N. R.G. [redacted]

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

TRIBUNALE ORDINARIO di MILANO

SESTA CIVILE

Il Tribunale, nella persona del Giudice dott. Francesco Ferrari ha pronunciato la seguente

SENTENZA

nella causa civile di I Grado iscritta al n. r.g. [redacted] promossa da:

[redacted] (C.F. [redacted]), con il proc. dom. avv. [redacted] e l'avv [redacted]

parte attrice

contro

[redacted] (C.F. [redacted]), con il proc. dom. avv. [redacted]

parte convenuta

CONCLUSIONI

Per parte attrice:

In via principale:

accertata e dichiarare la responsabilità da inadempimento per violazione della diligenza professionale della [redacted] *– per le ragioni tutte di cui al presente atto, nei confronti del Sig.* [redacted] *per i danni patrimoniali subiti quale conseguenza immediata e diretta del suo inadempimento, condannare la* [redacted] *– al risarcimento dei danni sofferti dal Sig.* [redacted]*, quale conseguenza immediata e diretta del dedotto inadempimento, che si quantificano in complessivi euro 12.377,00 oltre interessi, oltre a quanto liquidato in ragione del profilo del danno non patrimoniale ex art. 2059 cod. civ. da quantificarsi in via equitativa per i motivi sopra esposti.*

In via subordinata:

condannare la convenuta al pagamento in favore del Sig. [redacted] *di quella diversa somma che il Tribunale adito dovesse ritenere comunque dovuta ed accertata a titolo di risarcimento del danno patrimoniale, se del caso anche a mezzo CTU contabile ovvero, in via di estremo subordine, in via equitativa, oltre a quanto liquidato in ragione del profilo del danno non patrimoniale ex art. 2059 cod. civ da quantificarsi in via equitativa per tutti i motivi sopra esposti.*

In via ulteriormente subordinata:

Nella remota, denegata e non creduta ipotesi in cui venga valutato dal Giudice adito un profilo di corresponsabilità, Voglia il Tribunale riconoscere una responsabilità se non esclusiva quanto meno prevalente in capo a [redacted]*, per tutti i motivi fin ora esposti.*

In via istruttoria:

Si insiste nuovamente per l'ammissione delle istanze istruttorie formulate ex art. 183, co. VI n. 2 c.p.c. non accolte, che ivi si ritrascrivono integralmente:

- ammettersi la prova per testi sui seguenti capitoli di prova, tutti preceduti dalla locuzione "vero che" ed espunti da qualsivoglia valutazione, se inibita:

1) Vero che, in data 28.07.2020, sin dalla prima mattinata a sera, Lei si trovava in compagnia del Sig. [redacted]

2) Vero che, sino alle ore 16:30 circa, il Sig. [redacted] *non riceveva alcuna chiamata telefonica da soggetti terzi?*

3) Vero che, in data 28.07.2020 alle ore 16:48, il Sig. [redacted] *riceveva una chiamata dal servizio clienti della* [redacted] *con cui l'Istituto bancario segnalava la conclusione di una serie operazioni sospette sul conto corrente di suo fratello, per un totale di euro 12.337,00?*

4) Vero che il Sig. [redacted] *veniva a conoscenza delle operazioni effettuate sul proprio conto corrente nel momento in cui ha ricevuto la chiamata di cui al precedente capitolo n. 2 di prova?*

5) Vero che, nel corso della chiamata di cui al capitolo n. 2, lei sentiva il Sig. [redacted] *riferire al proprio interlocutore che "disconosco le operazioni sul mio conto corrente" e "vi chiede il blocco immediato conto corrente"?*

6) Vero che, al termine della chiamata di cui al capitolo n. 2, il Sig. [redacted] *le rappresentava il contenuto della stessa e cosa era accaduto al proprio conto corrente?*

7) Vero che il Sig. [redacted] *sin dall'apertura del conto corrente avvenuta in data 19.12.2019, custodiva e controllava le proprie credenziali bancarie in modo che le stesse non fossero conoscibili a terzi?*

8) Vero che il Sig. [redacted]*, nella giornata del 28.07.2020, non effettuava alcuna operazione sul proprio conto corrente?*

9) Vero che il Sig. [redacted]*, di regola, utilizza la propria carta di credito per operazioni relative ai bisogni quotidiani (quali, a titolo esemplificativo, acquisti presso supermercati, farmacie, ristoranti, rifornimento di carburante) e relativamente ad importi di misura decisamente inferiore, inferiore normalmente ad euro 1.000,00, rispetto alle operazioni avvenute in data 28.07.2020, come anche da documento 12 allegato all'atto di citazione che le si rammostra?*

10) Vero che, all'epoca dei fatti oggetto di causa (i.e. luglio 2020), il [redacted] *possedeva, quale telefono cellulare, un iPhone X?*

11) Vero che il Sig. [redacted] *solo in via eccezionale effettuava bonifici a soggetti privati, utilizzando il servizio c.d. ordinario e quasi mai il servizio di bonifico istantaneo?*

12) Vero che le entrate del Sig. [redacted] *ammontano a circa euro 3.000,00/4.000,00 al mese, come risulta dagli estratti conto prodotti all'allegato n. 12 che si rammostrano?*

13) Vero che il Sig. [redacted] *aveva depositato tutti i suoi risparmi sul conto corrente aperto presso la* [redacted] *circostanza che gli garantiva una certa tranquillità economica?*

Si indica a testimonio: Sig. [redacted] *(C.F.* [redacted]*), nato a* [redacted] *– in data 27.05.1981, e ivi residente alla* [redacted]

- ordinare alla convenuta, ai sensi dell'art. 210 c.p.c., l'esibizione di tutti gli avvisi (c.d. alert), sottoforma di mail e/o messaggi, che sarebbero stati presuntivamente inviati (secondo controparte) al Sig. [redacted] *al verificarsi di tutte le operazioni oggetto di causa avvenute in data 28.07.2020, per come meglio dettagliate nell'atto di citazione, nonché della registrazione della telefonata effettuata dalla* [redacted] *al Sig.* [redacted] *in data 28.07.2020 alle ore 16:48.*

***Infine, ci si oppone all'ammissione delle istanze** istruttorie avversarie formulate nella memoria ex art. 183, co. VI n. 2 c.p.c., essendo le stesse inammissibili per come sostenuto nella memoria attorea ex art. 183, co. VI n. 3 c.p.c.*

In ogni caso:

condannare, infine, la convenuta alla refusione delle spese e competenze del presente giudizio, oltre accessori nella misura di legge da distrarsi in favore dei procuratori antistatari.

Per parte convenuta:

- respingere le domande dell'attore, anche eventualmente in applicazione dell'art. 1227, I e/o II comma, c.c..

Con vittoria di spese e onorari.

SVOLGIMENTO DEL PROCESSO

Con atto di citazione ritualmente notificato [redacted] conveniva in giudizio il [redacted] chiedendone la condanna alla ripetizione delle somme indebitamente prelevate e addebitate sul suo conto corrente acceso presso la filiale virtuale [redacted] dell'istituto di credito convenuto, pari ad euro

12.377,00, oltre al risarcimento dei danni.

L'attore in particolare esponeva:

- che il conto corrente da lui intrattenuto presso la banca convenuta veniva utilizzato esclusivamente per una movimentazione quotidiana mediante bancomat e sempre per importi contenuti, senza che mai fosse stato disposto alcun bonifico urgente *online*;
- che il 28.7.2020 l'attore veniva contattato dal servizio clienti della banca, il quale segnalava delle operazioni sospette effettuate sul suo conto corrente;
- che l'attore effettuava un controllo nel corso della stessa telefonata e riscontrava numerose operazioni da lui non autorizzate;
- che, in particolare, nell'arco di un'ora risultavano essere state compiute 8 operazioni, tra ricariche di carta prepagata allo stesso intestata e poi subito svuotata e bonifici istantanei;
- che la banca era responsabile della sottrazione del denaro patita dall'attore;
- che, infatti, la convenuta non si era dotata di misure idonee a evitare intromissioni non autorizzate da parte di estranei nel proprio sistema informatico, consentendo agli sconosciuti di appropriarsi dei codici segreti e dei dati sensibili dell'attore;
- che, in ogni caso, la banca non aveva vigilato correttamente a fronte di una operatività del tutto anomala rispetto al pregresso, consentendo l'esecuzione di operazioni anomale nella tempistica e, peraltro, dalla stessa banca riconosciute come sospette, tanto da contattare l'attore.

Si costituiva ritualmente in giudizio il [redacted]., chiedendo, in via principale, il rigetto della domanda attorea e, in via subordinata, di ridurre l'eventuale condanna in proporzione del concorso di colpa di parte attrice nella determinazione dell'evento o del danno, al netto della franchigia.

Deduceva, a tal fine:

- che la banca aveva adottato, per consentire ai clienti di operare a distanza, la *Strong Customer Authentication*, un sistema di autenticazione forte del cliente basato sull'uso di due o più elementi classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce, come una password o un PIN), del possesso (qualcosa che solo l'utente possiede, come uno *smartphone* o un dispositivo personale) ed, eventualmente, dell'inerenza (qualcosa che caratterizza l'utente, come l'impronta digitale o altri dati biometrici);
- che in particolare l'accesso al conto a distanza richiedeva, per coloro che avevano scaricato la *"SmartApp"*, come nel caso di specie, l'inserimento: a) delle credenziali personali (codice cliente e codice d'accesso, entrambi segreti e noti solo al cliente); b) di una specifica autorizzazione conferita, di volta in volta, proprio tramite l'*App* della Banca (installata sullo *smartphone* in uso esclusivo al cliente);
- che tutte le operazioni risultavano essere state regolarmente autorizzate mediante l'utilizzo dei codici personali e della password temporanea inviata dalla banca;
- che, pertanto, o le operazioni erano state disposte direttamente dall'attore o, più verosimilmente, questi aveva con negligenza inescusabile messo a disposizione di terzi truffatori tutte le credenziali necessarie per consentire loro di operare, dopo avere scaricato e installato l'*App* della banca sul proprio *smartphone*.

Espletata l'attività istruttoria secondo le istanze delle parti, nei limiti in cui erano ritenute ammissibili e rilevanti, il giudice rinviava all'udienza dell'1.12.2022 per la precisazione delle conclusioni; adempiuto a detto onere processuale, la causa era trattenuta in decisione, previo deposito di comparse

conclusionali e di memorie di replica ad opera delle parti.

MOTIVI DELLA DECISIONE

La domanda attorea è infondata e, pertanto, non può trovare accoglimento.

Sul quadro normativo relativo alle operazioni di pagamento non autorizzate

In materia di servizi di pagamento, il d.lgs. 27/01/2010, n. 11, in attuazione della direttiva 2007/64/CE, ha allocato, in ragione della capacità organizzativa e preventiva dei prestatori dei servizi di pagamento (di seguito, PSP), i rischi derivanti da attività fraudolente a danno degli utenti.

La direttiva citata, su cui sono intervenute diverse novelle, è stata successivamente abrogata dalla direttiva 2015/2366/UE, relativa ai servizi di pagamento nel mercato interno, la quale è stata attuata, nel nostro ordinamento, con d.lgs. 15/12/2017, n. 218, che ha apportato modifiche al d.lgs. 11/2010.

La direttiva è stata, infine, integrata a livello eurounitario con il regolamento delegato 2018/389/UE del 27 novembre 2017 della Commissione europea per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

La disciplina in materia di servizi di pagamento ruota intorno al consenso, preventivo, contestuale o successivo, del pagatore, ossia "*il soggetto titolare di un conto di pagamento a valere sul quale viene impartito un ordine di pagamento ovvero, in mancanza di un conto di pagamento, il soggetto che impartisce un ordine di pagamento*" (art. 1, d.lgs. 11/2010). L'art. 5, co. 1, d.lgs. 11/2010, stabilisce, infatti, che "*il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento. In assenza del consenso, un'operazione di pagamento non può considerarsi autorizzata*".

Il consenso del pagatore deve essere distinto dall'ordine di pagamento il quale, nella normalità dei casi, lo presuppone, costituendone la manifestazione procedimentalizzata e autenticata tramite le moderne procedure informatiche. L'ordine di pagamento è, infatti, l'istruzione formale data dall'utente al proprio PSP, con la quale viene chiesta l'esecuzione di un'operazione di pagamento.

Il consenso è il presupposto volitivo dell'ordine di pagamento, ossia la volontà del pagatore di dare avvio ad un'"*operazione di pagamento*" avvalendosi dei "*servizi di pagamento*" offerti da un "*prestatore di servizi di pagamento*". In sostanza, con un esempio che si addice al caso in esame, è la volontà del cliente di ordinare alla propria banca di disporre un bonifico bancario in favore di un beneficiario determinato.

L'art. 5, co. 2, d.lgs. 11/2010 recepisce la distinzione tra i due concetti, in armonia con l'evoluzione tecnologica delle infrastrutture tecniche di comunicazione e, in particolare, delle procedure di autenticazione che consentono ai clienti di identificarsi e di disporre, a distanza, gli ordini di pagamento alla propria banca. Istituisce, pertanto, una procedimentalizzazione della manifestazione del consenso del pagatore ("*il consenso ad eseguire un'operazione di pagamento o una serie di operazioni di pagamento è prestato nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento*") e, di questa caratteristica, ne tiene conto in sede di allocazione dei rischi derivanti, tra le altre cose, dalle condotte fraudolente dei terzi che simulano un consenso del pagatore, dando avvio ad un'operazione di pagamento non voluta.

Per comprendere la distribuzione degli obblighi di protezione e delle rispettive responsabilità, si deve tener presente che, alla luce del complessivo impianto normativo, nazionale ed eurounitario, i PSP sono considerati i soggetti più idonei ad investire risorse per prevenire i rischi connessi alla trasmissione del

consenso e, pertanto, nella loro sfera giuridica (nel c.d. rischio di impresa) sono posti sia l'obbligo di assicurare che le credenziali di autenticazione attribuite ai propri clienti "*non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento*" sia i "*rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate*" (artt. 8 e 11 d.lgs. 11/2010). In generale, come verrà di seguito chiarito, è quindi configurata una responsabilità aggravata del PSP nel caso abbia dato seguito ad un'operazione non autorizzata, proprio in virtù di questa sua maggiore capacità di elaborare meccanismi sicuri di gestione e trasmissione del consenso, nonché di tempestiva ed esatta esecuzione degli ordini di pagamento così ricevuti. In quest'ottica, la dir. 2366/2015/UE, prima, e il reg. del. 2018/389/UE della Commissione, poi, hanno imposto agli PSP, salvo alcune eccezioni, di predisporre meccanismi di autenticazione forte, per la trasmissione del consenso, basati su due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza, con la generazione di un codice di autenticazione.

Come contraltare di questa disciplina impositiva per gli PSP, sono stati introdotti degli obblighi di diligenza in capo agli utenti di tali servizi per quanto concerne la propria sfera di influenza. Costoro, infatti, ricevono e devono custodire le credenziali di sicurezza personalizzate per accedere ai propri conti di pagamento ed impartire quegli ordini di pagamento che sono la manifestazione procedimentalizzata al PSP della propria volontà di dare corso ad un'operazione di pagamento. In quest'ottica, l'art. 7, d.lgs. 11/2010, prescrive che "*1. L'utente abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso e che devono essere obiettivi, non discriminatori e proporzionati; b) comunicare senza indugio, secondo le modalità previste nel*

contratto quadro, al prestatore di servizi di pagamento o al soggetto da questo indicato lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza. 2. Ai fini di cui al comma 1, lettera a), l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate". Ciò è, infatti, necessario per una completa prevenzione dai rischi connessi a queste operazioni, senza estendere eccessivamente la responsabilità, e i correlativi obblighi, dei PSP, responsabilità che inevitabilmente comporterebbe un irrigidimento e un rallentamento del mercato, con danno per i consumatori stessi. Questa esigenza di fluidità e celerità dei pagamenti, garantita dalla procedimentalizzazione della manifestazione del consenso e dalla sua automatica processazione, è, invero, espressamente riconosciuta nella dir. 2366/2015/UE (si veda considerando 79 e 80) ed è un valore su cui gli utenti possono fare affidamento: "*Il funzionamento corretto ed efficiente del sistema di pagamento dipende dal fatto che l'utente possa fare affidamento sul fatto che il prestatore di servizi di pagamento esegua l'operazione di pagamento in modo corretto ed entro i tempi stabiliti*" (considerando 85; si veda inoltre il considerando 77). Essa è alla base di diversi istituti, tra cui l'irrevocabilità del consenso non appena ricevuto dai PSP, i ristretti termini per adempiere ad un ordine di pagamento e la responsabilità dei PSP in caso di ritardo. Risponde, pertanto, ad un interesse del mercato e, come riconosciuto dalla Corte di Giustizia, anche dei consumatori stessi: "*È nell'interesse, infatti, non soltanto del prestatore di servizi di pagamento, ma anche del suo cliente, disporre, purché quest'ultimo lo desideri e sia sufficientemente tutelato, di mezzi di pagamento innovativi, rapidi e di facile utilizzo*" (Corte giustizia Unione Europea, Sez. I, Sent., 11/11/2020, n. 287/19)

Il delicato bilanciamento delle responsabilità in capo ad ambo le parti risente, ciononostante, dello

spartiacque della comunicazione di cui all'art. 7, co. 1, lett. b), la quale mette il PSP nelle condizioni di comprendere, per tempo, la discrasia tra consenso e manifestazione procedimentalizzata dello stesso.

Ciò premesso, è opportuno circoscrivere l'analisi del riparto di responsabilità alle sole operazioni di pagamento non autorizzate eseguite dal PSP a seguito della corretta ricezione di un ordine di pagamento. Difatti, trattandosi di operazioni non autorizzate, ossia eseguite senza il consenso dell'utente, il decreto legislativo pone sul PSP (la banca) l'onere di "*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*" (art. 10 d.lgs. 11/2010). In difetto di tale prova, non vi sarebbe alcun dubbio sulla responsabilità del PSP, il quale non potrebbe altrimenti aver fatto affidamento su un apparente consenso dell'utente manifestato attraverso quella procedimentalizzazione e autenticazione a cui si ha accennato.

Al di fuori di tale ipotesi, e prima della comunicazione di cui all'art. 7, co. 1, lett. b), d.lgs. 11/2010, si possono verificare sostanzialmente tre situazioni: il PSP risponde, di regola, di tutte le operazioni di pagamento non autorizzate a cui ha dato corso, salvo fornisca la prova del caso fortuito o della forza maggiore (o nei casi l'evento dannoso si sia verificato a causa dell'adeguamento del PSP a "*vincoli derivanti da altri obblighi di legge*", art. 28, d.lgs. 11/2010); la responsabilità del PSP concorre a quella dell'utente nel caso di colpa lieve di quest'ultimo (si veda, a contrario, l'art. 12, co. 2-*ter*, d.lgs. 11/2010), il quale è così tenuto a sopportare le perdite nei limiti dell'importo di cui all'art. 12, co. 3 e 4, d.lgs. 11/2010; la responsabilità del PSP è, infine, esclusa nel caso in cui esso dimostri che il proprio utente pagatore abbia agito in modo fraudolento o non abbia adempiuto, con dolo o colpa grave, agli

obblighi di diligenza e di tempestiva comunicazione di cui all'art. 7 (art. 12, d.lgs. 11/2010).

Il regime di responsabilità del PSP si aggrava, infine, dopo la comunicazione di cui all'art. 7, co. 1, lett. b), d.lgs. 11/2010, oppure nel caso in cui non abbia predisposto degli strumenti adeguati a consentire al proprio cliente di inviare tale comunicazione tempestivamente o, infine, nelle ipotesi in cui il sistema di autenticazione con il PSP non esiga un'autenticazione forte del cliente nel trasmettere gli ordini di pagamento. In tutti questi casi, il PSP può liberarsi dalla propria responsabilità solo provando che il proprio cliente abbia agito in modo fraudolento.

Per completare il quadro, il riferimento ad *"altri inconvenienti"* contenuto nell'art. 10, co. 1, d.lgs. 11/2020 comporta un'estensione della responsabilità dei PSP per tutte le cause e fattori sconosciuti che hanno condotto all'esecuzione di operazioni di pagamento non autorizzate.

Sulla colpa grave dell'utente pagatore

Nel caso di specie, è pacifico, poiché allegato dalla convenuta e non specificamente contestato *ex* art. 115 c.p.c., che [redacted] avesse adottato un'autenticazione forte per le comunicazioni degli ordini di pagamento con il cliente.

È pacifico, poiché allegato dalla convenuta non specificamente contestato *ex* art. 115 c.p.c., che [redacted] abbia dato corso a degli ordini di pagamento correttamente autenticati, ancorché disposti contro la volontà consapevole dell'attore.

Per quanto concerne, invece, le modalità con cui terzi sconosciuti sono entrati illegalmente in possesso delle credenziali di autenticazione del [redacted] e hanno disposto. c ordini di pagamento a [redacted] presso cui era aperto il conto corrente intestato all'attore, quest'ultimo si è limitato a negare di avere mai comunicato le proprie credenziali riservate a terzi e che, quindi, le stesse fossero

state carpite attraverso una illecita violazione del sistema informatico della banca.

Da parte sua la convenuta ha prodotto l'estratto dei *log* relativi alle operazioni compiute, nonché agli avvisi a t *smartphone* abilitato, attestando in tal modo come il *device* originariamente abilitato dal [redacted] a operare attraverso l'*App* della banca fosse stato sostituito con uno *smartphone* differente, evidenziando come le parti nel contratto avessero pattuito come, in caso di contestazioni in ordine a operazioni, avrebbero fatto fede i *log* estratti dal server della banca.

La difesa attorea non ha contestato la provenienza q e t n a a es e dai *server* della banca è stata confermata testimonialmente dall'operatore che aveva curato detta operazione), ma, viceversa, li ha a sua volta invocati quale conferma, a suo dire, della responsabilità della convenuta, la quale non si sarebbe avveduta che le operazioni abusive compiute dai truffatori fossero state disposte utilizzando uno *smartphone* con sistema operativo Android, quando, invece, lo *smartphone* in uso all'attore e da questi abilitato operasse con sistema operativo Iphone.

Tale rilievo non può trovare condivisione, in quanto dalla stessa operatività documentata attraverso i *log* e i tabulati degli *alert* emerge inequivocabilmente come la sostituzione dello *smartphone* abilitato sia avvenuta in seguito all'attuazione da parte dell'attore o, quanto meno, sfruttando l'ingenua cooperazione di quest'ultimo, dell'apposita procedura di sostituzione del *device* abilitato.

In particolare emerge come, una volta avviata la procedura, la banca abbia inviato in due differenti occasioni *password* temporanee (il cui inserimento era indispensabile per procedere) sulla vecchia utenza telefonica, ossia quella del [redacted] e sull'indirizzo mail dell'attore e che tali *password* sono state effettivamente utilizzate per portare a termine l'operazione di sostituzione dello *smartphone*.

Le cautele utilizzate per effettuare tale sostituzione, ossia l'invio di due *password* temporanee al

cliente, consente di non ritenere sospetta l'operazione in quanto tale, la quale di norma viene effettuata da tutti i clienti, nel momento in cui cambiano il telefono cellulare o una utenza; se, infatti, per poter procedere è necessario utilizzare codici temporanei inviati sull'utenza del cliente, è chiaro che solo quest'ultimo ne possa disporre e, quindi, possa essere abilitato a dare corso alla sostituzione dello *smartphone*.

Il semplice cambio di *device*, pertanto, non può essere considerato motivo di allarme o di sospetto, come vorrebbe sostenere la difesa attorea.

Al contrario, l'utilizzo delle password temporanee costituisce un indice inequivoco che porta a presumere come la sostituzione dello *smartphone* abilitato sia avvenuta con la negligente cooperazione dell'attore, il quale deve avere messo a disposizione i codici di volta in volta solo a lui inviati, al fine di consentire il completamento della procedura.

Una volta completata la sostituzione dello *smartphone* abilitato, i truffatori, in possesso dell'*id* e del *pin* dell'attore (in quanto deve presumersi da questi comunicati in occasione della operazione di cui sopra), hanno potuto utilizzare il *token* installato sul loro *smartphone* per poter liberamente operare sul conto corrente de[redacted].

Le circostanze di fatto in cui si è svolta la vicenda, così come sopra ricostruita, conducono, quindi, a ritenere provata l'esclusiva responsabilità, per colpa grave, dell'attore.

Come chiarito nel considerando 72 della direttiva, che deve essere assunto quale criterio interpretativo della normativa nazionale di attuazione, "*per valutare l'eventuale negligenza o grave negligenza da parte dell'utente di servizi di pagamento, dovrebbero essere prese in considerazione tutte le circostanze. È opportuno che di norma le prove e il grado della presunta negligenza siano valutati*

sulla base del diritto nazionale. Non di meno, il concetto di negligenza implica la violazione del dovere di diligenza, mentre per negligenza grave si dovrebbe intendere un comportamento che si spinge oltre la semplice negligenza e implica un grado significativo di mancanza di diligenza; ad esempio, lasciare le credenziali usate per autorizzare un'operazione di pagamento vicino allo strumento di pagamento, in un formato aperto e facilmente individuabile da terzi". **In sintesi, possono costituire colpa grave solo le condotte negligenti dell'utente pagatore che afferiscono alla propria sfera di influenza, condotte che, in particolare, comportano una grave violazione degli obblighi di cui di cui all'art. 7, tra cui il dovere di** custodia e sicurezza delle credenziali personalizzate di autenticazione.

L'attore ha divulgato le proprie credenziali necessarie per attivare la Smart *App* sul dispositivo dei **truffatori, nonostante gli avvisi ricevuti in ordine all'operazione in corso, dimostrando per ciò stesso l'inescusabile ne**gligenza con cui ha gestito le proprie credenziali e in tal modo ha vanificato le misure di sicurezza predisposte proprio al fine di evitare raggiri come quello oggetto di causa.

Questi elementi dimostrano la violazione, per colpa grave, dell'obbligo di cui all'art. 7, co. 2, d.lgs. 11/2010, nella parte in cui prescrive all'utente di adottare "*tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate*".

Sul dovere di monitoraggio e di intervento preventivo

L'attore ha insistito sulla responsabilità dell'istituto bancario invocando un suo dovere di monitorare gli schemi comportamentali del cliente e di avvertire o, addirittura, sospendere le operazioni di **pagamento anomale, prima di darne esecuzione. L'anomalia, nel caso di spe**cie, si evincerebbe dalla frequenza dei pagamenti disposti in un breve lasso di tempo e dalla tipologia di operazioni, ossia bonifici istantanei, in precedenza mai disposti.

Sul punto, è bene premettere quanto segue: l'obbligo di monitoraggio e di sospensione dei pagamenti (o di qualche altra forma di intervento), in caso di *"anomalia"* degli stessi, non è sancito esplicitamente né all'art. 8 d.lgs. 11/2010, né all'art. 70 dir. 2366/2015/UE di cui ne costituisce attuazione. Ciononostante, secondo alcuni autori, tali obblighi, con le relative responsabilità, si desumerebbero, a livello interpretativo, dal generale obbligo dei PSP di garantire la sicurezza delle credenziali di autenticazione personalizzate (art. 8, co. 2, d.lgs. 11/2010; art. 70, co. 2, Dir. 2366/2015/UE). Il monitoraggio sarebbe consentito, in termini di trattamento dei dati, ai sensi dell'art. 29, d.lgs. 11/2010: *"1. I prestatori di servizi di pagamento e i gestori di sistemi di pagamento possono trattare dati personali ove ciò sia necessario a prevenire, individuare e indagare casi di frode nei pagamenti"*. Il potere unilaterale di sospensione sarebbe, inoltre, attribuito dall'art. dall'art. 6, d.lgs. 11/2010, che recepisce l'art. 68, par. 2, della Direttiva (UE) 2015/2366: "*Se concordato nel contratto quadro, il prestatore di servizi di pagamento può riservarsi il diritto di bloccare lo strumento di pagamento per motivi obiettivamente giustificati legati alla sicurezza dello strumento di pagamento, al sospetto di un utilizzo non autorizzato o fraudolento dello strumento di pagamento oppure, nel caso di uno strumento di pagamento dotato di una linea di credito, al significativo aumento del rischio che il pagatore non sia in grado di adempiere ai propri obblighi di pagamento*" (art. 68, par. 2, dir. cit.). Nel caso di specie, peraltro, non è stata provata e, per la verità, non è stato neppure allegata alcuna specifica pattuizione intercorsa fra le parti in proposito.

L'obbligo di monitoraggio e di intervento, per prevenire operazioni anomale, discenderebbe, infine, dall'obbligo di buona fede nell'esecuzione del contratto.

Queste considerazioni, in quanto volte ad imporre al PSP di intervenire ogniqualvolta il proprio utente

pagatore disponga uno o più bonifici di importo anomalo, non sono supportate da adeguata base giuridica e, a normativa vigente, confliggono con l'obiettivo di garantire certezza e celerità dei pagamenti, anche nell'interesse dei consumatori stessi, e con il delicato bilanciamento normativo di riparto delle reciproche responsabilità, secondo le rispettive sfere di influenza.

Come anticipato, un obbligo di monitoraggio, preordinato a prevenire operazioni anomale per il loro ammontare o frequenza, non è contemplato né all'art. 8 d.lgs. 11/2010, né all'art. 70 dir. 2366/2015/UE. Ai PSP, già onerati da una responsabilità aggravata, anche per fattori sconosciuti, è consentito di fornire la prova liberatoria della colpa grave dei propri utenti pagatori, per le condotte gravemente negligenti inerenti alla relativa sfera di influenza con violazione di obblighi di custodia espressamente incombenti sui medesimi ai sensi degli artt. 7 D.lgs. 11/2010 e 69 Dir. 2366/2015/UE.

Se il legislatore europeo avesse voluto introdurre un obbligo di monitoraggio preordinato ad un obbligo di sospensione dell'esecuzione del contratto (o di qualche altra forma di intervento) lo avrebbe inevitabilmente sancito, avendo predisposto una dettagliata disciplina di riparto di responsabilità ed obblighi. E invece, laddove ha previsto un obbligo di monitoraggio, non l'ha mai correlato a un dovere di intervento preventivo, evidentemente per evitare prevedibili, frequenti e potenzialmente pregiudizievoli intoppi del mercato dei servizi di pagamento. In particolare, un obbligo di monitoraggio è stato introdotto nel Reg. Del. 2018/389/UE, art. 2, al solo di fine di chiarire in quali ipotesi sia consentito alle parti di omettere il meccanismo dell'autenticazione forte, senza per ciò solo comportare quell'aggravamento della responsabilità di cui all'art. 12, co. 2-*bis*, D.lgs. 11/2010 (art. 74, par. 2, Dir. 2366/2015/UE). Infatti, l'art. 2, par. 1, finalizza esplicitamente i meccanismi di monitoraggio all'attuazione delle *"misure di sicurezza di cui all'articolo 1, lettera a) e b)"*, ossia ai soli fini della

scelta tra "*applicare la procedura dell'autenticazione forte del cliente conformemente all'articolo 97 della direttiva (UE) 2015/2366*" ed "*esonerare dall'applicazione dei requisiti di sicurezza dell'autenticazione forte del cliente, a condizioni specifiche e limitate, sulla base del livello di rischio, dell'importo e della frequenza dell'operazione di pagamento e del canale di pagamento utilizzato per l'esecuzione dell'operazione*". Un'altra previsione di monitoraggio è contemplata all'art. 8, D.M. 30.04.2007, n. 112, Ministero dell'Economia e delle Finanze, che chiarisce, ai soli fini di una comunicazione a posteriori all'archivio informatizzato di cui agli artt. 2 e 3 l. 166/2005, cosa si intende per "*rischio di frode*" nei pagamenti con carte di pagamento. Anche in questo caso, è introdotto un obbligo di monitoraggio a fini diversi da quelli di esecuzione del contratto e non è previsto alcun obbligo di intervento, ma solo la collaborazione ad un'attività amministrativa a posteriori, circoscritta peraltro alle sole carte di pagamento.

La tesi che riconduce l'obbligo di sospensione del pagamento all'interno del più generale obbligo di garantire la sicurezza delle credenziali è, peraltro, smentita dal dato normativo: gli art. 6, d.lgs. 11/2010 e 68, par. 2, della Dir. 2366/2015/UE rimettono questo potere all'autonomia delle parti, sicché è un'opzione meramente eventuale, diversamente dall'obbligo di protezione menzionato. Ciò illumina la *mens legis* della disciplina europea, che non si è (sinora) spinta fino a prevedere un obbligo di monitoraggio preordinato al blocco dello strumento di pagamento, consapevole dell'impatto che questo potrebbe avere sulla fluidità del sistema dei pagamenti.

Inoltre, l'eventualità che il PSP si sia riservato in concreto (art. 68, par. 2, Dir. 2366/2015/UE "*può riservarsi*") il potere di sospendere (o bloccare) lo strumento di pagamento non comporta l'insorgenza di un obbligo in proposito. In termini di dogmatica generale e di interpretazione sistematica del quadro

normativo, una cosa è la posizione giuridica di potere, esercitabile secondo il prudente apprezzamento del suo titolare, un'altra è la posizione giuridica dell'obbligo, a cui corrisponde un diritto dell'interessato, la quale comporta inevitabilmente un'equazione tra anormalità del pagamento e necessità di intervento.

In difetto di parametri di riferimento, non può nemmeno invocarsi il principio di buona fede integrativa. I PSP gestiscono cospicui traffici di pagamento, non governabili senza software automatici che eseguano gli ordini di pagamento correttamente autenticati. Imporre ai medesimi di intervenire ogni qualvolta un'operazione superi, per importo o frequenza, uno schema di comportamento storico, comporterebbe un discrezionalità difficilmente compatibile con la *ratio* del sistema normativo: infatti, in difetto di parametri di riferimento, i PSP dovrebbero autonomamente scegliere la lunghezza del periodo di osservazione su cui costruire lo schema normale di azione del proprio utente pagatore, stabilire dopo quale soglia intervenire, come intervenire (con ulteriore SMS o con sospensione), dopo quanti pagamenti anomali, con possibile nocumento della fiducia dei consumatori sulla fluidità, efficacia e celerità del sistema. Ciò comporterebbe incertezza e gravi disagi ai consumatori stessi, con possibili profili di responsabilità dei PSP, sia in caso di (erroneo) intervento sia in caso di inerzia (all'origine ritenuta giustificata). Come anticipato, a questo fine non potrebbe soccorrere il parametro di cui all'art. l'art. 8, D.M. 30.04.2007, n. 112, Ministero dell'Economia e delle Finanze, sia perché previsto per finalità differenti, sia perché circoscritto alle sole carte di pagamento.

Che il sistema dei servizi di pagamento sia improntato sulle rispettive sfere di influenza, con il limite di sicuri meccanismi di autenticazione e della colpa grave dell'utente, si evince indirettamente anche dall'art. 24 D.lgs. 11/2010 (cfr. art. 88, 2366/2015/UE), che disciplina il caso di divergenza tra il

consenso dell'utente pagatore e l'identificativo univoco dallo stesso fornito con l'ordine di pagamento, per quanto riguarda l'identità del destinatario. Questa norma tutela, infatti, l'affidamento del PSP su **quanto indicato nell'ordine di pagamento; non contempla alcuno spazio per l'eventualità che il terzo** avente causa sia un beneficiario atipico (o anomalo) o abbia un conto di riferimento presso un Paese terzo, non affidabile. Ciò su cui il PSP può fare affidamento, in tal caso, è la corretta autenticazione e la **corrispondenza tra il conto del beneficiario e l'identificativo univoco indicato dal proprio utente pagatore: "***1. Se un ordine di pagamento è eseguito conformemente all'identificativo unico, esso si ritiene eseguito correttamente per quanto concerne il beneficiario e/o il conto indicato dall'identificativo unico. 2. Se l'identificativo unico fornito dall'utente è inesatto, il prestatore di servizi di pagamento non è responsabile, ai sensi dell'articolo 25, della mancata o inesatta esecuzione dell'operazione di pagamento. Il prestatore di servizi di pagamento del pagatore compie tuttavia sforzi ragionevoli per recuperare i fondi oggetto dell'operazione di pagamento. Il prestatore di servizi di pagamento del beneficiario è tenuto a collaborare, anche comunicando al prestatore di servizi di pagamento del pagatore ogni informazione utile. Se non è possibile il recupero dei fondi, il prestatore di servizi di pagamento del pagatore, su richiesta scritta del pagatore, è tenuto a fornirgli ogni informazione disponibile che sia utile ai fini di un'azione di tutela. Ove previsto nel contratto quadro, il prestatore di servizi di pagamento addebita all'utente le spese sostenute per il recupero dei fondi. 3. Il prestatore di servizi di pagamento è responsabile solo dell'esecuzione dell'operazione di pagamento in conformità con l'identificativo unico fornito dall'utente anche qualora quest'ultimo abbia fornito al suo prestatore di servizi di pagamento informazioni ulteriori rispetto all'identificativo unico***".**

Né, infine, è condivisibile la contestazione mossa dalla difesa attorea in ordine a una condotta

negligente della banca, la quale solo dopo le otto operazioni contestate aveva pensato di contattare l'attore sull'utenza telefonica originaria.

Sul punto, infatti, va rilevato come tutte le operazioni compiute dai truffatori sono state accompagnate da una mail di *alert*, senza che allo stesso fosse seguita una reazione da parte dell'attore; in difetto di previsioni contrattuali che imponessero e regolamentassero interventi telefonici, non pare possibile prospettare una responsabilità della banca per non avere contattato prima (quando? Dopo quante operazioni?) l'attore per una verifica di quanto già disposto.

Conclusioni.

La domanda attorea deve essere, conseguentemente, rigettata.

Le spese di lite seguono la soccombenza e si liquidano in complessivi euro 2.990,00, oltre i.v.a. e c.p.a., di cui euro 390,00 per spese generali.

P.Q.M.

Il Tribunale in composizione monocratica, definitivamente pronunciando nel contraddittorio delle parti, ogni diversa istanza disattesa:

- rigetta la domanda proposta da [redacted] nei confronti di [redacted].;
- condanna l'attore a a rifondere la convenuta delle spese di lite, liquidate in complessivi euro 2.990,00, oltre i.v.a. e c.p.a., di cui euro 390,00 per spese generali.

Così deciso in Milano il 28 febbraio 2023

Il giudice

Francesco Ferrari