Sentenza, Tribunale di Palermo, Giudice Andrea Illuminati, n. 4739, del 26/10/2023

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
TRIBUNALE DI PALERMO

Il Giudice nella persona del dr. Andrea Illuminati, nella causa di primo grado iscritta al N. xxxx/2021 RG, ha pronunciato la presente

SENTENZA

tra

C.C. (avv.ti omissis)

- attori

e

SOCIETA' S.p.A., in persona del legale rappresentante pro - tempore (avv. omissis)

- convenuta

oggetto: "rapporti di c/c e altri contratti bancari"

SVOLGIMENTO DEL PROCESSO - MOTIVI DELLA DECISIONE

Con atto di citazione ritualmente notificato, C.C. ha convenuto in giudizio, innanzi a questo Tribunale, **la SOCIETA' S.p.A** per sentirla condannare a titolo risarcitorio a pagamento della somma di Euro 13.600,00 in dipendenza di una truffa informatica perpetrata in suo danno.

L'attrice lamenta che terzi soggetti avrebbero posto in esser un'attività fraudolenta consistente nell'avere effettuato illecite disposizioni di pagamento per complessivi Euro 13.600,00 utilizzando l somme giacenti sul suo conto corrente, sebbene questa non avess mai autorizzato tali disposizioni di bonifico.

Stando alla ricostruzione della attrice, la responsabilità di tale attività fraudolenta sarebbe addebitabile alla convenuta ai sensi degli artt. 11 e 12 del D.Lgs. n. 11 del 2010, non avendo l'intermediario predisposto idonee garanzie atte a fronteggiare indebite intromissioni di terzi soggetti nel sistema informatico della banca utilizzato per effettuare le operazioni contestate.

Radicatasi la lite, si è costituita in giudizio la **SOCIETA' S.p.a.** la quale ha chiesto il rigetto delle avverse domande in ragione della loro ritenuta infondatezza.

Una volta assunte le prove orali ed espletata una CTU, la causa è stata trattenuta per la decisione all'udienza in epigrafe indicata, con concessione dei termini ex art. 190 c.p.c.

Ciò posto, la domanda di risarcimento danni proposta dall'attrice è infondata per le ragioni appresso spiegate.

Il giudizio de quo verte sull'accertamento della responsabilità del prestatore di servizi di pagamento nel caso in cui il cliente abbia disconosciuto un'operazione eseguita tramite home banking, da terzi ignoti, con mezzi fraudolenti.

Pertanto, la normativa di riferimento è quella che regola le operazioni di pagamento a distanza di cui al D.Lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore del D.Lgs. 15 dicembre 2017, n. 218 (di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno).

Con riferimento all'ipotesi - verificatasi nel caso che ci occupa - in cui il cliente neghi di aver autorizzato un'operazione di pagamento già eseguita, l'art. 10 del citato d.lgs. stabilisce che sia onere dell'intermediario dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute; e, a norma del successivo art. 12, co. 4, è altresì onere dell'intermediario fornire la prova di tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore. In mancanza di tale duplice prova, la B. sopporta integralmente le conseguenze delle operazioni disconosciute, senza alcuna limitazione o franchigia.

L'intenzione del legislatore è all'evidenza quella di sollecitare la fissazione - da parte del prestatore di servizi - di elevati standard di trasparenza e sicurezza e di riversare su di esso, almeno in linea di principio, le conseguenze sfavorevoli dell'uso fraudolento o non autorizzato degli strumenti di pagamento, tanto in base alla logica per cui la B., quale operatore professionale che gestisce il servizio di pagamento, è il soggetto più idoneo a sopportare il rischio delle operazioni non autorizzate.

La lettura nei termini sopra precisati del sistema delineato dal D.Lgs. n. 11 del 2010 trova diretta conferma nella giurisprudenza della SC, alla cui condivisibile stregua, "In tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo" (citata in massima Cassazione civile sez. I, 20/05/2022, n. 16417; conformi: Cassazione civile sez. I, 03/02/2017, n. 2950).

Sotto il profilo della prova del dolo o della colpa grave del cliente, la medesima giurisprudenza ha inoltre chiarito che la stessa debba essere fornita positivamente dal prestatore di servizi, non potendo presumersi in ragione dell'idoneità delle protezioni adottate dalla banca, al fine di evitare l'esecuzione di operazioni fraudolente. Così ha statuito in proposito Cassazione civile sez. VI, 26/11/2020, n. 26916: "La responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha natura contrattuale e, quindi, va esclusa solo se ricorre una situazione di colpa grave dell'utente. (Nella specie, la S.C. ha cassato con rinvio la decisione di merito che, disattendendo il principio di cui in massima, aveva ritenuto che, essendo stata raggiunta la prova presuntiva dell'idoneità delle protezioni adottate dal prestatore dei servizi di pagamento contro l'uso non autorizzato della carta cd. prepagata "postepay", gravasse sul cliente l'onere di dimostrare di avere tenuto un comportamento esente da colpa nella custodia della carta e dei codici, in modo da evitare furti o smarrimenti)".

Ciò debitamente premesso in punto di diritto, con specifico riferimento al caso in esame l'intermediario ha dato prova di aver adottato un sistema di autenticazione multifattoriale consistente nell'inserimento delle credenziali statiche di accesso al canale di home banking, di un codice OTP inviato tramite notifica push, e una ulteriore password - c.d. codice OTS - inoltrata tramite sms sul cellulare certificato dell'attrice; nonché di avere correttamente registrato e contabilizzato l'operazione oggetto di giudizio.

Le suddette evenienze emergono dai disposti accertamenti peritali, che danno conto delle operazioni svolte dai conti corrente delle attrice sul portale home banking della banca e consentono di ricostruire lo svolgimento dei pagamenti in contestazione.

Le operazioni peritali espletate comprovano che le operazioni disconosciute - "ricariche via web di carte prepagate" e "bonifico on line" del 29.1.21 - sono state correttamente autenticate con l'inserimento della OTP e della OTS ed escludono un'anomalia operativa o un malfunzionamento del servizio predisposto dall'intermediario, secondo quanto previsto dall'art. 10 del D.Lgs. n. 11 del 2010. Infatti, le credenziali "statiche" (nome utente e codice PIN) sono state opportunamente digitate per effettuare l'accesso alla H.B., e le credenziali dinamiche (OTP e OTS) sono state correttamente generate e inserite ai fini delle operazioni di bonifico, con conseguente obbligo della banca di darne esecuzione.

SOCIETA' s.p.a. abbia provato che i pagamenti disconosciuti siano stati autenticati nel rispetto della normativa vigente e attraverso strumenti di sicurezza idonei a garantire elevati standard di sicurezza (c.d. sistema di autenticazione c.d. forte), la circostanza non vale di per sé ad escludere la responsabilità della convenuta, essendo necessario che l'intermediario - alla stregua dell'art. 12, co. 4 D.Lgs. n. 11 del 2010 e della giurisprudenza sopra richiamati - dimostri elementi fattuali caratterizzanti le modalità esecutive dell'operazione dai quali possa ricavarsi la colpa grave dell'utente.

Sotto tale aspetto si osserva che per quanto risulta dalle dichiarazioni contenute nella querela sporta dalla C. in relazione ai fatti oggetto di causa (all. 4 fasc. attrice), dagli esiti della prova per interpello con la stessa parte (v. verbale del 14.6.22) e dai disposti accertamenti tecnici (v. p. 4 - 13 dell'elaborato peritale), le operazioni bancarie in contestazione sono frutto di una attività fraudolenta (denominata "phishing") perpetrata da terzi truffatori in danno dell'attrice.

In particolare, dalle dagli elementi di prova raccolti nel corso del giudizio emerge che:

- in data 29.01.2021, ore 13:29, la sig.ra C. riceveva un SMS da un numero (apparentemente riconducibile alla banca ma in realtà risultato riferibile ai truffatori, avente il seguente contenuto: "ATTENZIONE! un dispositivo non autorizzato risulta connesso al suo conto on - line se disconosce tale accesso clicca il modulo correlato ispcertificated.com"; trattasi quest'ultimo di dominio, non più attivo, "listato nei domini a rischio dal servizio Google Safe Browsing: in particolare indicato come sito di Phishing" (v. p. 5 - 6 CTU);
- inoltre, alle ore 13:34 dello stesso giorno la sig.ra C. veniva contattata telefonicamente da un falso operatore dell'Istituto di credito il quale la informava di aver riscontrato la presenza di n. 4 pagamenti

indebiti effettuati nella stessa data con la carta di credito intestata all'attrice; circostanza questa rivelatasi, poi, non corrispondente al vero;
- il falso operatore riferiva inoltre che l'attrice era ancora in tempo per annullare le operazioni, e che a tal fine sarebbe stato necessario bloccare la carta di credito;
- l'attrice forniva, quindi, al falso operatore il codice CVV della propria carta di credito, quelli personali e quello OTS (meglio indicati alla p. 9 della CTU) ricevuti via SMS sul proprio numero telefonico e provenienti dal sistema informatico dell'istituto di credito convenuto; la comunicazione di tali dati avveniva su specifica richiesta del truffatore che sosteneva di averne bisogno per compiere le operazioni di blocco della carta;
- il falso operatore, dopo aver ottenuto i dati richiesti, concludeva la conversazione telefonica non prima di aver informato l'attrice che per mezz'ora la stessa non avrebbe potuto accedere al conto on-line per l'operazione di blocco in corso e che, una volta terminata, la stessa sarebbe stata ricontattata;
- seguivano gli indebiti prelievi dal conto corrente dell'attrice per un importo complessivo di Euro. 13.600,00;
- non ricevendo alcuna comunicazione degli esiti delle operazioni di blocco, l'attrice contattava telefonicamente la banca e apprendeva degli indebiti prelievi effettuati sul conto corrente proprio grazie ai numeri da ella comunicati ai truffatori.
In relazione alla truffa sopra sinteticamente descritta, la cui esatte modalità sono rimaste in parte sconosciute anche all'esito dei disposti accertamenti peritali, va comunque registrato il comportamento gravemente colposo dell'attrice che ha fornito ai truffatori i dati della carta di credito e gli ulteriori codici ricevuti via SMS. Proprio la comunicazione di tali dati ha infatti reso possibile il perfezionamento della truffa; dati che - in base alla diligenza esigibile nel caso concreto ex art. 1176 c.c. - l'attrice non avrebbe dovuto fornire, noto essendo che i codici de quibus sono strettamente personali e che gli istituti di credito non possono richiederli per telefono ai loro clienti.
La condotta dell'attrice è ancora più negligente ove si consideri che la cliente è venuta meno all'obbligo a suo carico, in base al contratto my-key agli atti (v. art. 2), di custodire le credenziali di accesso all'home banking e di attuare a tal fine "tutte le misure idonee a proteggerle da utilizzi non autorizzati".
Vale richiamare sul punto il precedente citato dalla banca convenuta a sostegno della dedotta colpa grave della cliente (cfr. Cass. n. 7217/2023) il quale si riferisce a caso, analogo al presente, in cui era stato positivamente accertato che il cliente, violando gli obblighi di custodia dei codici personali di accesso ai sistemi di pagamento offerti dalla banca, aveva colposamente fornito tali dati ai truffatori, cosi permettendo il compimento della frode informatica in suo danno. In tale fattispecie è stata esclusa la responsabilità dell'intermediario in ragione del grave contegno colposo serbato dal cliente.
Alla stregua delle considerazioni che precedono, dovendo dunque ritenersi raggiunta la prova liberatoria posta a carico della banca dall'art. 12, co. 4 D.Lgs. n. 11 del 2010, la domanda risarcitoria proposta dall'attrice va respinta.
Le spese di lite - che si liquidano in dispositivo ex D.M. n. 55 del 2014 (e succ. mod.) - seguono la soccombenza dell'attrice. Alla luce dei relativi esiti, i costi della CTU, liquidata con separato decreto, vanno posti a carico della medesima parte.

P.Q.M.

Il Tribunale, definitivamente pronunciando sulla presente controversia, ogni altra istanza ed eccezione disattesa, così provvede:
- rigetta le domande della parte attrice;
- condanna l'attrice a rifondere alla parte convenuta le spese di lite che si quantificano in Euro. 3.100,00 per compensi di avvocato, oltre ad oneri e accessori di legge;
- pone i costi della CTU, liquidata con separato decreto, a carico degli attori in solido.

Così deciso in Palermo, il 26 ottobre 2023.
Depositata in Cancelleria il 26 ottobre 2023.