Sentenza n. 215/2024 pubbl. il 06/02/2024
RG n. 667/2022
Repert. n. 274/2024 del 06/02/2024

N. R.G. 667/2022

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

TRIBUNALE ORDINARIO di PESCARA

OBBLIGAZIONI E CONTRATTI CIVILE

Il Tribunale, nella persona del Giudice dott. Patrizia Franceschelli
ha pronunciato la seguente

SENTENZA

nella causa civile di I Grado iscritta al n. r.g. **667/2022** promossa da:

ell'avv. DI ROCCO
) CHIETI presso il

dell'avv. DI ROCCO
) CHIETI presso il

difensore avv. DI ROCCO MASSIMO

ATTORI

contro

POSTE ITALIANE SPA (C.F. 01114601006), con il pat

nte domiciliato presso

CONVENUTA

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b03505515efa623b37c

OGGETTO: risarcimento danni

CONCLUSIONI: come in atti.

FATTO E DIRITTO

1) Con atto di citazione notificato in data 09-02-2022, convenivano in giudizio innanzi al Tribunale di Pescara Poste Italiane s.p.a., chiedendo l'accoglimento delle seguenti conclusioni: "*in via principale, accertare e dichiarare la responsabilità contrattuale esclusiva delle Poste Italiane S.p.A. (p.i. 01114601006), ai sensi dell'art. 1218 c.c., per il danno subito dagli attori derivante dalle operazioni di pagamento meglio indicate al punto 12) sub a), b) e c) delle premesse, eseguite in assenza di autorizzazione da parte dei medesimi attori, pari a complessivi € 5.151,00 (eurocinquemilacentocinquantuno/00) e, per l'effetto, condannare detta convenuta al risarcimento integrale di detta somma, oltre rivalutazione ed interessi; in via alternativa, accertare e dichiarare la responsabilità ex art. 2050 c.c., esclusiva delle Poste Italiane, nella determinazione del danno subito dagli attori derivante dalle operazioni di pagamento meglio indicate al punto 12) sub a), b) e c) delle premesse, pari a complessivi € 5.151,00 (eurocinquemilacentocinquantuno/00) e, per l'effetto, condannare detta convenuta al risarcimento integrale di detta somma, oltre rivalutazione ed interessi. Con vittoria di spese ed onorari di giudizio*";

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b03505515efa623b37c

A sostegno della domanda gli attori riferivano "di essere co-titolari del conto corrente postale nr. 1009618743 acceso presso Poste Italiane S.p.A., filiale di Collercorvino (PE), cui venivano associate, per le relative operazioni su conto, nr. 2 (due) carte Postamat, che ciascuno degli attori utilizzava esclusivamente per effettuare prelievo di denaro contante presso gli sportelli automatici abilitati, e di aver installato sui rispettivi apparecchi telefonici smartphone l'applicazione (c.d. app.) "BANCOPOSTA" che veniva dagli stessi utilizzata per effettuare il pagamento on line delle sole utenze (energia, telefono, gas, etc.), oltre che per controllare periodicamente l'esito delle operazioni effettuate ed il saldo. Sostenevano che in data 23-01-2021, alle ore 08.30 circa, si erano recati presso l'Ufficio Postale filiale di Penne (PE) per svolgere alcune operazioni sul proprio conto corrente e, nell'occasione, l'impiegato addetto allo sportello aveva riferito loro che, per il completamento di dette operazioni, era necessario inserire il codice OPT (one time password) che Poste Italiane avrebbe inviato via sms di lì a breve, sul telefono associato al conto corrente (utenza telefonica della). In effetti, alle ore 08.59 ed alle ore 09:02, sull'utenza telefonica della Bongrazio erano stati ricevuti nr. 2 sms automaticamente generati dall'utenza "PosteInfo", indicata come "Centro Assistenza: +393711000111", a mezzo dei quali erano stati inviati due distinti codici OTP, da comunicare all'addetto allo sportello al fine di concludere le operazioni (All.1). Nove giorni dopo, ovvero in data 01.02.2021, alle ore 18:48, sulla medesima utenza telefonica intestata ed in uso alla Sig.ra a era stato inoltrato un ulteriore messaggio sms proveniente da Poste Info che però non era stato dalla stessa visualizzato. Ulteriormente, in data 26.02.2021, alle ore 15:00, sempre sull'utenza telefonica della sig.ra B era giunto un ulteriore sms, proveniente da "PosteInfo" (mittente +39.371.1000111), con il quale era stato testualmente comunicato "Sicurezza Web, il sistema ha sospeso la sua utenza per mancato aggiornamento psd2 Accedi ora per attivarlo https://is.gd/pzYfn0" (All.2). L , considerato che detto sms era stato inoltrato dal medesimo mittente (PosteInfo) e numero (mittente +39.371.1000111) che aveva inviato i precedenti due sms del 23.01.2021, allorquando si era trovata all'interno della filiale di Penne - circostanza confermata anche dal fatto che il predetto messaggio era nella medesima casella e seguiva quelli contenenti il codice OTP, ritenendo sicura ed affidabile la provenienza del messaggio – aveva provveduto immediatamente ad effettuare l'accesso presso l'indicato sito web, cliccando sul link a cui era stata indirizzata, procedendo all'inserimento dei dati personali che le erano stati richiesti. Nell'effettuare l'accesso – però - l'istante aveva riscontrato alcune anomalie nel sistema che non le avevano consentito di completare l'aggiornamento richiesto, senonché era stata subito contattata dall'utenza numero + alla quale un soggetto, con voce maschile, si era qualificato quale operatore del servizio "Sicurezza Web" di Poste Italiane (All.3), quale addetto il cui compito consisteva nel coadiuvare la nel completamento dell'aggiornamento richiesto e nell'utile procedura di inserimento dei dati. Erano seguite altre telefonate dal medesimo interlocutore ed altri sms sempre provenienti dall'utenza PosteInfo (All.4), che avevano consentito alla di procedere all'aggiornamento richiesto previo rilascio verbale di dati ed indicazioni personali che l'operatore aveva acquisito a convalida di quelli già presenti e riportati sul sistema telematico di Poste Italiane. Nella serata del 26.02.2021, il Sig. , coniuge della Sig.ra a e cointestatario del summenzionato conto corrente postale, recatosi presso uno sportello Postamat al fine di prelevare del contante, non aveva potuto far altro che riscontrare - con grande sconcerto e sgomento - che il conto corrente risultava essere privo di liquidità. Il giorno seguente, 27.02.2021, gli istanti si erano recati prontamente presso l'ufficio postale di Collecorvino (PE) ove, richiesto un estratto conto (All.5), avevano ricevuto dal cassiere l'amara conferma che il conto corrente cointestato nr. 1009618743 risultava essere stato svuotato, residuando un attivo di appena € 3,99. Le operazioni addebitate sul conto corrente postale nr. 1009618743, difatti, erano risultate essere state compiute mediante i seguenti illegittimi, illeciti, non autorizzati e non acconsentiti "movimenti" per l'ammontare complessivo di € 5.151,50 (eurocinquemilacentocinquantuno/50), come da operazioni di seguito indicate: a) movimento n. 2021 0302 0013 0882 1536 del 26.02.2021, codice operazione BIBOPOSE,

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b0350551 5efa623b37c

causale 043, Descrizione "26.02.2021 ore 17:14, WWW.PAGACOMODO.IT MILANO ITA OPERAZIONE 612096 CARTA 4456160" operato sul conto 84130 001009618743, dell'importo di € 2.451,50 (All.6); b) movimento n. 2021 0226 7733 3383 0666 del 26.02.2021, codice operazione RICR, causale 38RICR, Descrizione "Addebito Conto Corrente per sottoscrizione" delle ore 17:25, operato sul conto 84130 001009618743, dell'importo di € 1.720,00 (All.7); c) Movimento n. 2021 0302 0013 0882 1535 del 26.02.2021, codice operazione BIBOPOSE, causale 043, Descrizione "26.02.2021 ore 18:18 www.goldbet.it +390640400860 ITA OPERAZIONE 613869 CARTA 4456160" operato sul conto 84130 001009618743, dell'importo di € 980,00 (All.8). Preso atto di ciò, gli istanti avevano provveduto immediatamente a bloccare le carte ed a chiudere il conto corrente acceso presso l'Ufficio Postale di Penne, tanto che, appena usciti dall'ufficio, si era recava presso la Stazione dei Carabinieri di Collecorvino dove aveva presentato denuncia-querela in ordine ai fatti occorsi e descritti (All.9). Ancor più, in data 02.03.2021, gli attori avevano sottoscritto "modulo di contestazione addebito per i servizi bancoposta/claim form for bancoposta services" con il quale avevano provveduto immediatamente a contestare le sopra citate operazioni, in quanto non autorizzate, avanzando contestualmente richiesta di rimborso alle Poste Italiane. In data 05.03.2021 gli istanti, previo disconoscimento delle operazioni di pagamento contestate, avevano inviato formale "diffida ad adempiere con contestuale costituzione in mora e interruzione termini prescrizione" (All.10) chiedendo la restituzione/rimborso delle somme indebitamente ed illegittimamente prelevate, siccome non autorizzate. In riscontro alla predetta diffida le Poste Italiane S.p.A., con missiva del 31.03.2021, avevano informato il sottoscritto procuratore che era emersa la necessità di svolgere più approfondite verifiche, il cui esito sarebbe stato comunicato, salvo poi omettere qualsivoglia ulteriore informazione in ordine a tali accertamenti (All.11). Gli attori adivano quindi l'autorità giudiziaria per la tutela dei propri diritti"

2) Si costituiva in giudizio Poste Italiane s.p.a., contestando ogni addebito di responsabilità, che sarebbe stata ascrivibile, per contro, ai medesimi attori, e concludeva per il rigetto di tutte le domande formulate perché infondate in fatto ed in diritto.

3) Espletata l'istruttoria a mezzo di produzione documentale e prova orale, la causa, previa revoca del provvedimento con cui veniva fissata la discussione orale ex art. 281 sexies c.p.c., veniva trattenuta in decisione ai sensi dell'art. 190 c.p.c.

4) Nel caso di specie si configura evidentemente una condotta di "phising", termine con il quale si definisce una condotta illecita mediante cui la vittima viene indotta a fornire online informazioni personali, dati finanziari o codici di accesso, in risposta a SMS "esca" oppure ad e-mail ingannevoli, creati ed inviati dall'autore della truffa (phisher). Fornendo le informazioni richieste, la vittima consente così al phisher di accedere ai suoi conti bancari.

Sulla natura della responsabilità della banca in siffatti casi si è verificata una evoluzione degli orientamenti interpretativi. Nelle prime pronunce, le condanne irrogate agli intermediari bancari erano fondate sulla normativa di cui al D. Lgs. n. 196/2003 che all'art.15 (articolo abrogato dall'art. 27, comma 1, lettera a), numero 2), del D. Lgs. 10/08/2018, n. 101) prevedeva che chiunque cagionasse un danno ad altri per effetto dell'illecito trattamento di dati personali fosse tenuto al risarcimento ai sensi dell'art. 2050 c.c. (cfr. Tribunale Palermo, 12/01/2010; recentemente, ancora in questo senso, si segnala la sentenza di Corte Appello di Ancona sez. I, 13/01/2021 n. 18). Successivamente, i giudici hanno preferito richiamare, a fondamento delle proprie decisioni, la responsabilità contrattuale della banca in forza della disciplina del mandato ex art. 1856 c.c. e i relativi criteri di ripartizione dell'onere della prova; così, di recente, si è espresso il Tribunale Monza sez. I, 03/02/2021 n.207, sulla scorta del più risalente arresto del Tribunale Verona, 02/10/2012).

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b0350551 5efa623b37c

L'interpretazione si è poi orientata (soprattutto nelle decisioni dell'ABF) verso la configurazione di una responsabilità oggettiva in capo all'intermediario, sulla scorta della giurisprudenza della Corte di Cassazione, secondo la quale "*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 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. Ne consegue che, anche prima dell'entrata in vigore del d.lgs. n. 11 del 2010, attuativo della direttiva n. 2007/64/CE relativa ai servizi di pagamento nel mercato interno, la banca, cui è richiesta una diligenza di natura tecnica, da valutarsi con il parametro dell'accorto banchiere, è tenuta a fornire la prova della riconducibilità dell'operazione al cliente*" (Cass. Sez. 1 - , Sentenza n. 2950 del 03/02/2017, Rv. 643717 - 01).

La banca è tenuta quindi ad approntare misure idonee a verificare la riconducibilità delle operazioni alla volontà del cliente ed escludere la possibilità di una abusiva utilizzazione delle credenziali di accesso da parte dei terzi (a meno che non ricorra il dolo del titolare); è la banca a dover fornire la prova della riconducibilità dell'operazione al cliente; la prova liberatoria a carico del prestatore di servizi, nell'ottica del regime delle attività pericolose, non può prescindere dalla valutazione concreta delle misure tecnologiche offerte dal progresso scientifico per i sistemi di home banking. Nel rapporto contrattuale di home banking, la veste di contraente qualificato della banca comporta che essa non solo sia tenuta ad adeguarsi all'evoluzione tecnica dei sistemi di sicurezza, bensì, per andare esente da responsabilità, dimostri di aver adottato tutte le misure idonee ad evitare il danno e fornisca la prova positiva di una causa esterna. Ma gli obblighi della banca non si esauriscono qui. Infatti, secondo gli interpreti essi si spingono fino a ricomprendere un obbligo di monitoraggio puntuale delle operazioni dei correntisti. In altre parole, compete all'intermediario verificare anche il regolare andamento delle operazioni e segnalare quelle che appaiono anomale, specie se emergano transazioni effettuate in contrasto con la usuale operatività del conto (ABF, Collegio di Bologna, provvedimento n. 7884 del 23/03/2021, Tribunale di Arezzo, 08/04/2020, n. 272; Tribunale Parma, 06/09/2018, n. 1268; ABF Collegio di Bologna n. 5874 dell'11/04/2022).

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b03505515efa623b37c

La banca, nei casi di phishing, risponde anche ai sensi del D.Lgs. n. 11/2010, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno L'art. 10 del D.Lgs. n. 11/2010 (Prova di autenticazione ed esecuzione delle operazioni di pagamento) così dispone: "*1. Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente 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 malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; 2. Quando l'utilizzatore di servizi di pagamento 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 a uno o più degli obblighi di cui all'articolo*". In forza di tale previsione, dunque, l'intermediario ha l'onere di fornire la prova della corretta autenticazione, registrazione e contabilizzazione delle operazioni disconosciute dal cliente, nonché dell'assenza di malfunzionamenti dei propri sistemi. Il successivo art. 10-bis (Autenticazione e misure di sicurezza) impone al prestatore di servizi di predisporre un'autenticazione forte del cliente quando quest'ultimo accede al suo conto di pagamento online, ovvero dispone un'operazione di pagamento elettronico o effettua qualsiasi azione, mediante un canale a distanza, che può comportare una frode nei pagamenti o altri abusi. Infine, l'art. 11 (Responsabilità del prestatore di servizi di pagamento per le operazioni di pagamento non autorizzate) prevede che: "*1. Fatto salvo l'articolo 9, nel caso in cui un'operazione di pagamento non sia stata autorizzata, il prestatore di servizi di pagamento rimborsa immediatamente al pagatore l'importo dell'operazione medesima. Ove per l'esecuzione dell'operazione sia stato addebitato un conto di pagamento, il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo; 2. In caso di motivato sospetto di frode, il prestatore di servizi di pagamento può sospendere il rimborso di cui al comma 1 dandone immediata comunicazione all'utilizzatore; 3. Il rimborso di cui al comma 1 non preclude la possibilità per il prestatore di servizi di pagamento di dimostrare anche in un momento successivo che l'operazione di pagamento era stata autorizzata; in tal caso, il prestatore di servizi di pagamento ha il diritto di chiedere ed ottenere dall'utilizzatore la restituzione dell'importo rimborsato; 4. Il risarcimento di danni ulteriori subiti può essere previsto in conformità alla disciplina applicabile al contratto stipulato tra l'utilizzatore e il prestatore di servizi di pagamento*". L'art. 7 (Obblighi a carico dell'utente dei servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate) prevede, invece, una serie di oneri a carico del cliente della banca, quali la tempestiva comunicazione dell'altrui utilizzo indebito dello strumento, l'adozione delle misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo.

La responsabilità oggettiva del prestatore di servizi incontra un limite laddove venga accertata la condotta dolosa o gravemente colposa dell'utente, che può ad esempio configurarsi nel caso in cui il medesimo inserisca le proprie credenziali a seguito della ricezione di e-mail redatte con evidenti errori e lessico non corretto.

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b0350551 5efa623b37c

Ai fini della valutazione della colpa del cliente deve dunque condursi una verifica caso per caso, valorizzando le peculiarità delle fattispecie concrete, quali, ad esempio: la presenza di anomalie nel messaggio inviato dal phisher, che avrebbero potuto allarmare il correntista in merito all'autenticità e alla provenienza del messaggio (ad esempio, errori grammaticali, spazi fra le parole del testo ecc.); la provenienza dell'SMS esca (o della email), ad esempio, se esso provenga dalla stessa utenza telefonica utilizzata dalla banca per le comunicazioni relative al servizio di home banking ovvero da numero diverso e sconosciuto al cliente; se il cliente abbia seguito le ordinarie cautele nella protezione del proprio computer o cellulare (ad esempio, con l'adozione di idonei software antivirus). Secondo la giurisprudenza (in tal senso: Corte di Appello di Milano, sez. I, 23/07/2021 n.2419), la sussistenza di grave negligenza in capo al cliente va provata dalla banca, che deve allegare circostanze a supporto (sulla scorta della sentenza della Cassazione del 12/04/2018, n. 9158, secondo cui la banca va esente da responsabilità e non risponde del danno patito dal cliente, solo qualora dimostri che il fatto sia attribuibile al dolo del correntista o a comportamenti particolarmente incauti).

Con una recente pronuncia, la Corte di Cassazione – nell'affrontare il caso di una correntista che agiva in giudizio contro Poste Italiane s.p.a. per ottenere la condanna al risarcimento della somma fraudolentemente sottratta dal suo conto – ha precisato che "*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)*" (Cass. Sez. 6 - 3, Ordinanza n. 26916 del 26/11/2020, Rv. 659904 – 01; Cass. Sez. 3 - , Sentenza n. 18045 del 05/07/2019, Rv. 654563 – 01).

La Banca, pertanto, nel caso di operazioni effettuate con strumenti elettronici come l'*home banking* è tenuta a risarcire il danno patito dal correntista vittima di *phishing*, salvo che dimostri che il fatto sia attribuibile a dolo o colpa grave del cliente o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo.

5) Sulla base di tale quadro normativo e giurisprudenziale, può ritenersi che la domanda formulata dalla parte attrice sia fondata e debba essere accolta.

Dalle risultanze processuali emerge che l'sms proveniente da PosteInfo, contenente una richiesta di dati del seguente contenuto "*Sicurezza Web, il sistema ha sospeso la sua utenza per mancato aggiornamento psd2- acceda ora per attivarlo*", cui seguiva un link per accedere al sistema e procedere all'aggiornamento, ricevuto in data 26-2-2021 dalla Bongrazio sulla propria utenza cellulare, appariva provenire da Poste Italiane e addirittura dallo stesso numero (+39.371.1000111) dal quale la aveva ricevuto pochi giorni prima, e precisamente in data 23-1-2021, i due precedenti sms, allorquando aveva – unitamente al cassiere delle Poste Italiane – svolto un'operazione all'interno dell'Ufficio Postale di Penne, circostanza questa non contestata e risultante sia dallo screenshot prodotto da parte attrice (all. 1 fascicolo parte attrice), che evidenzia come il messaggio del 23-1-2021 inviato in precedenza da Poste Info fosse identico nei caratteri e nella presentazione, potendo dunque quello del 26-2-2021 essere ritenuto pienamente attendibile, sia dalla Consulenza Tecnica di Parte (all. 14), prodotta dagli attori e pure non contestata.

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b0305515efa623b37c

In detta relazione peritale, nonché nella deposizione testimoniale resa in giudizio, il prof. Antonio Cilli, esperto consulente informatico del Tribunale, riferiva come, a seguito della verifica tecnica dell'apparato mobile in uso alla e dall'estrapolazione dei contenuti, riportati anche in perizia, aveva accertato che gli sms ricevuti dall'attrice provenissero da PosteInfo. Egli precisava altresì che "PosteInfo (mittente ufficiale degli sms inviati da Poste italiane) non ha un identificativo numerico riconducibile a una numerazione telefonica e pertanto l'utente non ha la possibilità di verificare il vero mittente del messaggio", potendo invece "confidare" nell'attendibile provenienza di esso sulla base della denominazione PosteInfo e dei precedenti messaggi ricevuti dallo stesso numero.

E' emerso poi che, nello svolgimento della procedura richiesta con l'sms di cui sopra, la veniva prontamente contattata da un operatore telefonico delle Poste Italiane che le forniva istruzioni su come comunicare i dati necessari all'aggiornamento richiesto. Successivamente, venivano effettuati movimenti on line che avevano provocato lo svuotamento del conto corrente degli attori, come appreso dal marito della , la sera del 26-2-2021, dopo esseri recato presso uno sportello Postamat per prelevare denaro contante (v. deposizione teste e).

Orbene, il fatto che la fosse stata contattata appena dopo aver ricevuto gli sms di cui agli screenshot prodotti in atti, e i cui contenuti sono riportati nella perizia del ha evidentemente indotto la stessa a ritenere che vi fosse in atto un effettivo controllo da parte delle Poste.

Nonostante la convenuta Poste Italiane abbia dichiarato di aver adottato tutte le misure di sicurezza e precauzionali, conformi allo stato più avanzato della tecnologia, appare evidente che l'anomalia delle operazioni concluse in un solo giorno e che hanno portato allo svuotamento del conto corrente non sia stata assolutamente rilevata dai sistemi informatici della Banca.

6) Deve dunque ritenersi che, nel caso di specie, la Poste Italiane non abbiano dimostrato l'adozione di tutte le più avanzate misure di sicurezza idonee a garantire il cliente, essendo anzi terzi riusciti a inviare sulla utenza cellulare di un cliente messaggi apparentemente riconducibili alla convenuta e telefonate apparentemente provenienti dalla stessa convenuta, né abbiano provato la riconducibilità delle operazioni effettuate alla volontà dell'utente o, comunque, a suo dolo o colpa grave.

Gli attori non possono essere ritenuti certamente esperti di questioni attinenti ai sistemi informatici di sicurezza; inoltre, gli sms inviati all'attrice non risultano essere scritti in italiano maccheronico o sgrammaticato.

Peraltro, non vi è prova della campagna informativa che la Poste Italiane S.p.A. avrebbe intrapreso per contrastare fenomeni di fishing, avendo la convenuta prodotto una risalente mail del 2005 contenente un avviso antiphishing ma senza prova alcuna della eventuale ricezione da parte degli attori, e due articoli di quotidiani, uno locale ("Il Centro") e l'altro dei Castelli Romani, risalenti al 2018 e che ben potrebbero non essere stati letti dagli attori stessi.

7) Deve essere dunque ritenuta la responsabilità contrattuale della società convenuta per le operazioni eseguite in assenza di autorizzazione da parte degli attori, pari a complessivi € 5.151,00 (cinquemilacentocinquantuno/00) e, per l'effetto, la stessa deve essere condannata alla corresponsione, nei confronti degli attori, di detta somma, oltre agli interessi legali dalla data della messa in mora (missiva del 5-3-2021 sub all. 10 fascicolo attori) fino al soddisfo.

Le spese di lite seguono la soccombenza della convenuta e vengono liquidate come in dispositivo.

P.Q.M.

Definitivamente pronunciando nel giudizio iscritto al R.G. n. 667/2022, per le causali di cui in motivazione così provvede:

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b03505515efa623b37c

accerta e dichiara la responsabilità della convenuta in ordine alle operazioni non autorizzate di cui in motivazione e, per l'effetto, la condanna alla corresponsione, nei confronti di e I della somma di € 5.151,00, oltre interessi legali dalla data della messa in mora fino al soddisfo;

condanna Poste Italiane S.p.A., in persona del legale rappresentante pro tempore, alla rifusione, in favore degli attori, delle spese del presente giudizio, che si liquidano in complessivi € 2.650,00, di cui € 98,00 per spese ed € 2.552,00 per compensi, oltre rimborso forfettario 15% (art.3/2 D.M. 10-3-2014 n. 55), IVA e CPA come per legge.

Pescara, 5 febbraio 2024

Il Giudice
dott. Patrizia Franceschelli

Firmato Da: FRANCESCHELLI PATRIZIA Emesso Da: ARUBAPEC S.P.A. NG CA 3 Serial#: 2cb3e87c97863b03505515efa623b37c