REP. 161/13

TRIBUNALE DI BARCELLONA P.G.

SEZIONE Distaccata di Milazzo

Il Giudice

sciogliendo la riserva assunta all'udienza del 19.4.2013 nella causa n. 15456/12 R.G.;
letti gli atti e i verbali di causa;

OSSERVA

parte ricorrente ha agito in giudizio al fine di ottenere previo accertamento della responsabilità di parte resistente la condanna di quest'ultima al rimborso della somma di € 9.180,150, oltre interessi e rivalutazione.

La stessa ha esposto di essere stata vittima di una frode telematica in quanto, in data 14.12.11, le è stata sottratta dal suo conto corrente la somma sopra indicata a seguito di un bonifico bancario effettuato ad opera di terzi ignoti.

Ritenendo responsabile dell'accaduto la [redacted] per omessa diligenza nell'esecuzione del contratto, parte ricorrente ha contestato l'omessa predisposizione ad opera dell'istituto bancario di adeguate misure di sicurezza idonee ad evitare intrusioni non autorizzate ad opera di terzi.

Il ricorso è fondato e, come tale, deve essere accolto.

Con riferimento alla descrizione dei fenomeni di natura informatica presi in esame nel presente procedimento, appare opportuno esporne una breve descrizione.

Con il termine *"pishing"*, si fa riferimento ad un'attività illegale che consiste nell'invio massivo di e-mail (o SMS) con falsa l'intestazione della banca, contenenti un link di collegamento a un "sito clone" (apparentemente identico al sito originale) ed un invito ad accedervi.

Cliccando sopra il link, si aprirà una falsa pagina di accesso al proprio conto corrente online, del tutto simile a quella vera.

Inserendo i dati personali, i malviventi avranno la possibilità di registrarli per poi accedere al tuo conto e ed effettuare operazioni illecite.

Con il termine di *"pharming"*, invece, si fa riferimento ad ulteriori tecniche di attacco informatico che prevedono o la modifica degli abbinamenti tra il dominio e l'indirizzo IP corrispondente a quel dominio -- cosicchè gli utenti connessi a quel Provider così, pur digitando il corretto indirizzo URL, verranno inconsapevolmente reindirizzati ad un server trappola appositamente predisposto per carpire le informazioni -- o un attacco al PC della vittima con l'ausilio di programmi trojan o tramite altro accesso diretto.

Ciò premesso, in materia di home banking, la tecnologia oggi disponibile ha consentito di raggiungere elevati livelli di sicurezza nella gestione delle transazioni finanziarie disposte dal cliente dalla propria postazione remota.

Al riguardo, i sistemi di sicurezza oggi comunemente adottati dagli istituti di credito sono sostanzialmente basati su un sistema di protezione c.d. *"di doppio livello"*.

Il cliente accede alla propria home page personale sul sito internet della banca tramite l'utilizzo di un codice cliente (c.d. user-id) che identifica univocamente l'utente nei sistemi informatici dell'istituto di credito, e di una password scelta dal cliente secondo determinati criteri, ad esempio password lunghe almeno otto caratteri, con uso di numeri, di lettere maiuscole o di caratteri speciali.
Attraverso questi codici identificativi, il cliente accede alle informazioni personali del suo conto, può verificare le disposizioni ed i pagamenti eseguiti, le spese contabilizzate sul conto, i movimenti della carta di credito collegata al conto, le eventuali domiciliazioni di bollette, ecc..
Questo sistema è comunemente noto come *"home banking informativo"*.
Non appare superfluo precisare che il cliente ha, chiaramente, l'obbligo di conservare diligentemente sia la user id che la password e di non comunicarle a terzi.
A questo primo livello di sicurezza se ne aggiunge un secondo nel momento in cui il cliente richiede l'attivazione anche delle funzioni c.d. *"dispositive"* che gli consentono di operare via internet effettuando pagamenti di utenze ed imposte varie, disponendo bonifici, ricariche telefoniche, ecc.: funzioni c.d. *"dispositive"* che per alcuni istituti sono fornite a richiesta del cliente, per altri fanno parte del pacchetto unico per l'operatività via internet.
Tre sono i sistemi di sicurezza comunemente adottati dagli istituti di credito per consentire all'utente l'accesso al c.d. *"home banking dispositivo"*; l'utilizzo di un card di sicurezza, l'invio di un sms al numero di cellulare del cliente o, come nel caso di specie, l'impiego di un token.
Nel precisare che tutti e tre i sistemi sopra indicati hanno la funzione di garantire il cliente da operazioni dispositive non autorizzate, ci si soffermerà sul funzionamento del token.
Il token è un piccolo apparecchio consegnato dalla banca al cliente al momento della sottoscrizione del servizio dispositivo di home banking attraverso il quale si genera, attraverso un algoritmo, una password dispositiva, diversa da quella che si è utilizzata per accedere alla propria home page, valida solo per un breve lasso di tempo (normalmente 30 secondi) e per la singola operazione in corso (password c.d. *"usa e getta"*), con la quale è possibile autorizzare l'operazione dispositiva voluta dal cliente.
Eseguita l'operazione o scaduto il breve termine di validità della password generata dal token, questa diventa inefficace e, quindi, non riutilizzabile ed occorrerà generarne un'altra per eseguire l'attività voluta.
Al momento dell'attivazione, inoltre, il token viene sincronizzato con i server dell'istituto di credito ed abbinato al conto corrente dell'utente in maniera tale che soltanto attraverso quel token si potrà generare una password dispositiva valida per quello specifico conto corrente.
Appare di tutta evidenza che anche in questo caso obbligo ineludibile del cliente è quello di conservare il token evitando che soggetti non autorizzati possano disporne liberamente; se ciò avvenisse, infatti, un terzo, a conoscenza della user id e della password, unitamente alla disponibilità del token, potrebbe agevolmente compiere operazioni dispositive sul conto del cliente.
Da ultimo, elemento assolutamente importante e non trascurabile ai fini della sicurezza del sistema di home banking dispositivo è anche la valutazione del livello di protezione del sito cui si accede, protezione che è assicurata dalla predisposizione di un sistema di criptazione delle comunicazioni

correnti tra il cliente e la banca e la cui operatività è immediatamente riscontrabile dal cliente attraverso la verifica di un simbolo a forma di lucchetto che compare accanto alla barra degli indirizzi del proprio browser e dall'esistenza dell'incipit *"https"* all'inizio dell'indirizzo internet digitato.

Orbene, parte attrice ha descritto le modalità con le quali sarebbe venuto a conoscenza della sottrazione di fondi dal suo conto corrente ed ha dedotto, per la verità, genericamente, che tale sottrazione sarebbe da imputare non ad un caso di *"phishing"*, bensì di *"pharming"*.

Invero, prescindendo dalla considerazione che l'attore, omettendo di chiedere una consulenza tecnica d'ufficio sul computer in uso, ha perso la possibilità di provare sia l'assenza sul proprio computer di programmi nocivi che abbiano reso possibile o, comunque, agevolato la sottrazione dei fondi (malware, trojan horse, ecc.), sia che l'asserita truffa subita sarebbe riconducibile ad un caso di pharming e non, piuttosto, di phishing, osserva questo Giudice che anche a voler considerare accertata, nel caso in esame, un'ipotesi di pharming, la dinamica dell'accaduto si presenta, comunque, oscura.

Ed infatti anche ipotizzando che un terzo non autorizzato, attraverso la sovrapposizione di un sito internet contraffatto a quello dell'istituto di credito, sia riuscito a carpire la user id e la password del ricorrente e che tramite le suddette credenziali sia poi riuscito ad entrare nella home page personale del ricorrente, così accedendo alle informazioni del suo conto corrente (saldo, lista movimenti, ecc.), ciò che non si comprende è come il terzo abbia potuto disporre il bonifico in uscita a carico del ricorrente senza fare uso del token, strumento il cui impiego è, come sopra chiarito, indispensabile al fine di compiere operazioni dispositive.

Né potrebbe sostenersi che in occasione della sottrazione delle credenziali di accesso nel corso di un precedente ingresso del ricorrente sulla propria home page, sia stata sottratta anche la password generata dal token.

Invero, se anche nel corso dell'ultimo accesso autorizzato al proprio conto corrente il ricorrente avesse disposto un operazione – ad esempio, un bonifico o una ricarica telefonica – per la quale era necessario l'impiego di una password dispositiva generata dal token, e questa fosse stata in quell'occasione sottratta, non sarebbe comunque possibile spiegare per questa via la sottrazione della somma.

E ciò perché, come sopra già chiarito, la password generata dal token è temporanea e non riutilizzabile, il che implica che una volta utilizzata per l'operazione richiesta dal privato, se anche questa password fosse stata sottratta, non sarebbe stata idonea ad autorizzare una seconda transazione, anche se eseguita a breve distanza di tempo.

A fronte di tali deduzioni – peraltro in parte articolate dall'istituto di credito nella sua comparsa di costituzione e risposta – il ricorrente non ha articolato nessuna difesa il che, unitamente alla mancanza di richiesta di mezzi di prova, rende il ricorso infondato per mancanza di prova sia della violazione di un qualsivoglia obbligo di prudenza e diligenza da parte dell'istituto di credito resistente, sia, ancor prima, per la mancata prova del nesso di causalità, sotto il profilo della mancata comprensione delle circostanze e modalità che hanno reso possibile la sottrazione della

somma dal conto del ricorrente

In diritto, nella fattispecie in esame assume rilevanza il principio di diligenza contrattuale in relazione al quale, in materia bancaria, la Suprema Corte di Cassazione ha affermato che *"La banca, svolgendo attività professionale, deve adempiere a tutte le obbligazioni, con la diligenza particolarmente qualificata dell'accorto banchiere, assunte nei confronti dei propri clienti, non solo con riguardo all'attività di esecuzione di contratti bancari in senso stretto, ma anche in relazione ad ogni tipo di operazione oggettivamente esplicata (art. 1176 c.c.). Pertanto la banca risponde di tutti i rischi tipici della sua sfera professionale per la cui eliminazione non ha provveduto alla adozione di mezzi idonei (nella fattispecie è responsabile del prelievo fraudolento fatto con bancomat trattenuto dallo sportello automatico manomesso"* (v. Cass. 13777 del 2007).

Orbene, nel caso di specie, nessuna responsabilità può attribuirsi alla banca per mancanza di diligenza contrattuale avendo questa predisposto, per quanto sopra osservato, mezzi assolutamente idonei ad evitare frodi informatiche (credenziali d'accesso e token), e non avendo, inoltre, parte ricorrente dedotto quali ulteriori strumenti di protezione avrebbe potuto e dovuto predisporre l'istituto di credito al fine di evitare la sottrazione dei fondi a danno del ricorrente.

Purtuttavia, è risultato provato *per tabulas* che il ricorrente, il giorno dopo l'avvenuta disposizione non autorizzata del bonifico, ha avvisato la banca dell'accesso non autorizzato (v. alleg. 2), chiedendo al contempo la sospensione della disposizione.

A tale richiesta l'istituto non ha dato corso, pur dovendosi attivare immediatamente per effettuare le opportune indagini e dovendo, medio tempore, dare corso all'immediata sospensione della disposizione.

Tale conclusione deriva dalla considerazione della particolarità della fattispecie in esame laddove il bonifico aveva ad oggetto una somma di notevole entità ed era stato disposto non su un conto corrente italiano, bensì su un istituto di credito straniero ed all'ordine di tale Lukacsovics Marcel.

A fronte di una specifica richiesta del cliente, la banca resistente avrebbe dovuto, in ottemperanza al principio della buona fede e correttezza in corso di esecuzione del contratto – principio che richiamando *"...nella sfera del creditore la considerazione dell'interesse del debitore e nella sfera del debitore il giusto riguardo all'interesse del creditore", deve essere inteso in senso oggettivo ed enuncia un dovere di solidarietà, fondato sull'art. 2 della Costituzione, che, operando come un criterio di reciprocità, esplica la sua rilevanza nell'imporre a ciascuna delle parti del rapporto obbligatorio, il dovere di agire in modo da preservare gli interessi dell'altra, a prescindere dall'esistenza di specifici obblighi contrattuali o di quanto espressamente stabilito da singole norme di legge. Dalla violazione di tale regola di comportamento può discendere "ex se", ove provato, un danno risarcibile"* (v. Cass., n. 23273/06) – attivarsi immediatamente al fine di evitare il prodursi o l'aggravarsi di conseguenze pregiudizievoli a carico del cliente, in attesa dei necessari approfondimenti di natura tecnica in merito ad una situazione oggettivamente non chiara e caratterizzata da rilevanti profili di criticità.

P.Q.M.

1) accoglie il ricorso;

2) condanna parte resistente alla rifusione delle spese processuali in favore del ricorrente che liquida in € 230,00 per spese vive ed € 900,00 per onorari di avvocato, di cui € 600,00 per la fase di studio, € 300.00 per la fase introduttiva, oltre I.V.A. e C.P.A. come per legge.

Si comunichi.

Milazzo, 24.5.13

Il Giudice

(dott.ssa Rossella Busacca)

DEPOSITATO IN CANCELLERIA

Milazzo, 31.5.13

IL FUNZIONARIO GIUDIZIARIO