Sentenza, Tribunale di Milano, Giudice Francesco Ferrari, n. 847, del 02/02/2023

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. xxxx/2022 promossa da:

D.G.A. (C.F. (...)) e F.D.I. (C.F. (...)), con il proc. dom. avv. omissis

parte attrice

contro

C. S.P.A. (C.F. (...)), con il proc. dom. avv. omissis

parte convenuta

SVOLGIMENTO DEL PROCESSO

Con atto di citazione ritualmente notificato D.G.A. e F.D.I., rispettivamente marito e moglie, convenivano in giudizio C. s.p.a., chiedendone la condanna alla ripetizione, in loro favore, della somma indebitamente prelevata e addebitata sul loro conto corrente cointestato acceso presso l'istituto di credito convenuto, pari ad Euro 46.500,00, oltre al risarcimento dei danni.

Gli attori in particolare esponevano:
- che il conto corrente da loro intrattenuto presso la banca convenuta veniva utilizzato esclusivamente per l'accredito dello stipendio e della pensione, nonché per una movimentazione quotidiana mediante bancomat e sempre per importi contenuti, senza che mai fosse stato disposto alcun bonifico online;

- che il 26.6.2020 per la prima volta sul conto corrente in questione veniva accreditata una somma ingente, pari ea Euro 71.060,77, relativa alla liquidazione in conseguenza della cessazione di un rapporto lavorativo;

- che l'8.7.2020 gli attori ricevevano sull'utenza telefonica intestata alla D.I. una chiamata da parte di un operatore della banca convenuta, con la richiesta di conferma di un bonifico che sarebbe stato disposto il giorno precedente per la somma di Euro 48.000,00;

- che gli attori negavano di avere mai disposto detto bonifico e nella circostanza l'operatore della convenuta informava loro che il 6.7.2020 erano stati disposti altri due bonifici dell'importo rispettivamente di Euro 24.500,00 ed Euro 22.000,00;

- che gli attori disconoscevano anche tali primi due bonifici e provvedevano immediatamente a sporgere denuncia per quanto accaduto;

- che, a seguito della denuncia, la banca convenuta riusciva a bloccare il bonifico di Euro 48.000,00, mentre lo stesso non avveniva per i primi due bonifici, procurando un danno agli attori di Euro 46.500,00;

- che, come successivamente appurato, entrambi tali bonifici risultavano essere stati disposti in favore di un conto corrente acceso in Spagna;

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

- che gli attori erano all'oscuro delle modalità con cui era stato possibile perpetrare a loro danni tale frode;

- che, in particolare, il fatto che i bonifici fossero stati disposti solo pochi giorni dopo l'accredito della liquidazione faceva ipotizzare una responsabilità da parte di qualche dipendente infedele della banca;

- 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 due bonifici con destinatario e causale assolutamente sospette.

Si costituiva ritualmente in giudizio C. s.p.a., 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 S.C.A., 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 "S.", 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'A. della Banca (installata sullo smartphone in uso esclusivo al cliente);

- che per attivare la prima volta la S., erano previsti i seguenti passaggi: 1) scaricare l'A. sul proprio smartphone; 2) inserire le proprie credenziali di accesso all'homebanking (cioè codice cliente e codice di accesso) nonché le ultime 4 cifre del numero di cellulare; 3) attendere la ricezione del messaggio automatico del sistema tramite S., al numero di cellulare dal cliente (in precedenza già verificato e 'certificato'), con un codice PIN temporaneo; 4) inserire nello spazio apposito il predetto PIN temporaneo; 5) scegliere, su richiesta del sistema, un codice PIN personale di cinque cifre di esclusiva appartenenza al cliente e sconosciuto anche al personale della banca;

- che il codice PIN così generato era necessario, ma non sufficiente, per autorizzare, da quel momento in poi, tutte le operazioni disposte online dal cliente (sia da pc tramite home-banking, sia da smartphone tramite A. di C.!);

- che il processo di attivazione della S. era infatti funzionale ad associare in modo unico e univoco ad un certo device telefonico il software (c.d. token software), presupposto per la generazione dei codici dinamici OTP, parimenti necessari per l'autorizzazione delle singole operazioni di disposizione sul conto corrente. Tale associazione univoca integrava, dunque, il c.d. requisito PSD del "possesso";

- che, in assenza dell'uno o dell'altro elemento, non era possibile processare l'operazione di pagamento. Infatti, quando il cliente inseriva il codice "statico", il token software generava una password OTP "usa-e-getta" che aveva durata limitata ed era univocamente associata alla specifica autorizzazione che era stata richiesta;

- per autorizzare un'operazione di pagamento tramite A. (ad esempio un bonifico come quelli effettuati nel caso in esame), il sistema di generazione degli OTP necessitava dei seguenti parametri per poter procedere: il giorno e orario esatti in cui l'operazione veniva richiesta, calcolato direttamente dal sistema tramite l'orologio interno del dispositivo; il beneficiario dell'operazione, ottenuto tramite i dati inseriti dal cliente nella preparazione online del pagamento tramite pc o smartphone; l'importo dell'operazione

inserito sempre dal cliente; il PIN del cliente, inserito dal cliente tramite A. installata sul proprio smartphone;

- che il token non poteva essere associato contemporaneamente a due device e, pertanto, il suo eventuale spostamento su un altro dispositivo ne comportava l'inutilizzabilità sul precedente; non erano dunque ipotizzabili clonazione o duplicazioni di codici;

- che era, infatti, possibile per i clienti modificare le modalità di autorizzazione delle operazioni o trasferire l'A. di C. su un altro numero di cellulare tramite un complesso procedimento, chiamato "Reset della Strong Authentication", che prevedeva: 1) l'inserimento dei codici personali del cliente (codice accesso e codice cliente); 2) l'inserimento del numero del documento di identità e del codice fiscale del cliente; 3) l'inserimento di una OTP di verifica, idonea a confermare l'operazione di reset, inviata dal sistema via S. sul numero di cellulare certificato dal cliente; 4) l'inserimento delle ultime 4 cifre del numero di cellulare del cliente; 5) l'inserimento di un nuovo PIN temporaneo specificamente collegato all'operazione richiesta, inviato via S. al numero di cellulare certificato dal cliente che permetteva di attivare la S.C.! (del seguente tenore: "Ecco il Pin temporaneo per attivare la tua S.:****** Per la tua sicurezza non comunicarlo ad altre persone, nessun operatore C. te lo può richiedere"); 6) scelta del PIN personale di 5 cifre della S. per l'operatività successiva;

- che si trattava, dunque, di un processo complesso che poteva essere posto in essere solo dal cliente, in quanto richiedeva la conoscenza di informazioni note solo a quest'ultimo e ignote addirittura anche alla banca, che vengono appositamente inviate sul numero telefonico del cliente.

- che, una volta associato il token software al device telefonico, l'utente - per poter accedere alla A. e per effettuare eventuali operazioni di pagamento - doveva inserire un codice statico, ossia il predetto codice PIN personale di cinque cifre (l'elemento della "conoscenza"), che tuttavia non autorizzava direttamente l'operazione, ma che (associato all'elemento di "possesso" del token software sopra evidenziato) era necessario per creare il codice OTP, dinamico;

- che il CORRENTISTA aveva con colpa grave comunicato i codici richiesti nel corso di una conversazione telefonica con un finto operatore della banca, nonostante l'avvertimento contenuto nell'S. ricevuto unitamente ai codici, del seguente tenore: "Ecco il Pin temporaneo per attivare la tua S.:****** Per la tua sicurezza non comunicarlo ad altre persone, nessun operatore C.! te lo può richiedere";

- che l'interlocutore, grazie alle informazioni fornitegli telefonicamente, aveva dunque installato e configurato l'A.C.! sul proprio smartphone;

- che, dunque, i truffatori avevano potuto operare sul conto corrente degli attori, disponendo i tre bonifici.

Espletata l'attività istruttoria secondo le istanze delle parti, nei limiti in cui erano ritenute ammissibili e rilevanti, il giudice rinviava all'udienza dell'8.11.2022 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 gennaio 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 dicembre 2017, n. 218, che ha apportato modifiche al D.Lgs. n. 11 del 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. n. 11 del 2010). L'art. 5, co. 1, D.Lgs. n. 11 del 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. n. 11 del 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. n. 11 del 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.

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

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. n. 11 del 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. n. 11 del 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. n. 11 del 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. n. 11 del 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. n. 11 del 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. n. 11 del 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. n. 11 del 2010).

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

Il regime di responsabilità del PSP si aggrava, infine, dopo la comunicazione di cui all'art. 7, co. 1, lett. b), D.Lgs. n. 11 del 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. n. 11 del 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 C. s.p.a. 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 C. s.p.a. abbia dato corso a degli ordini di pagamento correttamente autenticati, ancorché disposti contro la volontà consapevole degli attori.

Sono, inoltre, pacifiche e documentate le modalità con cui terzi sconosciuti sono entrati illegalmente in possesso delle credenziali di autenticazione dell'**CORRENTISTA** e hanno disposto, autenticandosi, ordini di pagamento a C. S.p.A., presso cui era aperto il conto corrente cointestato ad entrambi gli attori. Invero, nello stesso atto di citazione emerge come a seguito di una truffa telefonica, nella prassi denominata phishing, IL CORRENTISTA abbia comunicato il proprio codice utente e la propria password al sedicente dipendente di banca e abbia seguito le sue istruzioni sino a disattivare il c.d. token software dal proprio dispositivo cellulare e l'abbia attivato presso il dispositivo cellulare dell'autore della truffa, consentendogli di disporre liberamente dal suo conto corrente intestato presso C.

In particolare va evidenziato come la convenuta abbia fatto richiamo da un lato a quanto riferito dal **CORRENTISTA** al proprio operatore, una volta che questi aveva contattato gli attori sul l'utenza telefonica della D.I. in occasione del blocco del terzo bonifico di Euro 48.000,00; dall'altro sul tabulato riassuntivo degli alert inviati dalla banca in occasione dei fatti oggetto di causa.

Sul punto la difesa degli attori si è laconicamente limitata a obiettare come la convenuta non avesse provato le circostanze di fatto dedotte, in quanto non aveva prodotto la registrazione della telefonata, limitandosi a riportarne la trascrizione nella comparsa di risposta e di sentire come testimone il responsabile del servizio clienti, il quale ha risposto in base a quanto aveva appreso ascoltando la registrazione non prodotta; nonché aveva prodotto un tabulato dalla stessa predisposto e, quindi, non idoneo a fornire prova di quanto ivi riportato.

Sennonché va rilevato come parte attrice, circoscrivendo la contestazione a un difetto di prova, non ha mai negato il contenuto della conversazione telefonica intrattenuta dall'**CORRENTISTA** con l'operatore della convenuta e, quindi, non ha mai negato che l'attore avesse dichiarato quanto riportato nella trascrizione agli atti; parimenti, limitandosi a rilevare come il tabulato degli alert non costituirebbe prova adeguata dell'invio degli stessi, non ha negato che gli alert con il contenuto ivi riportato fossero stati effettivamente ricevuti e che, in particolare, l'attore avesse ricevuto il messaggio telefonico di avviso del cambio dell'utenza telefonica abbinata all'operatività del conto corrente, con indicato il nuovo numero e l'invito a contattare la banca qualora l'operazione di cambio dell'utenza non fosse stata da lui disposta.

Tali circostanze di fatto (il contenuto della conversazione telefonica e la ricezione degli alert con il contenuto riportato nel tabulato), quindi, non avendo formato oggetto di contestazione, devono

considerarsi pacifiche e, quindi, non necessitanti di prova, vanificando per ciò solo la contestazione esclusivamente sul piano probatorio formulata dalla difesa attorea.

Le circostanze di fatto in cui si è svolta la vicenda conducono, quindi, a ritenere provata l'esclusiva responsabilità, per colpa grave, di D.G.A..

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.

La CORRENTISTA ha divulgato le proprie credenziali credendo di rispondere ad un impiegato della convenuta, avendo ricevuto una chiamata da un numero che appariva, sul proprio cellulare, riferito all'utenza di quest'ultima. Secondo la prospettiva attorea sarebbe un errore incolpevole, considerato inoltre che la telefonata con il sedicente impiegato era stata preceduta dalla ricezione di alcuni messaggi telefonici che avvisavano di presunti malfunzionamenti e poi di operazioni di aggiornamento dell'A. di C. S.p.A.

Se però si considera come la CORRENTISTA abbia fornito al suo interlocutore il PIN temporaneo necessario per attivare la Smart App sul dispositivo dei truffatori nonostante fosse chiaramente scritto, nel medesimo messaggio in cui era contenuto, "Per la tua sicurezza non comunicarlo ad altre persone, nessun operatore C. te lo può richiedere" emerge l'inescusabile negligenza con cui l'attore 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, di D.G.A. dell'obbligo di cui all'art. 7, co. 2, D.Lgs. n. 11 del 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

Gli attori hanno 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 specie, si evincerebbe dalla frequenza e dall'entità dei pagamenti disposti in un breve lasso di tempo.

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. n. 11 del 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. n. 11 del 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. n. 11 del 2010:

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

"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. n. 11 del 2010, che recepisce l'art. 68, 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, 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. n. 11 del 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. n. 11 del 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. n. 11 del 2010 (art. 74, 2, Dir. 2366/2015/UE). Infatti, l'art. 2, 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 aprile 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. n. 166 del 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. n. 11 del 2010 e 68, 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, 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 S. 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 aprile 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. n. 11 del 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 il terzo bonifico aveva pensato di contattare gli attori sull'utenza della D.I., preso atto della mancata risposta dell'CORRENTISTA sulla nuova utenza indicata dai truffatori.

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano

Sul punto, infatti, va rilevato come a seguito dei primi due bonifici la banca avesse inviato il messaggio di avviso dell'operazione sulla nuova utenza, ritenendo fondatamente che questa fosse nella disponibilità dell'**CORRENTISTA**, non avendo questi comunicato alcunché nonostante l'alert inviato sulla vecchia utenza relativo al cambio del numero telefonico abbinato al conto online; solo in seguito al terzo bonifico, avendo bloccato l'operazione, la banca ha cercato di contattare l'attore per una verifica e, dopo avere provato inutilmente a interloquire sulla nuova utenza (sulla quale, ovviamente, il truffatore non rispondeva), ha provato con l'utenza della D.I.; prima di questo momento, quindi, non era sorto un legittimo motivo di diffidenza verso la nuova utenza, tale da giustificare il contatto sulla seconda utenza indicata dalla D.I. e ciò è sufficiente per escludere anche solo un concorso di colpa della banca convenuta.

La domanda attorea deve essere, conseguentemente, rigettata.

Considerata la novità delle questioni sollevate dalle parti, le spese del giudizio devono essere compensate.

P.Q.M.

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

- rigetta la domanda proposta da D.G.A. e da F.D.I. nei confronti di C. S.p.a.;

- compensa fra le parti le spese di lite.

Così deciso in Milano, il 1 febbraio 2023.

Depositata in Cancelleria il 2 febbraio 2023.

Rivista di informazione giuridica, registrata al Tribunale di Napoli al numero 12 del 05/03/2012
Registro affari amministrativi numero 8231/11
Direttore Responsabile Avv. Antonio De Simone – Direttore Scientifico Avv. Walter Giacomo Caturano