Responsabilità civile

Phishing e responsabilità della banca per omessa adozione di adeguate misure di sicurezza

di **Alessandra Sorrentino, Avvocato**

Cass. civ., Sez. III, sent., 12.02.2024, n. 3780 – Pres. Scarano – Rel. Moscarini

Phishing – Responsabilità della banca – Diligenza dell'accorto banchiere – Prova liberatoria

[1] La responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare verifica della loro riconducibilità alla volontà del cliente, mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, va esclusa se ricorre una situazione di colpa grave dell'utente, configurabile, ad esempio, nel caso di protratta attesa prima di comunicare l'uso non autorizzato dello strumento di pagamento, ma il riparto degli oneri probatori, posto a carico delle parti, segue il regime della responsabilità contrattuale. Mentre, pertanto, il cliente è tenuto soltanto a provare la fonte del proprio diritto ed il termine di scadenza, il debitore, cioè la banca, deve provare il fatto estintivo dell'altrui pretesa, sicché non può omettere la verifica dell'adozione delle misure atte a garantire la sicurezza del servizio. Ne consegue che, essendo la possibilità della sottrazione dei codici al correntista, attraverso tecniche fraudolente, una eventualità rientrante nel rischio d'impresa, la banca per liberarsi dalla propria responsabilità deve dimostrare la sopravvenienza di eventi che si collochino al di là dello sforzo diligente richiesto al debitore.

CASO

L'attrice aveva citato in giudizio Poste Italiane S.p.A., onde ottenere l'accertamento della relativa responsabilità, in relazione ad una frode subìta sulla propria carta "Postepay Evolution".

Nella specie, l'attrice aveva comunicato in buona fede, in risposta ad una e-mail ingannevole, apparentemente proveniente da Poste Italiane, le proprie credenziali di accesso agli *account* bancari, subendo, quindi, un attacco di c.d. *phishing*.

Entrati in possesso delle credenziali di accesso dell'attrice, ignoti terzi addebitavano, sul

relativo conto, delle spese di importo pari a € 2.900,00, che la stessa non aveva mai effettuato.

In primo grado il Giudice di Pace adito, aderendo alle conclusioni di Poste Italiane, secondo cui la responsabilità, in simili casi, fosse imputabile esclusivamente all'incauto cliente, per aver comunicato a terzi i propri dati di accesso, rigettava la domanda dell'attrice, che proponeva successivamente appello dinanzi al Tribunale, che accoglieva il gravame.

Il Tribunale in secondo grado riconosceva la responsabilità di Poste Italiane, in quanto tenuta a rispondere delle conseguenze dannose, conseguenti all'esercizio di un'attività pericolosa, implicante il trattamento di dati personali.

Secondo il Giudice d'appello, l'uso dei codici di accesso al sistema da parte di terzi rientra nel rischio professionale del prestatore di servizi di pagamento, il quale deve prevenire ed evitare simili condotte con appropriate misure tecniche, le quali, nella specie, non erano state adottate. Di conseguenza, l'istituto Poste Italiane non aveva fornito la prova della riconducibilità dell'operazione al cliente.

Avverso la decisione del Tribunale in secondo grado, parte soccombente proponeva ricorso in cassazione.

SOLUZIONE

La sentenza in commento afferma il principio secondo il quale le banche sono tenute a risarcire i correntisti, che abbiano subìto una frode informatica, come il *phishing*, in quanto tale eventualità rientra nel proprio rischio di impresa, a meno che non provino di aver adottato misure idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento, in base al principio di buona fede nell'esecuzione del contratto.

Per andare esente da responsabilità, la banca deve provare il sopravvenire di fatti, che si collochino al di là della condotta diligente richiesta al debitore.

QUESTIONI

La sentenza in commento rappresenta un vero e proprio cambio di rotta nell'ambito della difesa contro la frode informatica rappresenta dal c.d. *phishing*, in cui il truffatore induce la vittima a divulgare dati sensibili o personali (quali, ad esempio, numeri di carte di credito, estremi del conto corrente bancario, credenziali di accesso), mediante e-mail fraudolente, messaggi di testo o siti web.

Meno di un anno prima della pronuncia in esame, gli Ermellini, in un caso analogo in cui una coppia di correntisti aveva comunicato in buona fede, in risposta ad una e-mail ingannevole, le proprie credenziali di accesso agli *account* bancari, avevano escluso la responsabilità dell'istituto di credito per l'addebito sul conto corrente eseguito da un terzo truffatore, a seguito della sottrazione delle credenziali autorizzative tramite *phishing*.

In quella fattispecie, la Corte di cassazione aveva ritenuto che la condotta colposa dei correntisti fosse stata causa esclusiva dell'operazione fraudolenta commessa ai loro danni e che siffatta condotta avesse assunto i caratteri del caso fortuito, idoneo ad interrompere il nesso causale tra condotta truffaldina ed evento dannoso, con conseguente esclusione di ogni responsabilità in capo alla Banca (Cass. civ., ord., 7214/2023).

Dal canto suo, quest'ultima, invece, aveva dimostrato di aver adottato un sistema di sicurezza adeguato all'esecuzione di operazioni bancarie per via telematica (misure rappresentate dalle informazioni inserite sul sito istituzionale della banca, nel quale era indicato espressamente che l'istituto non richiedeva mai i codici personali attraverso messaggi di posta elettronica, lettere e/o telefonate), che i codici di accesso a detto sistema (username, pin e *password*) erano nell'esclusiva disponibilità dei correntisti, che avrebbero dovuto custodirli, ed infine che tali codici erano stati utilizzati da un terzo, previa illecita sottrazione.

Pertanto, l'ordinanza 7214/2023 attribuiva ai correntisti l'esclusiva responsabilità dell'evento dannoso occorsogli, in quanto erano stati vittima di una credulità colpevole ed inescusabile, in ragione del fatto che la truffa tramite *phishing* è generalmente nota all'uomo comune e, quindi, facilmente evitabile, con un minimo di diligenza e prudenza.

Tuttavia, l'ordinanza suddetta non ha trovato conferma nelle pronunce dei giudici di merito, che unanimemente hanno sempre ritenuto necessaria una valutazione, da condurre caso per caso, del grado di colpa dell'utente, in base alla specifica fattispecie concreta, sostenendo che la Banca non sempre adotta misure di sicurezza, atte ad evitare accessi non autorizzati al sistema informatico degli *account* bancari (Trib. Milano, 18 gennaio 2023, n. 322; Trib. Roma, 25 giugno 2019, n. 13442). E solo laddove la Banca provi di avere adottato tutte le specifiche misure *antiphishing*, volte ad evitare fraudolente sottrazioni da parte di terzi truffatori, essa può andare esente da responsabilità.

In tale solco si inserisce la sentenza in commento, che, qualificato come contrattuale il rapporto di conto corrente tra banca e cliente e dunque come **contrattuale la responsabilità della banca**, ha affermato che la **diligenza posta a carico del professionista**, per quanto concerne i servizi posti in essere in favore del cliente, ha **natura tecnica** e deve essere valutata tenendo conto dei **rischi tipici della sfera professionale** di riferimento, assumendo come parametro quello dell'**accorto banchiere,** speciale declinazione del generale **principio civilistico** di buona fede contrattuale (art. 1176, co. 2 cc).

Ciò posto, spostandosi sul versante dell'onere probatorio, nel caso di operazioni effettuate tramite *home banking*, **spetta all'istituto di credito verificare la riconducibilità delle stesse alla volontà del cliente**, impiegando la **diligenza dell'accorto banchiere,** vale a dire (non di un generico soggetto di media diligenza, ma) di un professionista dedito a quel particolare ramo di affari e quindi dotato, in quel settore, di una specifica esperienza e competenza.

Ne consegue che l'eventuale uso, da parte dei terzi, dei codici di accesso al sistema della banca multicanale (*home banking*) rientra nel **rischio professionale** del prestatore dei servizi a

pagamento, il quale è **prevedibile ed evitabile con l'adozione di adeguate misure tecniche**, il cui scopo è quello di verificare la riconducibilità delle operazioni eseguite, tramite la banca *on line*, alla volontà del cliente.

In considerazione di ciò, la Banca non risponde del danno patito dal cliente, solo laddove provi che l'evento dannoso sia imputabile al **dolo del correntista o a comportamenti imprudenti** (Cass. civ., 23.5.2016 n. 10638), tali da non poter essere evitati con anticipo dall'istituto di credito, come ad esempio nel caso di protratta attesa, prima di comunicare l'uso non autorizzato dello strumento di pagamento.

Più semplice è la prova per il correntista in quanto, stante la natura contrattuale del rapporto, al creditore-correntista sarà sufficiente "*provare la fonte del proprio diritto ed il termine di scadenza*", "*mentre il debitore, cioè la banca, deve provare il fatto estintivo dell'altrui pretesa, sicché non può omettere la verifica dell'adozione delle misure atte a garantire la sicurezza del servizio*".

Gli Ermellini proseguono, sostenendo che "*ne consegue che, essendo la possibilità della sottrazione dei codici al correntista attraverso tecniche fraudolente una eventualità rientrante nel rischio d'impresa,* ***la banca per liberarsi dalla propria responsabilità, deve dimostrare la sopravvenienza di eventi che si collochino al di là dello sforzo diligente richiesto al debitore***".

Nella fattispecie in esame, la Suprema Corte, modificando l'orientamento espresso nell'ordinanza dello scorso anno (7214/2023), ha affermato che la Banca, al fine di andare esente da responsabilità, avrebbe dovuto conformarsi ad un elevato *standard* di diligenza tecnica ex art. 1176, co. 2, c.c., e, quindi, nella fattispecie avrebbe dovuto opportunamente provare "*di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento,* ***quali ad esempio l'invito al titolare della carta di appositi sms allert di conferma di ogni singola operazione, sulla base di un principio di buona fede nell'esecuzione del contratto***".

In mancanza di tale prova, conclude la Corte, non può che imputarsi alla Banca il rischio che terzi accedano ai profili dei clienti con condotte fraudolenti.

In conclusione, quindi, la pronuncia in esame stabilisce un precedente importante per la sicurezza bancaria, evidenziando la necessità per le banche e gli istituti di credito di adottare misure preventive efficaci contro le frodi informatiche.

La responsabilità di garantire la sicurezza del servizio non ricade unicamente sul cliente, al quale si richiede una condotta diligente ed accorta, ma anche sulla banca, che deve dimostrare di aver fatto tutto il possibile per prevenire accessi fraudolenti.