RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0116 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Paolo Caldarone

Il phishing bancario: principali strumenti di difesa e profili di responsabilità

Il contributo analizza la truffa informatica a danno degli istituti bancari, soffermandosi sui principali sviluppi giurisprudenziali e normativi compiuti dal legislatore comunitario e nazionale in materia di sicurezza delle nuove modalità di pagamento elettronico, concludendo con i diversi profili di responsabilità di *phisher* e financial manager.

Truffa informatica – Phishing – Sicurezza cibernetica – Dati personali

Banking phishing: main defense tools and responsibility profiles

The paper analyzes computer fraud to the detriment of banking institutions, focusing on the main case law and regulatory developments made by the EU and Italian legislation about new electronic payment methods security. In conclusion, different profiles of responsibility of phisher and financial manager are discussed.

Fraud – Phishing – Cybersecurity – Personal data

L'Autore è praticante avvocato e tirocinante *ex* art. 73 DL 69/2013 presso la Procura generale della Corte suprema di cassazione

1. Introduzione

Il presente lavoro concentra la propria attenzione sul *phishing* bancario nelle operazioni di pagamento elettronico a distanza, evidenziando i principali strumenti di attacco per l'accesso agli account sulla piattaforma di *internet banking* e le rispettive misure di sicurezza, concludendo con i diversi profili di responsabilità, tra cui quella dell'istituto bancario nei confronti del titolare di un conto corrente vittima di truffa informatica.

In particolare, il contributo si articolerà in tre parti. La prima sarà dedicata ad alcune considerazioni a carattere generale concernenti l'incessante aumento di incidenti cibernetici a livello mondiale e la presa di posizione del legislatore europeo, mediante l'introduzione di nuove misure di sicurezza e regole uniformi attraverso, soprattutto, le direttive PSD, PSD2, NIS 1 e la nuova NIS 2, e il loro recepimento dal legislatore nazionale, con l'obiettivo di incrementare le tutele dei consumatori nei c.d. pagamenti digitali all'interno dell'Eurozona. Nella seconda parte verranno analizzate le diverse tipologie di reati informatici a danno degli istituti bancari, specialmente i delitti di accesso abusivo ai sistemi informatici e telematici, nonché la truffa informatica e i suoi principali elementi distintivi rispetto al delitto di furto e di truffa, sia dal punto di vista normativo che giurisprudenziale, evidenziando le diverse lacune che sono state lasciate dal legislatore nazionale, in parte risolte con i molteplici interventi del giudice nomofilattico e dell'Arbitro Bancario e Finanziario. La terza parte, invece, si concentrerà sui diversi profili di responsabilità tra il *financial manager* e il *phisher* ravvisabile sia nel concorso di persone, nel caso in cui il direttore finanziario, consapevole dell'attività del c.d. "truffatore informatico" collabori con quest'ultimo aprendo un conto nuovo o mettendo a disposizione il suo personale per il trasferimento del provento illecito, sia nel concorso di reato con il delitto di riciclaggio, evidenziando gli interventi dell'ABF e della Cassazione in materia.

Le premesse di fondo consistono nel cercare di apportare chiarezza in una tematica in continua evoluzione e novità, cercando dove possibile, di evidenziare le soluzioni ricercate dagli studiosi nelle situazioni di conflittualità normative sia sostanziali che processuali da cui è caratterizzata la suddetta materia, poiché riguardano strumenti e tecnologie informatiche che mutano giorno per giorno, rendendo, pertanto, anche le condotte criminose del soggetto agente di difficile regolamentazione e inquadramento per garantire un corretto esercizio dell'azione penale.

2. L'introduzione e gli obiettivi della *Payment Services Directive* – PSD2 e le principali misure di sicurezza a tutela del cliente: lo *strong customer authentication*

L'incessante evoluzione delle moderne tecnologie informatiche e telematiche ha avuto una grande influenza anche nel settore bancario, estendendo le modalità di pagamento dell'utente, dal mondo reale alla dimensione digitale, attraverso sia l'utilizzo dello smartphone con la tecnologia NFC (*Near Field Communication*)[1], i sistemi Internet/WAP, il servizio SMS (*Smart Message Service*) a tariffazione maggioritaria e addebiti al pagatore per mezzo del gestore del servizio telefonico, sia i c.d. pagamenti elettronici che comprendono i pagamenti con carta a distanza attraverso l'invio dei dati via internet, la moneta elettronica[2] e i bonifici o addebiti diretti tramite il servizio di *internet banking*[3], sviluppato alla fine degli anni Ottanta, e consiste in un sistema che consente al cliente l'accesso ai servizi bancari attraverso la rete[4].

Numerosi e in costante aumento sono i gravi incidenti cibernetici, a cui la stampa ha dato risalto, e i più clamorosi hanno riguardato: il sovraccarico di lavoro del software di una nota banca di New York, generando, di conseguenza, problematiche relative alla consegna agli acquirenti dei titoli governativi ricevuti dai venditori certificati del Tesoro e attribuendo la responsabilità, per la mancata ricezione degli investimenti, in capo all'istituto bancario che fu costretto a richiedere un prestito, al tasso di interesse del 7,5% alla *Federal Reserve Bank*; e il blocco informatico del 1987, avvenuto al Centro informatico della *Federal Reserve Bank*, che impedì per un giorno intero sia le grandi transazioni interbancarie, causando un aumento del tasso d'interesse dal 7% al 30%, sia la disponibilità di liquidità per le grandi banche, determinando una ricerca disperata del contante da parte degli operatori bancari[5].

Negli ultimi anni il legislatore europeo è intervenuto nella regolamentazione dei servizi di pagamento con la direttiva 2007/64/CE[6] (la c.d. PSD[7] - *Payment Service Directive*), che ha consentito alle istituzioni europee di fondare un mercato unico europeo dei pagamenti al dettaglio (c.d. SEPA – *Single Euro Payment Area*), e con la più recente direttiva 2015/2366/UE[8] (la c.d. PSD2[9]), che ha

1. Rappresenta una tecnologia wireless che consente lo scambio di informazioni e la effettuazione di pagamenti tra due telefoni cellulari abilitati NFC quando si toccano o si avvicinano, attraverso un sistema di radiofrequenza (RFID), Jain-Dahiya 2015.
2. Disciplinata dal Parlamento europeo e dal Consiglio nella direttiva 2009/110/CE, che la definisce nell'art. 2 come «il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica», direttiva 2009/110/CE del Parlamento europeo e del Consiglio concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE.
3. Pascuzzi 2020, pp. 149-153.
4. Mukhtar 2015, pp. 1-5.
5. Sarzana 2010, pp. 15-17.
6. Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE, che abroga la direttiva 97/5/CE.
7. Il nostro ordinamento ha recepito la suddetta direttiva con il d.lgs. n. 11 del 27 gennaio 2010 "Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE".
8. Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.
9. L'Italia ha recepito la fonte europea con il d.lgs. n. 218 del 15 dicembre 2017, "Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE,

integrato il quadro normativo precedente, adeguandolo al fenomeno della *digital revolution*[10].

Più precisamente, l'intenzione del legislatore comunitario con la PSD è stata quella di disporre regole uniformi, fondate sulla trasparenza e sicurezza a tutela del consumatore, per promuovere l'utilizzo dei pagamenti elettronici e innovativi in tutta l'Eurozona, riducendo il costo di strumenti quali quelli cartacei e il contante; tuttavia, suddetta fonte unionale si è dimostrata inadeguata al fenomeno dell'*open banking*[11], che ha portato nuovi prestatori di servizi, operanti al di fuori dell'ambito bancario, e alle nuove modalità di pagamento, necessitando di strumenti di sicurezza più rigidi a tutela dei consumatori, determinando l'introduzione della direttiva PSD2.

Le nuove misure di sicurezza, finalizzate a ridurre il rischio che si verifichino operazioni di pagamento non autorizzate dall'utente, introdotte dalla direttiva, impongono la c.d. autenticazione forte (*Strong Customer Authentication*), una procedura finalizzata a verificare l'identità dell'utente e la validità dell'uso di uno specifico sistema di pagamento basata, ai sensi dell'art. 4 n. 30 della direttiva PSD2, «sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione»[12].

L'ambito di applicazione della nuova direttiva non si riferisce più soltanto ai classici enti creditizi e Istituti di Pagamento (IP), ma si estende anche a Banche, Istituti di Moneta Elettronica (IMEL), imprese diverse da quest'ultimi, autorizzati a prestare i servizi di pagamento dall'Autorità di Vigilanza che consentono di ampliare, sfruttando le potenzialità delle nuove tecnologie (come ad esempio: smartphone), il settore dei pagamenti elettronici[13].

3. La truffa informatica e la sua apparente similitudine al delitto di furto e di truffa: la classificazione del *phishing* nel diritto interno e la principale tecnica di attacco informatico nel settore bancario

Nello scenario attuale e ancor di più nel futuro, dove la quasi totalità delle azioni umane sfruttano e sfrutteranno innumerevoli servizi digitali, interconnessi e comunicanti, la truffa informatica è divenuta, pariteticamente all'implementazione di misure sempre più efficienti ed efficaci per la mitigazione del rischio *cyber*, un fenomeno criminoso ontologicamente in evoluzione e difficile da classificare, in quanto sono molteplici le tecniche con cui viene messa in atto; ciononostante, sono tutte accomunate dall'influenza psicologica sulla vittima e dalla strumentalizzazione dell'identità digitale di un soggetto, con finalità di ingiusto profitto.

Tale trasformazione digitale e i rischi, che si concretizzano in attacchi molto più devastanti di quelli visti fino ad ora, hanno avuto conseguenze anche in ambito penale, aprendo un forte dibattito tra gli studiosi per individuare la "giusta" tutela normativa dei nuovi beni giuridici informatici e, in rapporto alla *quaestio iuris*, due sono state le

2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta".

10. Il suddetto fenomeno ha portato alla nascita della c.d. Fintech, che semanticamente deriva dall'unione della parola "finanza" e "tecnologia" ed è traducibile in "tecnologia applicata alla finanza" e consiste in un ampio insieme di innovazioni che sono rese possibili dall'impiego delle nuove tecnologie sia nell'offerta di servizi agli utenti sia nei processi produttivi interni agli operatori finanziari, D'Agostino-Munafò 2018, p. VIII.
11. Consiste in un nuovo modello bancario che garantisce alle terze parti, fornitrici di servizi finanziari (TPP), un accesso libero a servizi bancari, transazioni e altri dati finanziari dei clienti tramite l'uso di interfacce tecnologiche intertemporali API (*Application Programming Interface*), rimuovendo l'esclusiva concentrazione delle informazioni finanziarie in capo alle banche tradizionali e consentendo la condivisione di dati e conti, Ferretti 2021, p. 4.
12. Sica-Sabatino 2021, pp. 1-4.
13. Olivieri 2021, pp. 450-454.

soluzioni: introdurre nuove fattispecie criminose o utilizzare norme già esistenti, adattandole, per via interpretativa, alle nuove esigenze.

Sebbene in un primo momento le c.d. truffe online siano state ricondotte all'art. 640 c.p.[14], per evitare sia forzature interpretative che la violazione del principio di legalità, in quanto alcuni comportamenti non potevano essere ricondotti alle fattispecie tradizionali[15], successivamente, il legislatore nazionale ha disciplinato, con la legge n. 547 del 23 dicembre 1993[16] e rispettive modifiche, il delitto di truffa informatica nell'art. 640-*ter* c.p.[17] individuando come oggetto di tutela il patrimonio del soggetto danneggiato, la regolarità del funzionamento del sistema telematico e informatico e, infine, la riservatezza nel suo utilizzo[18].

Dal punto di vista classificatorio, i reati informatici comprendono sia quelli commessi mediante l'uso delle tecnologie informatiche sia quelli in danno alle tecnologie stesse; inoltre, la dottrina ha distinto i reati commessi su Internet, riconducendo tutti quei crimini che non potrebbero essere attuati in assenza delle tecnologie informatiche, dai reati commessi attraverso Internet, intendendo la rete come mero strumento di supporto per la realizzazione dell'illecito e, di conseguenza, riferendosi ai c.d. reati tradizionali già contemplati nel codice penale e nelle leggi speciali[19].

La forma più comune di attacco informatico è quella del *deceptive phishing*, ossia il c.d. "phishing[20] ingannevole", in cui il truffatore si appropria di tutti i codici bancari dell'utente, condizionandolo a cliccare, attraverso l'invio di una email piuttosto similare a quella dell'istituto bancario, su un link, oggetto del messaggio, che lo indirizzerà ad una pagina web, pressoché identica a quella del sito ufficiale, dove dovrà inserire tutte le informazioni necessarie per accedere all'*internet banking*[21].

14. Cfr. Alibrandi-Corso 2022, p. 315. Nel delitto di truffa «Chiunque, con artifizi o raggiri, inducendo taluno in errore, 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 pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: 1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità; 2-*bis*. se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente».
15. Bartoli-Pelissero-Seminara 2020, pp. 331-333.
16. Legge 23 dicembre 1993, n. 547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
17. Cfr. Alibrandi-Corso 2022, pp. 315-316. Ai sensi dell'articolo in esame la frode informatica punisce «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 pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema. 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. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età».
18. Bartoli-Pelissero-Seminara 2020, pp. 333-334.
19. Circelli 2015, pp. 132-133.
20. In particolare, il *phishing* è una truffa attraverso la quale si persuade il destinatario con la simulazione di messaggi elettronici di noti fornitori di servizi, per ottenere informazioni riservate dell'utente, D'Agostino-Panebianco 2020, p. 242.
21. Cipolla 2012, pp. 2686-2688.

Dal punto di vista definitorio, si è pronunciato anche il giudice di legittimità al riguardo, definendo il *phishing* come «quell'attività illecita in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici c.d. *malware*) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (user e password) di un utente, codici che, poi, utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancari o postali che vengono rapidamente svuotati»[22].

In relazione alla struttura del reato di *phishing* si può individuare, apparentemente, una similitudine al delitto di truffa, in quanto ricomprende una moltitudine di condotte fraudolente idonee a conseguire un profitto e un danno alla vittima, e di furto, poiché l'aggressione è unilaterale; tuttavia, gli elementi distintivi in relazione al furto, consistono nella realizzazione dell'evento di profitto e di danno[23], mentre in rapporto alla truffa, mancano nella struttura oggettiva della condotta punibile sia l'induzione in errore della vittima sia gli artifici e i raggiri commessi dal soggetto agente, entrambi difficilmente realizzabili con una macchina, in quanto priva delle caratteristiche dell'essere umano[24]. Infatti, la Cassazione[25] ha precisato che «il reato di frode informatica si differenzia dal reato di truffa 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 della medesima, attraverso la manipolazione di detto sistema». Tuttavia, come il reato di truffa, anche quella informatica prevede come elemento psicologico in capo al soggetto agente del reato, il dolo generico, consistente nella consapevolezza e nella volontà di procurare a sé o ad altri un profitto ingiusto con altrui danno, sulla base del risultato irregolare di un procedimento di elaborazione di dati, ottenuto mediante l'alterazione del sistema di funzionamento dell'elaboratore, ovvero intervenendo senza esserne autorizzati sui dati o sulle informazioni oggetto di trattamento[26].

Prima di analizzare la condotta incriminatrice del *reo*, è importante porre alcune definizioni semantiche: per sistema informatico si intende un sistema completo di apparecchiature di elaborazione composto sia da elementi hardware, sia da elementi software, funzionanti in reciproca implementazione; il sistema telematico, invece, è il complesso di elementi che costituiscono un'apparecchiatura per la trasmissione a distanza di dati; tuttavia, entrambi devono essere dotati di misure di sicurezza volte a selezionare ed individuare i soggetti abilitati all'accesso al sistema protetto[27].

Per quanto riguarda la condotta fraudolenta tenuta dall'autore del reato, questa può realizzarsi in qualsiasi modalità ma deve necessariamente consistere in un'alterazione di un sistema informatico o telematico, con modalità diverse, attraverso la quale gli schemi predefiniti del sistema vengono modificati o manipolati, al fine di perseguire un ingiusto profitto con l'altrui danno; ovvero, l'intervento, con qualsiasi modalità, sui dati, le informazioni o i programmi contenuti nel sistema, al fine di realizzare un ingiusto profitto con l'altrui danno[28].

La fattispecie criminosa in esame prevedeva, inizialmente, due ipotesi di circostanze aggravanti: la prima si riferiva essenzialmente al caso in cui il fatto veniva commesso ai danni dello Stato; la seconda, invece, al fatto commesso con abuso della qualità di operatore di sistema, una nozione atecnica in quanto comprende qualsiasi mansione che implichi l'attività di utilizzazione di un

22. Cass. pen., sez. II, sentenza 11 marzo 2011, n. 9891.

23. Bartoli-Pelissero-Seminara 2020, pp. 334-336.

24. Bartoli 2011, pp. 384-387.

25. Cass. pen., sez. II, sentenza 11 novembre 2009, n. 44720.

26. Dolcini-Gatta 2021, pp. 2668-2670.

27. Fiandaca-Musco 2020, pp. 362-365.

28. *Ivi*, pp. 205-207.

elaboratore[29]. Con la novella del 2021[30], il legislatore nazionale ha introdotto una nuova circostanza aggravante per il delitto di cui all'art. 640-*ter* c.p. nel caso in cui il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale, in risposta alla necessaria sanzione di suddetta condotta prevista dall'art. 6 della direttiva 2019/713/UE[31], contrapponendo la valuta virtuale a quella monetaria, senza, tuttavia, rispettare la specifica indicazione del legislatore europeo che, come specificato nell'art. 2 lett. d) della medesima direttiva, si concentra sulla tutela penale della sola valuta che abbia una certa diffusione sul mercato[32].

Dal punto di vista giurisprudenziale sono molteplici gli interventi da parte della Cassazione in materia di frode informatica, che hanno permesso di colmare diverse lacune applicative di suddetta fattispecie da parte del legislatore nazionale. In particolare, il giudice di legittimità con sentenza n. 47302/2021 ha escluso per la consumazione del delitto di truffa aggravata ai danni dello Stato, la condotta relativa alla sostituzione di schede "clonate" nelle slot machine che alterava il funzionamento del sistema informatico di suddette apparecchiature, impedendo la comunicazione dei dati delle giocate effettive all'Amministrazione finanziaria, in quanto costitutive del delitto di frode informatica[33].

Oltre a ciò, con sentenza n. 40862/2022, il giudice nomofilattico ha precisato, in relazione all'aggravante prevista all'art. 640-*ter* c.p., la portata applicativa della nozione di "identità digitale" applicandola anche per l'accesso alla piattaforma di *home banking* gestita da privati. In particolare, ha statuito che «in tema di frode informatica, la nozione di "identità digitale", che integra l'aggravante di cui all'art. 640-*ter*, comma terzo, c.p., non presuppone una procedura di validazione adottata dalla Pubblica amministrazione, ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati»[34].

Giova, inoltre, indicare la recentissima sentenza n. 13713/2023 con cui la Corte di Cassazione ha chiarito che l'elemento specializzante del reato di cui all'art. 640-*ter* c.p. è rappresentato dall'utilizzazione fraudolenta del sistema informatico, poiché costituisce presupposto assorbente rispetto alla portata generica del delitto di indebita utilizzazione di carte di pagamento di cui all'art. 55, comma 9, d.lgs. 21 novembre 2007, n. 231. Infatti, ha statuito che «integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di pagamento di cui all'art. 55, comma 9, d.lgs. 21 novembre 2001, n. 231, la condotta di chi, servendosi di carte per l'erogazione di carburante in precedenza clonate, acceda ai sistemi informatici predisposti presso i relativi impianti, con successivo prelievo abusivo di carburante»[35].

Quest'ultima sentenza è risultata fondamentale, in quanto ha risolto le complicanze interpretativo-applicative a cui il quadro normativo è stato sottoposto con le integrazioni verificatesi mediante l'attuazione della direttiva 2019/713/UE nel nostro ordinamento, che faceva ritenere, l'uso di codici

29. Parodi 1997, pp. 1540-1545.

30. Art. 2 del d.l. 8 novembre 2021, n. 184, "Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio".

31. Infatti, l'articolo in questione prevede che «Gli Stati membri adottano le misure necessarie affinché l'atto di effettuare o indurre un trasferimento di denaro, di valore monetario o di valuta virtuale, arrecando illecitamente a terzi una perdita patrimoniale allo scopo di procurare un ingiusto profitto all'autore del reato o a una terza parte sia punibile come reato, se commesso intenzionalmente nel modo seguente: a) ostacolando, senza diritto, il funzionamento di un sistema di informazione o interferendo con esso; b) introducendo, alterando, cancellando, trasmettendo o sopprimendo, senza diritto, dati informatici», direttiva (UE) 2019/713 del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio.

32. Crescioli 2022, pp. 10-11.

33. Cass. pen., sez. II, sentenza 14 settembre 2021, n. 47302.

34. Cass. pen., sez. II, sentenza 20 settembre 2022, n. 40862.

35. Cass. pen., sez. II, sentenza 9 febbraio 2023, n. 13713.

e numeri di carte di credito clonate per penetrare abusivamente il sistema informatico bancario ed effettuare operazioni indebite, come condotta non soltanto integrativa del delitto di frode informatica, bensì anche realizzazione del delitto di indebita utilizzazione di carte di pagamento [36].

Gli interventi da parte della Cassazione non hanno riguardato, tuttavia, soltanto profili sostanziali di suddetta fattispecie criminosa, bensì anche alcuni aspetti processuali riguardo il giudice territorialmente competente. Infatti, in relazione a suddetto profilo, sebbene il giudice territorialmente competente in materia di truffa informatica sia molto difficile da identificare, soprattutto attraverso il criterio generale del *locus commissi delicti*, ai sensi dell'art. 8, comma 1, c.p.p., a causa della moneta elettronica che consente l'utilizzo della carta in qualsiasi sportello ATM (*Automated Teller Machine*) ed operazioni di bonifici on-line, il giudice nomofilattico ha chiarificato suddetta questione[37], attribuendo la competenza al giudice del luogo in cui si è verificata l'esecuzione dell'attività manipolatoria del sistema, spostando l'attenzione al momento e, non soltanto al luogo in cui l'autore dell'illecito consegue l'ingiusto profitto, con la conseguente *deminutio patrimonii* della vittima, mentre nel caso in cui l'operazione avvenga mediante i sistemi di trasferimento bancario on-line, il giudice di legittimità[38] si è pronunciato individuando come competente il giudice del luogo in cui il destinatario ha aperto il conto corrente presso l'istituto bancario[39].

Occorre, inoltre, evidenziare che da suddetta condotta emergono diversi profili di responsabilità inerenti il *data breach*[40] ed il principio di accountability[41], in capo al titolare del trattamento di dati e al suo specifico obbligo di istruzione e formazione; infatti, la Suprema Corte di Cassazione ha precisato che «in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema [il che rappresenta interesse degli stessi operatori], è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo. Ne consegue che, anche prima dell'entrata in vigore del d.lgs. n. 11 del 2010, attuativo della direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, la banca, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente»[42].

4. I diversi profili di responsabilità tra *financial manager* e *phisher*: il concorso tra ricettazione e frode informatica, l'intervento dell'ABF e la recentissima sentenza della Cassazione n. 7214 del 2023

Nelle frodi informatiche ruolo centrale è rivestito dal *financial manager*, cioè colui che riceve, in accordo con il *phisher*, le somme sottratte

36. Crescioli 2022, p. 4.
37. Cass. pen., sez. II, sentenza 17 marzo 2020, n. 10354.
38. Cass. pen., sez. feriale, sentenza 8 settembre 2016, n. 37400.
39. Pecorella 2012, pp. 113-116.
40. Per violazione dei dati personali; il c.d. *data breach*, ai sensi dell'art. 4, n. 12 GDPR, è «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati», regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
41. Introdotto proprio dal GDPR secondo il quale il titolare del trattamento deve adottare le misure adeguate ed attuare i principi e le disposizioni del regolamento conformemente alle caratteristiche specifiche del trattamento e comprovare di avere svolto suddetta attività, Finocchiaro 2022, p. 312.
42. Cass. civ., sez. I, sentenza 3 febbraio 2017, n. 2950.

indebitamente da quest'ultimo e le trasferisce, dopo aver ricevuto il proprio corrispettivo, dal proprio conto a terzi, attraverso l'utilizzo delle piattaforme che svolgono in necessari servizi.

In relazione alla condotta tenuta dal direttore finanziario si possono configurare due profili criminologici: da un lato, sussiste il concorso, ai sensi dell'art. 110 c.p., nel delitto di frode informatica, nel caso lo stesso sia consapevole dell'attività illegale compiuta dal *phisher*, tanto da assicurarne la propria collaborazione; dall'altro, nel caso in cui, lo stesso non è a conoscenza della condotta ma comunque mette a disposizione il proprio conto per il trasferimento del provento illecito – o ne apre uno a tal fine – e successivamente, trasferisce denaro a terzi, risponde di ricettazione o riciclaggio, a titolo di dolo eventuale[43].

Dal punto di vista giurisprudenziale sono molteplici le pronunce che non riconoscono un concorso di reati tra frode informatica e riciclaggio nei confronti del *financial manager*[44], mentre altre[45] sostengono che risponde, nel caso in cui il medesimo è consapevole della frode e assicura la propria collaborazione, di concorso nell'attività delittuosa, senza commettere ulteriori crimini[46]. Più precisamente, in quest'ultima ipotesi il dolo di ricettazione sussiste solo nel caso in cui, in base a precisi elementi di fatto, il direttore finanziario si sia rappresentato l'eventualità che le somme di denaro trasferite derivano da attività illecita e ne abbia comunque trasferito a terzi i proventi[47].

Inizialmente, sul profilo di responsabilità tra il *financial manager* e l'autore della frode informatica, in mancanza di interventi della giurisprudenza di legittimità e del legislatore nazionale, si è espresso l'Arbitro Bancario Finanziario[48] (ABF)[49], sebbene tali decisioni siano prive di vincolatività rispetto alle pronunce giurisprudenziali, tuttavia, devono essere rispettate dall'intermediario finanziario. In particolare, le decisioni del Collegio di coordinamento nn. 3498/2012[50] e 1820/2013 hanno distinto le truffe informatiche in ipotesi di *phishing* tradizionale via email, telefonico (c.d. *vishing*) e via SMS (c.d. *smishing*) con il quale si invita il cliente a digitare le proprie credenziali di acceso su una piattaforma di *internet banking* simile a quella ufficiale[51].

Inoltre, la decisione n. 1820/2013 ha sancito che nel caso di specie, il prelievo fraudolento effettuato sul conto corrente del cliente mediante bonifico non autorizzato è dipeso dalla negligenza di quest'ultimo, poiché la frode è stata attuata con modalità note dai consociati e di immediata riconoscibilità anche per un utente non esperto, dato che il messaggio email del *phisher* era inviato da un indirizzo assolutamente generico, redatto con un

43. Di Paolo 2017, pp. 14-19.

44. In particolare, la Cassazione ha precisato che «Nel phishing (truffa informatica effettuata inviando una email con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati quali numero di carta di credito, password di accesso al servizio di *home banking*, motivando tale richiesta con ragioni di ordine tecnico), accanto alla figura dell'hacker (esperto informatico) che si procura i dati, assume rilievo quella collaboratore prestaconto che mette a disposizione un conto corrente per accreditare le somme, ai fini della destinazione finale di tali somme. A tal riguardo, il comportamento di tale soggetto è punibile a titolo di riciclaggio ex art. 648-*bis* c.p., e non a titolo di concorso nei reati con cui si è sostanziato il *phishing* (art. 615-*ter* e 640-*ter* c.p.), giacché la relativa condotta interviene, successivamente, con il compimento di operazioni volte a ostacolare la provenienza delittuosa delle somme depositate sul conto corrente e successivamente utilizzate per prelievi di contanti, ricariche di carte di credito o ricariche telefoniche», Cass. pen., sez. II, sentenza 9 febbraio 2017, n. 10060.

45. Cass. pen., sez. II, sentenza 17 giugno 2011, n. 25960.

46. Reccia 2022, pp. 13-20.

47. Piancastelli 2015, pp. 6-7.

48. Per approfondire si segnala: Muttini 2021, pp. 41 ss.

49. L'ABF è un sistema di risoluzione stragiudiziale, alternativo, più rapido e meno costoso della giustizia ordinaria, competente per le controversie che possono nascere tra i clienti, le banche e gli intermediari finanziari ed è attivo dal 2009, Morera 2023, pp. 24-26.

50. Arbitro Bancario Finanziario, decisione 26 ottobre 2012, n. 3498.

51. Calisai 2015, pp. 83-85.

italiano approssimativo, con errori lessicali e grammaticali e, pertanto, non sussiste alcuna responsabilità in capo all'intermediario finanziario[52].

È opportuno precisare che, ai sensi dell'art. 9, comma 1, del d.lgs. 27 gennaio 2010, n. 11 (novellato dalla direttiva PSD2), si considera contestata l'operazione disconosciuta dal cliente nel termine di 13 mesi dalla data di addebito[53].

Per quanto riguarda gli oneri probatori in capo alla banca, gli viene richiesto di dimostrare la corretta autenticazione del cliente sul sito di *internet banking*, attraverso la produzione dei c.d. log, nonché la colpa grave dell'utente, ossia l'esistenza di un comportamento abnorme, non scusabile del cliente[54].

In particolare, la recentissima sentenza n. 7214, pubblicata il 13 marzo 2023, della Cassazione Civile ha escluso il risarcimento per il correntista rimasto vittima di *phishing*, introducendo, conseguentemente, un principio che rappresenta per gli istituti di credito uno "scudo" di fronte a suddette richieste di risarcimento danni dei truffati online, mentre per i correntisti una maggiore responsabilizzazione nell'uso dei codici personali e dichiarando che «non può dubitarsi del comportamento decisamente imprudente e negligente del danneggiato, il quale aveva digitato i propri codici personali (verosimilmente richiestigli con una e-mail fraudolenta), in tal modo consentendo all'ignoto truffatore di utilizzarli successivamente, per effettuare una disposizione di bonifico dal conto del danneggiato (esclusa, nella specie, la restituzione delle somme prelevate da un conto corrente mediante bonifico online, atteso che la responsabilità era da addossarsi al danneggiato che aveva incautamente fornito i propri codici personali verosimilmente a causa di un'attività di *phishing*)». Nel caso di specie, l'esclusione della responsabilità di suddetto istituto di credito è dipesa dalla condotta colposa dell'utente, che ha determinato l'addebito della somma, consistente in un comportamento imprudente e negligenze poiché l'utente ha digitato, contrariamente a quanto indicato nel foglio informativo, nonché nei messaggi pubblicitari *anti-phishing* sul sito internet di Poste italiane S.p.A., che forniscono le necessarie informazioni per evitare frodi informatiche, i propri codici identificativi personali senza alcuna precauzione nella loro custodia e nel loro corretto utilizzo[55].

Con quest'ultima sentenza si può certamente constatare il recepimento della soluzione evidenziata dall'ABF in materia di esclusione di responsabilità della banca se il titolare del conto corrente è stato negligente, nel caso in cui la truffa di cui è stato vittima sarebbe stata immediatamente riconosciuta anche per un utente non esperto, se avesse seguito la c.d. informativa anti-truffa pubblicizzata dall'istituto di credito.

5. Considerazioni conclusive

In relazione a quanto riportato, sono stati fondamentali gli interventi di chiarificazione dell'ABF, seppure non vincolanti, in rapporto ai profili di responsabilità in materia di *phishing* e dei particolari oneri probatori in capo agli istituti di credito, a causa delle ampie lacune normative lasciate dal legislatore.

A tal riguardo, come visto, un chiarimento deriva dalla recentissima sentenza della Cassazione Civile n. 7214 del 13 marzo 2023 che ha escluso il risarcimento del danno degli utenti truffati verso gli istituti bancari, se questi fanno un uso imprudente e negligente dei codici personali di accesso, non seguendo le indicazioni pubblicitarie anti-frode delle banche, benché appaia palesemente insufficiente, in relazione alla effettiva tutela dell'utente, una sorta di "brochure" informativa per i correntisti sui rischi connessi al *phishing*; sarebbe, invece, necessaria una sorta di educazione digitale concreta dei rischi connessi all'utilizzo di queste piattaforme degli utenti più "deboli", come coloro che non appartengono ai c.d. nativi digitali, attraverso corsi formativi che spieghino in maniera chiara, immediata e, sempre

52. Arbitro Bancario Finanziario, decisione 5 aprile 2013, n. 1820.

53. Art. 9 del d.lgs. 27 gennaio 2010, n. 11, "Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE".

54. Minneci 2022, pp. 1052-1056.

55. Cass. civ., sez. I, sentenza del 13 marzo 2023 n. 7214.

in aggiornamento, le modalità, i rischi e gli strumenti per evitare le truffe informatiche.

Tuttavia, a causa dell'accrescimento delle frodi informatiche in Italia nel corso del 2022, dove sono state frodate 156 grandi, medie e piccole imprese, per un ammontare complessivo di oltre 20 milioni di euro di profitti illeciti, dei quali oltre 4 milioni di euro sono stati recuperati in seguito all'intervento della polizia postale e delle comunicazioni, si può stimare, in merito ai fenomeni di *phishing*, *smishing* e *vishing* un aumento di €. 5.419.752 delle somme sottratte, rispetto all'anno precedente.

In particolare, la causa principale dell'espansione del fenomeno di *financial cybercrime* è stata sicuramente l'emergenza sanitaria Covid-19 che ha comportato il cambiamento radicale di alcune abitudini di vita consolidate, ampliando l'utilizzo di tecnologie sia in ambito lavorativo, con lo *smart-working*, sia in ambito scolastico con l'utilizzo di piattaforme telematiche per lo studio[56]. Non si esclude a priori che suddetto fenomeno criminoso possa aumentare ulteriormente con i conflitti in corso, portando sicuramente il legislatore europeo e nazionale a introdurre ulteriori misure di sicurezza a tutela delle infrastrutture critiche.

Tuttavia, un ulteriore accrescimento di norme regolamentari in materia penale, come già avvenuto con la novella del 2021 sul reato di frode informatica, che il legislatore nazionale ha dovuto compiere per uniformarsi alla legislazione europea, risulta controproducente dal punto di vista applicativo sotto diversi aspetti, in quanto la novella non ha recepito correttamente, come evidenziato nei paragrafi precedenti, la direttiva 2019/713/UE in rapporto alla circostanza aggravante sancita nell'art. 640-*ter*, comma 3, c.p., non precludendo delle future contestazioni dalla Commissione europea; c'è inoltre una sovrapposizione di molteplici norme penali, facendo ricondurre ad un illecito contemporaneamente più incriminazioni diverse tra loro, rendendo necessario l'intervento chiarificatore del giudice di legittimità.

Si dovrebbe, pertanto, ridurre il carico normativo in materia penale, ed evitare il fenomeno del c.d. populismo penale introducendo sempre più fattispecie criminose, in quanto la funzione di suddetta materia deve essere preventiva e non limitarsi ad una operazione repressiva, soprattutto per crimini che sono in continua evoluzione, con un semplice aumento dei reati e, conseguentemente, attentando sempre più alla libertà personale, nonché compromettendo l'effettivo e corretto esercizio dell'azione penale.

Riferimenti bibliografici

L. Alibrandi, P. Corso (2022), *Codice penale e di procedura penale e leggi complementari*, La Tribuna, 2022

R. Bartoli (2011), *La frode informatica tra «modellistica», diritto vigente, diritto vivente e prospettive di riforma*, in "Il diritto dell'informazione e dell'informatica", 2011, n. 3

R. Bartoli, M. Pelissero, S. Seminara (2020), *Diritto penale. Lineamenti di parte speciale*, Giappichelli, 2020

F. Calisai (2015), *Il Phishing: profili civilistici ed evoluzione delle forme di tutela alla luce delle decisioni dell'Arbitro Bancario Finanziario*, in "Diritto Mercato Tecnologia", 2015, n. 2

P. Cipolla (2012), *Social network, furto di identità e reati contro il patrimonio*, in "Giurisprudenza di merito", 2012, n. 12

S. Circelli (2015), *I reati informatici*, in "La voce del foro", 2015

C. Crescioli (2022), *Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche*, in "Archivio Penale", 2022, n. 2

56. Polizia postale 2023.

G. D'Agostino, P. Munafò (2018), *Prefazione* alla collana dedicata al Fintech, in C. Schena, A. Tanda, C. Arlotta, G. Potenza (a cura di), "Lo sviluppo FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale", Quaderni FinTech, 1° marzo 2018

M. D'Agostino Panebianco (2020), *Lineamenti di responsabilità derivanti dalla violazione al trattamento dati*, in "Europa e Diritto Privato", 2020, n. 1

E. Dolcini, G.L. Gatta (2021), Codice penale commentato, Ipsoa, 2021

F. Ferretti (2015), *L'*open banking *e le troppe zone grigie del conflitto tra legislazione europea sui pagamenti e la tutela dei dati personali*, in "federalismi.it", 2021, n. 10

G. Fiandaca, E. Musco (2020), *Diritto penale. Parte speciale. I delitti contro il patrimonio*, Zanichelli, 2020

G. Finocchiaro (2022), *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in "Diritto dell'Informazione e dell'Informatica", 2022, n. 2

G. Jain, S. Dahiya (2015), *NFC: Advantages, limits and future scope*, in "International Journal on Cybernetics & Informatics" (IJCI), vol. 4, 2015, n. 4

U. Minneci (2022), *Pagamenti elettronici non autorizzati: la tutela del cliente alla luce degli orientamenti dell'ABF*, in "Giurisprudenza commerciale", 2022, n. 6

U. Morera (2023), *Il costo "zero", lo* jus variandi *e l'Arbitro Bancario Finanziario*, in "Banca borsa titoli di credito", 2023, n. 1

M. Mukhtar (2015), *Perceptions of UK Based Customers toward internet Banking in the United Kingdom*, in "Journal of Internet Banking and Commerce", 2015, n. 1

L. Muttini (2021), *Frodi informatiche e responsabilità della banca: i nuovi orientamenti dell'Arbitro Bancario Finanziario*, in "Rivista di diritto bancario", 2021, n. 1

G. Olivieri (2021), *PSD2 e tutela della concorrenza nei nuovi mercati dei servizi di pagamento digitali*, in "Giurisprudenza commerciale", 2021, n. 3

C. Parodi (1997), *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in "Diritto penale processuale", 1997

G. Pascuzzi (2020), *Il diritto dell'era digitale*, il Mulino, 2020

C. Pecorella (2012), *Truffe on-line: momento consumativo e competenza territoriale*, in "Rivista italiana diritto e procedura penale", 2012, n. 1

S. Piancastelli (2015), *La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, in "Diritto Penale Contemporaneo", 3 marzo 2015

Polizia postale (2023), *Resoconto attività 2022 della polizia postale e delle comunicazioni e dei centri operativi sicurezza cibernetica*, 3 gennaio 2023

E. Reccia (2022), *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria*, in "Archivio Penale", 2022, n. 2

C. Sarzana (2010), *Informatica, internet e diritto penale*, Giuffrè, 2010

S. Sica, B.M. Sabatino (2021), *Disintermediazione finanziaria e tutela del cliente e dell'utilizzatore*, in "Diritto dell'informazione e dell'informatica", 2021, n. 1