IusTrend
il verso del diritto

Le frodi informatiche e le Banche. Profili di responsabilità

GIUGNO 2022

LaScala
SOCIETÀ TRA AVVOCATI

www.lascalaw.com - www.iusletter.com

Milano | Roma | Torino | Bologna | Vicenza | Padova | Ancona

IusLetter
informazione e aggiornamento giuridico

SOMMARIO

Le frodi informatiche e le banche. Profili di responsabilità

LaScala

IusLetter
informazione e aggiornamento giuridico

Le frodi informatiche e le banche. Profili di responsabilità

LaScala

La tipologia di truffa informatica. La normativa italiana ed europea

A cura di Simona Daminelli, Partner, La Scala Società tra Avvocati

Il cyber crimine costituisce una tematica di grande attualità, come comprovato dal fatto che l'Italia negli ultimi due anni ne è risultato uno degli Stati più colpiti.

Dalle indagini statistiche condotte, è emerso nel 2021 in Italia sono stati registrati circa 800 reati informatici al giorno, pari al 15% del totale dei reati denunciati, e, in particolare, le frodi informatiche sono cresciute del 28% rispetto al 2020.

Tale incremento trova in gran parte la sua giustificazione nella pandemia. Infatti, il Covid-19, se da un lato ha favorito la digitalizzazione, dall'altro lato – stante l'incremento delle operazioni on-line – ha comportato anche un aumento delle frodi informatiche.

Peraltro, è importante evidenziare che, a fronte dell'acquisizione da parte delle imprese e delle istituzioni di strumenti di protezione sempre più elaborati, anche le truffe informatiche diventano ogni giorno più sofisticate e spesso difficili da rilevare.

L'incremento delle frodi on-line ha necessariamente richiesto un tempestivo intervento legislativo a livello nazione e comunitario.

In tale ottica, nel 2007 è stata approvata la prima Direttiva sui servizi di pagamento (n. 2007/64/CE, cosiddetta PSD - Payment Services Directive-), volta a definire un quadro giuridico comunitario moderno e coerente per i servizi di pagamento elettronici. In particolare, la Direttiva si proponeva di:

-regolamentare l'accesso al mercato per favorire la concorrenza nella prestazione dei servizi;

-garantire maggiore tutela degli utenti e maggiore trasparenza;

-standardizzare i diritti e gli obblighi nella prestazione e nell'utilizzo dei servizi di pagamento per porre le basi giuridiche per la realizzazione dell'Area unica dei pagamenti in euro (Sepa);

-stimolare l'utilizzo di strumenti elettronici e innovativi di pagamento per ridurre il costo di strumenti inefficienti, come il contante.

La PSD è stata recepita nell'ordinamento nazionale con il D. lgs. n. 11 del 27 gennaio 2010, entrato in vigore il 1° marzo 2010, ed effettivamente ha avuto il pregio di rendere le operazioni di pagamento europee più semplici ed efficaci.

Tuttavia, ci si è resi ben presto conto che la stessa era insufficiente a garantire un'adeguata tutela degli utenti stante il continuo evolversi delle truffe e, pertanto, il 13 gennaio 2018 è entrata in vigore nell'Unione Europea la seconda direttiva sui servizi di pagamento, cosiddetta PSD2, che è stata recepita nell'ordinamento nazionale con il D. lgs. n.218 del 15 dicembre 2017.

Il termine di applicazione per gli Stati Membri era fissato al 14 settembre 2019, ma su richiesta della EBF (European Banking Federation) sono state concesse delle proroghe stante la complessità dei cambiamenti che le banche e i fornitori di servizi di pagamento avrebbero dovuto apportare. Per quanto concerne il nostro Paese, Banca d'Italia ha concesso un rinvio di 18 mesi per l'adeguamento alla nuova Direttiva e la PSD2 è, quindi, divenuta operativa a partire dal 1° gennaio 2021.

L'ambito di maggiore novità della PSD2 è relativo alle nuove procedure di sicurezza per l'accesso al conto online ed ai pagamenti elettronici, nonché ai nuovi servizi di pagamento offerti nell'area dell'e-commerce e dello shopping online. Infatti, la seconda Direttiva ha previsto un sistema di autenticazione più rigoroso, denominato Strong Customer Authentication (cosiddetto SCA), che prevede l'utilizzo di una combinazione di fattori.

Questi ultimi sono individuati sulla base dei seguenti elementi:

1. conoscenza: ovvero qualcosa che solamente l'utente conosce (ad esempio il PIN o la risposta ad una domanda);
2. possesso: ossia qualcosa che soltanto l'utente possiede (ad esempio un indirizzo e.mail o un token);
3. inerenza: ovvero qualcosa che caratterizza solamente un utente (ad esempio i parametri biometrici o l'impronta digitale).

   Perché l'autenticazione sia forte è necessario che ricorrano almeno due di questi tre fattori, che devono altresì essere indipendenti l'uno rispetto all'altro.

L'obiettivo della PSD2 è stato, pertanto, quello di rendere le operazioni più sicure, uniformando altresì i sistemi di pagamento all'interno dell'Unione Europea. Questo, a sua volta, favorisce l'efficienza del mercato dei pagamenti e una maggiore concorrenza del medesimo.

A seguito del recepimento della seconda Direttiva, sono state conseguentemente modificate alcune norme del D. Lgs. n. 11/2010, che disciplina in Italia la materia.

In particolare, i servizi di pagamento sono contemplati agli artt. 7 – 12, di cui si riportano di seguito le disposizioni principali.

Articolo 7 - oneri dell'utente

Il legislatore ha ritenuto opportuno porre degli oneri anche in capo all'utente che si avvale dei sistemi di pagamento informatici. Più precisamente l'utente è tenuto a:

- utilizzare lo strumento ricevuto in conformità con i termini indicati nel contratto quadro stipulato con il prestatore di servizi;
- comunicare tempestivamente, con le modalità indicate in contratto, lo smarrimento, il furto, la sottrazione o l'uso non autorizzato dello strumento, appena ne viene a conoscenza;
- adottare tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate. Quest'ultimo dovere riveste particolare importanza, perché ove non rispettato consente in sede giudiziale di escludere ogni responsabilità del prestatore di servizi, in caso di operazioni non autorizzate.

Articolo 8- oneri del prestatore

A sua volta, anche il prestatore di servizi deve soddisfare alcuni obblighi. In particolare deve:

- assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usarle;
- astenersi dall'inviare strumenti di pagamento non richiesti;

- assicurare che siano sempre disponibili strumenti adeguati affinché l'utente possa effettuare la comunicazione di cui all'art. 7 e chiedere il blocco dello strumento di pagamento;
- consentire all'utente di rendere la dichiarazione che precede a titolo gratuito;
- impedire qualsiasi uso dello strumento di pagamento, dopo che l'utente ne abbia comunicato lo smarrimento, il furto, la sottrazione o l'uso non autorizzato.

Articolo 9 – notifica di operazioni non autorizzate

Qualora l'utente venga a conoscenza di un'operazione di pagamento non autorizzata ha il diritto di ottenerne la rettifica, a condizione che ne dia tempestiva notizia al proprio prestatore di servizi di pagamento, secondo le modalità e tempistiche previste in contratto. La comunicazione, in ogni caso, deve essere effettuata al massimo entro 13 mesi dalla data dell'operazione.

Articolo 10 – prova delle operazioni

Se l'utente nega di aver autorizzato un'operazione di pagamento o sostenga che la stessa non sia stata correttamente eseguita, il prestatore di servizi di pagamento è tenuto a dimostrare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata e che non sia frutto di un malfunzionamento delle procedure.

Tale prova non è, però, sufficiente per dimostrare che l'operazione sia stata autorizzata proprio dall'utente, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave ad uno degli oneri su di lui gravanti. Infatti, Il prestatore di servizi di pagamento è tenuto a provare anche la frode, il dolo o la colpa grave dell'utente.

Articolo 10 bis – autenticazione forte

I prestatori di servizi devono applicare l'autenticazione forte del cliente quando questi:

- accede al suo conto di pagamento on-line;
- dispone un'operazione di pagamento elettronico;

- effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Articolo 11 – responsabilità del prestatore per le operazioni non autorizzate

Qualora sia eseguita un'operazione di pagamento non autorizzata, il prestatore di servizi di pagamento rimborsa al pagatore il relativo importo, immediatamente o comunque entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una comunicazione in merito. Il rimborso può essere sospeso solo in caso di motivato sospetto di frode.

In ogni caso, il prestatore di servizi di pagamento può dimostrare, anche in seguito, che l'operazione era stata autorizzata dall'utente e, in detta ipotesi, ha diritto alla restituzione dell'importo rimborsato.

Articolo 12 – responsabilità del prestatore per l'uso non autorizzato dei servizi

Salvo il caso in cui abbia agito con frode, l'utente non sopporta alcuna perdita derivante dall'uso di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente, se l'utilizzo sia intervenuto dopo la comunicazione di cui all'art. 7.

Analogamente, l'utente non patisce alcuna perdita se il prestatore di servizi di pagamento non esiga una sua autenticazione forte.

Le frodi online possono essere distinte in tre tipologie, in base all'identità del truffatore:

- nella prima ipotesi l'identità è irrilevante (ad esempio nel caso di una finta vendita on-line);
- nella seconda ipotesi il truffatore carpisce l'identità di una persona fisica o giuridica che l'utente conosce per fama (ad esempio quella di un ente benefico);
- nella terza ipotesi il truffatore carpisce l'identità di una persona fisica o giuridica con cui l'utente ha rapporti diretti e di fiducia (ad esempio quella di una banca). In questa tipologia rientrano per la maggior parte le frodi ai danni degli istituti di credito.

E', dunque, opportuno analizzare sinteticamente le frodi informatiche più diffuse.

A. Phishing

Consiste in un messaggio ingannevole inviato tramite e.mail, che induce il destinatario a compiere un'azione, che ha come scopo quello di carpirne l'identità o i dati personali, per accedere poi ai suoi conti bancari o alle carte di credito o ad altre informazioni / siti riservati.

Infatti, le azioni richieste consistono essenzialmente nel cliccare su un link dove inserire poi le proprie credenziali, nell'installare inconsapevolmente un malware ovvero nel rispondere direttamente fornendo i propri dati.

Spesso è difficile individuare queste truffe, atteso che i messaggi sembrano provenire dalla propria banca o altra persona conosciuta, ma ci sono diversi elementi che possono aiutare o quanto meno che devono far sorgere dei dubbi. Ad esempio la mail può contenere errori di battitura o di grammatica, avere un dominio diverso rispetto ai soliti .it o .com, l'oggetto solitamente è poco chiaro e, ancora, il messaggio spesso segnala un'urgenza e invita espressamente all'azione.

B. Smishing

In questo caso i truffatori cercano di carpire le informazioni riservate mediante sms (ad esempio chiedendo di collegarsi ad un link o di scaricare un'app).

C. Vishing

La truffa è telefonica e normalmente il frodatore cerca di indurre la vittima a fornire dati personali, fingendosi rappresentante di una azienda. L'inganno si basa su alcune tecniche, che fanno leva sui sentimenti innati nelle persone, come la fiducia, la paura o l'altruismo. Cercando di evocare questi sentimenti, infatti, il visher induce emozioni che possono offuscare la capacità di giudizio della vittima, inducendola in errore.

D. Man in the broser

Tramite un messaggio di phishing viene installato sul computer dell'utente un malware.

Quest'ultimo non crea alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione, ma resta silente fino a che la vittima si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino. In quel momento il malware si attiva e capta il collegamento dell'utente, proponendogli una pagina-video esattamente

identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario.

Successivamente, il malware attiva una finestra a modulo, che pare sempre di provenienza dal sito della banca in cui l'utente crede di operare, ove è richiesta una conferma di sicurezza con l'invito a compilare i campi del modulo con le proprie credenziali. L'utente compila così i campi del modulo fittizio e il truffatore carpisce tutti i codici di autenticazione e può utilizzarli in tempo reale.

E. Sim swap

In un primo momento il frodatore ottiene i dati personali della vittima attraverso attacchi informatici (phishing, malware, ...).

La scheda telefonica (SIM) della vittima viene, quindi, duplicata rivolgendosi, con un documento falso e una falsa denuncia di smarrimento, direttamente a un negozio di telefonia.

A questo punto il truffatore inizia a operare con l'home banking della vittima, ricevendo sulla SIM duplicata le notifiche e gli sms necessari per autorizzare le operazioni.

La vittima si accorge di non riuscire più a telefonare e usare il proprio cellulare, ma riceve anche finti messaggi di rassicurazione da parte della compagnia telefonica sulla pronta risoluzione del disguido occorso; nel frattempo, la truffa viene consumata con l'esecuzione di un bonifico verso un conto o una carta prepagata nella disponibilità del frodatore.

Purtroppo, la difficoltà di individuare le frodi informatiche ha portato la giurisprudenza a valutare con particolare rigidità la responsabilità degli istituti di credito. Infatti, al fine di garantire la fiducia degli utenti nella sicurezza del sistema, è spesso ritenuto congruo ricondurre le conseguenze negative delle truffe nell'area di rischio professionale del prestatore dei servizi di pagamento, ritenuto – forse non del tutto correttamente - in grado di verificare con appropriate misure la riconducibilità delle operazioni alla volontà del cliente.

I principali orientamenti della giurisprudenza e dell'Abf. La frode informatica: casistica

A cura di Antonio Ferraguto, Partner, La Scala Società tra Avvocati

1. Illecito trattamento dei dati personali ex art. 2050 c.c.

Le prime pronunce in materia di frodi informatiche risalgono all'inizio degli anni duemila. L'eventuale accoglimento delle domande degli utenti vedeva la condanna dei prestatori di servizi di pagamento irrogata prevalentemente in base alla normativa di cui al **D. Lgs. n. 196/2003 – "*Codice in materia di protezione dei dati personali*" -** che all'**art.15**[1] prevedeva che **chiunque cagionasse un danno ad altri per effetto dell'illecito trattamento di dati personali fosse tenuto al risarcimento ai sensi dell'art. 2050 c.c.**[2].

Un esempio di tale orientamento è una sentenza del **Tribunale di Palermo** del **12 gennaio 2010**. Il caso vedeva gli attori, titolari di un conto corrente abilitato all'operatività on line, disconoscere un bonifico di € 6.000,00 effettuato dal loro conto.

Com'è noto, costituisce regola generale quella secondo cui il creditore che agisce in giudizio sia per l'adempimento sia per la risoluzione ed il risarcimento del danno, deve fornire la prova della fonte negoziale del suo diritto, limitandosi ad allegare l'inadempimento della controparte, sulla quale incombe l'onere di dimostrazione del fatto estintivo o costitutivo dell'adempimento[3].

[1] Articolo abrogato dall'art. 27, comma 1, lettera a), numero 2), del D. Lgs. 10/08/2018, n. 101).
[2] Cfr., Tribunale Palermo, 12 gennaio 2010; recentemente, ancora in questo senso, si segnala la sentenza di Corte Appello di Ancona sez. I, 13 gennaio 2021 n. 18.
[3] Cassazione Civile Sezioni Unite, 30 ottobre 2001, Sentenza n. 13533.

Nel caso di specie, gli attori avevano provato l'esistenza del rapporto obbligatorio in forza del quale agivano e allegato l'inadempimento della convenuta, mentre il PSP nulla aveva dimostrato in ordine al corretto adempimento delle proprie obbligazioni. Quest'ultimo si era limitato ad affermare che il correntista "*potrebbe aver fornito a terzi*" codici e chiavi di accesso ai servizi dispositivi, indicando le misure di sicurezza predisposte per evitare l'accesso al sistema, senza spiegare e giustificare le ragioni della loro idoneità ad impedire l'accesso.

Invero, il Tribunale rilevava che il sistema predisposto dalla società convenuta non appariva adeguato alla tecnologia esistente: il PIN richiesto era di sole quattro cifre e l'identificativo utente corrispondeva all'indirizzo e-mail del cliente nel database del PSP, pertanto, facilmente ricavabile. Infine, contrariamente a quanto previsto contrattualmente, la società convenuta non aveva dato conferma, a mezzo posta elettronica dell'avvenuto bonifico, di cui gli l'attori avrebbero avuto conoscenza solamente alcuni giorni dopo.

Il Tribunale riteneva che il PSP avrebbe "***dovuto adottare tutte le misure di sicurezza, tecnicamente idonee e conosciute in base al progresso tecnico, a prevenire danni***, *come quelli verificatisi in capo agli attori,* ***non essendo sufficiente la non violazione di norme di legge***, *posto che* ***la diligenza richiesta deve essere valutata con maggior rigore***, *atteso che la prestazione inerisce all'esercizio di un'attività professionale.*

Invero, la società convenuta non impedendo a terzi di introdursi illecitamente nel sistema ha cagionato un danno ai propri risparmiatori, quale titolare del trattamento dei dati personali"

La sentenza precisava quindi che è "*ritenuta applicabile al caso di specie la previsione di cui all'****art. 15 del d.lgs. n. 196/2003****, la quale statuisce che* ***chiunque cagiona danno ad altri per***

effetto del *trattamento di dati personali è tenuto al risarcimento* ***ai sensi dell'articolo 2050 del Codice civile****.*

In questo passaggio possiamo chiaramente leggere l'applicazione dell'**art. 2050 c.c.** come criterio di liquidazione dei danni, il principio di una dottrina che ben presto si consolida in materia. Difatti, la **dimostrazione di aver implementato misure di sicurezza adeguate al progresso tecnico** è tutt'oggi uno degli elementi essenziali per escludere la responsabilità dei prestatori di servizi di pagamento[4], sia pure – come diremo - con diversa base normativa.

2. Responsabilità contrattuale ex 1856 c.c.

Qualche anno più tardi, la giurisprudenza ha iniziato a richiamare a fondamento delle proprie decisioni anche la **responsabilità contrattuale** della banca in forza della disciplina del mandato **ex art. 1856 c.c.** e i relativi criteri di ripartizione dell'onere della prova[5].

Ad esempio, nella sentenza del **Tribunale di Verona** del **2 ottobre 2012** viene affermato che *"La banca, nei rapporti contrattuali con il cliente, "risponde secondo le regole del mandato" (art. 1856 c.c.) e la diligenza a cui è tenuta va valutata con particolare rigore [...] La* ***diligenza del buon banchiere*** *deve essere qualificata dal maggior grado di prudenza e attenzione che la connotazione professionale dell'agente consente e richiede.*

[...] Cosi individuato il contenuto dell'obbligazione alla quale è tenuto l'istituto di credito occorre rammentare che, vertendosi in tema di ***responsabilità contrattuale****, grava su di esso*

[4] Tribunale di Palermo, 12 gennaio 2010.
[5] Così, di recente, si è espresso il Tribunale Monza sez. I, 03 febbraio 2021 n.207, sulla scorta del più risalente arresto del Tribunale Verona, 02 ottobre 2012.

l'onere di fornire la prova del proprio adempimento, in conformità al ***principio di vicinanza della prova****"*[6]*.*

Il PSP viene dunque ritenuto, dalla giurisprudenza, la parte che può e deve essere meglio fornita di mezzi per ricostruire le vicende e tutelarsi dalle truffe essendo, oltretutto, un operatore professionale.

3. L'orientamento europeo. La Direttiva PSD2

Un passaggio decisivo interviene con la **PSD 2**, **Direttiva sui Servizi di Pagamento del 2015,** trasposta all'interno della normativa nazionale con il D. lgs. n. 218 del 15 dicembre 2017, modificando il D.lgs. 11/2010.

Uno dei focus del legislatore europeo, nel contrastare l'aumento dei rischi di sicurezza delle operazioni di pagamento con l'uso di device elettronici, è l'autenticazione di quest'ultime. Se, da un lato, il contratto quadro stipulato tra un prestatore di servizi e un utente è un contratto come tutti gli altri - e quindi si stipula per iscritto in banca sottoscrivendo un modulo prestabilito dalla banca stessa[7]-; dall'altro lato, invece, è molto più complicato il consenso delle singole operazioni di pagamento, con particolare riferimento ai rischi che possono sorgere.

Il tema principale in materia è **l'autenticazione forte dell'utilizzatore**, la c.d. **SCA** (*strong costumer authentication*). Si tratta di un fenomeno che sta a metà fra il diritto e la tecnologia: quando si fa un bonifico si usa l'impronta digitale, o si inserisce un pin, o un **OTP** ***(one time password)***, tramite **token virtuale** o **token fisico**.

[6] Cassazione Civile, 30 ottobre 2001, sentenza n.13533.
[7] § Artt.1341, 1342 c.c., stipulazione di contratti tipo tramite moduli o formulari.

Ovviamente in quest'ambito siamo ai limiti della tradizione giuridica, perché un consenso contrattuale prestato con una OTP è qualcosa che non rientra nell'esperienza consueta del giurista. Proprio per questa ragione, la PSD 2 è stata integrata da un regolamento delegato, ossia emanato dalla Commissione Europea per prevedere gli standard tecnici di regolamentazione per questa materia. Questo regolamento è stato predisposto e scritto da **EBA** (*European Banking Authority*), ossia l'autorità indipendente europea che ha il compito di predisporre gli standard tecnici, che poi devono essere applicati dalla BCE e dalle autorità nazionali di vigilanza nello svolgimento delle loro funzioni. Al centro di questo regolamento delegato, è presente il **concetto di autenticazione forte del cliente**. Tale autenticazione forte si realizza ogni volta che noi autorizziamo un bonifico o un pagamento fatto con la carta di credito. Nel regolamento redatto dall' **EBA** possiamo riscontrare quali sono i fattori definiti come idonei per procedere con la SCA (*strong costumer authentication*). I fattori individuati sono rispettivamente:

- di **conoscenza**, ossia essere in possesso di un dato che solo l'utente conosce (per esempio, le credenziali per accedere al proprio *home banking*);
- di **inerenza**, ossia un attributo che solo l'utente possiede (per esempio, un'impronta digitale);
- di **possesso**, qualcosa che solo l'utente ha in suo possesso (per esempio, il possesso di un device).

I fattori **devono essere tali da far sì che la violazione di uno di essi non comprometta la sicurezza degli altri.** Possiamo dunque affermare che sono tra loro **indipendenti.**

4. **Principio della responsabilità oggettiva: orientamento della Corte di Cassazione**

Con tre decisioni della **Suprema Corte di Cassazione, rispettivamente due sentenze ed un'ordinanza tra il 2016 e il 2018**[8], l'orientamento giurisprudenziale aderisce ai principi della Direttiva e dunque diventa più rigoroso verso i prestatori di servizi di pagamento, **configurandosi una sorta di responsabilità oggettiva in capo a quest'ultimi**.

Queste tre decisioni seguono tutte il seguente *iter*[9]:

a) Anzitutto, viene definitivamente confermato[10] il principio per cui la **sicurezza del sistema in cui possono effettuarsi operazioni online o strumenti elettronici, va ricondotta nell'area del rischio professionale dell'intermediario prestatore dei servizi di pagamento**[11]. L'istituto di credito è dunque tenuto ad un'elevata diligenza, valutabile sulla scorta del modello dell'operatore professionale. Secondo questa lettura, **la corretta operatività del servizio bancario mediante collegamento telematico o strumento elettronico** – che corrisponde oltretutto ad un interesse della banca medesima – **rientra nel rischio d'impresa**, con la conseguenza che **grava sulla banca una responsabilità di tipo oggettivo, da cui la stessa va esente solo provando che le operazioni contestate dal cliente sono allo stesso riconducibili**.

Questo principio si legge chiaramente nella **Sentenza della Corte di Cassazione** del **2017**: *"al fine di garantire la fiducia degli utenti nella sicurezza del sistema (ciò che rappresenta interesse degli stessi operatori), appare del tutto ragionevole **ricondurre nell'area del rischio professionale del prestatore di servizi di pagamento**, **prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del***

[8] Cassazione Civile, Sezione I, Sentenze, n. 2950/2017 e n. 10638/2016 e ordinanza n. 9158/2018
[9] Sintesi tratta da *Phishing: il cliente della banca vince facile.* (s.d.). Diritto.it. https://www.diritto.it/phishing-il-cliente-della-banca-vince-facile/. Ultimo accesso: 11.05.2022
[10] Cfr., in origine, Tribunale Milano, sez. VI, 04 dicembre 2014.
[11] Cfr., Tribunale Parma sez. I, 06 settembre 2018, sentenza n.1268.

cliente, la possibilità di una utilizzazione dei codici da parte di terzi*, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo."*[12].

b) Viene inoltre ribadito che la banca è tenuta ad agire nell'ottica dell'accorto banchiere, dunque ad implementare dei sistemi di sicurezza adeguati per tracciare **le operazioni e poterle così ricondurre alla volontà del cliente**. Si sottolinea che "*la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei* ***rischi tipici della sfera professionale di riferimento*** *ed assumendo quindi come parametro la figura dell'****accorto banchiere***"[13];

c) **Il terzo passaggio logico è che** *"la banca (...) è tenuta a fornire la prova della* ***riconducibilità dell'operazione al cliente****"*[14]. Secondo questa interpretazione, ormai maggioritaria, il PSP sopporterebbe un rischio che sarebbe prevedibile ed evitabile con **appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente**.

In particolare, il PSP deve quantomeno dimostrare di aver posto in essere tutte le necessarie misure tecniche idonee ad evitare il rischio di intrusione di terzi.

Al riguardo, in una delle tre decisioni storiche citate si legge che "*la c.t.u.* – riferendosi al giudizio di primo grado - *aveva consentito di appurare che il* ***sistema implementato*** [dal PSP] ***non consentiva in sé, ai terzi, di venire a conoscenza dei dati necessari per compiere operazioni all'insaputa del destinatario****, donde non era possibile che l'operazione de qua fosse avvenuta senza che la correntista avesse comunicato i propri codici identificativi"*[15].

[12] Corte di Cassazione, 3 febbraio 2017, sentenza n. 2950.
[13] Corte di Cassazione, 12 giugno 2007, sentenza n. 13777; v. anche Corte di Cassazione, 23 maggio 2016, sentenza n.10638.
[14] Corte di Cassazione, 12 aprile 2018, ordinanza n. 9158.
[15] Corte di Cassazione, 23 maggio 2016, sentenza n.10638.

5. La responsabilità dei prestatori servizi di pagamento

Va sottolineato che, successivamente alla citata Direttiva europea, il substrato decisionale in materia è composto in parte determinante da decisioni dell'**ABF**, Arbitro Bancario e Finanziario.

Difatti, questo organo stragiudiziale di risoluzione controversie è lo strumento più utilizzato dai clienti dei PSP per denunciare le truffe informatiche. Anche quest'ultimo si è allineato alla normativa e alla giurisprudenza delineate finora.

I principi introdotti dalla nuova Direttiva, combinati con le sentenze della Suprema Corte, sono stati recepiti e sviluppati nelle decisioni in materia in modo rigoroso nei confronti degli istituti di credito. Come anticipato, se inizialmente la Banca doveva dimostrare di aver adeguato il proprio sistema di sicurezza al progresso tecnologico, a seguito della modifica del comma 2 dell'art. 10 del D.lgs. 11/2010 **si è giunti a pretendere la dimostrazione**, da parte del PSP, **della colpa grave o il dolo dell'utilizzatore**, dunque il suo coinvolgimento, prove da fornire, comunque, per via presuntiva.

Ad esempio, in una decisione dell'**ABF Collegio di Bologna** del **marzo 2021**, il sistema di sicurezza predisposto dall'intermediario all'epoca dei fatti era stato ritenuto **inadeguato** in quanto per portare a termine le operazioni di pagamento erano richieste soltanto password statiche (credenziali di accesso al conto) e non anche password dinamiche (OTP inviato tramite sms). Il ricorrente, per contro, dichiarava di non avere alcuna responsabilità, non avendo mai consentito a terzi l'utilizzo dell'home banking, né smarrito le proprie credenziali. Dunque, il Collegio di Bologna nella sua decisione scrive che *"l'intermediario non ha adempiuto all'**onere***

di provare *la corretta autenticazione delle operazioni* ***a norma dell'art. 10, D. Lgs. n. 11/2010***"[16].

L'anno successivo, nel **gennaio 2022**, il **Collegio dell'ABF di Roma** asserisce che una volta dimostrato di *(i)* aver adottato adeguate misure di sicurezza e *(ii)* la riconducibilità dell'operazione al cliente, il PSP avrebbe dunque soddisfatto l'onere probatorio. Nella vicenda in esame "*L'intermediario ha dimostrato,* ***attraverso i log relativi all'autenticazione e agli ordini di pagamento,*** *che le operazioni disposte attraverso l'internet banking della società ricorrente sono state* ***correttamente autenticate, attraverso un sistema di autenticazione forte a due fattori, con ricezione delle OTP e delle OTS via SMS sul telefono cellulare registrato dalla ricorrente****.[17]"* Secondo il collegio, dunque, non vi erano motivi per accogliere il ricorso dell'utilizzatore.

6. Casistica giurisprudenziale

Va poi sottolineato, in linea di principio generale, che nella maggior parte delle decisioni arbitrali si tende ad utilizzare una più accentuata severità nei confronti del cliente/utilizzatore allorquando la frode, perpetrata ai suoi danni, sia riconducibile a tecniche di *phishing* note al pubblico e ricorrenti *"tanto che qualunque utente dotato di quella normale avvedutezza e prudenza che si richiede a chi utilizzi servizi di home banking dovrebbe essere in grado di sottrarsi all'inganno."*[18].

[16] Arbitro Bancario Finanziario, Collegio di Bologna, 23 marzo 2021, decisione n. 7884.
[17] Arbitro Bancario Finanziario, Collegio di Roma, 31 gennaio 2022, decisione N. 1876.
[18] Arbitro Bancario Finanziario, Collegio di Roma, 16 maggio 2014, decisione n. 3262.

6.1. Ipotesi di colpa dell'utilizzatore

I casi in cui, generalmente, anche l'**ABF** ha riconosciuto come evidente la colpa grave del cliente sono i seguenti:

(a) Quando vi è irragionevole **credulità** del cliente, il quale avrebbe agito con colpa nel credere a delle patenti truffe. Ciò rappresenta un elemento liberatorio in capo all'intermediario[19].

(b) La **consegna** volontaria delle **proprie credenziali** a soggetti diversi da sé configura colpa grave in capo all'utente. Difatti, nemmeno il proprio PSP può richiederle all'utilizzatore.

6.2. Casi di esclusione della colpa dell'utilizzatore

(a) Diverso da quest'ultime ipotesi è il caso in cui lo **strumento di pagamento** venga **affidato temporaneamente ad un familiare affinché effettui un'operazione**. In questo caso, **l'affidamento temporaneo ad un familiare delle credenziali non è considerato colpa grave.**

L'arbitro bancario-finanziario ha infatti sottolineato che questo **non può essere considerato un comportamento intollerabile socialmente, anche alla luce della sua diffusione pratica**; quanto più un comportamento è diffuso, tanto più non si può considerare come grave la colpa di chi lo ha tenuto[20].

(b) Altra ipotesi in cui l'**ABF esclude quasi sempre la colpa grave dell'utilizzatore**, è il fenomeno del "**man-in-the-middle"**: una sofisticata e insidiosa truffa informatica molto frequente. "*E' un malware che viene inserito come un virus nel computer dell'utente, senza che questi ne consenta l'inserimento cliccando su un link ricevuto via e-mail o*

[19] Così, ABF, Collegio Di Coordinamento, 26 ottobre 2012, decisione n. 3498; Collegio di Roma, 16 maggio 2014, decisione n. 3262 e, più di recente, Collegio di Milano, 4 maggio 2017, decisione n. 4785.
[20] Cfr., Arbitro Bancario Finanziario, Collegio di Milano, 06 dicembre 2013, decisione n. 6349.

SMS"[21]. Questo ha diverse conseguenze, per esempio, **quando cerchiamo di accedere al portale web della propria banca per effettuare operazioni, la truffa si verifica reindirizzando l'utente automaticamente ad un portale falso** quasi identico a quello della banca, in cui discosta solo di poco l'indirizzo web del sito.

La responsabilità derivante da frodi informatiche di questo tipo, sempre più sofisticate ed ingannevoli resta tendenzialmente in capo all'intermediario.

Come affermato in una decisione del **Collegio di Torino** del **marzo 2022** "*L'intenzione del legislatore, europeo e nazionale, è evidentemente quella di* ***premere sul prestatore dei servizi perché garantisca elevati standard di trasparenza e sicurezza*** *e* ***patisca****, almeno in linea di principio,* ***le conseguenze sfavorevoli del loro uso fraudolento o comunque non autorizzato*** *(cfr. tra le molte, Arbitro Bancario Finanziario, Collegio di Torino, nn. 3464/18 e 6454/18). Non è solo questione di generico favor per l'utilizzatore, a sua volta gravato da precisi obblighi di cooperazione (ad es. artt. 7 e 9 D.Lgs. 11/2010), ma anche di* ***vicinanza della prova, la quale può e deve essere meglio fornita da chi operi professionalmente nel mercato dei servizi di pagamento***[22] *".*

6.3 Ipotesi di furto

La responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento. Nel caso di strumento di pagamento smarrito, sottratto o utilizzato indebitamente, l'**art. 12** del **D.lgs. 11/2010** dispone che **salvo il caso in cui abbia agito in modo fraudolento, l'utilizzatore non sopporta alcuna perdita se:**

1) intervenuta dopo la comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera *b);*

[21] V., tra le altre, Arbitro Bancario Finanziario, Collegio di Bologna, 23 marzo 2022, decisione n. 4917.
[22] Arbitro Bancario Finanziario, Collegio di Torino, 28 marzo 2022, decisione n. 5136.

2) il PSP non ha adempiuto all'obbligo di cui all'articolo 8, comma 1, lettera *c)*;
3) il PSP non esige un'autenticazione forte del cliente;
4) non poteva notare prima di un pagamento il furto/smarrimento dello strumento di pagamento;
5) si tratta operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento;

Qualora l'utente, invece, abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate.

Un tale onere probatorio può essere soddisfatto dall'intermediario anche **in via presuntiva**, secondo quanto affermato dal **Collegio di Coordinamento** nel 2014, mediante *"**indizi chiari, precisi e concordanti** idonei a comprovare che [...] la ricorrente non abbia custodito la carta di pagamento con la dovuta diligenza".* Nel caso di specie, il PSP ha dimostrato di aver implementato tutti i sistemi di sicurezza in linea con il progresso scientifico del tempo e che "*l'operazione disconosciuta è stata posta in essere mediante l'impiego della carta e del codice dispositivo, sicché – dato credito all'affermazione del ricorrente secondo cui la carta stessa è sempre rimasta in suo possesso – deve trarsi la ragionevole conclusione che il cliente non l'abbia custodita con la dovuta diligenza, tanto da non accorgersi che qualcuno occasionalmente la sottraeva e la utilizzava con il relativo PIN*[23]*".*

Sempre secondo quanto asserito dal Collegio di Coordinamento in una decisione del 2019, la relativa prova dal quale possa trarsi la colpa grave dell'utente può essere fornita con *"una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa*

[23] Arbitro Bancario Finanziario, Collegio di Coordinamento, 14 febbraio 2014, decisione n. 897.

*trarsi la prova, **in via presuntiva**"*, anche se – in quel caso - ha ritenuto nel merito che non fossero stati dedotti elementi di fatto particolarmente univoci e convergenti, al punto che potesse ragionevolmente ritenersi che l'utilizzo fraudolento fosse effettivamente riconducibile sul piano causale alla condotta dell'utilizzatore[24].

Si tratta quindi di criteri elastici che il giudice valuterà secondo il suo prudente apprezzamento e tenuto conto delle circostanze del caso concreto.

Va detto, per completezza, che una tesi minoritaria più rigorosa ritiene che la prova presuntiva non sia accettabile.

Tutto quanto finora puntualizzato vale solo per le operazioni che si verifichino **prima che il titolare dello strumento di pagamento si accorga di furto, smarrimento o appropriazione indebita** perché, non appena se ne accorge, ha l'obbligo di bloccare lo strumento di pagamento. L'**art. 7 del D.lgs. 11/2010** (***Obblighi a carico dell'utente dei servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate***) prevede una serie di oneri a carico del cliente della banca, quali **la tempestiva comunicazione dell'altrui utilizzo indebito dello strumento**, l'adozione delle misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo. La **tardività nel blocco dello strumento di pagamento costituisce colpa grave**.

Una volta che lo strumento è bloccato, invece, nessuna operazione di pagamento può essere addebitata e se addebitata, l'importo dovrà essere senz'altro restituito indipendentemente dalla eventuale colpa grave del titolare dello strumento di pagamento.

[24] Arbitro Bancario Finanziario, Collegio di Coordinamento, 10 ottobre 2019, decisione n. 22745.

Il **tempismo** è poi un elemento importante per riscostruire i fatti in sede di giudizio o decisione arbitrale.

È necessario sottolineare che, a volte, la breve distanza tra un evento e l'altro, è stata ritenuto invece un fattore dimostrativo della colpa grave del cliente. Ne è un esempio una recente sentenza di **aprile 2022** del **Collegio di Bologna**, in cui la motivazione dell'organo arbitrale era del seguente tenore: *"Nel caso di specie l'intermediario, nelle proprie controdeduzioni, dopo aver allegato evidenza documentale della regolare esecuzione delle operazioni, **eccepisce che il breve lasso temporale tra sottrazione dello strumento di pagamento e l'operazione contestata fa presumere che il PIN fosse custodito congiuntamente allo strumento**; quindi, la cliente non ha adempiuto agli obblighi di custodia dello strumento di pagamento*[25]*".*

6.4 Focus on *simjacking*

La cosiddetta "*sim swap fraud/scam*", conosciuta anche come "*simjacking*", è una delle tecniche più sofisticate e insidiose che ha registrato molte vittime negli ultimi anni. La frode consiste letteralmente nello scambio di SIM e nello sfruttamento di eventuali debolezze del meccanismo a due fattori. I truffatori individuano una vittima e, attraverso tecniche come il *phishing* si impossessano di una o più credenziali statiche dell'utente vittima. Successivamente, contattano l'operatore telefonico del cellulare della vittima e lo inducono ad attivare il numero di telefono di quest'ultima su una carta SIM di cui i truffatori sono in possesso (ad esempio fingendosi il proprietario del numero di telefono). Una volta che ciò avviene, i truffatori hanno il controllo del numero di telefono. Chiunque chiami o mandi messaggi a questo numero contatterà il dispositivo dei truffatori, non lo smartphone della vittima. La banca invierà quindi un codice via SMS - l'autenticazione a due fattori - al numero

[25] Arbitro Bancario Finanziario, Collegio di Bologna, 06 aprile 2022, decisione n. 5700.

dello smartphone della vittima, un codice che verrà inserito dai truffatori per accedere al conto online dell'utente e agire indisturbati.

Come è stato asserito dal **Collegio di Roma** nel **maggio 2020**, "*In diritto la vicenda qui considerata si inquadra nella* ***casistica del furto di strumenti di pagamento e di identità elettronica*** *e va pertanto valutata alla luce delle vigenti disposizioni normative in materia di servizi di pagamento, con particolare riguardo agli artt. 7, 10 e 12 del d.lgs. n. 11/2010*". Di conseguenza, *"l'intermediario che non intenda farsi carico delle perdite sofferte dal cliente per operazioni che non siano state effettivamente autorizzate, ha* ***l'onere (i) di provare innanzitutto di aver adottato un sistema di "autenticazione forte"*** *per l'utilizzo degli strumenti di pagamento da parte del cliente nonché, nel caso specifico, che le operazioni siano state correttamente autenticate, registrate e contabilizzate;* ***(ii)*** *e poi, fornita questa preliminare prova,* ***di provare altresì, se non il dolo, almeno la colpa grave del cliente nell'aver reso possibile il compimento delle operazioni non autorizzate***"[26]. L'orientamento prevalente in materia configurava dunque la responsabilità del danno cagionato all'utilizzatore in capo al PSP e all'operatore telefonico.

Tale orientamento prevalente è stato arrestato da una sentenza dell'**aprile 2022** del **Tribunale di Milano**, in cui il giudice ha configura la responsabilità della truffa in via congiunta all'utilizzatore e all'operatore telefonico. Nella sentenza, viene affermato che *"****al fine di eludere il sistema di sicurezza è necessario non solo disporre dell'utenza telefonica del correntista, in modo da poter ricevere il codice OTP, ma prima ancora bisogna conoscere le credenziali statiche del correntista, in quanto solo attraverso di esse è possibile accedere al conto online*** *(anche se per operarvi è poi necessario la password temporanea).*

[26] Arbitro Bancario Finanziario, Collegio di Roma, 26 maggio 2020, decisione N. 9504.

Ne discende, pertanto, che ***la sola richiesta illecita di duplicato della sim non può essere stata sufficiente a consentire al truffatore di disporre sul conto corrente dell'attore****, ma* ***certamente questi già conosceva anche le credenziali statiche dell'[utilizzatore].”***

Ne consegue che debba ritenersi operante la scriminante della condotta gravemente colposa del cliente nonché configurata la responsabilità in capo all'operatore telefonico, con conseguente effetto liberatorio per la banca convenuta.

6.5 Rapporti di home banking

Anche con riguardo al rapporto di *home banking*, la veste di **contraente qualificato della banca** comporta che per essere esente da responsabilità, essa non solo sia tenuta ad adeguarsi all'evoluzione tecnica dei sistemi di sicurezza, bensì dimostri di aver adottato tutte le misure idonee ad evitare il danno e fornisca la prova positiva di una causa esterna. Taluni interpreti si spingono fino a ricomprendere un **obbligo di monitoraggio puntuale delle operazioni dei correntisti**. In altre parole, **competerebbe all'intermediario verificare anche il regolare andamento delle operazioni e segnalare quelle che appaiono anomale, specie se emergano transazioni effettuate in contrasto con la usuale operatività del conto**.

Tuttavia, la sussistenza di un simile onere viene contestato dai PSP e qualche volta la loro tesi viene accolta dal giudicante.

In un recentissimo ricorso all'**ABF Collegio di Torino** del **marzo 2022**, ad esempio, un istituto di credito è stato accusato dal ricorrente, suo cliente, di non aver monitorato adeguatamente le **operazioni del conto corrente** di quest'ultimo, il che non ha consentito di bloccare una truffa informatica in corso. La banca ha spiegato che sarebbe impossibile monitorare gli indirizzi IP

di tutti i clienti, ossia quel codice che identifica univocamente un dispositivo, e segnalarlo ogni volta che quest'ultimo cambi. Se non vi sono precise prove di forzatura di accesso al conto del cliente, non c'è necessità di allertarsi se un pagamento viene fatto da un dispositivo diverso. Ad oggi, tutti hanno in possesso almeno due dispositivi elettronici con cui effettuare un pagamento. Nella ricostruzione della decisione dell'ABF in analisi, si legge che *"gli indirizzi IP riconducibili all'operatività disconosciuta e quelli invece riferiti all'operatività della cliente, di per sé sola non può essere intesa quale segnale che debba automaticamente allertare i sistemi bancari poiché altrimenti, vista l'operatività odierna degli utenti, la stessa* ***operatività bancaria sarebbe soggetta a continui blocchi: in altri termini, paralizzata****."* Nel caso di specie, il ricorso è stato respinto e dunque si è data ragione alla banca. Essa, difatti, "*ha dimostrato, mediante le schermate prodotte in atti, che le operazioni risultano autorizzate con inserimento sia delle credenziali di accesso statiche, sia di quelle dinamiche, conformemente alla disciplina dei sistemi di autenticazione forte*[27]*"*.

In definitiva, anche se gli sviluppi giurisprudenziali e arbitrali non possono dirsi completi, l'attuale assetto normativo prevede, a carico del Prestatore di Servizi di pagamento, l'onere di provare congiuntamente *(i)* che il proprio sistema di sicurezza ed autenticazione sia adeguato al progresso tecnologico e *(ii)* che vi è stata frode, dolo o colpa grave dell'utente, anche in modo presuntivo.

[27] Arbitro Bancario Finanziario, Collegio di Torino, 28 marzo 2022, decisione n. 5133.

Le difese della Banca: profili pratici e aspetti operativi

A cura di Emiliano Branca, Ufficio cause e procedure legali, Banco BPM

Le frodi *on line* rappresentano ormai da qualche anno una parte piuttosto cospicua del totale dei ricorsi all'Arbitro Bancario Finanziario. In base alla casistica sinora esaminata è possibile individuare le seguenti tipologie di frodi ai danni degli utenti di servizi *home banking.*

PHISHING

La presente frode si compone di due fasi distinte; parte da una comunicazione scritta - solitamente un SMS (*smishing*) – volta a carpire le credenziali c.d. "statiche" unitamente al numero di telefono e prosegue tramite un contatto telefonico (*vishing*) volto a volta a ottenere le credenziali c.d. "dinamiche".

Occorre premettere che non si tratta di una frode *ad personam* in quanto non avviene in maniera mirata, ma con l'invio massivo (c.d. "a pioggia") di un SMS, fittiziamente proveniente da un istituto di credito, a migliaia di potenziali utenti di svariati servizi di home banking.

A tal fine i frodatori utilizzano la tecnica dello *spoofing* ovvero del camuffamento. Tramite dei *software* modificano l'identificativo del mittente del messaggio in modo che l'SMS venga visualizzato dal destinatario con il nome del prestatore del servizio di pagamento (PSP).

È bene precisare che non vi è nessuna violazione dei dati dei personali dei clienti custoditi dalla banca, in quanto i recapiti telefonici utilizzati per la frode non vengono attinti dagli archivi informatici dell'intermediario, ma vengono messi a disposizione dei malfattori dai clienti medesimi in totale buona fede. Al giorno d'oggi, infatti, la comunicazione a terzi della propria utenza telefonica è un dato di fatto che difficilmente può essere messo in discussione, basti pensare solo per fare un esempio ai siti di compravendite *on line*.

I frodatori dispongono di liste contenenti migliaia di utenze telefoniche delle quali ignorano i nominativi dei titolari. L'invio dell'SMS civetta viene fatto "al buio" in quanto i frodatori non possono sapere con esattezza a priori di quale banca risulti cliente il titolare di quell'utenza telefonica; proprio per tale motivo solo un ristretto numero di frodi – dove appunto si trova l'abbinamento delle due utenze - può (tentare di) avere successo.

Come ampiamente sottolineato dai Collegi ABF la stragrande maggioranza dei tentativi di truffa posti in essere con modalità telematiche in materia di servizi di pagamento si svolgono secondo uno schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti di comunicazione, a comunicare e/o a inserire su dispositivi 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.

Questi messaggi hanno delle caratteristiche che ne palesano l'inverosimiglianza una su tutte la presenza di un *link* mediante il quale l'utente viene invitato ad effettuare un *login* al fine di porre rimedio ad una determinata criticità, *link* che molto spesso non contiene neppure vagamente il nome dell'intermediario.

I messaggi civetta inoltre sono caratterizzati da una sintassi piuttosto scadente, e sovente dalla presenza di veri e propri errori ortografici.

Proprio per questi motivi i Collegi ABF attualmente ritengono che tale tipologia di frode sia perfettamente riconoscibile da un utente mediamente avveduto. Di contro il cliente che incappa in una frode di questo tipo è – a detta dell'Arbitro - vittima di "colpevole credulità" e quindi, in generale, non meritevole di tutela. Viene riconosciuta un'attenuante nell'ipotesi in cui il messaggio truffaldino si sia accodato ad un precedente SMS effettivamente proveniente dall'intermediario, in quanto ciò ha contribuito ad alimentare nell'utente il convincimento che anche quest'ultimo fosse genuino.

L'utente a seguito del click sul *link* contenuto nell'SMS civetta viene rinviato ad un sito clone di quello dell'intermediario nel quale gli viene richiesto l'inserimento di: codice cliente, password mnemonica e utenza telefonica.

Tali dati vengono carpiti dai frodatori per il prosieguo della frode; in particolare il numero di telefono verrà utilizzato di lì a poco per il perfezionamento del *vishing*.

Nelle difese è bene eccepire che la richiesta di inserimento - in fase di autenticazione all'area protetta - del numero di cellulare è una pratica inusuale che dovrebbe allertare il singolo utente in quanto il sito della banca, in osservanza delle linee guida sulla sicurezza dei pagamenti e come ribadito dalla PSD2, non richiede l'inserimento del numero di cellulare quale credenziale di sicurezza, bensì l'inserimento di una password temporizzata (codice OTP).

Anche il contatto telefonico avviene sotto mentite spoglie "grazie" ad applicazioni che consentono lo *spoofing* telefonico. In pratica il frodatore nasconde il suo reale numero di

telefono, camuffandolo con l'utenza telefonica che vuole che appaia al destinatario come ID chiamante.

Fino a qualche tempo fa i frodatori coprivano la loro utenza telefonica facendo apparire il numero verde del servizio clienti della banca. In sede di difese veniva precisato ai ricorrenti che i numeri verdi, per loro stessa natura, sono attivi solo in "entrata", sono cioè abilitati unicamente alla ricezione di chiamate provenienti dall'esterno, e non vengono mai utilizzati per le comunicazioni alla clientela che avvengono con il numero c.d. sottostante.

Probabilmente proprio per questo motivo i truffatori hanno iniziato ad utilizzare per il *vishing* un numero di telefonia fissa. In questo caso, prima di redigere le difese, è necessario accertare se quel numero esiste effettivamente ed è in qualche modo riconducibile alla banca in questione.

Durante il contatto telefonico il frodatore, spacciandosi per un operatore telefonico dell'intermediario che giunge in soccorso del cliente, può adottare diverse strategie al fine di raggiungere l'obiettivo di disporre delle giacenze di conto.

L'*iter* preferito fino a qualche tempo fa consisteva nel perfezionare *l'enrollment* dell'App della banca sul proprio dispositivo; operazione volta a creare un legame fra l'App, il dispositivo su cui viene installata e l'utente titolare delle credenziali.

A tal fine il frodatore scarica sul proprio *smartphone* l'App ufficiale dell'intermediario e inserisce le credenziali statiche carpite al titolare dell'*home banking* tramite l'espediente del sito clone. Ciò scatena l'invio di due password temporizzate presso i recapiti certificati del cliente; dapprima un OTP-SMS e di lì a poco un OTP-mail.

A questo punto il sedicente operatore telefonico cerca di farsi comunicare dall'utente i suddetti codici al fine di perfezionare il processo di *enrollment*. Solitamente asserisce di essere stato lui stesso a scatenarne l'invio e lo invita a comunicarglieli al fine di perfezionare *l'iter* di identificazione del cliente.

È bene rilevare che la comunicazione a terzi di tali OTP è indice di grave negligenza in quanto gli stessi sono solitamente contenuti in comunicazioni c.d. "parlanti"; sia l'SMS che l'e-mail non si limitano a riportare la password temporizzata, ma spiegano la finalità per la quale la stessa viene inviata. Va da sé che un'attenta lettura delle comunicazioni dovrebbe indurre l'utente - mediamente avveduto - a rendersi conto del fatto che sta autorizzando la certificazione dell'App su un altro dispositivo.

Spesso capita che le vittime di frodi sollevino obiezioni in ordine alla sicurezza della procedura di certificazione dell'App della banca sul nuovo dispositivo, asserendo la stessa ha contribuito in maniera decisiva alla causazione della frode.

In questo caso è bene evidenziare nelle difese che il processo l'*enrollment* è avvenuto con modalità formalmente corrette in quanto si è perfezionato con l'utilizzo di password temporizzate inviate ai recapiti, telefonici e di posta elettronica, del cliente. L*'iter* sopra indicato è tale da garantire la sicurezza dell'operazione nella misura in cui il titolare del rapporto, presso il quale vengono inviate le due quantità di sicurezza necessarie alla certificazione dell'App su un nuovo dispositivo, non divulghi a terzi tali informazioni.

È di tutta evidenza che la procedura di sicurezza, di per sé sola, non può essere in grado di sapere se il dispositivo che si intende abilitare è in possesso del cliente o si trova a mani di ignoti malfattori. Resta il fatto che se non vi fosse questa procedura, ogni sostituzione dello *smartphone* abilitato ad operare sul rapporto (ad es. per danneggiamento dello stesso), presupporrebbe la chiusura del servizio di *home banking* in essere e la sua riapertura, previa ricontrattualizzazione dell'intero servizio, con assegnazione di un diverso codice cliente.

Una volta entrato in possesso dei due codici OTP il malfattore è in grado di completare la certificazione dell'App sul proprio dispositivo e può operare con un certo grado di autonomia inserendo disposizioni fraudolente. A questo punto la collaborazione del cliente è necessaria solo a fini l'autorizzativi.

Per l'autorizzazione della disposizione viene infatti inviata una password temporizzata di "*Strong Customer Authentication con Dynamic Linking*" (c.d. SCAD); si tratta di un fattore di sicurezza introdotto dalla PSD2 a tutela di chi effettua operazioni di pagamento *on line*, che permette di collegare la transazione in modo dinamico e univoco all'importo e al beneficiario specificati dall'utente al momento in cui dispone il pagamento. Nel concreto viene inviato un SMS di tipo "parlante" che subordina l'esecuzione di quel determinato pagamento all'inserimento del codice OTP ivi riportato.

Anche in questo caso la condotta del cliente che comunica a terzi tale codice è connotata da colpa grave; per tale motivo la sua pretesa risarcitoria non viene solitamente ritenuta meritevole di tutela.

Più di recente i frodatori cercano di ottenere il controllo da remoto del dispositivo del cliente sul quale è già enrollata l'App della banca.

A tal fine durante il colloquio telefonico convincono l'utente ad effettuare la scansione del proprio *smartphone* con un antivirus scaricabile tramite un *link* contenuto in un ulteriore SMS che gli viene inviato seduta stante.

Ovviamente tale applicazione nasconde in realtà un *malware* tramite il quale i malfattori riescono ad ottenere il completo controllo dello *smartphone* del cliente.

Disponendo di due fattori di autenticazione, ovvero la password precedentemente carpita tramite l'espediente del sito clone (elemento di conoscenza) e il dispositivo del cliente sul quale è enrollata l'app della banca (elemento di possesso), i frodatori riescono a operare in totale autonomia.

Una caratteristica di questa operatività rispetto a quella che prevede l'effettuazione dell'*enrollment* risiede nel fatto che le transazioni fraudolente sono eseguite dal dispositivo del cliente e sotto l'indirizzo IP normalmente utilizzato da quest'ultimo.

In sede di ricorso ABF i clienti truffati fanno leva sull'insidiosità di tale *modus operandi* al fine di ottenere una pronuncia favorevole motivata dall'assenza di una loro colpa grave.

A fini difensivi assumono particolare rilevanza le decisioni n. 3498/2012 e n. 1820/2013 del Collegio di Coordinamento ABF, con le quali sono state distinte le truffe realizzate mediante metodi ormai conosciuti alla clientela (le classiche e-mail di *phishing*), dalle truffe più insidiose in cui maggiore è la difficoltà di avvedersi della situazione di apparenza generata dal *malware*.

In particolare, il Collegio di Coordinamento ha distinto:

"*a) le ipotesi di phishing tradizionale caratterizzate dall'invio di un semplice messaggio telefonico (cd. vishing), e-mail (cd. smishing) o SMS (cd. 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, e-mail, SMS o altri strumenti di comunicazione, a comunicare e/o ad inserire su dispositivi 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 intrusione 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" (cd. "Man in the Middle" o "Man in the Browser", cioè un malware che viene inserito come un virus nel computer dell'utente, senza che questi ne consenta l'inserimento cliccando su un link ricevuto via e-mail o SMS).

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.

Nel caso di phishing tradizionale e nelle sue varianti sopra descritte, l'assenza di cautela dell'utente appare difficilmente scusabile, trattandosi appunto di fenomeni diffusamente noti, che qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso del cd. home banking, deve essere in grado di individuare, non facendosi trarre in inganno.

Nell'ipotesi del phishing tradizionale, il cliente è pertanto vittima di una colpevole credulità, in quanto è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario.".

Solitamente i legali dei ricorrenti censurano l'adeguatezza dei sistemi antifrode dell'intermediario, rei di non aver impedito l'esecuzione delle operazioni fraudolente. E' utile ribattere che nei casi in questione l'elemento di vulnerabilità è stato costituito da una condotta gravemente colposa del ricorrente, in quanto connotata da "colpevole credulità" e sistematica violazione degli avvisi antifrode diramati dalla banca.

In realtà non vi è stata alcuna falla nei sistemi antifrode dell'intermediario; l'*iter* di perfezionamento delle operazioni *on line*, intese sia come accesso all'home banking che come disposizioni strettamente operative, si basa sulla corretta gestione degli elementi che costituiscono la c.d. identità digitale (User ID, password, OTP-SMS/OTP-mail, dispositivo su cui è enrollata l'App della banca, ...) ed è tale da garantire la sicurezza delle operazioni medesime nella misura in cui il titolare del rapporto, il solo a conoscenza delle credenziali statiche ed in possesso del dispositivo accreditato a ricevere gli OTP, non ceda a terzi tali elementi. E' di tutta evidenza infatti che la procedura di sicurezza, di per sé sola, non può avere quel grado di onniscienza che le consente di sapere se quell'operatività, formalmente corretta, è posta in essere dal cliente o da ignoti malfattori.

MAN IN THE BROWSER

La tipologia di frode in questione, a differenza della precedente, è costituita da un vero e proprio attacco informatico realizzato tramite un elemento malevolo che si frappone nel dialogo digitale intercorrente tra il dispositivo del cliente ed i sistemi della banca.

Nell'attacco "Man in the browser" (M.I.T.B.) un virus inoculato nel *browser* permette di intercettare, registrare e manipolare qualunque comunicazione tra l'utente e il Web.

Di fatto il cliente ritiene di interagire con i servizi della propria banca, mentre il browser "infetto" con cui sta navigando riesce ad intercettare e a modificare le operazioni impartite tramite il servizio *home banking*; può così accadere che il cliente, tramite il browser "infetto", disponga un ordine di pagamento voluto, che però il virus intercetta e modifica, inoltrando alla banca un ordine in favore di un diverso soggetto, sconosciuto al cliente ma complice *dell'hacker*.

Si comprende quindi un fondamentale elemento di differenziazione rispetto ai casi di *phishing* nei quali il cliente non intende disporre alcun bonifico (a prescindere dal beneficiario del medesimo); la transazione disconosciuta non è generata dall'utente e modificata dal frodatore, ma generata *in toto* da quest'ultimo.

Molto spesso l'attacco M.I.T.B. viene invocato a sproposito dai ricorrenti, vittima in realtà di normali casi di *phishing*, al solo fine di poter sostenere la sofisticatezza della frode e l'assenza di colpa grave da parte loro. In questo caso, prima di predisporre le difese, è importante accertare che il dispositivo e l'indirizzo IP utilizzati per la frode fossero riconducibili al cliente.

Diversamente la truffa ricadrà nell'ambito dell'attacco M.I.T.B., ovvero in una tipologia di frode sofisticata nella quale l'Arbitro è solitamente portato ad escludere la colpa grave del cliente.

In questi casi le difese della banca sono legate all'invio del già citato OTP-SMS di SCAD; tale messaggio riporta infatti il codice IBAN ricevuto dalla banca dopo la modifica apportata dall'*hacker*. E' quindi possibile sostenere una certa negligenza del cliente che ha avallato l'operazione inserendo l'OTP contenuto nell'SMS ricevuto senza aver prima controllato attentamente l'IBAN ivi riportato.

SIM SWAP FRAUD

La frode in questione - nota anche come "furto dell'identità telefonica" - costituisce a rigore la seconda fase di una truffa più complessa che inizia attraverso la captazione di alcuni dati personali dell'utente, tra cui le credenziali di accesso al servizio di *home banking*.

Potrebbe quindi essere utilizzata, dopo un episodio di *smishing*, quale alternativa al *vishing* telefonico.

I frodatori, una volta entrati in possesso di alcuni dati personali dell'utente, richiedono al gestore di telefonia mobile di quest'ultimo il trasferimento dell'utenza telefonica su altra sim in loro possesso, con la conseguenza che tutto il traffico telefonico - sia voce che messaggi (ivi compresi i codici di sicurezza necessari ad autorizzare operazioni bancarie) – perviene unicamente sul loro dispositivo.

E bene evidenziare che gli intermediari rendono edotti i propri clienti in ordine a tale tipologia di frode mediante avvisi pubblicati nel sito istituzionale della banca e nell'area protetta di ciascun utente; alla clientela viene spiegato in cosa consiste tale attacco e quale comportamento deve essere tenuto al fine di impedire utilizzi fraudolenti del proprio conto (ad es. contattare la propria compagnia telefonica in presenza di assenza di segnale protratta nel tempo).

Nonostante ciò e nonostante il fatto che il trasferimento di un'utenza telefonica da una sim ad un'altra è un qualcosa che esula dalla sfera di controllo e di competenza della banca fornitrice del servizio di home banking, l'orientamento dell'Arbitro è molto penalizzante nei confronti degli intermediari in quanto la quasi totalità di questi ricorsi viene accolta.

I Collegi ABF argomentano le loro decisioni nei seguenti termini:

"*Posto che la OTP è un sistema di controllo dell'identità dinamico e monouso, essa consiste generalmente in un codice alfanumerico - generato da un algoritmo – trasmesso all'utente su un canale fuori banda (nella specie, messaggistica SMS), per cui è sempre necessaria, ai fini della sua utilizzazione, una tecnologia supplementare (Token software in questo caso).*

Dalla descritta logica di autenticazione, consegue che l'operazione di modifica dell'utenza telefonica sulla quale ricevere la OTP o la semplice possibilità di venire a conoscenza del numero di telefono, può rischiare di svuotare la password dinamica della propria funzione protettiva di verificare la genuinità dell'operazione e, dunque, costituisce di per sé un'operazione o una situazione anomala.

L'inadeguatezza del sistema appare anche da un altro punto di vista. La logica della cosiddetta strong customer authentication (SCA) è quella di consentire l'accesso al sistema del soggetto che effettua la transazione tramite l'inserimento non di uno, ma di almeno due elementi identificativi per aumentare la sicurezza del servizio di pagamento. Ora, dalla narrativa di entrambe le parti, emerge che agli autori della sottrazione è stato sufficiente ottenere le

credenziali statiche per poter sia accedere al portale titolari, sia di venire a conoscenza del numero di utenza cui vengono inviati i codici alfanumerici, che intervenire sulla relativa sim e appropriarsi di questi ultimi.

In buona sostanza, la violazione di una singola misura di sicurezza ha compromesso anche l'affidabilità dell'altra, quando, al contrario, la piena operatività del sistema di autenticazione multifattore si fonda sull'indipendenza tra le singole misure di sicurezza (cfr. Collegio di Milano, decisioni n. 1066/2019 e n. 5895/2020). L'esistenza di una relazione funzionale tra di esse consente di eludere il doppio controllo delle credenziali, e rendere, nei fatti, il sistema di autenticazione (non più forte ma) debole.

La portata dirimente del suddetto requisito di indipendenza tra misure di sicurezza è del resto riconosciuta anche dalla Direttiva 2015/2366/UE (cosiddetta Direttiva PSD2), la quale lo prescrive come caratteristica obbligatoria (art. 4, par. 1, lett. 30) che deve improntare il rapporto tra singole misure di sicurezza di un sistema di autenticazione forte.".

In tale contesto l'unica possibilità per cercare di limitare l'incidenza della condanna è quella di cercare di dimostrare un contributo di parte ricorrente alla causazione della truffa. Tale potrebbe essere il caso in cui il furto dell'identità telefonica è stato preceduto, come verosimilmente avviene, da uno *smishing* ed il ricorrente ha allegato la cronologia messaggi.

Frodi informatiche e protezione dei dati personali

A cura di Francesco Rampone, Of Counsel, La Scala Società tra Avvocati

Il problema, molto attuale, delle frodi informatiche bancarie ha strettissime connessioni con la normativa in tema di trattamento dei dati personali.

Non v'è dubbio, infatti, che la frode informatica – ovvero la frode condotta «*alterando in qualsiasi modo il funzionamento di un sistema informatico e telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti*» (art. 640 c.p.) – consiste sostanzialmente nella "penetrazione" delle misure di sicurezza adottate dal **titolare del trattamento** (la banca stessa), e cioè nell'evidente sfruttamento da parte del frodatore della debolezza di tali misure le quali, ai sensi del GDPR (Regolamento UE 2016/679), devono sempre essere aggiornate in un continuo processo di adeguamento alle miglior prassi e ad elevati standard tecnologici.

Si tratta quindi di una perenne gara tra fornitori di servizi di pagamento e hacker informatici nella quale, peraltro, vige un regime di responsabilità "invertita" *ex* art. 2050 c.c. a tutela del terzo correntista. Se i primi, infatti, nella competizione con i secondi segnano il passo – ad esempio diminuendo gli investimenti in security o apprestando un presidio privacy inadeguato –, saranno per ciò solo responsabili delle conseguenze della frode, senza ulteriore indagine sul **nesso causale** tra condotta illecita del frodatore, o incauta del correntista, e danno sofferto da quest'ultimo.

Inversione del normale onere probatorio nel D.Lgs. 11/2010

L'aspetto "regolamentare" che disciplina la responsabilità dei prestatori di servizi di pagamento in ordine alle frodi informatiche si intreccia e ricalca quello "civilistico" previsto dal GDPR.

Il D.Lgs. 11/2010[28] (il **Decreto**), all'art. 10 (Prova di autenticazione ed esecuzione delle operazioni di pagamento) inverte il normale onere probatorio e dispone che ove il correntista «*neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento* [la banca, ndr] *provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*»[29].

[28] Attuativo, con successive modifiche, della Direttiva (UE) 2015/2366 (c.d. **PSD2**, operativa in Italia dal 1 gen. 2021) relativa ai servizi di pagamento nel mercato interno.

[29] La norma estende al comma 1-bis l'inversione dell'onere probatorio anche ai prestatori di servizi di disposizione di ordine di pagamento.

È pur vero che ancorché l'onere sia invertito, il correntista (l'utilizzatore di servizi di pagamento) è comunque tenuto ad un certo grado di diligenza; ma si badi bene, la circostanza dell'utilizzo fraudolento delle chiavi non dimostra *di per sé solo* il difetto di tale diligenza.

Prosegue infatti la norma chiarendo che «*Quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'**utilizzo di uno strumento di pagamento** [...] non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7*» (ovvero gli obblighi di utilizzare lo strumento di pagamento in conformità ai termini di contratto, nonché l'obbligo di comunicare senza indugio alla banca lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza e, in generale, l'obbligo di adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati).

Non solo, è chiarito che «*È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente*».

La banca, quindi, non solo deve dimostrare che l'operazione di pagamento è stata correttamente eseguita (autenticata, registrata e contabilizzata), ma, se vuole andare esente da responsabilità, deve anche **dimostrare il dolo o la colpa grave del correntista** sulla base di prove anche presuntive, ma che non si limitino alla mera allegazione del fatto dell'accesso abusivo allo strumento di pagamento.

Peraltro, la responsabilità della banca sussiste in talune ipotesi anche se il cliente ha agito con **colpa grave**. Dispone infatti l'art. 12 del citato decreto che «*Salvo il caso in cui abbia agito in modo fraudolento, l'utente non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b)*» (ovvero dopo la comunicazione alla banca dell'avvenuto smarrimento, furto, appropriazione indebita o uso non autorizzato dello strumento di pagamento non appena ne viene a conoscenza)[30].

In altri termini, la legge pone in capo alla banca che non ha adottato misure idonee a prevenire l'uso abusivo dello strumento di pagamento (ovvero il dispositivo o le procedure impiegate per eseguire gli ordini di pagamento) l'obbligo di risarcire il correntista anche se questo agisce con colpa grave, ovvero, per esempio, cade vittima di un phishing maldestro o è colpevole di omessa custodia delle chiavi[31]. Non si tratta pertanto di una responsabilità per condotta altrui,

[30] Altre ipotesi di responsabilità della banca sono richiamate dalla norma. Ad esempio, se questa non ha apprestato metodi adeguati di comunicazione utente-banca oppure se non ha adottato metodi di *autenticazione forte* (secondo, ad esempio, le Linee Guida di EBA).

[31] Cfr. Trib. Parma, 1268/2018, secondo cui se l'incauta custodia delle chiavi di accesso al conto in modalità *home banking* ha determinato l'accesso abusivo all'account del correntista e il compimento di disposizioni di bonifico abusive, la banca che non ha apprestato cautele adeguate di prevenzione, è tenuta al rimborso degli importi. A bene leggere la sentenza, il giudice – derogando all'art. 2051 c.c per cui il custode risponde dell'utilizzo abusivo delle cose in custodia – non ritiene necessario un nesso causale tra difetto di misure di sicurezza e frode, ma ravvisa la responsabilità della banca per il sol fatto di non aver apprestato adeguate cautele.

ma di una **responsabilità per condotta propria**: ovvero il non aver apprestato a priori idonee misure di sicurezza. Sicché, la banca risponde del danno occorso al correntista non tanto perché essa ha effettivamente una qualche colpa nel non aver impedito il fatto, ma perché, per ragioni di equità sostanziale, il legislatore ha scelto di allocare il rischio frode in capo alla parte forte del rapporto bancario. Siamo di fronte ad una sorta di responsabilità oggettiva del fornitore, solo un po' attenuata dalla prova liberatoria (e diabolica) del dolo del correntista.

Inversione del normale onere probatorio nel GDPR

Come accennato, l'impianto normativo del Decreto nella nuova formulazione che recepisce la PSD2, ricalca l'impostazione del GDPR. Le due normative, infatti, sottendono la medesima *ratio*: il prestatore di servizi di pagamento, così come il titolare del trattamento, è sempre un soggetto che compiendo un'attività di impresa espone i clienti ad un rischio grave che incide su interessi e diritti fondamentali della persona.

Da un lato, vi sono interessi di carattere economico del cliente consistenti nella perdita dei fondi in deposito o giacenza presso il prestatore di servizi di pagamento. Dall'altro, vi sono diritti fondamentali sulla protezione dei dati personali per cui «*Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano*» (Art. 8 della Carta dei diritti fondamentali dell'Unione Europea – nota come Carta di Nizza).

Alla luce di quanto sopra, non sorprende che anche in tema di trattamento di dati personali la legge disponga l'inversione dell'onere probatorio.

L'art. 82.3. GDPR recita: «*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2* [n.d.r.: per i danni causati da violazione del GDPR] *se dimostra che l'evento dannoso non gli è in alcun modo imputabile*».

Il portato della disposizione appena richiamata è chiarito dal Considerando 146 del GDPR: «*Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile*»[32].

Quanto sopra esprime un principio del GDPR (già presente nella precedente direttiva 95/46/CE) e cioè che il titolare del trattamento è sempre tenuto a fornire la prova della sua completa estraneità all'evento dannoso. Si tratta, come nel caso del Decreto, di una **prova diabolica** la quale è tuttavia possibile dare, come suggerisce lo stesso GDPR, dimostrando di aver adottato *idonee misure di sicurezza*.

[32] La nuova formulazione del GDPR, nella sostanza, non è diversa da quella, ora abrogata, del vecchio testo del Codice Privacy (D.Lgs. 196/2003) che, all'art. 15 (Danni cagionati per effetto del trattamento) prevedeva «1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 [principi del trattamento]». Va quindi richiamato l'art. Art. 2050: «Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno». L'inversione dell'onere probatorio recepito dal Codice Privacy fin dal 2003 è peraltro mero adeguamento alla prima Direttiva 95/46/CE (art. 23, comma 2).

Misure di sicurezza

L'art. 24 GDPR dispone che «*il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*». In particolare, il titolare del trattamento è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di **dimostrare** la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure (considerando 74 GDPR).

Andando più nel particolare, per dimostrare la conformità con il GDPR, il titolare del trattamento deve (considerando 28 GDPR):

A. adottare procedure e policy di trattamento dati, anche verso i responsabili del trattamento (disporre politiche aziendali e verificare periodicamente i loro rispetto);

B. provvedere alla protezione dei dati fin dalla progettazione (*privacy by design*);

C. proteggere i dati per *impostazione predefinita*, ovvero nella prospettiva degli interessi del soggetto interessato (*privacy by default*);

D. ridurre al minimo il trattamento dei dati personali (minimizzazione);

E. pseudonimizzare i dati personali non appena possibile;

F. offrire trasparenza per quanto riguarda le finalità e il trattamento di dati personali (informativa specifica);

G. mettere a disposizione del soggetto interesso strumenti di facile esercizio dei diritti (contatti email, tempestivo riscontro);

H. provvedere a ciclo continuo alla revisione delle procedure e delle misure di sicurezza;

I. essere in grado di dimostrare documentalmente tutto quanto precede.

Si tratta di una lista indicativa, ma non sufficiente, degli adempimenti che un titolare del trattamento deve eseguire (e mantenere) per andare esente da responsabilità in caso di frode informatica.

È infatti opportuno che il titolare sia continuamente aggiornato delle fonti indicative delle miglior prassi di tutela dei dati personali e che, soprattutto, incardini un "sistema" di sorveglianza e verifica efficacie.

A tale riguardo è per esempio utile fare riferimento al **Provvedimento 192** del 12 maggio 2011 (in tema di circolazione delle informazioni riferite a clienti all'interno dei gruppi bancari e ´tracciabilità´ delle operazioni bancarie) il quale indica quali sono le misure necessarie e opportune nell'esercizio dell'attività bancaria e che integrano quanto previsto dal GDPR:

a) corretta e tempestiva designazione dei responsabili del trattamento (monitoraggio della loro attività);

b) tracciamento con log di sistema delle operazioni effettuate dai soggetti incaricati (e conservazione non inferiore a 24 mesi);

c) predisposizione di *alert* di operazioni di *inquiry* eseguite dagli incaricati del trattamento[33];

d) svolgimento periodico, almeno annuale, di audit interni.

L'importanza di adottare misure di sicurezza "idonee", conformi cioè alle indicazioni del GDPR, del Garante Privacy e della miglior prassi, non è solo una questione di responsabilità del titolare (banca), ma anche di misura del danno risarcibile. Un **corretto presidio privacy** infatti – che non sia cioè solo formale (predisposizione di documenti), ma anche sostanziale (effettiva conoscenza della privacy aziendale da parte di tutto il personale del titolare) – è tanto più importante se si considera che, a differenza di quanto previsto per la violazione del Decreto, in caso di violazione del GDPR il titolare del trattamento risponde anche per responsabilità per danno non patrimoniale.

Importanza del GDPR: il danno non patrimoniale.

Come visto, mentre il Decreto mira a tutelare il risparmio, e quindi un interesse prettamente economico, il GDPR mira a tutelare un diritto fondamentale dell'individuo.

Per tale ragione, la misura del danno risarcibile, in caso di violazione del GDPR, travalica i limiti della dimensione patrimoniale e sconfina nel **danno non patrimoniale**, ovvero quel danno che non ha ricadute di ordine monetario sul soggetto leso, ma ricadute meramente soggettive di sofferenza interna (patema d'animo) che si riflettono nella sua qualità della vita, nelle relazioni personali e, in generale, nella percezione di sé e, in modo riflesso, nella percezione che gli altri hanno di noi.

Ebbene, ai sensi dell'art. 82.1. del GDPR «*Chiunque subisca un danno materiale o immateriale*[34] *causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*».

Non v'è dubbio, pertanto, che il danno non patrimoniale sia una voce di risarcimento nuova e diversa rispetto a quella già prevista dal Decreto e che, in un'ottica di tutala dei dati personali e degli effetti per il loro trattamento illegittimo, il titolare deve sempre prendere in seria considerazione.

Accade infatti che mentre il danno patrimoniale è, il più delle volte, facilmente quantificabile in termini contabili e pari quindi all'ammontare del credito frodato, il danno non patrimoniale viaggi su logiche completamente diverse. Allorché il giudice deve apprezzare tale voce di danno, si possono aprire scenari assai incerti con la possibilità di liquidazione del danno per somme rilevanti.

(*Segue*) Sanzioni amministrative

[33] Ma vedi, ad esempio, l'obbligo introdotto dal D.Lgs. n. 90/2017 di predisporre (già in recepimento della c.d. IV direttiva AML) degli *alert* da implementare nel sistema di monitoraggio per la verifica e segnalazione di operazioni sospette.

[34] L'espressione «*danno materiale e immateriale*» va inteso, secondo il lessico giuridico nostrano, come «danno patrimoniale e non patrimoniale».

La frode informatica, nella prospettiva del GDPR, apre la possibilità non solo al danno non patrimoniale, ma anche alle sanzioni amministrative del Garante Privacy.

Un presidio privacy non adeguato, accertato come tale a seguito di una denuncia per frode informatica, espone infatti il titolare del trattamento alle sanzioni comminate dall'autorità di controllo che, ai sensi del GDPR, sovrintende al rispetto della normativa privacy anche attraverso provvedimenti punitivi e di deterrenza.

In tale prospettiva, il compito del Garante Privacy non è risarcire il correntista danneggiato (per questo occorre avviare un'azione giudiziaria o innanzi all'ABF), ma è sanzionare il titolare che non ha adottato misure di sicurezza efficaci nella prevenzione delle frodi informatiche. Il più delle volte, il provvedimento sanzionatorio è il primo passo per l'azione giudiziaria e che ne avvalora i presupposti.

A tale riguardo, vale la pena ricordare che le sanzioni, nei casi più gravi, possono arrivare ad un massimale di 20 milioni di Euro o del 4% del fatturato mondiale del titolare del trattamento (art. 83 GDPR) e che si assiste da qualche tempo ad un progressivo innalzamento delle sanzioni effettivamente comminate dalle autorità europee.

Conclusioni

In tema di frodi informatiche rileva sempre un profilo di trattamento illecito di dati personali, tale essendo senz'altro quello attuato in primo luogo dal frodatore (accesso non autorizzato ai dati del correntista, quanto meno quelli finanziari), ma senza per ciò escludere anche quello che investe direttamente la banca in caso di difetto di adozione di misure di sicurezza adeguate.

La normativa applicabile (il Decreto e il GDPR), infatti, introduce una sorta di **responsabilità oggettiva attenuata** in capo al fornitore di servizi di pagamento secondo la quale egli risponde salvo che dimostri il dolo del cliente ovvero di aver adottato le migliori misure di sicurezza logiche, fisiche ed organizzative disponibili al momento della frode.

Per di più, il GDPR, nell'accertamento del danno e delle conseguenze economiche per il titolare, introduce elementi di quantificazione generale che vanno ben al di là di quanto previsto dalla normativa regolamentare del D.Lgs. 11/2010. La banca, infatti, per la violazione della normativa privacy, può rispondere anche per **danno non patrimoniale** procurato al correntista frodato e, in termini amministrativi, può essere destinataria di **provvedimenti sanzionatori** di importo assai elevato.

Truffa informatica e la tutela penale della Banca

A cura di Stefano Gerunda, Partner, La Scala Società tra Avvocati

1. Reati informatici: maggiore attenzione del legislatore e dell'autorità giudiziaria. "La vittima al centro".

Vi è sempre maggiore attenzione da parte del legislatore penale in merito ai reati informatici e alle frodi commesse tramite strumenti telematici. Ciò è dovuto anche alla forte spinta europea e sovranazionale che tiene conto del sempre maggior uso da parte di soggetti dediti alla commissione di crimini di nuove e articolate tecnologie informatiche.

È necessario, infatti, considerare che questa tipologia di frodi è sempre più comune e il numero di denunce da parte delle vittime di tali reati è aumentato esponenzialmente con l'arrivo della pandemia di COVID-19 (nel biennio 2020 – 2021 c'è stato un vero e proprio "boom" di denunce da parte delle vittime di delitti informatici).

Ciò è dovuto, da un lato, alla iniziale impossibilità durante il periodo di *lockdown* del delinquente comune di allontanarsi dal domicilio per compiere reati, costringendolo dunque a "reinventare" la propria attività criminale. Dall'altro lato, il dilagare del lavoro in regime di *smart-working* ha comportato per le aziende e i lavoratori una maggiore esposizione al rischio che terzi malintenzionati acquisiscano illecitamente dati informatici ed in seguito li sfruttino.

Tale aumento della commissione di frodi informatiche – *trend* positivo che comunque era già rilevabile prima dell'avvento della pandemia ma che, come detto, con il *lockdown* ha subito una vera e propria crescita esponenziale – ha spinto il legislatore ad introdurre specifiche fattispecie di reato finalizzate a punire condotte predatorie commesse tramite strumenti telematici. Da ultimo, a fine 2021 sono state introdotte alcune nuove fattispecie di reato poste a tutela di coloro che si avvalgono di strumenti di pagamento diversi dal contante e che puniscono le frodi commesse tramite strumenti di pagamento telematici (carte di credito, bonifici disposti tramite sistemi *home banking* ecc.).

Alla maggiore attenzione del legislatore al fenomeno delle frodi informatiche ha fatto da contraltare l'Autorità Giudiziaria, la quale ha impiegato – ed impiega – sempre più risorse nel contrasto dei delitti informatici. Basti pensare che le indagini concernenti reati informatici sono soprattutto di competenza della Procura distrettuale, la quale è di norma competente ad indagare su delitti che destano particolare allarme sociale (mafia, terrorismo, violenza sessuale, ecc.). Proprio la Procura distrettuale di Milano è sempre più orientata al contrasto di crimini informatici con uno specifico Pool investigativo specializzato (appunto detto "Pool reati informatici").

L'allarme sociale provocato dai reati informatici ha portato Pubblici Ministeri e Giudici a porre particolare riguardo alla vittima di detti delitti, la quale molte volte non trova ristoro nel procedimento penale poiché gli autori del reato hanno già speso tutto il profitto o non hanno beni intestati. Di conseguenza, l'azione civile di risarcimento del danno nell'ambito del procedimento penale non solo si rivela infruttuosa ma spesso consiste solo in spese legali sostanzialmente inutili da parte della vittima. Si aggiunga poi che non sono rari i casi in cui gli autori del reato non vengono affatto individuati dall'Autorità Giudiziaria, rimanendo dunque impuniti.

Inoltre, anche nei casi in cui i criminali vengano effettivamente individuati, nell'ambito del processo penale la scelta più frequente dei truffatori informatici è quella di aderire a riti alternativi al dibattimento, quali il rito abbreviato o il patteggiamento. Tali riti alternativi escludono la possibilità che la vittima chieda il risarcimento del danno nell'ambito del processo penale (nel caso del patteggiamento) o comunque limitano fortemente la possibilità del danneggiato di provare l'entità del pregiudizio subito (nel caso del rito abbreviato).

L'attenzione per la vittima di reati informatici ha portato la giurisprudenza e le istituzioni a prevedere dunque sistemi diversi ed ulteriori affinché le vittime di delitti informatici trovino ristoro, come la creazione di fondi *ad hoc* finalizzati a indennizzare la persona offesa dal reato.

2. I reati informatici commessi con maggiore frequenza.

Fatta tale premessa, è necessario evidenziare quali sono le principali fattispecie di reato commesse dai c.d. *hacker*.

La prima fattispecie che viene commessa dal delinquente è l'accesso abusivo ad un sistema informatico, punito dall'art. 615 ter c.p. Tale norma, come emerge già dal titolo del reato, punisce chiunque si introduca in un sistema informatico protetto da misure di sicurezza – banalmente, qualsiasi sistema protetto da una *password* – contro la volontà del proprietario. Tale fattispecie viene quasi sempre integrata da colui che commette il c.d. *phishing*, il quale prevede appunto l'apprensione delle *password* della vittima del reato al fine di accedere ai propri *account* personali.

La seconda norma da tenere in considerazione è l'indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti *ex* art. 493 *ter* c.p. (introdotto a fine 2021 con il D. Lgs. 184/2021). La norma punisce chi commette frodi tramite l'utilizzo non autorizzato di strumenti di pagamento telematici o tramite una loro falsificazione. Si pensi, ed è un caso che avviene con relativa frequenza, a colui che carpisce illecitamente i dati di una carta di credito e poi la utilizzi all'insaputa dell'intestatario per compiere acquisti *online*.

La terza norma rilevante è il delitto di frode informatica (art. 640 ter c.p.) che prevede la punizione della reclusione per chiunque alteri in qualsiasi modo il funzionamento di un sistema informatico procurando a sè o ad altri un ingiusto profitto con altrui danno. Per evidenziare un esempio di frode informatica si pensi sempre al *phishing*. Secondo la giurisprudenza penale, il *phisher*, dopo aver acceduto illecitamente al sistema informatico, commette il delitto di frode informatica se trasferisce valori o altre utilità in favore suo o di terzi, provocando un danno alla vittima. Il caso tipico è quello dell'accesso abusivo ad un *account* bancario, ove il *phisher* trasferisce a sé o ad altri tramite bonifico il denaro del correntista.
Ciò fino all'introduzione del reato di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti, *supra* analizzato.
Dopo l'introduzione dell'art. 493 *ter* c.p., avvenuta come detto a novembre 2021, parrebbe essere applicabile l'art. 493 *ter* c.p. a tutte le ipotesi di utilizzo illegittimo di mezzi di pagamento immateriali e di considerare come residuale l'art. 640 *ter* c.p., vista la specificità della nuova norma. Dunque, l'illecito trasferimento di valori commesso dal *phisher* parrebbe integrare oggi il nuovo reato di utilizzo indebito di strumenti di pagamento diversi dal contante.

Altra fattispecie integrata frequentemente nell'ambito dei reati informatici è la sostituzione di persona *ex* art. 494 c.p. Tale norma viene violata quanto l'*hacker* carpisce l'identità della vittima e si avvale di essa per compiere operazioni *online* – anche finanziarie e spesso illecite – a suo nome.

Ulteriori norme penali rilevanti sono quelle che disciplinano il mero danneggiamento di sistema informatico, punito dagli artt. 635 *bis*, *ter* e *quater* c.p. Tali norme sono integrate quando l'*hacker* non pone in essere trasferimenti di valori ma quando esegue azioni finalizzate solo a danneggiare un sistema informatico. Esempio tipico è l'attacco cibernetico ai sistemi bancari che bloccano (anche temporaneamente) i sistemi di pagamento elettronici o comunque non permettono agli Istituti di credito di operare tramite le proprie reti *intranet*.

Ultimo reato rilevante è il riciclaggio di denaro (art. 648 *bis* c.p.) commesso solitamente quando l'*hacker*, una volta ottenuti illecitamente valori tramite un reato informatico, si avvalga di ulteriori conti correnti bancari per "lavare" il denaro provento del delitto oppure impieghi tale provento in altre attività finanziarie, come l'acquisto di criptovalute.

3. Problemi in sede penale per la Banca in caso di truffe informatiche poste in essere ai danni dei clienti.

Ovviamente, la commissione di reati informatici può avere dei risvolti critici per un Istituto di credito qualora vittima della frode sia il cliente della Banca e il truffatore si sia avvalso dei sistemi telematici dell'Istituto per commettere il delitto.

Il primo attiene alla possibilità del cliente (che è persona offesa dal reato e può costituirsi parte civile nell'ambito di un processo penale a carico del criminale informatico) di agire contro la banca in sede penale, la quale potrebbe venire citata in giudizio come responsabile civile per ottenere il risarcimento del danno patito.

In altri termini, il cliente – anziché agire in sede civile nei confronti della Banca – cita l'istituto nel procedimento penale ed in tale sede chiede il risarcimento del danno subito.

Il secondo profilo di criticità riguarda invece la possibilità che una Procura distrettuale particolarmente zelante svolga atti d'indagine in merito alle procedure della Banca.

Atti d'indagine aventi una duplice finalità: i) la prima è verificare se vi sia una qualche collusione di dipendenti dell'ente con i truffatori che commettono frodi informatiche (il c.d. basista); ii) la seconda è quella di verificare che la Banca abbia trattato correttamente i dati personali della clientela. Il trattamento illecito dei dati personali dei clienti della Banca potrebbe infatti costituire una violazione della normativa in tema di *privacy* con conseguente integrazione delle fattispecie di reato previste dal Codice della Privacy agli artt. 167 e ss.[35]

4. La tutela penale nel caso in cui la vittima della frode sia direttamente la Banca.

Qualora invece la Banca sia vittima della frode informatica (da sola o insieme al cliente correntista), intendendo con il termine "vittima" il fatto che la Banca abbia subito una perdita patrimoniale diretta, la tutela penale consiste nel depositare una querela alla Procura

[35] Art. 167: "1. *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.*
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 sexies e 2 octies, o delle misure di garanzia di cui all'articolo 2 septies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.
3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.
6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita";
Art. 167 *bis*: "*1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2 ter, 2 sexies e 2 octies, è punito con la reclusione da uno a sei anni.*
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione
3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167";
Art. 167 *ter*: "*1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.*
2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167".

distrettuale competente (eventualmente compiendo parallelamente indagini interne al fine di cristallizzare le prove "informatiche", ossia i dati).

Parimenti, anche qualora la truffa sia posta ai danni dei soli clienti (e dunque la banca non subisca un danno) pare opportuno informare la Procura della Repubblica di quanto avvenuto con un esposto c.d. difensivo e preventivo, tenendo sempre presente la possibilità che la magistratura indaghi sulla correttezza e idoneità delle procedure di sicurezza e controllo di cui la Banca si è dotata. A tal fine, si consideri che comunque con ragionevole certezza lo stesso cliente presenterà denuncia-querela all'Autorità Giudiziaria e dunque in ogni caso la Procura della Repubblica potrà porre in essere indagini sulle procedure dell'Istituto di credito.

5. Frodi informatiche e responsabilità amministrativa da reato *ex* D. Lgs. 231/2001 a carico della Banca: può esservi responsabilità penale della Banca per inadeguata protezione dei clienti dalle frodi informatiche?

Da ultimo, è necessario analizzare quali siano le conseguenze di una compiuta frode informatica per la Banca sotto il profilo della responsabilità amministrativa dell'ente *ex* D. Lgs. 231/2001. Tale decreto, come è noto, ha previsto una serie di sanzioni a carico della società applicabili dal Giudice penale quando venga commesso da un dipendente o un apicale dell'ente uno dei reati previsti dal decreto – i cc. dd. "reati presupposto" – a vantaggio o nell'interesse della società stessa.

Sanzioni che possono essere anche estremamente afflittive per l'ente imputato. Infatti, il legislatore ha previsto che alle società imputate possano essere applicate sanzioni pecuniarie e/o anche interdittive, finanche alla cessazione dell'attività d'impresa o alla revoca di permessi e concessioni pubbliche (di cui godono certamente gli Istituti di credito per esercitare la propria attività).

Proprio nel novero dei reati presupposto rientrano alcuni dei principali delitti commessi di frequente dall'*hacker*. Vien dunque da chiedersi se, in seguito alla commissione di un delitto informatico perpetrato tramite i sistemi bancari ai danni della clientela, possano essere applicate in sede penale alla Banca le sanzioni *ex* D. Lgs. 231/2001.

Attualmente la mancata previsione di strumenti di tutela del cliente dalle frodi informatiche (quale, ad esempio, l'autenticazione a plurimi fattori) non dovrebbe comportare una responsabilità della Banca ai sensi del D. Lgs. 231/2001.

Infatti, i principali reati informatici previsti dal D. Lgs. 231/2001 idonei a fondare la responsabilità dell'ente sono reati dolosi e dunque non parrebbe sussistere alcuna posizione di garanzia della Banca nella protezione della clientela da attacchi informatici.

La responsabilità amministrativa da reato in capo all'Istituto di credito potrebbe comunque sussistere qualora il reato venisse commesso anche con il contributo di un dipendente o apicale della Banca e sempre che quest'ultima ne avesse tratto un vantaggio o avesse avuto un interesse alla commissione del delitto.

Seppur siffatta ipotesi appaia remota, pare in ogni caso opportuno che la Banca si doti di idonee procedure finalizzate a prevenire il rischio che all'interno di essa possano essere commessi reati informatici, anche con l'ausilio di dipendenti o apicali dell'Istituto.

Autori:

Simona Daminelli, Partner, La Scala Società tra Avvocati

Antonio Ferraguto, Partner, La Scala Società tra Avvocati

Emiliano Branca, Ufficio cause e procedure legali, Banco BPM

Francesco Rampone, Of Counsel, La Scala Società tra Avvocati

Stefano Gerunda, Partner, La Scala Società tra Avvocati

Marta Casile, Trainee, La Scala Società tra Avvocati

Contatti: iusletter@iusletter.com

Supplemento a IusLetter del 29/06/2022

Testata registrata il 24.09.2001, presso il Tribunale di Milano, al n. 525/01.

LaScala
SOCIETÀ TRA AVVOCATI