PREMESSA INTRODUTTIVA

In un mondo informatizzato e globale il crimine sempre più spesso fuoriesce dalle fattispecie di reato "classiche" seguendo di pari passo l'innovazione tecnologica.

Sin dagli anni Ottanta / Novanta del passato secolo si constatò un *boom* di clonazione di carte di credito e utilizzo indebito di sistemi POS.

In questo primo scorcio del Duemila la nuova frontiera del crimine, grazie allo sviluppo impetuoso di *internet* e, soprattutto, ai suoi servizi che consentono di poter disporre subito dei nostri beni con un semplice ordine impartito dalla tastiera di un computer (il concetto del c.d. "*home banking*"), mira a sottrarre in qualsiasi modo i codici di accesso dei singoli soggetti così da potersi sostituire a loro e, naturalmente, impossessarsi in maniera illegittima di denaro o informazioni di natura privata e sensibile[1].

Sempre più spesso soggetti che operano e compravendono su *internet* scoprono, loro malgrado, di esser stati vittima del c.d. "*phishing*"[2]: in modo fraudolento, in genere tramite invio di *e –mail* che simulano la grafica ed il contenuto di istituti bancari od enti, vengono carpite le *password* (o dati sensibili) personali così da sottrargli una parte del proprio patrimonio o, comunque, poter accedere a pagine internet private.

Il legislatore italiano, in questi anni, ha tentato di correre ai ripari introducendo all'interno del codice penale nuove fattispecie di reato[3] oppure estendendo la disciplina sanzionatoria in modo

[1] Solo nella provincia di Milano si contavano circa 7.000 casi di truffa telematica nel solo anno 2003 (articolo di Alberto Berticelli, "*Reati ed arresti in aumento. Record delle truffe online*", Il Corriere della sera, 23 dicembre 2003); nel settembre 2012 quasi un terzo dei casi affrontati dall'Arbitro Bancario Finanziario in tema di problemi utenti / istituto di credito riguardano questo annoso problema (articolo di Manlio Torquato, " *Quando scatta il phishing il cliente può «salvarsi»*", Il Sole 24 ore, 29 settembre 2012).

[2] Termine ripreso dalla cultura anglosassone per intendere la sottrazione delle password di accesso ad un sistema elettronico; oltre a ciò si rammenta l'acquisizione fraudolenta dei codici delle carte di credito (*skimming*) e duplicazione degli stessi (*impriting)*

[3] Da ultimo, in tema di violazione telematica a sistemi protetti, vedasi l'art. 615 ter c.p.

tale da ricomprendere ogni violazione che scaturisca da queste nuove modalità ed offra una maggior tutela alla collettività[4].

Questi ed altri tentativi di bloccare questi episodi criminosi, purtroppo, vanno incontro ad un evidente limite: spesso l'autore della truffa non risiede (o comunque, è presente) fisicamente nel territorio nazionale ed utilizza server ed indirizzi IP di altri utenti, magari assolutamente ignari di esser "complici" del sistema truffaldino.

In definitiva, quindi, il soggetto leso, depauperato delle proprie credenziali e, nel caso di accesso illegale ai conti bancari, pure di una somma di denaro magari consistente, non ottiene alcun ristoro patrimoniale della perdita subita, dovendosi accontentare di presentare una semplice denuncia – querela avanti all'Autorità Giudiziaria ai danni di ignoti, quasi sempre irreperibili.

In questo breve studio, senza avere l'ambizione di ricostruire ogni singolo aspetto connesso alla materia, si indaga maggiormente sugli eventuali rimedi civilistici che possono essere esperiti da un soggetto – consumatore il quale, fatto oggetto di una truffa di tal genere, ipotizzi di voler chiedere al proprio intermediario / istituto di credito di tenerlo garantito per la somma pecuniaria illecitamente sottratta oppure di chiedere un risarcimento del danno a seguito della grave violazione della propria c.d. "*privacy*".

La strada, pur oggettivamente tutt'altro che semplice, può comunque poter riservare un risultato positivo.

[4] Nota, in tale materia, una delle prime condanne per "*phising*": Tribunale di Milano, sentenza del 10.12.2007 - est. Gamacchio (Giudice per l'udienza preliminare).

Si precisa subito che, a prescindere dalla volontà o meno di intraprendere concretamente una causa civile, vi sono alcuni passaggi che devono essere imprescindibili nel caso si sia vittima di "*phising*" al fine di tutelare al meglio i propri diritti.

RIMEDI GENERALI

Dapprima, constatata la violazione, sia essa di natura patrimoniale o meno, occorre attivarsi prontamente contattando l'istituto che gestisce il servizio al fine di ottenerne l'immediato blocco e limitare, per quanto possibile, i danni.

In genere l'istituto, avuta la comunicazione, agisce in via cautelare bloccando subito l'operatività dell'accesso e richiedendo, per ufficializzare e rendere definitivo il provvedimento assunto, la presentazione di una apposita denuncia – querela che potrà esser avanzata avanti all'Autorità Giudiziaria, in modalità scritta o anche orale, entro al massimo sessanta giorni dalla scoperta dell'evento.

Ciò, come sopra esposto, anche se difficilmente porterà alla precisa individuazione del reo od al recupero di quanto illegittimamente sottratto, avrà l'effetto di indurre (*rectius* : dovrebbe indurre…) l'Autorità Giudiziaria ad indagare sull'evento.

In prospettiva futura, comunque, la denuncia – querela potrebbe esser prodotta come prova documentale in sede di procedimento civile dimostrando che il soggetto si è fatto parte diligente, attivandosi subito appena resosi conto dell'evento lesivo.

Quest'atto formale, altresì, potrebbe fornire ulteriori prove a favore del danneggiato: le indagini, infatti, pur senza giungere all'individuazione del reo, potrebbero fornire elementi interessanti quali l'indirizzo IP da cui ha avuto origine la violazione, se ha colpito serialmente, in che modo

eventualmente è riuscito ad aggirare i sistemi di sicurezza dell'istituto che doveva custodire i dati.

Tutto ciò aiuta a chiarire la pericolosità effettiva e il grado di sicurezza concretamente offerto dall'intermediario che custodiva i dati.

Appare opportuno coltivare la denuncia recandosi periodicamente ad assumere informazioni presso l'Autorità e facendo presente (col suggerimento di farlo verbalizzare) sin dal primo momento che si vuole essere informati in caso di archiviazione della *notitia criminis*, così, in futuro, quando sarà comunicato il provvedimento del PM, valutare se sia il caso di opporsi a tale richiesta oppure rinunciare definitivamente alla prosecuzione[5].

In questo modo, a prescindere dai risultati finali delle indagini, si potranno raccogliere preziose informazioni per il tramite di un canale ufficiale e sicuro, qual è quello delle forze di polizia.

Spesso, una volta bloccato il servizio e presentata la denuncia – querela, può essere utile contattare l'istituto chiedendo sin da subito la restituzione degli importi sottratti illegittimamente oppure un risarcimento per il danno alla c.d. "*privacy*" derivante dalla violazione subita.

In tale richiesta potrebbe essere opportuno richiedere all'intermediario altresì di verificare l'IP del computer da cui è partita l'operazione fraudolenta.

Ciò, come sopra espresso, sarà fatto anche dall'Autorità che indaga sulla vicenda ma potrebbe mettere "pressione" all'istituto[6] e far emergere eventuali mancanze.

[5] Richiesta ai sensi e per gli effetti dell'art. 408 c.p.c., con possibilità di opporsi ad un'eventuale archiviazione delle denuncia – querela.

[6] Questa attività di ricerca e controllo è molto facile per istituti professionisti. Di recente, il Tribunale di Siracusa, con sentenza 15.05.2012, ha ritenuto sussistere tale responsabilità in capo alla convenuta proprio perché "*le Poste*

Si precisa sin da subito che, in genere, queste richieste sono frustate dal rifiuto dell'istituto.

Quest'ultimo, spesso, a propria difesa sostiene che la colpa dell'intera vicenda possa imputarsi al danneggiato stesso poiché non diligente nell'evitare che la *password* fosse carpita da soggetti terzi.

Si ricordi, infatti, che se da un lato l'istituto ha un preciso obbligo di vigilanza, dall'altro ogni soggetto che aderisce ad un servizio *online* ha il preciso obbligo di usare la dovuta diligenza nell'utilizzo delle proprie credenziali.

Il soggetto, altresì, deve dimostrare di avere a disposizione una protezione efficace da eventuali virus o *malware* che, in caso contrario, potrebbero aver infettato il computer e fornito i dati necessari al truffatore.

A questo punto, se il soggetto ritiene di proseguire nella sua azione, ritenendo oggettivamente di non aver posto in essere una condotta in alcun modo rimproverabile, vi sono più soluzioni.

Si può avanzare una richiesta avanti ad uno degli istituti di mediazione riconosciuto dal Ministero della Giustizia[7] preparando una memoria scritta che riassuma quanto accaduto ed un piccolo elenco con tutti i documenti raccolti a suffragio della propria tesi.

Il ricorso viene analizzato da un esperto mediatore nel settore il quale, lette anche le memorie difensive dell'istituto, cerca, in sede di incontro fra le parti, spesso assistite da legali, di far trovare un accordo che possa sistemare la questione in maniera soddisfacente.

La strada ora indicata è caldamente consigliata.

---

avevano subito rilevato l'anomalia rappresentata dall'insolito indirizzo IP utilizzato per la transazione e difatti avevano segnalato l'accaduto allo specifico servizio antifrode" pur senza poi bloccare l'ordine di bonifico.

[7] L'organismo deve essere iscritto presso il Ministero della Giustizia del registro degli Organismi di Mediazione, come da disposizioni contenute nel P.D.G. del 15/09/2011 ai sensi del Decreto Legislativo 4 marzo 2010 n. 28 e successive modifiche

Occorre precisare infatti come, a seguito dell'entrata in vigore di alcune norme c.d. "Decreto Fare"[8], a partire dal 21.09.2013 è stata introdotta[9] l'obbligatorietà della mediazione in tema di servizi bancari o responsabilità extracontrattuale così che, prima di poter procedere alla causa civile, occorrerà necessariamente adire un istituto di mediazione per esperire un tentativo di conciliazione.

A seguito del fallimento di quest'ultimo, per impossibilità all'accordo o mancata presenza di una delle parti, sarà "finalmente" possibile adire la strada giudiziaria per il riconoscimento delle proprie ragioni.

RIMEDI IN AMBITO DI AZIONE GIUDIZIARIA CIVILE

Analizziamo ora le tematiche di diritto che potrebbero essere fatte valere in corso di causa precisando subito che attengono a fattispecie ove sia sorto sia un danno patrimoniale che non patrimoniale (es. correntista che ha visto sottrarsi illegittimamente il proprio denaro, perdendo così le somme e, contestualmente, sia stato così vulnerato nel proprio diritto alla riservatezza ed al controllo dei propri dati personali), ma alcune sono utilizzabili anche da soggetti che non abbiano subito direttamente un danno strettamente economico ma, piuttosto, un *vulnus* al proprio diritto alla riservatezza (es. sottratta la *password* universitaria)

- *VIOLAZIONE OBBLIGHI DEL MANDATARIO AI SENSI E PER GLI EFFETTI DELL'ART. 1711 C.C. E 1856 C.C.*

[8] L'obbligatorietà della mediazione è stata reintrodotta con il decreto legge 21 giugno 2013, n. 69 (poi convertito dalla legge 9 agosto 2013, n. 98), dopo che la Consulta nel 2012 aveva dichiarato incostituzionale la precedente disciplina, contenuta nel d.lgs 28/2010, in tema di mediazione obbligatoria.

[9] *rectius*: reintrodotta visto che sussisteva già dal marzo 2011 all'ottobre 2012

Il rapporto contrattuale che lega l'istituto al singolo cliente – consumatore integra un rapporto di conto corrente bancario *ex* art. 1838 c.c.

Ai sensi dell'art. 1856 c.c. l'istituto di credito risponde dell'esecuzione di incarichi per conto del cliente – risparmiatore secondo le regole del mandato sancite dagli artt. 1703 ss. c.c.

Nel contratto di attivazione del rapporto, poi, si prevede la possibilità per il cliente (che, si ricordi, è un consumatore) di poter usufruire del servizio "*home banking*", cioè consentire alla parte di dar mandato all'intermediario di utilizzare le proprie sostanze disponibili nel conto corrente per le operazioni espressamente indicate e consentite.

Come insegna l'art. 1710 c.c. ss. (richiamato dall'art. 1856 c.c.) il mandatario, cioè nel caso di specie la convenuta, è tenuto a eseguire il mandato con la diligenza del buon padre di famiglia e non può in alcun modo eccedere i limiti di quanto ordinato.

Si precisa infatti che ogni atto esorbitante tali ordini resta a carico del mandatario.

Contestualizzando la disciplina testé enunciata, appare evidente come l'istituto debba eseguire in modo diligente ciò ordinato dal cliente.

Se si eseguono operazioni senza questo necessario consenso, l'operazione stessa resta in capo al mandatario poiché, logicamente, mai voluta dal mandante.

Secondo la giurisprudenza, infatti, nel momento stesso in cui il mandante disconosce l'operazione, scatta l'obbligo restitutorio e reintegrativo.

L'operazione fraudolenta, quindi, è inquadrabile come atto estraneo al mandato e, come tale, completamente in capo al mandatario.

Tale impostazione è stata confermata, più di recente, da sentenze dell'Arbitro Finanziario Bancario (sez. Napoli, 18.04.2011) in cui si enuncia questo fermo principio: "*Nella presente*

vicenda sembra al Collegio che la prima delle due domande proposte dal cliente - quella con cui si chiede la "restituzione" dell'importo oggetto del bonifico "disconosciuto" in quanto impartito fraudolentemente da terzi dal cliente - si collochi nella prospettiva delineata dall'art. 1711 c.c., con la conseguenza, allora, che una volta soddisfatta la condizione del tempestivo disconoscimento dell'operazione come - il che può dirsi senz'altro avvenuto nel caso di specie, avendo il cliente proceduto tempestivamente anche alla denuncia della frode sofferta alle forze dell'ordine (oltre che alla Procura della repubblica) - resta evidentemente esclusa qualsiasi considerazione in punto di concorso di colpa del cliente".

Se l'intermediario ritenesse che la colpa fosse da imputarsi in capo al privato non potrebbe limitarsi ad asserire che spetti a esso provare di aver adottato tutte le cautele[10] quanto, piuttosto, dovrebbe attivarsi dimostrando che l'ordine derivi proprio dal soggetto e, in caso contrario, dimostrare la colpa dallo stesso, peraltro con il requisito della gravità di quest'ultima!

Infatti il D.Lgs. 11 del 2010, all'art. 10, affrontando la tematica delle truffe informatiche, sancisce, al secondo comma, che «*quando l'utilizzatore dei servizi di pagamento neghi di aver autorizzato un'operazione, l'utilizzo di uno strumento di pagamento registrato dal prestatore 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*».

La *ratio* di tale disciplina è chiara.

Nei casi di truffe informatiche sussiste la contrapposizione di due parti in causa: il cliente – consumatore danneggiato e l'intermediario professionista.

[10] Appare una *probatio diabolica* in capo al cliente – consumatore.

Pretendere, come spesso fanno gli intermediari, che spetti al consumatore privato dimostrare di aver ben operato e non aver posto in essere condotte che potrebbero aver messo a rischio le proprie credenziali, supera la possibilità oggettiva del singolo.

Ad ogni modo nessun eventuale valore può esser concesso a clausole contrattuali che si pongano in senso di gravare l'utente di tale onere probatorio e che, spesso, sono contenute nei contratti *standard* fatti sottoscrivere alla clientela.

Tale indirizzo si basa sugli orientamenti emersi a tutela della disciplina posta dalla previsione dell'art. 33, comma 2, lettera b) del codice del consumo (d. lgs. n. 206/2005), alla stregua del quale "*si presumono vessatorie fino a prova contraria le clausole che hanno per oggetto, o per effetto, di (…); b) escludere o limitare le azioni o di diritti dei consumatori nei confronti del professionista o di un'altra parte in caso di inadempimento totale o parziale o di adempimento inesatto da parte del professionista. Pertanto, una clausola siffatta, in quanto vessatoria, deve ritenersi inopponibile al consumatore: la legge citata (art. 36, comma 3) ne sancisce infatti la nullità, la quale "opera soltanto a vantaggio del consumatore e può essere rilevata d'ufficio dal giudice*".

Tale orientamento, infine, segue il principio generale previsto dall'art. 2698 c.c. che impedisce che le parti possano invertire l'onere della prova ove quest'ultima sia eccessivamente complessa o cagioni oneri eccessivi in capo alla parte gravata.

Quindi l'eventuale onere della prova, secondo quanto appena esposto, pone l'eventuale onere della prova in tema di scarsa diligenza nella conservazione delle *password* (o, più in generale dei dati sottratti) da parte dell'utente in capo all'intermediario.

La giurisprudenza, a sostegno di quanto appena esposto, è intervenuta con alcuni pronunciamenti.

Si osservi che "*ad avviso del Collegio,* (tali disposizioni) *indicano che l'onere della prova che l'operazione sia stata effettivamente autorizzata dal cliente sia oggi posto, inderogabilmente, a carico dell'intermediario, e che dunque non possano considerarsi più valide clausole, come quelle di specie, che accollando sempre e comunque al cliente la paternità dell'ordine per il solo fatto che si sia riscontrato un uso delle chiavi di identificazione contrattualmente attribuitegli, mirano a ribaltare l'impostazione imperativamente prevista a tutela dell'utilizzatore del servizio di pagamento, e quindi ad onerare quest'ultimo della dimostrazione - costituente, all'evidenza, una probativo diabolica, anche perché relativa ad un fatto negativo - che egli non abbia, imprudentemente, reso noto a terzi le proprie credenziali di identificazione, ovvero non abbia, imprudentemente, abboccato a tentativi di pishing"* (ABF Napoli, 18.04.2011).

Fatta questa premessa in tema di onere probatorio, totalmente in capo all'intermediario per le motivazioni appena analizzate, si osserva come l'eventuale dimostrazione dell'eventuale profilo di colpa imputato al privato (magari correntista), non potrà fermarsi alla dimostrazione della semplice "disattenzione" od ingenuità dello stesso ma dovrà sancire una <u>colpa grave e certa</u>.

L'art. 12 D.Lgs 11/10, legiferando in materia a seguito dell'adeguamento del nostro ordinamento alla direttive dell'Unione Europea 2007/64/CE afferma, infatti, che la responsabilità è sempre presente in tale materia in capo all'intermediario "*salvo il caso in cui l'utilizzatore abbia agito con dolo o colpa grave"*.

L'onere probatorio che dimostri la colpa nella sua "gravità" dovrà essere accurato e preciso, non bastando una "presunzione" per imputare concretamente una colpa "grave".

Infatti sempre una statuizione dell'ABF (Roma, 18.01.2011) afferma che l'esser oggetto di azioni di *phishing "quand'anche non valgano ad escludere un comportamento colposo del cliente, certamente non valgono a dimostrare la sua colpa grave".*

OBBLIGHI RISARCITORI IN CAPO ALL'INTERMEDIARIO

Secondo l'impostazione giurisprudenziale, come sopra meglio analizzato, gli intermediari professionisti hanno i mezzi e le capacità tecniche per "intercettare" un insolito IP da cui sorge l'ordine di bonifico, potendo cercare di prevenire la truffa.

Oltre a ciò l'intermediario ha sempre un preciso e chiaro obbligo di diligenza e controllo su tutte le operazioni svolte.

Da questa inerzia, scaturiscono due profili di responsabilità risarcitoria.

- *VIOLAZIONE DETTATO EX ART. 15 E 31 D.LGS.196/03*

A cagione della violazione del sistema (e della carenza di rimproverabilità in capo al privato essendosi comportato in maniera diligente), si può imputare all'intermediario la violazione del dettato dell'art. 31 del d.lgs 196/03 (il c.d. "Codice per la protezione dei dati personali") che disciplina le misure che vanno adottate per la custodia ed il controllo dei dati.

Tali prescrizioni parlano chiaro e mirano a ridurre al minimo, attraverso la predetta attività di controllo e custodia, la distruzione o perdita, anche accidentale, dei dati oppure un accesso non autorizzato oppure trattamento non consentito o non conforme alla finalità della raccolta.

A seguito di tale violazione l'intermediario dimostra di non aver tutelato il diritto alla c.d. "*privacy*", con grave *vulnus* morale (oltre che materiale) in capo all'utente.

L'art. 31 sopra meglio enunciato, infatti, si combina con l'art. 15 della medesima norma il quale così statuisce: "*art. 15. Danni cagionati per effetto del trattamento 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".

- *VIOLAZIONE DEL DOVERE DI DILIGENZA IN CAPO ALL'INTERMEDIARIO*

In virtù di quanto esposto, appare chiaro che le contestazioni all'intermediario non si fermano al non aver rispettato la diligenza del buon mandatario, ma si potrebbe contestare anche la violazione della diligenza del "buon banchiere" a cui erano stati affidati i risparmi e che, lungi dall'insospettirsi per un'operazione magari insolita (soprattutto se si usa poco l'*home banking*) e/o per un consistente ed anomalo importo e/o per il tramite di un computer con IP estero, non hanno vigilato sui risparmi depositati affidandosi, comunque, a strumentazioni vulnerabili ed inaffidabili.

Il fenomeno del *phising* non è purtroppo nuovo e moltissimi utenti della rete ne sono stati vittime.

Ciò impone un dovere di diligenza e controllo che non può (né deve) limitarsi a "scaricare" ogni eventuale danno in capo all'utente – consumatore, soprattutto alla luce dei progressi tecnologici, anche a favore di soggetti malintenzionati, i quali possono carpire tramite programmi, all'apparenza innocui, informazioni vitali.

Tale affermazione non trae spunto da un pensiero isolato ed, anzi, la giurisprudenza afferma un dovere in capo all'istituto che riceve l'ordine di verificarne l'autenticità e la verisimiglianza, come in T. Firenze, 30-04-2007 "*La banca, nell'esecuzione di un ordine di bonifico, è tenuta ad attenersi ai principi di correttezza e buona fede nell'esecuzione delle obbligazioni, e in particolare il suo comportamento deve improntarsi alla diligenza richiesta, in tema di mandato,*

dagli art. 1710 e 1711, 2º comma, c.c., come richiamati dall'art. 1856; tale diligenza comporta, in primo luogo, la verifica della conformità della firma a quella depositata e, in secondo luogo, richiede un'attenta valutazione di tutte le particolarità della fattispecie che possano fare dubitare della provenienza dell'ordine del mandante".

A conclusione si rammenti Cass. civ., sez. III, 09-02-2004, n. 2428 in cui si prevede "*In tema di mandato oneroso, il mandatario convenuto a seguito di azione di rendiconto deve fornire la prova non soltanto dell'entità e della causale degli esborsi, ma anche di tutti gli elementi di fatto sulle modalità di esecuzione dell'incarico utili per la valutazione del suo operato, in relazione ai fini perseguiti, ai risultati raggiunti e ai criteri di buona amministrazione e di condotta prescritti dagli art. 1710-1716 c.c.*"

L'intermediario, quindi, avrebbe dovuto attivarsi per vigilare e prevenire tali intrusioni illecite.

EVENTUALE DOMANDA SUBORDINATA RISPETTO ALLE RICHIESTE PRINCIPALI SOPRA FORMULATE: RESPONSABILITÀ DELL'INTERMEDIARIO OLTRE IL MASSIMALE DELLA FRANCHIGIA STABILITA EX ART. 12 C. 3 D.LGS 11/2010

Persino nell'eventualità in cui le tesi sopra esposte non apparissero sufficienti, la difesa del privato danneggiato potrebbe richiamarsi ai principi emersi dalla legislazione europea, e per inciso, dalla direttiva 2007/64/CE, trasfusa nel nostro ordinamento dal D.Lgs 11/2010, in cui, all'art. 61 della citata direttiva, si prevede "*1. (…) il pagatore sopporta, a concorrenza massima di 150 EUR, la perdita relativa ad operazioni di pagamento non autorizzate derivante dall'uso di uno strumento di pagamento smarrito o rubato o, se il pagatore non ha conservato in condizioni di sicurezza le caratteristiche di sicurezza personalizzate, dall'appropriazione indebita di uno strumento di pagamento. /2. Il pagatore sostiene tutte le perdite relative ad operazioni di*

pagamento non autorizzate subite agendo in modo fraudolento o non adempiendo uno o più degli obblighi a lui incombenti (…) intenzionalmente o con negligenza grave. In tali casi il massimale di cui al paragrafo 1 del presente articolo non si applica".

Tale principio è stato trasfuso nell'art. 12 c. 3 D.Lgs 11/2010 ove, si afferma, "*salvo il caso in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento, prima della comunicazione eseguita ai sensi dell'art. 7, co. 1, lettera b) (e cioè prima della comunicazione, rivolta al prestatore di servizi di pagamento, dell'appropriazione indebita o dell'uso non autorizzato dello strumento di pagamento da parte di terzi, n.d.r.) l'utilizzatore medesimo può sopportare per un importo comunque non superiore complessivamente a € 150 la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto o smarrimento*".

La disciplina testé riprodotta deve ritenersi applicabile non solo ai casi testualmente previsti.

Essa, infatti, "*risulta applicabile anche alla fattispecie contigua in cui oggetto del furto o comunque dell'utilizzo non autorizzato siano soltanto i codici personali identificativi di un determinato utilizzatore, a lui evidentemente sottratti attraverso una delle diverse tecniche all'uopo escogitate e note sotto il nome di "phishing", "trojan banking", ecc. tecniche già riscontrate e descritte da questo Arbitro in numerose precedenti occasioni"* (ABF, sez. Roma, n. 1258 /2011 e ABF sez. Roma n. 2478/2011).

In applicazione della ricordata regola, se "*può essere giustificata l'imposizione di una franchigia di € 150 a carico del cliente, altrettanto giustificato è che, per il rimanente, la perdita sia posta a carico della banca. Ciò in applicazione del principio del "rischio d'impresa" ma anche in*

considerazione dell'obbligo della banca, alla stregua di un criterio di diligenza professionale qualificata (la "diligenza del buon banchiere", connotata dal maggior grado di prudenza e di attenzione che la particolare qualificazione professionale dell'agente consente e richiede: cfr., ex multis, Cass., sez. I civile, 24 settembre 2009, n. 20543), nell'esecuzione di qualsiasi incarico conferitole dal cliente (cfr. art. 1856 c.c.), di adottare, nell'interesse dei clienti, tutti i presidi di sicurezza che l'attuale stadio di sviluppo della tecnica e della tecnologia consente" (cfr. Cass., sez. I civile, 12 giugno 2007, n. 13777).

CONSIDERAZIONI CONCLUSIVE

Giunti in conclusione all'esposizione, si avanzano poche considerazioni finali.

Un privato, danneggiato da un'operazione di "*phising*", potrà ben agire per il ristoro del proprio danno, sia esso di natura prettamente patrimoniale o non patrimoniale od entrambi, tenendo però ben conto delle concrete difficoltà esposte.

In particolare, per poter ottenere una pronuncia favorevole, dovrà essere in grado di ribattere ad eventuali osservazioni dell'intermediario in merito alla sua diligenza avendo cura di possedere un sistema antivirus sempre aggiornato e cercando di utilizzare con estrema accuratezza i propri dati personali.

Come meglio esposto, infatti, in capo all'intermediario non spetterà dimostrare una semplice colpa ma anche il requisito della "gravità", intendendosi una imperizia / negligenza / imprudenza di una norma di "buon senso" notevole.

Inutile aggiungere che il ristoro patrimoniale sarà solamente un lenitivo che non potrà mai ripagare interamente dai disagi subiti e l'unico effettivo rimedio concreto per ovviare a tali casi

resta l'utilizzo con la massima diligenza delle *password* e dei dati sensibili ed il controllo continuo delle operazioni compiute *online*.

(a cura di Bruno Ravagnan)

STUDIO LEGALE POLATO
30174 VENEZIA – MESTRE, VIA C. BATTISTI N. 7
TEL. 041 98 53 77 FAX 041 95 20 53
31100 TREVISO, STRADA COMUNALE CORTI N. 56 INT. 2
TEL. 0422 42 33 50 FAX 0422 31 60 98
studiolegalepolato@tiscali.it
www.banca-borsa.it