Collegio di Napoli, 30 luglio 2010, n.835

Categoria Massima: Responsabilità della banca / Home banking, Home banking / Obblighi per la banca

Parole chiave: Diligenza professionale, Frodi, Internet banking o home banking, Presidi tecnici, Responsabilità della banca

Deve riconoscersi la responsabilità della banca laddove appaia incontrovertibile che, pur avendo questa adottato determinati accorgimenti tecnici allo scopo di proteggere la sicurezza nell'uso della rete per l'esecuzione da parte dei clienti di operazioni sui propri conti correnti (c.d. internet banking o home banking), ciononostante, all'epoca dei fatti controversi, la tecnologia aveva già messo a disposizione dispositivi più raffinati, sicuri ed affidabili di quelli in concreto adottati e perciò maggiormente adeguati rispetto all'obiettivo suddetto in quanto capaci di offrire al cliente un terzo livello di protezione, come le serie numeriche casuali e random, generate da dispositivi automatici quali chiavette o token, digipass, et similia.

Testo sentenza:

IL COLLEGIO DI NAPOLI

composto dai signori:

- Prof. Avv. Enrico Quadri (Presidente)
- Prof. Avv. Ferruccio Auletta (Membro designato dalla Banca d'Italia)
- Avv. Leonardo Patroni Griffi (Membro designato dalla Banca d'Italia)
- Prof.ssa Marilena Rispoli Farina (Membro designato dal Conciliatore Bancario Finanziario - Estensore)
- Avv. Roberto Manzione (Membro designato dal C.N.C.U.)

nella seduta del 06 luglio 2010 dopo aver esaminato

- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario e la relativa documentazione;
- la relazione istruttoria della Segreteria tecnica

FATTO

Con reclamo del 20 maggio 2009, la cliente – titolare di un rapporto di conto corrente acceso il 22.10.2008 "*che gestisce normalmente on-line*" – disconosce un'operazione di bonifico estero, dell'importo di € 3.760,00, effettuata in data 5.5.2009. Riferisce di essersi accorta dell'operazione in data 19.5.2009 e di aver presentato reclamo all'intermediario – come pure querela presso la Polizia di Stato – il giorno successivo e di aver inoltre provveduto al blocco del conto .

Nel reclamo la cliente – non avendo mai autorizzato la suddetta operazione e ritenendo "*evidente* ", per tale motivo, "*l'esclusiva responsabilità di tale operazione*" in capo all'intermediario – invita la banca a rimborsarle la somma oggetto di bonifico. Non avendo ricevuto alcuna risposta in esito al reclamo, con nota del 10.9.2009, intima nuovamente alla banca la restituzione della somma di cui al bonifico oltre le spese legali sino al soddisfo.

Con nota del 15.9.2009, la banca rigetta la richiesta della ricorrente ed esclude che possa esserle imputata la responsabilità dell'accaduto. L'argomentazione spesa a tal fine è che il bonifico è stato effettuato con l'utilizzo di "*dati che solo* [la reclamante] *poteva conoscere*" *sicché " è possibile che qualcuno, carpendo la buona fede della citata cliente, sia entrato in possesso degli elementi che hanno consentito di far apparire l'operazione come se fosse stata effettuata dalla stessa"*.

Nel ricorso – che riproduce in sostanza il contenuto del reclamo – la cliente chiede il rimborso della somma oggetto di bonifico, ritenendo di essere stata vittima di una truffa. In sede di controdeduzioni la banca chiede il rigetto del ricorso, ritenendolo infondato, sul presupposto che "solo la [ricorrente] poteva conoscere il PIN che ha consentito di *effettuare il bonifico oggi contestato*". Precisa, infatti, al riguardo, che il (primo) codice fornito alla cliente serve soltanto per accedere al sistema e che, effettuato l'accesso, "*il* sistema impone di modificare il PIN fornito dalla banca". Soggiunge che "la conoscenza *del PIN deve rinviare alla [ricorrente] o a persona cui la stessa volontariamente o involontariamente ha fornito il PIN"*.

Afferma inoltre che i suoi "*sistemi informatici non sono stati mai violati*" e che, comunque, " *non è stata fornita alcuna prova in tal senso da parte della ricorrente"*.

Conclude citando l'art. 6 del contratto "*home banking famiglia*", sottoscritto dalla ricorrente, a norma del quale "il cliente dichiara inoltre di tenere indenne la banca da ogni *conseguenza dannosa o molestia che potesse derivare anche da parte di terzi"*.

DIRITTO

Il ricorso in oggetto concerne un'ipotesi di frode informatica nell'utilizzazione di un conto *on line*. Si pone a questo Collegio il compito di accertare, da un lato, l'eventuale responsabilità della banca che è tenuta all'adozione, con specifico riferimento ai servizi *on line*offerti alla clientela, di tutte le cautele e gli accorgimenti idonei, in base al criterio della diligenza professionale, a evitare e a prevenire il rischio di frode telematica; dall'altro di valutare il comportamento del cliente che è tenuto a custodire i codici di accesso onde evitare a soggetti estranei l'utilizzo del servizio.

In merito al primo profilo si segnala, al riguardo, l'autorevole indirizzo della giurisprudenza di legittimità secondo il quale "ai fini della valutazione della responsabilità contrattuale *della banca [...] non deve essere omessa la verifica dell'adozione da parte dell'Istitutobancario delle misure idonee a garantire la sicurezza del servizio (nella specie l'operativitàon line del conto corrente) da eventuali manomissioni [...]: infatti, la diligenza posta acarico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischitipici della sfera professionale di riferimento ed assumendo quindi come parametro la*figura dell'accorto banchiere" (Cass., 12 giugno 2007, n. 13777; cfr. altresì Cass., 7 marzo 2003, n. 3389; Cass., 31 luglio 2002, n. 11382). Tale indirizzo è corroborato, su un piano più generale, dall'espressa previsione normativa ex artt. 2381 e 2403 c.c. dell'obbligo, posto a carico dell'organo gestorio, di munire in ogni caso l'impresa di assetti organizzativi adeguati e dell'obbligo, posto a carico dell'organo di controllo, di vigilare sull'adeguatezza di tali assetti.

Ai fini della decisione il Collegio rileva innanzitutto che non emergono, dalla documentazione presente agli atti, le caratteristiche tecniche di funzionamento del servizio di *home banking* offerto dalla banca e, in particolare, i presidi di sicurezza informatica adottati per scongiurare episodi di pirateria informatica e garantire la sicurezza delle transazioni *on line*. Il contratto

allegato dispone, al riguardo, che "*la banca proponente indica al cliente le procedure e gli strumenti necessari per le operazioni di identificazione,bilateralmente efficace, delle parti, da eseguire all'atto dell'avvio del collegamento e/odurante i successivi scambi di flussi*" (art. 6). Sulla base di quanto dichiarato dalla banca nelle controdeduzioni, tuttavia, non sembra che il sistema sia strutturato in modo da garantire anche una cd. "*protezione di terzo livello*". La riuscita delle frodi informatiche infatti è correlata alla tipologia dei codici di accesso e al livello di protezione garantito dalla banca. Per consentire le operazioni (bonifici, giroconti, trading on line) gran parte degli istituti di credito, ormai da tempo, utilizza - oltre ai normali codici di accesso al sito di home banking - anche una protezione di terzo livello (ulteriore password dispositiva, firma digitale, chiavette elettroniche personalizzate che creano una password diversa ogni 30 secondi, etc.). Ciò fa sì che eventuali intercettazioni abusive dei meri codici di accesso non siano sufficienti a consentire alcuna operazione dispositiva da parte di terzi. Pertanto (ferme restando le implicazioni penali per gli autori della frode), i presidi di sicurezza posti in essere dall'Istituto di credito assumono rilevanza ai fini di una eventuale responsabilità civile della Banca.

Va, dall'altro, considerato che al cliente ricorrente, che ha segnalato con immediatezza l'operazione fraudolenta (il giorno successivo a quello in cui ne ha avuto contezza) non possano essere imputati comportamenti negligenti che possano aver concorso al compimento della frode.

Ai fini della decisione, va considerato il recente, e pienamente condivisibile, orientamento del Collegio ABF di Roma, che nella decisione n. 33/2010 ha affermato la responsabilità della Banca, perché, "se non è controvertibile che questa avesse adottato determinati *accorgimenti tecnici allo scopo di proteggere la sicurezza nell'uso della rete per*l'esecuzione da parte dei clienti di operazioni sui propri conti correnti (c.d. internet banking *o home banking) , è altrettanto incontrovertibile che, all'epoca dei fatti per cui è controversia, la tecnologia aveva già messo a disposizione dispositivi più raffinati, sicuri ed affidabili di quelli in concreto adottati e perciò maggiormente adeguati rispetto all'obiettivo suddetto in quanto capaci di offrire al cliente un terzo livello di protezione, come le serie numeriche casuali e random , generate da dispositivi automatici quali chiavette o token, digipass, etsimilia".*

P.Q.M.

Il Collegio, in accoglimento del ricorso, dichiara l'intermediario tenuto a rimborsareal cliente

l’importo di € 3.760,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l’intermediario corrisponda alla Banca d’Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Enrico Quadri