N. R.G. 17520/2015

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

TRIBUNALE DI CATANIA

QUARTA SEZIONE CIVILE

Il Tribunale, nella persona del Giudice dott. Mariano Sciacca
ha pronunciato la seguente

SENTENZA

nella causa civile iscritta al n. r.g. **17520/2015** promossa da:

BANCO (P.I. , con il patrocinio dell'Avv. MONTEROSSO TITO, ivi elettivamente domiciliato VIA VITTORIO EMANUELE ORLANDO n. 56, CATANIA presso il difensore avv. MONTEROSSO TITO, giusta procura in atti;

APPELLANTE/I

contro

(C.F.), con il patrocinio dell'Avv. elettivamente domiciliato in VIA presso il difensore avv. giusta procura in atti;

(C.F.), con il patrocinio dell'Avv. elettivamente domiciliato in VIA presso il difensore avv. , giusta procura in atti;

RESISTENTE/I

CONCLUSIONI

All'udienza del 31.01.2017 veniva posta in decisione sulle precisate conclusioni.

MOTIVI DELLA DECISIONE IN FATTO ED IN DIRITTO

Con atto di citazione in appello notificato in data 4.11.2015 il Banco Popolare Società Cooperativa impugnava la sentenza n. 72/2015 emessa dal Giudice di Pace di Biancavilla nel giudizio rubricato al R.G. n. 262/c/14 depositata in data 16.04.2015.

L'appellante lamentava l'erroneità della sentenza del Giudice di prime cure relativamente: alla parte in cui ha riconosciuto parziale responsabilità della Banca per non aver adottato tutte le misure idonee ad evitare frodi informatiche; alla parte in cui ha condannato la banca al risarcimento del danno in via equitativa; alla parte in cui ha disposto la condanna alle spese a carico della banca ritenendola prevalentemente soccombente.

Con comparsa di risposta ed appello incidentale, del 26.01.2016, si costituivano in giudizio e i quali assumevano la correttezza della sentenza appellata nella parte in cui aveva riconosciuto la responsabilità della Banca e chiedevano, in via incidentale, oltre che il rigetto

dell'avverso gravame, la riforma della sentenza nella parte in cui aveva riconosciuto ad essa una percentuale di responsabilità pari al 50 % per il subito ammanco di denaro, chiedendo quindi di accertare e dichiarare l'esclusiva responsabilità del Banco , sì da condannarlo al pagamento dell'intero importo.

All'udienza del 31.01.2017 le parti precisavano le conclusioni ed il Giudice introitava la causa a sentenza con i termini di legge.

****

CONCISA ESPOSIZIONE DELLE RAGIONI DI FATTO E DI DIRITTO DELLA DECISIONE

In data 25.03.2014 l'appellata riceveva un'e-mail nella propria casella di posta elettronica con mittente "Banco ", avente come oggetto "*comunicazioni della Banco del 25 Marzo*" con la quale veniva invitata, per ragioni di sicurezza e protezione del proprio conto corrente, a scaricare e compilare un modulo allegato.

La stessa appellata, compilato il modulo e non riuscendo ad inoltrarlo, contattava il numero verde della banca e riceveva come risposta dall'operatore l'esortazione a cestinare l'e-mail e la rassicurazione che egli avrebbe immediatamente provveduto a modificare i codici di sicurezza.

Ciononostante la quella stessa sera, riusciva ad accedere al conto on-line utilizzando i precedenti codici di accesso e, quindi, si accorgeva di un ammanco di € 4.980,00, derivante da bonifico da ella non disposto né autorizzato, in favore di un certo

L'appellata, all'indomani, si recava presso la sede del Banco ove le si dava conferma dell'ammanco con invito a sporgere denuncia penale e la stessa, così, in data 26.03.2014, si recava presso la Polizia di Stato, compartimento Polizia Postale, per proporre denuncia-querela.

Il 30.04.2014, però, l'appellata riceveva dall'ufficio reclami del Banco il rigetto della richiesta di rimborso avanzata, che veniva giustificato col ravvisarsi nel comportamento dell'istante una colpa grave per via della quale il rimborso non le sarebbe spettato.

L'odierna appellata, a tal punto, agiva in giudizio innanzi al Giudice di Pace di Biancavilla al fine di conseguire il riconoscimento dei propri legittimi diritti.

Con la sentenza n. 72/15, resa dal Giudice di Pace di Biancavilla, del 16.04.2015, pubblicata il giorno 16.04.2015, il predetto Giudice accoglieva solo nella misura del 50% la domanda di rimborso proposta dall'odierna parte appellata ritenendo ascrivibile alla stessa una percentuale di responsabilità per l'ammanco di denaro, e, per l'effetto, condannava il BANCO a versare la somma di € 2.490,00 (pari alla metà della somma illecitamente sottratta di Euro 4.980,00), nonché l'importo di € 110,00 liquidato in via equitativa a titolo di risarcimento danni non patrimoniali, oltre interessi legali al soddisfo, spese processuali e spese generali, CPA ed IVA.

****

1. Censura parte appellante la parte della sentenza in cui il Giudice di Pace di Biancavilla ha ritenuto responsabile la Banca per non aver provveduto al blocco dell'operazione, così sostenendo: "*Banco Popolare ha sostenuto di adottare un sistema ampiamente tutelato e protetto, utilizzando il protocollo TCP-IP che consente 'una comunicazione sicura dalla sorgente al destinatario..., fornendo autenticazione, integrità e cifratura dei dati', ciò rappresenterebbe (stando a quanto sostiene la stessa convenuta) il massimo per la sicurezza e per la salvaguardia delle informazioni trasmesse via internet. Tuttavia, occorre chiedersi come mai Banco – che utilizza i protocolli di massima sicurezza, come dallo stesso sostenuto – non abbia rilevato l'anomalia del codice OTP token inserito per ben tre volte (alle ore 17.35.33 il frodatore ha inserito tale codice 'corretto ma fuori finestra di accettazione', idem alle ore 17.42.15, infine con operazione riuscita alle ore 17.42.23), come si legge nella stampa informatica prodotta dalla stessa convenuta*". Assume, infatti, che detta motivazione sia errata, stante l'adeguatezza dei sistemi adottati, ovvero il protocollo TCP/IP ed il protocollo SSL o "Secure Sockets Layer".

Il TPC/IP - Transfer Control Protocol \ Internet Protocol - rappresenta, sostanzialmente, l'insieme delle regole di comunicazione su Internet basandosi sulla nozione d'indirizzamento IP, ossia sul fornire un indirizzo IP ad ogni terminale di rete per poter inviare dei pacchetti di dati. L'SSL è un protocollo progettato per consentire alle applicazioni di trasmettere informazioni in modo sicuro e protetto. Le applicazioni che utilizzano i certificati SSL sono in grado di gestire l'invio e la ricezione di chiavi di protezione e di criptare/decriptare le informazioni trasmesse utilizzando le stesse chiavi. La certificazione SSL (Secure Sockets Layer) che abbia un sito internet è poi una certificazione ulteriore e differente rispetto al protocollo TCP/IP utilizzato dalla rete Internet che viene rilasciata quando vengono eseguiti dei protocolli crittografici che permettono una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti TCP/IP (ad esempio Internet), fornendo autenticazione, integrità e cifratura dei dati.

Ritiene l'appellante che il Giudice di prime cure, nell'affermare che "*occorre chiedersi come mai Banco – che utilizza i protocolli di massima sicurezza come dallo stesso sostenuto – non abbia rilevato l'anomalia del codice OTP token...*" abbia erroneamente assimilato i superiori protocolli crittografici a quello differente individuato dall'acronimo OTP, ritenendo la responsabilità della banca per non avere questa provveduto a bloccare l'operazione nonostante l'erroneo, plurimo, inserimento dello stesso codice.

Precisa infatti l'appellante che il codice OTP Token (One-Time-Password) indica un sistema che crea parole chiave usa e getta della durata di pochi secondi e che nel caso *de quo* l'operazione non poteva essere bloccata laddove il frodatore non inseriva un codice errato ma, piuttosto, inseriva il giusto codice fuori dal tempo massimo consentito, circostanza che (così come provata dal Banco tramite la produzione della stampa informatica riportante la cronologia degli accessi al servizio by web da parte del frodatore) non producendo alcuna anomalia, esulava la banca da qualsivoglia attività di controllo o addirittura di intervento. Ritiene, infatti, l'appellante che l'esito positivo della frode sia imputabile esclusivamente alla correntista la quale, incautamente e ripetutamente (per ben tre volte consecutive e ravvicinate), ha fornito i propri codici di accesso a terzi rispondendo ad una e-mail inviata da un indirizzo fittizio, facilmente riscontrabile tramite semplice ricerca sul web (informa@ it), collegandosi al sito internet allegato e, così, mortificando di fatto ogni possibile sistema anti frode applicabile.

Controbatte parte appellata proponendo appello incidentale avverso la medesima sentenza del giudice di pace nella parte in cui riconosce la sua parziale responsabilità.

Assume parte appellata, appellante in via incidentale, che il Giudice di prime cure abbia errato nell'individuare la corretta disciplina applicabile al caso *de quo*, non tenendo in debita considerazione le norme di cui al decreto legislativo n. 196 del 2003, c.d. Codice in materia di protezione dei dati personali.

Ai sensi dell'art. 31 del decreto "*I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento in modo da ridurre al minimo mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentilo o non conforme alle finalità della raccolta*"; inoltre, ai sensi dell'art. 15 dello stesso decreto "*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*".

La norma di cui all'art. 2050 c.c., dal decreto richiamata, statuisce che "*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*".

In base alle norme suddette, a parere dell'appellata, dovrebbe la condotta del Banco integrerebbe un'ipotesi di responsabilità oggettiva ed extracontrattuale per non avere lo stesso, nell'esercizio di un'attività pericolosa, adottato ogni precauzione idonea ad evitare danni ai terzi.

Infatti, a dire dell'appellata, il Banco avrebbe dovuto custodire e controllare i dati personali della correntista che invece sono stati diffusi a causa dei non adeguati standard di sicurezza utilizzati dall'appellante che hanno consentito al frodatore di violare la Bank side del sito web della banca (server, applicazioni ecc. della Banca) ed accedere all'elenco dei nominativi dei clienti home banking del Banco ed agli indirizzi e-mail degli stessi, tra i quali quello dell'appellata correntista.

Tale circostanza darebbe adito all'applicazione delle norme dettate dagli artt. 31 e 15 del d.lgs. 196/2003 con la conseguenza che la Società convenuta sarebbe tenuta al risarcimento del danno ai sensi dell'art. 2050 c.c., costituendo la sua condotta un'inescusabile negligenza, dovuta alla mancata adozione di sistemi di sicurezza adeguati a contrastare le nuove tecniche di malware informatico.

L'applicabilità della disciplina di cui all'art. 2050 c.c. al trattamento ed alla diffusione dei dati personali troverebbe, secondo parte appellata, riscontro in numerose recenti pronunce giurisprudenziali per le quali "*In tema di trattamento e di diffusione dei dati personali, la valutazione del comportamento tenuto dal gestore di tali dati deve essere svolta alla stregua dei principi ricavabili dall'art. 2050 c.c., richiamato dall'art. 15 del Codice della privacy (D. Lgs. n. 196 del 2003)*" (Trib. Milano, Sez. I,26/09/2012), e "*Ai sensi dell'art. 18 della legge n. 675 del 1996, confluito nell'art. 15 del D.Lgs. n. 196 del 2003 chiunque cagioni un danno in virtù del trattamento di dati personali, in applicazione dell'art. 2050 c.c., ha l'onere di risarcirlo. La responsabilità configuratasi, relativa all'esercizio delle attività pericolose, è di natura oggettiva, extracontrattuale e trova la sua ratio nel valore commerciale dei dati, contenuti nelle apposite banche, a disposizione degli operatori professionali*" (Trib. Bari, Sez. II, 23/07/2010).

La questione discussa tra le parti, nel caso di specie, riguarda quindi l'applicabilità allo stesso della disciplina di cui all'art. 15 del D. Lgs. n. 196/2003 che, in virtù del richiamo all'art. 2050 c.c., prefigura a carico del gestore dei dati una responsabilità oggettiva, la quale ha per scopo "*l'affermazione di un favor per il danneggiato, escludendo che nel caso del trattamento di dati personali possa porsi un problema di sussistenza o meno della colpa e di un'eventuale graduazione della stessa, trattandosi di ipotesi di responsabilità oggettiva*" (Trib. Mantova, 05/08/2009).

La statuizione dell'art. 15 del c.d. Codice sulla privacy, nel prefigurare, quindi, un'ipotesi di responsabilità oggettiva a carico del soggetto gestore dei dati personali nell'intento di dare maggior tutela al trattamento di quelli, esonera il danneggiato dal dimostrare la colpa del gestore rimettendo a quest'ultimo l'onere di dimostrare di aver fatto quanto possibile per evitare il danno, predisponendo tecniche di sicurezza adeguate.

Tanto premesso, osserva il Giudicante che il preteso richiamo ad un caso di responsabilità oggettiva o aggravata, se ha come conseguenza quella di comportare un'inversione dell'onere probatorio con riferimento all'elemento soggettivo in quanto solleva il danneggiato dalla prova del dolo o della colpa del danneggiante, non comporta totale inapplicabilità delle regole ordinarie in tema di onere probatorio, per le quali "*Chi vuol far valere un diritto in giudizio deve provare i fatti che ne costituiscono il fondamento. (...)*" (art. 2697 c.c.).

Nel caso che ci occupa, l'appellata si è limitata ad allegare il fatto dell'ammanco di denaro dal suo conto corrente ricollegandolo, asseritamente, ad una presunta negligenza della banca i cui sistemi di tutela dei dati non riteneva adeguati, senza d'altro canto avere allegato e provato alcuna circostanza specifica e concreta attraverso la quale dare prova della detta inadeguatezza, non essendo sufficiente in tal senso l'avere ribadito in linea generale e astratta l'esistenza di sistemi più evoluti, quali ad esempio il "mobile TAN" ed il "Securcall" (sistemi questi sviluppati solo successivamente al tempo dell'avvenuta frode) o il servizio di "sms alert" che la banca già prevedeva, ma che non era stato attivato dai correntisti.

Manca in sostanza il nesso causale tra il fatto causativo del danno e la condotta della banca, dalla presenza del quale potrebbe scaturire una responsabilità di quest'ultima, come disposto dall'art. 15 d. lgs. n. 196/2003 (Codice della privacy) "*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*".

Anche le pronunce richiamate dall'appellata richiamano un analogo percorso motivazionale: posto infatti che queste fanno riferimento a casi in cui vi erano stati effettuati bonifici non autorizzati, va osservato che nel caso a mano i dati d'accesso sono stati forniti dalla stessa correntista.
È necessario ricordare che si è in presenza del cd. fenomeno del phishing (acronimo inglese che letteralmente tradotto significa "pesca di parola chiave") ossia quella forma di illecito che consiste nel carpire, con metodi illeciti, le credenziali (password) di accesso di un conto bancario (o postale) online per usarle, conseguentemente, al fine di far transitare fondi su altri rapporti e non quello di un attacco informatico ai server della Banca.
L'e-mail di phishing, nel caso *de quo*, è stata inviata casualmente alla cliente della Banca, ovvero, recte, non è stato provato che il phisher abbia carpito le informazioni-contatto relative alla cliente attraverso il sito o i database della banca stessa.
Non può quindi ravvisarsi alcuna responsabilità della Banca, mancando la prova della negligenza circa le modalità e tecniche utilizzate dalla stessa a tutela dei dati personali di cui è gestore, la quale responsabilità risulta anche esclusa espressamente dalle condizioni generali di contratto sottoscritte in data 4.01.2010, ove all'art.14, comma 2, si legge che: "*la Banca non sarà ritenuta responsabile per la perdita, diffusione od alterazione di informazioni trasmesse in utilizzo al Servizio ascrivibili ad eventi al di fuori del suo diretto controllo od anche verificatisi in occasione o dipendenza di interventi sulla rete telefonica o sulla rete internet*".

2. L'appellante in via incidentale ritiene, poi, errata la sentenza del Giudice di pace nella parte in cui imputa alla correntista una percentuale di responsabilità, nella misura del 50%, assumendo che anche a prescindere dalla normativa di cui al Codice della privacy (D. Lgs. n. 196 del 2003), può ravvisarsi una responsabilità di natura contrattuale in capo alla Banca alla luce delle norme codicistiche.
La responsabilità di Banco potrebbe trovare il proprio fondamento giuridico, a parere dell'appellata, nella norma di cui all'art. 1176 c.c. che così statuisce "*Nell'adempiere l'obbligazione il debitore deve usare la diligenza del buon padre di famiglia. Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata*".
Ritiene, infatti, l'appellata che la società, nell'adempimento delle proprie obbligazioni contrattuali, non ha utilizzato la diligenza adeguata alla natura dell'attività esercitata, in quanto ha consentito il trasferimento di denaro senza adottare quei sistemi di sicurezza ritenuti più evoluti contro le indebite intrusioni e senza precedentemente assicurarsi che alcuno intercettasse i dati personali della cliente.
A parere dell'appellata l'aver fornito una password ed un PIN d'accesso all'utente, nonché un'ulteriore chiave di sicurezza da inserire di volta in volta nei vari accessi web, non pare coincidere con il massimo delle misure di sicurezza adottabili, considerato che la natura dell'attività professionale svolta esige di scrupolosi accorgimenti volti a limitare al minimo possibile l'insorgere di qualsiasi rischio per i clienti.
Si osserva che, dovendosi ritenere, come sopra rilevato, che il Banco abbia approntato tutte le cautele possibili per proteggere i dati dei propri clienti, non incorre in alcuna responsabilità, essendo l'utilizzo abusivo dei dati della cliente dovuta ad una condotta colposa della stessa.
La condotta colposa e negligente dell'appellata risulta confermata dall'audizione del teste che ha ammesso che la riferì "*subito dopo aver tentato di inviare il modello scaricato senza ricevere esito positivo dell'invio si è preoccupata ed ha telefonato al numero verde della Banca esponendo i fatti*".
Su analoga fattispecie, con una recentissima pronuncia, si è già soffermato il Tribunale di Agrigento, il quale ha precisato che "*Dallo stralcio prodotto in atti delle condizioni contrattuali afferenti l'apertura in favore degli attori del conto corrente in argomento (...), risulta che la convenuta avesse previsto per l'accesso all'utilizzo del suindicato servizio un sistema di sicurezza caratterizzato da appositi strumenti di riconoscimento (codice identificativo utente e PIN) che il correntista avrebbe dovuto*

custodire con ogni cura. Pertanto così come pattuito il cliente doveva ritenersi responsabile della custodia e dell'utilizzo corretto dell'identificativo utente, della parola chiave, del codice dispositivo segreto e della cifra di controllo che costituiscono la chiave di accesso al servizio stesso e la mancanza di precauzioni da parte del titolare nel mantenere segreti tali codici avrebbe potuto determinare il rischio di accessi illeciti al servizio e di operazioni fraudolente sul conto da parte di terzi" (cfr. sentenza n.266/2014 emessa in data 17/02/2014 dal Giudice del Tribunale di Agrigento).

Per le ragioni sopra esposte, così come non è ravvisabile una responsabilità oggettiva *ex* art. 2050 c.c. della Banca, allo stesso modo non trova fondamento alcuno la richiesta di risarcimento del danno ai sensi dell'art. 1176 c.c.

Neanche può trovare fondamento l'eccezione fondata sulla difformità dell'indirizzo IP da cui era stata compiuta l'operazione.

L'indirizzo IP (Internet Protocol) è un codice numerico che permette d'identificare un computer connesso alla rete ed ogni computer connesso ad internet ha un proprio indirizzo tanto da risultare impossibile che due computer connessi ad Internet abbiano lo stesso IP.

Correttamente, secondo l'appellata, il Giudice di primo grado ha sostenuto che "*occorre chiedersi come mai Banco Popolare – che utilizza i protocolli di massima sicurezza, come dallo stesso sostenuto – non abbia rilevato che l'operazione veniva disposta da indirizzo IP difforme da quello utilizzato normalmente dalla cliente*" e che "*deve ritenersi che i sistemi anti-frode di Banco popolare avrebbero dovuto allarmare la transazione disposta da un cliente mediante un indirizzo IP difforme da quello abitualmente utilizzato per effettuare operazione on line*".

Controbatte l'appellante che la concezione classica di indirizzo IP, considerato come codice identificativo fisso ed univoco di una macchina interfacciata alla rete, è stata modificata grazie alle innovazioni tecnologiche che consentono, attualmente, l'utilizzato di indirizzi IP dinamici, per i quali alla macchina viene assegnato un nuovo e diverso indirizzo IP ad ogni connessione ad Internet anche per permettere l'accesso alla rete da apparecchi di telefonia mobile (smartphone/tablet) che sfruttano le reti 3G/4G.

Si osserva che dalle considerazioni che precedono risulta inadeguato considerare l'indirizzo IP come un dato immutabile ed in particolare rispetto al servizio by web, sottoscritto dai correntisti con l'Istituto di Credito, non avrebbe alcun senso vincolare lo stesso all'univocità della macchina da cui poter accedere, considerato che tale servizio nasce per fornire al correntista un accesso più rapido al proprio conto corrente, senza la necessità di recarsi in filiale per effettuare le proprie operazioni.

Gli accorgimenti posti in essere dal Banco (due password per l'accesso e, successivamente, una password variabile per gli atti dispositivi) risultano assolutamente strumenti adeguati alla tutela della riservatezza dei dati personali e sensibili dei clienti che aderiscono al conto by web, tenendo anche conto che gli stessi strumenti sono previsti dalle norme contrattuali che disciplinano il servizio stesso e che sono state sottoscritte dalla correntista.

Per tali ragioni, non può ritenersi fondata la pretesa dell'appellata per cui la Banca avrebbe dovuto sospendere l'operazione solo perché eseguita da un indirizzo IP differente, in quanto imporre la sospensione dell'operazione in casi del tipo di quello che ci occupa, non solo contrasterebbe con la natura stessa del servizio by web, ma sopratutto finirebbe per bloccare tutto il sistema delle operazioni telematiche, comportando ritardi e malfunzionamenti.

3. In via subordinata, l'appellante in via riconvenzionale chiede che la responsabilità di Banco venga accertata e dichiarata ai sensi dell'art. 12 del D. lgs. del 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno.

Afferma l'appellata che il Decreto introduce una ripartizione del rischio connesso all'utilizzo di qualsivoglia strumento elettronico di pagamento tale da far ricadere sull'intermediario il rischio stesso, a meno che non risulti provata una colpa grave dell'utilizzatore-cliente e chiede al Giudicante la

pronuncia, sulla base di tale disposizione, di una sentenza di condanna della Banca a versare la somma illecitamente sottratta pari ad Euro 4.980,00, oltre interessi e rivalutazione dal dovuto al soddisfo.
L'eccezione è destituita di ogni fondamento.
Osserva il Giudice che l'art. 12, comma 3, del citato decreto così recita: "*Salvo il caso in cui l'utilizzatore abbia agito con dolo o colpa grave ovvero non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento, prima della comunicazione eseguita ai sensi dell'articolo 7, comma 1, lettera b), l'utilizzatore medesimo può sopportare per un importo comunque non superiore complessivamente a 150 euro la perdita derivante dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto o smarrimento*". Expressis verbis la norma esonera da responsabilità l'utilizzatore lo strumento di pagamento "*Salvo il caso in cui l'utilizzatore non abbia adottato le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento*".
La dedotta violazione risulta insussistente alla luce di quanto già rilevato, dovendosi ascrivere ad esclusiva responsabilità dell'appellata, la quale ha fornito colposamente i dati d'accesso.

4. Deve conseguentemente ritenersi assorbito l'ulteriore motivo di appello relativo alla parte della sentenza in cui il Giudice di prime cure ha condannato la banca al risarcimento, in favore della correntista, di un danno non patrimoniale. Osserva il Giudicante che la questione risulta infatti assorbita, ritenendosi che nessuna responsabilità della Banca per i fatti allegati possa essere predicata, non ravvisandosi alcuna fatto illecito, produttivo del preteso danno patrimoniale.

Per gli esposti motivi va accolto l'appello proposto dal Banco avverso la sentenza n. 72/2015 del Giudice di Pace di Biancavilla e vanno quindi condannati e alla restituzione delle somme loro corrisposte in esecuzione della sentenza impugnata, pari ad € 2.627,03, oltre interessi dalla data del pagamento per sorte capitale ed alla rifusione delle spese liquidate dal Giudice, pari alla somma di € 1.344,54.
Le spese seguono la soccombenza con riferimento ad entrambi i gradi di giudizio.

P.Q.M.

il Tribunale di Catania, in persona del giudice unico, definitivamente pronunziando sulla causa iscritta al ruolo con il n. R.G. 17520/2015, così statuisce:

1) accoglie l'appello principale proposto e, in riforma della sentenza n. 72/2015 emessa dal Giudice di Pace di Biancavilla in data 16.04.2015, rigetta le domande proposte da e e conseguentemente li condanna alla restituzione delle somme già percepite pari ad € 2.627,03, oltre interessi di legge dalla data del pagamento al soddisfo ed alla rifusione delle spese liquidate e corrisposte, pari a € 1.344,54.
2) Rigetta ogni altra domanda;
3) Condanna e al pagamento delle spese di entrambi i giudizi in favore dell'appellante banca che si liquidano in complessivi euro 3200, 00 per compenso di avvocato, oltre spese generali, iva e cpa, come per legge.

Così deciso in Catania, 19/05/2017.

Il GIUDICE
dott. Mariano Sciacca