mentre l'art. 615-*quater* c.p., che reprime condotte prodromiche, tutela la segretezza dei dati e dei programmi, già assicurata dall'incriminazione dell'accesso e della permanenza in un sistema informatico».

se tipologie di *phishing* e che, quand'anche non si ritenesse di operare una – comunque auspicabile – riforma organica del settore, potrebbe soccorrere già in una prospettiva di modifica del dato normativo di cui all'art. 640-*ter* c.p.
I tempi cambiano, la tecnologia corre veloce, ma l'unica risposta costituzionalmente corretta, pur implicante uno sforzo costante, razionale e complesso, di adeguamento del sistema normativo, certo non può "passare" per il sacrificio della legalità.