Sentenza, Tribunale di Vicenza, Giudice Eloisa Pesenti, n. 1303, del 06/07/2023

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
Tribunale Ordinario di Vicenza

Il Tribunale Ordinario di Vicenza, SEZIONE PRIMA in composizione monocratica in persona del magistrato dott. Eloisa Pesenti ha pronunciato la seguente

SENTENZA

definitivamente provvedendo nella causa n. xxxx/2021 promossa con atto di citazione e iscritta a ruolo il 17.12.2021 da:

SOCIETA' con sede legale in omissis (...), in persona del legale rappresentante F.P. C.F. (...) rappresentata e difesa dall'Avv. omissis, nata a J. di S. il (...) C.F. (...) PEC omissis.it e dall'Avv. omissis nata a T. il (...) C.F. (...) PEC omissis presso il cui studio elegge domicilio in omissis

parte attrice

CONTRO

BANCA SPA, (C.F.:(...)), con sede legale in omissis, Partita IVA (...) e C.F. (...), in persona del Procuratore Speciale, S.C., in forza della procura speciale rilasciata in data 14 aprile 2021 a rogito del notaio Dott.ssa C.D.S.M. di M., repertorio n. (...), raccolta n. (...) (doc. 1), rappresentata e difesa, giusta procura autenticata ai sensi dell'art. 83 c.p.c., dagli Avv.ti omissis (C.F. (...), fax (...), PEC omissis) e omissis (C.F. (...), fax (...), PEC omissis) del Foro di Milano, nonché dall'Avv. omissis (C.F. (...), fax (...), PEC omissis) del Foro di Vicenza, con elezione di domicilio presso lo studio di quest'ultimo in omissis

parte convenuta

SVOLGIMENTO DEL PROCESSO - MOTIVI DELLA DECISIONE
(ART.132 C.P.C.)

Con l'atto di citazione in epigrafe indicato parte attrice **SOCIETA'**, premesso di essere stata titolare del conto corrente n.(...) acceso presso l'istituto **BANCA**, sul quale venivano fatti accreditare i canoni di locazione di due immobili di cui è proprietaria, esponeva che tale conto sino alla data del 26.05.2020 portava un saldo attivo di Euro 26.633,5 ma " Il giorno 16.5.2020 (rectius 26.5.2020), verso le 11 del mattino, il sig.F. accedeva al proprio home banking tramite l'applicazione installata sul suo telefono cellulare, in quanto necessitava di verificare se fosse stato accreditato il canone di Locazione da parte della società C.F. e scopriva che il saldo del conto risultava essere pari ad Euro 429,00... controllava i movimenti ed appurava che quel giorno erano stati effettuati tre bonifici in uscita, rispettivamente di Euro 8.200, 8500 e 9.500 tutti con descrizione " **BONIFICO BANCA**" e con le seguenti causali :"Bonifico da Voi disposto a favore di PAY NL invoice 81 bing and popunder", "Bonifico da Voi disposto a favore di PAY NL invoice 78 google adv", "Bonifico da Voi disposto a favore di PAY NL invoice 77 camp set popunde".

Immediatamente F. contattava telefonicamente la Banca e si recava in filiale, dove un funzionario e il Direttore della Filiale affermavano che probabilmente egli avesse aperto qualche mail e involontariamente fornito a terzi i propri codici d'accesso;

"- A tali insinuazioni rispondeva negando decisamente che cio' potesse essere accaduto, ribadendo di essere certo di non aver mai fornito ad alcuno i propri codici

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

- A quel punto egli veniva invitato a formalizzare il disconoscimento delle operazioni, al seguito del quale egli avrebbe ricevuto il riaccredito delle somme mancanti, in attesa dell'esito di loro verifiche interne";

l'attore si era poi recato a sporgere denuncia presso i Carabinieri di Dueville e in data 8.6.2020, si era recato "presso il negozio S.V., ove vi era un centro di assistenza e vendita di cellulari . Dopo aver riferito al tecnico della truffa subita, chiedeva di poter far effettuare un back up dell'apparecchio telefonico - All'esito di tale operazione, il tecnico faceva presente al sig. F. che vi era un'app di **BANCA** che bloccava il sistema e che secondo lui si trattava di un'app "tarocca/fasulla", tant'é che si rendeva necessario trasferire i dati su altra scheda sim per poi riuscire ad eliminarla dal telefonino".

Il 16.9.2020 il direttore della Banca lo informava che, all'esito delle verifiche effettuate, l'Istituto non aveva alcuna responsabilità e che pertanto avrebbero provveduto a stornare le somme riaccreditate. L'attore aggiungeva che, "Una volta riattivato il servizio on line, constatava che l'APP richiedeva piu' passaggi rispetto a quanto avveniva precedentemente, richiedendo un ulteriore codice che veniva inviato sul telefono per poter accedere dal PC."

Parte attrice affermava che le operazioni di bonifico effettuate dal conto della F.B. snc non erano state effettuate né autorizzate ed erano avvenute a seguito di un'illecita intrusione nel sistema informatico della Banca o comunque a causa di gravi lacune nei sistemi di sicurezza della stessa . Riteneva pertanto responsabile la Banca e chiedeva la condanna della convenuta al pagamento a titolo di risarcimento dei danni dell'importo di Euro 26.200,00 oltre interessi e rivalutazione con decorrenza dalla data della disposizione.

Parte convenuta BANCA **SPA**, costituitasi, chiedeva il rigetto della domanda, eccependo che le obbligazioni a proprio carico ai sensi dell'art. 8, comma 1, lett. a), del D.Lgs. n. 11 del 2010, che onera la Banca ad "assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento", erano state assolte mediante la " messa a disposizione delle password one time (o One Time Password), fornite alla F.B. attraverso singoli messaggi SMS trasmessi dalla Banca sul numero di telefono cellulare del F., documentati dalle tracciature prodotte (doc. 3 di I., foglio SMS), che realizzavano un sistema di autenticazione c.d. "a due fattori", ritenuto, allo stato dell'evoluzione tecnologica, "il più sicuro" sistema "e tale da assicurare la migliore tutela degli utilizzatori in base all'attuale stato della tecnica" tanto da poterne affermare la "pressoché invulnerabilità".

Contestava l'affermazione attorea secondo cui alla riattivazione del servizio di home banking, esso sarebbe stato dotato di un sistema di autenticazione che richiedeva un ulteriore codice che veniva inviato sul telefono per poter accedere dal PC.

Secondo parte convenuta la distrazione dei fondi non poteva essere avvenuta che per responsabilità del F., il quale, verosimilmente a causa di una truffa on line (phishing) non aveva custodito correttamente i codici di accesso ai servizi di home banking ossia:

"1) un codice utente, rilasciato in filiale dalla Banca all'atto della sottoscrizione del contratto;

2) una password di accesso (o "Codice PIN"), fornita dalla Banca e modificata dalla correntista a seguito del primo accesso;

3) una one time password (o "OTP" o "dinamica" in virtù della propria temporaneità e continua modificazione), monouso, con validità limitata a pochi secondi, inviata via SMS al numero mobile dell'utente (c.d. funzionalità "O-Key SMS"). In virtù della sua natura, l'SMS di invio può definirsi "parlante", in quanto completo di una breve descrizione dell'operazione che l'OTP in esso contenuta è volta ad autorizzare, assolvendo pertanto anche una finalità informativa in favore del correntista.

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

Oltre a tali credenziali, comuni alla consueta operatività di home banking, può altresì essere richiesto un ulteriore codice autorizzativo, comunemente denominato "OTS", inviato all'utente attraverso un altro SMS al proprio numero mobile, sempre all'interno di apposito messaggio "parlante" e da digitarsi al fine di autorizzare operazioni ritenute sospette dai sistemi antifrode della Banca o altre attività di particolare importanza. "

La convenuta affermava che

" il 25 maggio 2020, alle ore 17:45, è registrata una richiesta di accesso al portale di home banking della F.B. da una connessione differente dalle precedenti (indirizzo IP n. 81.174.43.109). Rilevata tale richiesta, i sistemi di I. generavano e inviavano via SMS, al cellulare del signor F., un messaggio contenente il codice OTP richiesto, del seguente tenore:

"O-Key SMS - Usa 037418 per entrare nel sito M." (doc. 3, foglio SMS, riga 2).

Il codice "(...)" veniva correttamente immesso e, quindi, era avviata la sessione di home banking (doc. 3, foglio Tracciatura, riga 3, "NUOVA SESSIONE AUTENTICATA POST-LOGIN ATTIVA").

Successivamente, veniva registrata l'immissione dei bonifici disconosciuti.

In particolare, alle ore 17:45:33 e ss. era immesso l'ordine di bonifico di Euro 9.500,00 (doc. 3, foglio Tracciatura, righe 8-14), autorizzato attraverso la digitazione del codice OTP (doc. 3, foglio Tracciatura, riga 11, "OTP CORRETTA SU DISPOSITIVA") inviato via SMS al cellulare del signor F., unitamente al messaggio "O-Key SMS - Usa 651321 per autorizzare il pagamento del bonifico M. a Paynl per un importo di 9.500 sul sito M." (doc. 3, foglio SMS, riga 3).

Alle ore 17:49 veniva avviata una nuova sessione (doc. 3, foglio Tracciatura, riga 17), mediante OTP "511274" inviato via SMS ("O-Key SMS - Usa 511274 per entrare nel sito M.") al cellulare del signor F. (doc. 3, foglio SMS, riga 4).

Nell'ambito di tale sessione, era immesso il bonifico di Euro 8.500,00, autorizzato con codice OTP "616179" inviato al signor F. all'interno dell'SMS "O-Key SMS - Usa 616179 per autorizzare il pagamento del bonifico M. a Paynl per un importo di 8.500 sul sito M." (doc. 3, foglio SMS, riga 5). Tale bonifico risultava autorizzato correttamente ("OTP CORRETTA SU DISPOSITIVA" - doc. 3, foglio Tracciatura, riga 26), derivandosi che il codice OTP "616179" era stato correttamente digitato.

Analoga successione veniva registrata per il bonifico di Euro 8.200,00, immesso nell'ambito della sessione avviata con OTP "143402" inviato con SMS "O-Key SMS - Usa 143402 per entrare nel sito M." (doc. 3, foglio SMS, riga 6), quindi autenticato con codice OTP "113870" inviato con SMS "O-Key SMS - Usa 113870 per autorizzare il pagamento del bonifico M. a Paynl per un importo di 8.200 sul sito M." (doc. 3, foglio SMS, riga 7)...

il pomeriggio del 25 maggio 2020 al cellulare del correntista venivano inviati sei SMS, nessuno dei quali ha comunque destato l'attenzione del signor F. ....le sessioni di home banking del pomeriggio del 25 maggio 2020 paiono effettuate da una connessione non abituale (contraddistinta dall'indirizzo IP 81.174.43.109 - doc. 3, foglio Accessi, righe 48-53), mentre la sessione del 26 maggio 2020, eseguita dallo stesso signor F. per sua stessa ammissione, è associata alla connessione n. 79.44.183.138 (doc. 3, foglio Accessi, righe 54-55), già rinvenuta giorni prima (doc. 3, foglio Accessi, righe 22-45).

Considerato che l'operatività associata alla connessione 81.174.43.109 è stata contestata dal correntista, potremmo desumere che la stessa sia quindi da ricondursi ai truffatori e, in particolare scorrendo le tracciature, si nota alle 10:01 del 20 maggio 2020, ovvero cinque giorni prima del consumarsi della truffa, un accesso da altra connessione non abituale, dall'indirizzo IP 78.134.48.53. Potremmo quindi ipotizzare che, in tale occasione, il signor F. abbia riscontrato una comunicazione fraudolenta, non inviata da I., ed abbia seguito le ingannevoli istruzioni in essa contenute, tentando l'accesso al portale di

home banking utilizzando un link fasullo e, così facendo, ha scaricato ed installato l'APP "tarocca/fasulla" poi usata dai malfattori per compiere le transazioni del 25 maggio 2020 Perché ciò possa essere accaduto, è inevitabile che il signor F. abbia cercato di effettuare un accesso da un collegamento differente dall'indirizzo www.intesasanpaolo.com, immettendo le proprie credenziali su un portale non autorizzato ma controllato dai truffatori, consentendo loro di venire a conoscenza delle credenziali statiche della F.B. e quindi, dei codici OTP trasmessi via SMS."

Secondo la convenuta la APP fasulla doveva derivare da uno dei seguenti fatti:

"- parte attrice ha scaricato l'APP da un portale non ufficiale;

- parte attrice non ha eseguito correttamente gli aggiornamenti; sul punto si rammenta come, nelle guide sopra riportate, la Banca abbia espressamente previsto che "Gli aggiornamenti delle App avvengono sempre e solo attraverso gli store ufficiali";

- parte attrice ha dato seguito a comunicazioni fraudolente, cancellando l'APP di I. e scaricando software malevoli, come ad esempio un'APP "tarocca/fasulla", la cui natura malevola e provenienza non autorizzata non sono state riconosciute dall'utente, il quale ha continuato a farne uso erroneamente."

Parte attrice nella prima difesa successiva ribadiva di non avere mai ricevuto gli SMS del 25.5.20; di avere controllato il 26.5.2020 il conto solo in quanto attendeva l'accredito di determinati canoni di locazione ; di non avere mai effettuato operazioni dispositive tramite home banking su tale conto, atteso che le uniche erano quelle disconosciute e mai autorizzate; di non avere mai scaricato e installato una APP tarocca/fasulla, che era stata rinvenuta solamente il giorno 8.6.2021 a seguito di operazioni di verifica svolte da un tecnico specializzato, su incarico del sig. F., visto che nessuno da parte della Banca gli aveva fornito spiegazioni o gli aveva chiesto verifiche nell'immediatezza, limitandosi a formulare mere ipotesi su mail ipoteticamente ricevute dall'attore.

Nel corso della fase istruttoria veniva impartito:
alla parte attrice, ordine di esibizione delle email e dei messaggi SMS ricevuti in data 25 maggio 2020 e nei trenta giorni precedenti; all'operatore telefonico gestore, in data 25 maggio 2020, dell'utenza mobile (...) del F., l'esibizione dei tabulati telefonici di tale numero e relativi al giorno 25 maggio 2020, e la causa veniva rinviata per la precisazione delle conclusioni all'udienza del 23.3.2023.

Va preliminarmente osservato che l'attore ha ottemperato per quanto possibile all'ordine di esibizione, avendo richiesto a Microsoft il recupero delle mail non più esistenti nel proprio computer ed esibendo le foto di quelle tuttora visibili, e avendo chiesto al gestore della telefonia i tabulati del traffico sul proprio telefono cellulare, (doc.5-7, con esiti negativi non essendo state rilevate da Microsoft ulteriori mail e non essendo stati forniti da Windtre i tabulati in quanto afferenti a causa civile e non penale).

Dalla documentazione prodotta dalle parti risulta che l'attivazione del servizio di home banking e' avvenuta il 5 marzo 2020 col " Contratto servizi via internet, cellulare, telefono" doc. 2 di parte convenuta. Tale contratto prevede all'art.5 quanto segue :

3. Non appena a conoscenza dello smarrimento, del furto, della appropriazione indebita o in generale di un uso non autorizzato di tutti o di alcuni Codici o del Dispositivo, il Cliente deve darne tempestiva comunicazione alla Filiale, personalmente oppure a mezzo di lettera, oppure tramite l'apposito numero telefonico indicato nella Guida ai Servizi. Ricevuta la relativa comunicazione, la Banca provvede a bloccare l'utilizzo del Servizio interessato secondo quanto previsto nella Guida ai Servizi. La suddetta comunicazione può essere effettuata dal Superutente o dal Titolare per i Codici e il Dispositivo ad essi attribuiti.

4. La comunicazione è opponibile alla Banca:

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

- dal momento della ricezione, da parte della Banca, della comunicazione effettuata personalmente alla Filiale, oppure a mezzo dell'apposito servizio telefonico;

- dalle ore 24 del giorno di ricezione, da parte della Filiale, della comunicazione inviata per lettera.

5. Prima del momento in cui la segnalazione è opponibile alla Banca le conseguenze dannose derivanti dall'utilizzo indebito di tutti o di alcuni Codici sono integralmente a carico del Cliente.

6. Se il Cliente è una microimpresa il comma 5 non si applica. In questo caso, prima del momento in cui la segnalazione è opponibile alla Banca, la responsabilità del Cliente è regolata in base alle norme di legge. Pertanto:

(a)salvo il caso in cui il Cliente o il Superutente o un Titolare abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza di tutti o di alcuni Codici, il Cliente sopporta per un importo comunque non superiore complessivamente a 50 euro la perdita derivante dall'utilizzo indebito dei Servizi conseguente alla sottrazione, appropriazione indebita o smarrimento di tutti o di alcuni Codici;

b)qualora il Cliente o il Superutente o un Titolare abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di custodia e di segnalazione previsti al presente articolo con dolo o colpa grave, il Cliente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al punto precedente.

Tuttavia salvo il caso in cui il Cliente, il Superutente o un Titolare abbia agito in modo fraudolento, il Cliente non sopporta alcuna perdita:

-se la Banca per la disposizione di un ordine di pagamento non esige un'Autenticazione forte del Cliente, del Superutente o di un Titolare;

-se lo smarrimento, la sottrazione o l'appropriazione indebita dei Codici o del Dispositivo non potevano essere notati dal Cliente, dal Superutente o di un Titolare prima di un ordine di pagamento.

Inoltre, il Cliente non sopporta alcuna perdita derivante dallo smarrimento, dalla sottrazione o dall'appropriazione indebita dei Codici o del Dispositivo utilizzati per la disposizione di un ordine di pagamento se la stessa perdita è stata causata da atti o omissioni di soggetti di cui la Banca si avvale per l'esecuzione delle attività previste a suo carico nel contratto.

7.A partire dal momento in cui la segnalazione è opponibile alla Banca, il Cliente non è responsabile delle conseguenze dannose derivanti dall'utilizzo dei Codici, salvo il caso in cui il Cliente o il Superutente o il Titolare abbia agito con dolo.

Posto che parte attrice, società in nome collettivo con due soci (doc.1 attoreo, visura camerale), rientra nella nozione di microimpresa, le è applicabile il comma VI del predetto art.5 del contratto.

Non vi è alcuna prova che l'appropriazione dei dati del cliente da parte dei truffatori sia avvenuta a seguito di comportamenti incauti dello stesso, e tantomeno che egli abbia agito con colpa grave o dolo, essendo notorio che i metodi dei truffatori sono giunti a grande raffinatezza, riuscendo ad esempio a "clonare" perfettamente siti e comunicazioni delle banche , ad insinuarsi nella corrispondenza vera tra queste ultime e i clienti, a clonare le schede SIM dei telefoni dei clienti, a "deviare" i messaggi SMS verso gli apparecchi dei truffatori.

Va inoltre osservato che, secondo quanto affermato dall'attore e non contestato dalla convenuta, il F. dopo avere immediatamente denunciato il fatto alla banca e avere sporto denuncia ai Carabinieri, era stato inizialmente rassicurato dai funzionari della banca circa il riaccredito delle somme, e verosimilmente per effetto di tale rassicurazione aveva omesso di conservare il telefono cellulare nello

stato in cui era al momento della truffa subita, venendo avvisato solo dopo due mesi del mancato riaccredito, ed essendosi così privato della possibilità di fare sottoporre il telefono ad una consulenza tecnica.

Risultano invece manchevoli, ad avviso di questo giudicante, i presidi di sicurezza della convenuta, atteso che pur essendo stato percepito dal sistema in data 20.5.2020 un accesso da una connessione IP diversa dal solito (doc. 3 di parte convenuta, righe 46 e 47), nessuna forma di avviso è stato diramato al cliente, a differenza di quanto avviene da parte dei sistemi di altre banche, (o anche semplicemente della posta elettronica), che avvisano dell'avvenuto contatto da una fonte diversa dal solito e invitano a controllare. Tale semplice accorgimento, da tempo assai diffuso, avrebbe consentito al cliente di prendere cognizione dell'indice di anomalia , di rendersi conto del pericolo e conseguentemente di modificare la password o il codice PIN.

Parimenti, pur essendo stato percepito dal sistema in data 25.5.2020 un accesso da una connessione IP diversa dal solito e anche dalla precedente del 20.5.2020, nessuna forma di blocco temporaneo o controllo è stata posta in essere dalla convenuta.

Va inoltre rilevato che dal conto corrente in esame (doc.2 attoreo) non risulta alcun precedente movimento dispositivo effettuato via home banking, il che doveva rendere ancora più sospette le tre disposizioni di "bonifico europeo", di ingente importo e a distanza ravvicinata (tra le 17.45 e le 17.54 del 25.5.2020), che avevano grandemente ridotto la provvista esistente sul conto (da circa 25.000,00 a 429,00 euro).

La duplice anomalia, rappresentata dalla provenienza da una connessione nuova e diversa dall'abituale, e dalla imponenza degli esborsi apparentemente disposti, per la prima volta e in favore di conti esteri, avrebbe dovuto imporre la richiesta dell'ulteriore codice di sicurezza di cui la convenuta parla a pagina 3 della comparsa di costituzione (OTS).

Si ritiene quindi applicabile la previsione contrattuale di cui al sopra visto art. 5 del contratto intercorso tra le parti, e quindi la convenuta dovrà restituire alla parte attrice le somme uscite dal conto dello stesso senza sua autorizzazione, mentre parte attrice, della quale non è possibile affermare colpa grave o dolo, ma nemmeno escludere qualche colpa lieve, parteciperà della perdita in misura non superiore ad Euro 50,00.

In conclusione la parte convenuta deve essere condannata a pagare alla parte attrice Euro 26.150,00 oltre agli interessi di legge dalla domanda al saldo, esclusa la rivalutazione trattandosi di debito di valuta.

Il regolamento delle spese di lite segue la soccombenza, e la liquidazione viene effettuata come da dispositivo sulla base del D.M. n. 55 del 2014 , D.M. n. 37 del 2018 e D.M. n. 147 del 2022, in base alle attività espletate e alla complessità della lite.

P.Q.M.

definitivamente decidendo, disattesa ogni diversa domanda, eccezione o deduzione, il giudice così provvede:

1) condanna la parte convenuta a pagare alla parte attrice Euro 26.150,00 oltre agli interessi di legge dalla domanda al saldo;

2) condanna la parte convenuta a rifondere alla parte attrice le spese di lite, liquidate in Euro 545,00 per anticipazioni ed Euro 7.616,00 per compensi professionali, oltre al rimborso forfettario, CPA e IVA se dovuta.

Così deciso in Vicenza, il 5 luglio 2023.

Depositata in Cancelleria il 6 luglio 2023.

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