RG. 440/2019
SENT. 30/2024
DEP. 31/03/2024
CRON. 209/2024
REP. 27/2024

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO

Ufficio del Giudice di Pace

SULMONA

Il Giudice di Pace, nella persona della dott.ssa Gianna Cipriani, ha pronunciato la seguente

SENTENZA

nella causa civile n. 440/2019 R.G.A.C vertente

TRA

nato a il , residente in (AQ), via titolare della ; c.f. , ai fini della presente procedura elettivamente domiciliato in Pratola Peligna, via Amedeo Tedeschi n. 10, presso lo studio dell'avvocato Laila Coccovilli del Foro di Sulmona, dal quale è rappresentato e difeso in forza di mandato in calce all'atto di citazione (avvlailacoccovilli@puntopec.it)

ATTORE

E

-Banca di in persona del legale rappresentante *pro tempore*, con sede in , via P.I. ; ai fini della presente procedura elettivamente domiciliata in Sulmona, presso lo studio dell'avvocato del Foro di Sulmona, dal quale è rappresentata e difesa in forza di procura in calce alla comparsa di costituzione ( )

CONVENUTA

avente ad oggetto: risarcimento danni

1/5-0/2

Conclusioni: come da comparse conclusionali del 20.9.2020

MOTIVI DELLA DECISIONE

Con atto di citazione, ritualmente notificato il 12.9.2019, [redacted] conveniva in giudizio la Banca [redacted] per sentire accertare e dichiarare la responsabilità dell'Istituto convenuto per il danno subito a causa del dirottamento del bonifico effettuato in *home banking* verso altro destinatario, diverso dall'effettivo beneficiario.

Si costituiva in giudizio la convenuta, impugnando e contestando quanto *ex adverso* dedotto e concludendo per il rigetto della domanda.

Il tentativo di conciliazione dava esito negativo.

All'udienza del 14 luglio 2020 la causa era riservata in decisione, con termine per comparse conclusionali fino al successivo 20 settembre.

La domanda è meritevole di accoglimento.

La fattispecie in esame ha ad oggetto una intromissione illecita nelle comunicazioni digitali, in particolare un cosiddetto bonifico deviato con intenzioni fraudolente.

L'*hacker* in questione, tal [redacted] di [redacted] è stato individuato e successivamente condannato, unitamente ai suoi complici, dal Tribunale di Brescia per i reati di cui agli articoli 615 *quater*, 615 *ter* e 640 *ter* comma III del codice penale.

Orbene, ai fini del decidere sulla richiesta avanzata dall'attore si rinvia alla prevalente giurisprudenza in materia, *ex pluribus* alla ordinanza n. 9158 del 12.4.2018 della Suprema Corte VI sez. civ, che ha statuito il principio secondo cui 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, è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento (rischio 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.

L'orientamento dominante è dunque volto a tutelare il correntista e ad ascrivere la responsabilità alla Banca in quanto l'eventualità di sottrazione delle credenziali rientra nel rischio professionale dell'erogatore dei servizi di pagamento.

L'articolo 10 co. 1 del D.Lgs 11/2010 stabilisce che " qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita.....è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del

- 2/5-0/2

malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti" e che " quando l'utilizzatore neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento 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 o non abbia adempiuto con dolo o colpa grave ad uno o più degli obblighi di cui all'articolo 7", fra i quali figurano quelli di custodire diligentemente i codici di accesso ai sensi del contratto.

L'apparente corretta autenticazione non è quindi sufficiente a dimostrarne la riconducibilità all'utilizzatore che la disconosca.

E' dunque onere dell'intermediario, al fine di sottrarsi alla richiesta di rimborso del cliente, non quello di provare di essere esente da responsabilità bensì quello di provare la colpa grave o il dolo del cliente; tale prova nella fattispecie in esame non può ritenersi raggiunta.

L'Istituto di Credito ha certamente fornito al cliente lo strumento avanzato di sicurezza denominato OTP (*one time password*), consistente nell'impiego di un codice numerico o alfanumerico "usa e getta" che rende le transazioni molto più sicure in quanto utilizzabile una sola volta ed in virtù del quale non è sufficiente possedere le credenziali di accesso al conto corrente potendo l'operazione andare a buon fine solo dopo la digitazione di una ulteriore *password* utilizzabile una sola volta ed inviata tramite sms allo *smartphone* del titolare del conto (cfr. contratto di concessione OTP sottoscritto in data 12.4.2010).

L'intrusione fraudolenta del terzo soggetto non può tuttavia ricadere nella pur ristretta area di rischio che la legge pone a carico dell'utente, dovendo al contrario ritenersi che l'impiego del citato strumento non possa valere di per sé a lasciar irreversibilmente presumere una negligenza comportamentale del cliente (Collegio Napoli decisione 1583/2012).

Nella fattispecie l'attore è stato indiscutibilmente vittima di un *malware*.

Venerdì 12 agosto 2016 alle ore 11,27 il J spone bonifico di € 2.331,10, che viene dirottato sul conto dell'hacker.

Trascorsi l'intervallo del *week end* ed il Ferragosto, l'attore prende contezza della truffa ed il 18 agosto 2016 scrive alla Banca evidenziando l'accaduto e facendo riferimento alla telefonata del giorno precedente, peraltro non contestata (cfr. mail indirizzata a e per conoscenza a e)

Il successivo 26 agosto il scrive nuovamente alla Banca, suggerendo di consentire ai clienti, in sede di conferma invio bonifici, la possibilità di verificare i dati dei beneficiari (cfr. *mail* indirizzata a e per conoscenza a); in pari data sporge querela presso gli Uffici del Compartimento Polizia Postale e delle Comunicazioni Abruzzo di Pescara.

Con raccomandata A.R. ricevuta dalla Banca il 30 agosto 2017 il sporge reclamo al fine di ottenere il rimborso delle somme.

La Banca, dal canto suo, ha prodotto due *mail*.

La prima, del 29 agosto 2016, inviata da a Ufficio Bonifici Poste

3/5 - ele

Italiane ove si legge " la presente per richiedere il richiamo per frode (in allegato denuncia alla Polizia Postale) del bonifico di € 2.331,10 del 16.8.2016 a favore di IBAN IT), già richiamato in procedura il 19/08 con codice" TECH motivazioni tecniche hanno prodotto un SCT errato" e rifiutato con causale "NOAS nessuna risposta del beneficiario".

La seconda *mail,* datata 1° settembre 2016, inviata da di Poste Italiane a della ed di Poste Italiane in cui si legge " siamo spiacenti di non poter restituire il pagamento per fondi insufficienti sulla carta, la segnalazione per frode è stata inviata all'ufficio competente".

Orbene, dall'esame della documentazione in atti è evidente il ritardo della Banca nel'attivazione delle procedure di recupero.

La prima segnalazione è avvenuta a mezzo telefono il 17 agosto; la seconda con *mail* del 18 agosto; la Banca, per sua stessa ammissione nella mail indirizzata a Poste Italiane, conferma di essersi attivata soltanto il 19 agosto, mentre la somma veniva prelevata dal reo il 18 agosto.

Non va poi sottaciuto che il provvedimento attuativo della Banca d'Italia del 5.7.2011 prevede l'obbligo dell'intermediario di dar corso a fasi di verifica teorica e pratica della vulnerabilità dei presidi di sicurezza, con relativa revisione periodica del processo stesso nonché di definire un adeguato insieme di presidi di sicurezza logica e fisica per i sistemi informativi, un efficace processo di controllo interno, un appropriato piano di continuità operativa e una gestione dei rapporti contrattuali con i fornitori esterni, coerente con i suddetti vincoli: in breve, un preciso obbligo di costante ed effettivo monitoraggio dell'efficienza del sistema di sicurezza che, come tale, non può non tenere in debita considerazione l'evoluzione dei metodi di aggressione e la costante ricerca di soluzioni protese ad ovviarne o arginarne le offensive.

Con ciò l'obbligo organizzativo previsto dall' articolo 8 del D.Lgs 11/2010 torna ad assumere piena e dirimente valenza.

L'addossamento del rischio all'intermediario, come evidenziato dal Collegio di Coordinamento, appare ancor più giustificato dalla forte e incessante promozione all'uso di tali strumenti posta in essere dal mondo bancario, in ciò aiutato anche da un sistema legislativo che sempre più ne impone l'adozione .

Siffatta promozione comporta obiettivamente un sensibile beneficio economico per gli stessi intermediari, consentendo loro significativi ed evidenti risparmi rispetto ad un tradizionale operatività di sportello.

Un tale beneficio deve dunque trovare, come trova, nel dettato normativo, un giusto trasferimento, in capo allo stesso intermediario, del rischio portato dall'impiego dello strumentario tecnologico.

Nella fattispecie l'attore, immune da qualsivoglia colpa grave, non è tenuto a sopportare le conseguenze dell'accaduto.

Alla luce delle brevi osservazioni che precedono, la Banca dovrà rimborsare l'importo

-4/5-

addebitato al [redacted] in virtù dell'operazione fraudolenta.
Le spese del giudizio seguono la soccombenza e vanno liquidate con il dispositivo della sentenza

---

n. 440/2019 RGAC [redacted] / Banca [redacted]

PQM

Il Giudice di Pace di Sulmona, dott.ssa Gianna Cipriani,
pronunciando nella causa civile vertente

TRA

[redacted] nato a [redacted] il [redacted], residente in [redacted], via [redacted] titolare della [redacted], c.f. [redacted] al fini della presente procedura elettivamente domiciliato in Pratola Peligna, via Amedeo Tedeschi n. 10, presso lo studio dell'avvocato Laila Coccovilli del Foro di Sulmona, dal quale è rappresentato e difeso in forza di mandato in calce all'atto di citazione (avvlailacoccovilli@puntopec.it)

ATTORE

E

-Banca [redacted], in persona del legale rappresentante *pro tempore*, con sede in [redacted] P.I. [redacted], ai fini della presente procedura elettivamente domiciliata in Sulmona, [redacted] presso lo studio dell'avvocato [redacted], dal quale in Sulmona, è rappresentato e difesa in forza di procura in calce alla comparsa di costituzione ([redacted])

CONVENUTA

avente ad oggetto: risarcimento danni

così provvede

1) Accoglie la domanda e per l'effetto condanna la convenuta a corrispondere all'attore, a titolo di risarcimento, la complessiva somma di € 2.331,10, oltre interessi nella misura legale dal 18 agosto 2016 fino al soddisfo.
2) Condanna la convenuta al pagamento, in favore dello Stato, delle spese prenotate e/o anticipate per compenso d'avvocato, pari ad € 98,00 + 27,00 per spese prenotate a debito ed € 1.000,00 per compenso d'avvocato, oltre accessori come per legge (convenuto ammesso al beneficio del patrocinio a spese dello Stato con delibera n.184 del Consiglio dell'Ordine Avvocati di Sulmona in data 1/7/2019)

Così deciso in Sulmona, 20 marzo 2021

Dep. 31/3/21

Il Cancelliere
dott.ssa Cristina Di Francesco

IL GIUDICE DI PACE
dott.ssa GIANNA CIPRIANI