TI_GERICHTE 12.2022.106 vom 25. November 2022

TI Tribunale d'appello, 2022-11-25, IT

Quelle: https://mcp.opencaselaw.ch/entscheid/ti_gerichte_12.2022.106

FR: TI_GERICHTE 12.2022.106 du 25 novembre 2022

IT: TI_GERICHTE 12.2022.106 del 25 novembre 2022

Regeste

Banca - responsabilità per hackeraggio del sistema e-banking

Erwägungen

E. 1

L’art. 308 cpv. 1 lett. a CPC prevede che sono impugnabili mediante appello le decisioni finali di prima istanza, posto che in caso di controversie patrimoniali il valore litigioso secondo l'ultima conclusione riconosciuta nella decisione sia di almeno fr. 10'000.- (cpv. 2). In concreto, la decisione impugnata è una decisione finale in una controversia dal valore superiore ai fr. 10'000.-. Pacifica è dunque l’appellabilità del giudizio impugnato entro il termine di 30 giorni (art. 311 CPC). Introdotto il 24 agosto 2022 contro la decisione impugnata (notificata il 30 giugno 2022) l'appello è cosi tempestivo in virtù dell'art. 145 cpv. 1 lett. b CPC. Come è tempestiva (in virtù dell'art. 142 cpv. 3 CPC) la relativa risposta del 3 ottobre 2022 (art. 312 CPC).

E. 2

Nella decisione impugnata il Pretore, accertato che le parti erano legate da un contratto di conto corrente e da un contratto di giro bancario, ha ricordato che in relazione agli averi depositati sul conto il cliente dispone, di principio, di un'azione in esecuzione del contratto (Erfüllungsklage). Il denaro depositato è proprietà della banca, nei confronti della quale il cliente vanta un credito. Se quindi la banca agisce in esecuzione di un ordine del cliente (o di un suo rappresentante), essa acquisisce una pretesa di rimborso spese per la regolare esecuzione del mandato (art. 402 CO). Per converso, ove esegua le istruzioni di un terzo non autorizzato o un bonifico sulla base di un ordine falso, la banca agisce senza mandato (Putativauftrag) e non ha diritto al rimborso. Applicandosi i principi generali del contratto di mandato la banca sopporta dunque a priori il rischio di pagamento a un terzo non autorizzato, l'assenza di legittimazione e le falsificazioni non individuate rientrando nei cosiddetti "rischi inerenti" dell'attività bancaria, al pari dell'insolvenza del cliente. Ciò significa – ha precisato il primo giudice – che se la banca paga a un soggetto non autorizzato o esegue un bonifico sulla scorta di un ordine falso, essa non si libera dai suoi obblighi nei confronti del cliente, verso il quale rimane debitrice dell'importo trasferito. Il danno economico derivante da un siffatto pagamento indebito è così un danno della banca e non del cliente, a prescindere da una colpa della banca. La regolamentazione testé citata avendo carattere dispositivo, le condizioni generali delle banche possono prevedere delle "clausole di trasferimento dei rischi" che trasferiscono sul cliente il danno della banca in caso di esecuzione irregolare (compreso l'accesso indebito all' e-banking), sempre che a essa non sia imputabile una colpa grave o – se lo prevede espressamente il contratto – una lesione del dovere di diligenza (loc. cit., pag. 5 a 7). Ciò posto, il Pretore, riepilogata la recente giurisprudenza in materia (DTF 146 III 326), ha rilevato anzitutto che l'operazione

eseguita dalla convenuta su ordine di terzi non autorizzati si fondava su un Putativauftrag , di modo che la banca sopportava di per sé il rischio legato all'esecuzione dell'ordine. Il primo giudice ha constatato tuttavia che le condizioni generali per l'utilizzo dell' e-banking della convenuta prevedevano all'art. 3.4 una clausola che trasferiva sul cliente quel rischio. Egli ha ravvisato così una valida deroga convenzionale che ribaltava sull'attrice il danno derivante da un'esecuzione senza mandato. E in mancanza di prova contraria, che incombeva all'attrice recare (per esempio mediante una perizia), o di problematiche nel sistema e-banking della banca che non sono emerse dalla documentazione prodotta in edizione dalla convenuta, il Pretore, considerato anche il tenore dell'art. 8.1 delle note condizioni generali con cui “l’utente prende atto che nella fattispecie il proprio computer costituisce l’anello debole per l’accesso all’E-Banking via Internet”, è partito dal presupposto che l'atto di pirateria informatica era avvenuto nella sfera d'influenza dell'attrice, rispettivamente fuori dalla sfera d'influenza della banca (loc. cit., pag. 7 a 10). Il Pretore ha esaminato dipoi se alla banca fosse ascrivibile una colpa grave che rendeva inapplicabile la clausola di trasferimento dei rischi figurante all'art. 3.4 delle condizioni generali. Appurato che l'accesso alla piattaforma e-banking era avvenuto secondo le modalità pattuite (immissione di una password e del codice matrice), egli non ha riscontrato, sotto questo profilo, colpe gravi della banca. Quanto all'inusualità dell'ordine impartito, non risultava dagli atti – contrariamente a quanto pretendeva l'attrice – che le parti avessero concordato un'autorizzazione all'esecuzione di soli ordini di pagamento per salari, tant'è che nell'estratto conto figuravano anche altri bonifici senza specifica di sorta. Certo, la transazione litigiosa poteva dirsi inusuale per rapporto all'entità e alla destinazione "esotica" del pagamento allorché gli ordini di bonifico erano altrimenti limitati di norma alla Svizzera. Ciò nondimeno, per il Pretore non vi erano gli estremi per ravvisare una colpa della banca nel dare seguito all'ordine. Premesso che gli ordini trasmessi tramite e-banking sono eseguiti in forma automatizzata e senza interazioni tra ordinante e banca, il primo giudice ha evidenziato che la convenuta all'epoca dei fatti non disponeva di un sistema in grado di individuare e segnalare operazioni potenzialmente inusuali. Di conseguenza, neppure sotto questo aspetto era ravvisabile una colpa grave della banca. Né una grave mancanza della convenuta poteva desumersi dalle difficoltà di accesso all' e-banking del 5 settembre 2016, visto che tali problemi erano emersi alla banca soltanto successivamente e che C_____ L_____ non aveva segnalato, chiamando ad esempio l' hotline della banca, criticità alla convenuta. Applicandosi la clausola di trasferimento dei rischi, la petizione andava dunque respinta (loc. cit., pag. 10 a 14).

E. 3

L'appellante ripropone l'argomento per cui la banca avrebbe fra l'altro violato l'obbligo di diligenza per non avere bloccato per tempo, il 6 settembre 2016, l'esecuzione del pagamento contestato pur avendone la possibilità (memoriale, pag. 18 segg.). Il Pretore non si è chinato sulla questione ma si è limitato a rilevare che le versioni delle parti divergevano: mentre per l'attrice il proprio amministratore unico avrebbe immediatamente informato la convenuta, per quest'ultima la comunicazione sarebbe avvenuta soltanto verso le 9:15 (sentenza impugnata, Lett. E, pag. 3). Ora, su questo aspetto entrambe le parti si sono già espresse in prima (v. petizione, pag. 6; risposta, pag. 10) come in seconda sede. Nulla osta pertanto al suo esame in appello tanto più che il giudizio è maturo e nessuno postula un rinvio al Pretore per nuovo accertamento. Per economia processuale conviene trattare prioritariamente tale questione poiché se dovesse risultare che la convenuta aveva ancora la possibilità di bloccare l'operazione ciò renderebbe superfluo l'esame degli altri argomenti.

E. 3.1

Per l'attrice l'istruttoria avrebbe dimostrato che la chiamata di C_____ L_____ è avvenuta tra le 8:00 e le 8:30, come ha avuto modo di confermare la teste S_____ K_____, sua responsabile amministrativa nel verbale del 6 maggio 2021 (pag. 2). Tale affermazione non sarebbe stata rimessa in discussione dal teste G_____ M_____, consulente della convenuta, il quale ha indicato di non ricordare l'orario preciso della telefonata, pur stimandola in 15-30 minuti dopo che aveva ripreso a lavorare, ovvero intorno alle 9:00 (verbale 3 marzo 2021, pag. 3). Per l'appellante sarebbe inoltre significativo che, malgrado una specifica richiesta di edizione dei rapporti allestiti in merito ai contatti telefonici intercorsi, la convenuta non abbia prodotto nulla, il che – dato il contenzioso in corso – costituisce a suo avviso una "lacuna molto anomala", tanto più che la banca è tenuta a conservare ogni rapporto sui contatti con il cliente e che il teste G_____ M_____ non ha fornito spiegazioni per tale omissione. Dovendosi dunque dipartire da quanto dichiarato dalla teste S_____ K_____, la convenuta avrebbe avuto la concreta possibilità di bloccare immediatamente l'ordine al momento (tra le 8:00 e le 8:30) in cui C_____ L_____ ha telefonato, l'invio dell'ordine all' U___SA essendo avvenuto alle 8:15:20, l'accettazione da parte della medesima alle 8:33:59 e la sua trasmissione dall' U___SA alla banca turca alle 8:34:00. Senza contare che la convenuta, impartendo all' U___SA l'ordine di cancellazione soltanto alle 12:00:23, avrebbe commesso un'ulteriore negligenza (memoriale, pag. 18 a 21).

E. 3.2

Dal canto suo la convenuta obietta che la dichiarazione di S_____ K_____ è smentita dalla deposizione di G_____ M_____ oltre che da quanto rapportato internamente poco dopo i fatti (doc. 5 e doc. 10) e che riconduce alle 9:15 l'orario del contatto. A parte ciò, essa non comprende perché la controparte, contravvenendo all'onere probatorio che le incombeva, abbia omesso di richiedere al proprio operatore i tabulati telefonici che avrebbero potuto confermare la sua tesi. Comunque sia, anche seguendo per ipotesi la versione della teste S_____ K_____, ciò non muta che tra le 8:15:20 e le 8:34:00 qualsiasi reazione teoricamente ipotizzabile sarebbe stata inutile poiché non c'era più il tempo necessario per effettuare le comunicazioni tra i vari servizi interni ed esterni interessati e per impedire il trasferimento definitivo dei fondi (risposta, pag. 13 seg.).

E. 3.3

Contrariamente all'opinione dell'appellante, la deposizione di S_____ K_____ non è risolutiva. Oltre a ricondurre la telefonata entro un arco temporale di mezz'ora, la teste non si è detta certa della sua affermazione, avendola preceduta dalla premessa "se non sbaglio" (verbale 6 maggio 2021, pag. 2). A parte ciò, la teste ha riferito che quella mattina C_____ L_____ aveva eseguito l'accesso tramite il suo (di lui) personal computer (loc. cit., pag. 3), allorché il primo giudice ha accertato invece – senza contestazione al riguardo e sulla scorta di quanto emerso dall'ordine di perquisizione e sequestro 28 settembre 2016 del Ministero pubblico (doc. 4) – che tale collegamento era avvenuto tramite il computer di un collega (sentenza impugnata, lett. E). Ciò posto, l'orario – approssimativo – della telefonata non può ricavarsi con certezza dalla testimonianza di S_____ K_____. Come esso non può evincersi del resto – a dispetto di quanto sostiene la convenuta – dalla deposizione del suo consulente G_____ M_____ che ha proceduto a una stima, dopo avere premesso di non ricordarlo con precisione (verbale 3 marzo 2021, pag. 3), né dalla lettera 14 settembre 2016 del suo servizio giuridico

e compliance (assimilabile a una dichiarazione di parte) né tanto meno dal riscontro che l'attrice si è collegata quel 6 settembre 2016 al sistema e-banking alle 9:30, trattandosi dell' ultimo accesso di quel giorno (doc. 10, foglio 8).

E. 3.4

delle condizioni generali (di analogo tenore, come osserva la convenuta a pag. 13 della sua risposta, pure il loro art. 2.6 secondo cui " il cliente riconosce, senza riserve, tutte le transazioni contabilizzate, eseguite tramite E-Banking nell'ambito dei servizi concordati e dietro utilizzo dei dati di identificazione del cliente stesso. Sono ugualmente considerati come predisposti o autorizzati dal cliente tutte le istruzioni, gli ordini o le comunicazioni che giungono alla banca in questa modalità […]: doc. D), rimane da esaminare se alla banca – sempre in virtù di quella medesima clausola – fosse ascrivibile una colpa grave suscettibile di invalidarne gli effetti, come pretende l'appellante (memoriale, pag. 9 segg.).

E. 3.5

Ma quand'anche si volesse – per abbondanza – considerare la testimonianza di S_____ K_____, essa non dimostrerebbe ancora che la convenuta abbia avuto il tempo materiale per bloccare il pagamento. La teste ha dichiarato che C_____ L_____ ha chiamato la banca non appena si è avveduto dell'addebito. Se non che questo è intervenuto alle 8:15. L'attrice aveva così a disposizione un arco di tempo (assai) ristretto per chiamare la propria banca (nel caso specifico il proprio consulente G_____ M_____: doc. 7) e spiegare il problema, e per ottenere che i servizi competenti della convenuta (in concreto il responsabile compliance ALM, J_____ M_____ _____: doc. 6) intervenissero presso l' U___SA per impedire la transazione. Che ciò fosse materialmente possibile non è affatto provato (almeno secondo il grado della verosimiglianza preponderante), sicché l'attrice – che non contesta l'iter procedurale seguito dalla banca ma solo i tempi di reazione della stessa– sopporterebbe anche in siffatta ipotesi le conseguenze dell'assenza di prova. Poco importa invece, sotto questo profilo, che l'ordine di cancellazione della convenuta all' U___SA sia avvenuto soltanto alle 12:00 (doc. 7, pag. 1), tale circostanza essendo senza rilievo per stabilire se, agendo con tutta la diligenza e celerità possibile, la convenuta avrebbe potuto fermare in tempo l'operazione.

E. 4

Non potendosi dimostrare che la convenuta avrebbe potuto ancora bloccare l'operazione quel 6 settembre 2016, occorre stabilire chi, fra la banca e il cliente, si debba assumere le conseguenze del contestato bonifico di fr. 113'200.15. Secondo la più recente giurisprudenza in materia, se un attore allega che la banca ha eseguito dei versamenti o dei bonifici nonostante la mancanza di legittimazione dell'ordinante o in seguito a falsi non rilevati, il giudice esamina chi, tra la banca o il cliente, sopporta il danno che ne deriva, procedendo in tre tappe. In una prima tappa, chinandosi sull'azione principale del cliente in restituzione dei suoi averi non decurtati dei prelievi indebiti (Erfüllungsklage ; art. 107 cpv. 1 CO) il giudice deve esaminare se i prelievi sono stati eseguiti su mandato o senza mandato del cliente. Soltanto in quest'ultima ipotesi il giudice deve vagliare, in una seconda tappa, se il danno vada a carico della banca (sistema legale, trattandosi di un rischio inerente all'attività bancaria) oppure se in ragione di una clausola di trasferimento del rischio il danno vada addebitato al cliente. Se il danno è subito dalla banca conformemente al sistema legale, il giudice può ancora essere chiamato a esaminare, in una terza tappa, se essa può

opporre in compensazione all'azione in restituzione del suo cliente una pretesa di risarcimento danni per avere costui contribuito colposamente a causare o aggravare il danno violando i propri obblighi (art. 97 cpv. 1 CO; DTF 146 III 387 consid. 3.1, 326 consid. 4). Se invece le parti hanno concordato una clausola di trasferimento del rischio non v'è spazio per la terza fase. L'eventuale colpa concomitante del cliente (quale fattore d'interruzione del nesso di causalità adeguata o di riduzione dell'indennità spettantegli) andrà vagliata nell'ambito dell'esame della colpa grave della banca che – come si vedrà in appresso (consid. 6) – rimane riservata (art. 100 cpv. 1 CO per analogia; DTF 146 III 326 consid. 4.2).

E. 5

Per quel che è della prima fase, il Pretore ha accertato che il bonifico di fr. 113'200.15 è avvenuto su ordine di terzi non autorizzati dal cliente. La questione è pacifica e non necessita di ulteriori approfondimenti.

E. 6

Passando alla seconda fase, occorre esaminare anzitutto la validità della clausola di trasferimento del rischio conclusa dalle parti, interrogandosi in particolare se la banca abbia commesso una colpa grave nell'esecuzione degli ordini di bonifico fraudolenti. Generalmente una siffatta clausola determina che il rischio altrimenti sopportato dalla banca sia ribaltato sul cliente (Schadensabwälzung) e istituisce una responsabilità di quest'ultimo verso la banca che si estende anche ai casi fortuiti (Zufallshaftung). La validità di una simile clausola va esaminata in applicazione analogica degli art. 100 e 101 cpv. 3 CO che reggono i patti di esclusione della responsabilità in caso di inadempimento o adempimento imperfetto del contratto quantunque la clausola di trasferimento del rischio non risulti da un inadempimento contrattuale nel senso dell'art. 97 segg. CO (DTF 146 III 326 consid. 6.1 con rinvii).

E. 6.1

In una prima censura l'appellante ribadisce che la clausola di trasferimento del rischio, sancita all'art. 3.4 delle condizioni generali per l'utilizzo dell' E-Banking della AP 1 (sopra, Lett. A), non si applica in concreto poiché essa vale unicamente nel caso di utilizzo/abuso dei propri dati di identificazione o di quelli degli utenti autorizzati, il che presuppone che l'attacco informatico abbia colpito il proprio sistema informatico. Al proposito l'attrice contesta la valutazione del Pretore secondo cui spettava a lei dimostrare che l'attacco informatico avesse colpito la piattaforma e-banking della banca. Dal momento che era la banca a invocare la clausola di trasferimento del rischio, a suo avviso incombeva a quest'ultima dimostrare che si realizzavano le condizioni per l'applicazione della clausola. E in mancanza di specifici accertamenti riguardo alla sfera d'influenza colpita, il primo giudice non poteva concludere in suo sfavore, tanto più che l'istruttoria avrebbe dimostrato che i propri sistemi informatici erano adeguatamente protetti. L'istruttoria non avrebbe inoltre dimostrato che sarebbero stati carpiti i dati di identificazione dei propri computer o i codici matrice in possesso di C_____ L_____, i tentativi falliti di accesso del 5 settembre 2016 essendo irrilevanti ai fini di tale questione. Non applicandosi la clausola di trasferimento del rischio, l'appello andrebbe dunque accolto già solo per questo motivo (memoriale, pag. 5 a 9, n. 6).

E. 6.1.1

L'appellante perde di vista tuttavia che il Pretore non si è limitato a evidenziare che spettava a lei dimostrare la circostanza – da essa addotta – che l'attacco informatico aveva colpito la piattaforma e-banking della banca e non (solo) il proprio sistema informatico. Il primo giudice ha anche precisato che dalla documentazione prodotta dalla convenuta, segnatamente da quella chiesta in edizione "intesa a dimostrare le problematiche avute dal sistema e-banking della banca convenuta" non era emerso nulla e non era quindi dimostrato che l'hackeraggio fosse avvenuto nella sfera di competenza della banca. Tale constatazione, unitamente al tenore dell'art. 8.1 delle note condizioni generali con cui il cliente dava atto che il suo computer rappresentava l'anello debole della sicurezza dell'accesso via e-banking , avevano indotto il Pretore a concludere che l'attacco informatico alla base dell'ordine di bonifico fraudolento doveva essere avvenuto nella sfera di influenza dell'attrice ma comunque al di fuori della sfera di influenza della banca (sentenza impugnata, pag. 10). Ora, con questa doppia argomentazione l'appellante non si confronta nemmeno di scorcio, sicché al riguardo l'appello si rivela finanche irricevibile per carenza di motivazione (nel senso dell'art. 311 cpv. 1 CPC). Ciò posto, la conclusione del primo giudice, stando al quale l'hackeraggio dev'essere avvenuto al di fuori della sfera d'influenza della convenuta, sfugge alla critica.

E. 6.1.2

A parte ciò – come eccepisce la convenuta (risposta: pag. 6 a 8) – una serie di indizi (il concatenamento temporale tra gli accessi, riusciti e falliti, di C_____ L_____ e quelli degli hackers il 5 settembre 2016 [sopra, lett. B] cui era associato per altro lo stesso numero di contratto e di Login Name [doc. 8 e doc. D]; la motivazione dell'ordine di perquisizione e sequestro 28 settembre 2016, da cui si evince che ignoti sarebbero "riusciti ad impossessarsi illecitamente dei dati della denunciante per l'accesso al sistema bancario e-banking di AP 1" [doc. 4]; le difficoltà di accesso incontrate da C_____ L_____ il 6 settembre 2016 dalla propria postazione ma non da quella di un collega [doc. 4]) induce effettivamente a ritenere che l'attacco informatico sia avvenuto nella sfera d'influenza dell'attrice, la quale, in virtù della ricordata giurisprudenza, sarebbe comunque sia chiamata a rispondere anche dei casi fortuiti, ovvero degli eventi e dei comportamenti non imputabili alle parti al contratto (analogamente: DTF 146 III 326 consid. 6.2.1.2, 6.3.2.1 in fine e 6.3.2.3 in fine). Nulla muta al riguardo che l'attrice fosse protetta da un pacchetto (standard) antivirus/firewall/antispyware aggiornato anche perché, per quanto riferito dallo stesso responsabile esterno della sicurezza informatica dell'attrice (G_____ B_____), pur non essendo stata riscontrata alcuna anomalia, neppure i sistemi più performanti e aggiornati danno garanzia totale (verbale 6 maggio 2021 pag. 5).

E. 6.2

con rinvii). Agisce invece per colpa lieve colui che non adotta tutta la cautela che ci si poteva attendere da lui senza raggiungere tuttavia tale intensità. Il giudice valuta le azioni dell'autore negligente riferendosi alla diligenza che l'altra parte poteva attendersi da lui, segnatamente in virtù degli accordi contrattuali e degli usi professionali. L'onere della prova della negligenza grave della banca grava sul cliente (loc. cit.). Per quanto concerne l’autenticità degli ordini, in linea di principio la banca è tenuta a verificare solo che essi siano conformi alle modalità concordate tra le parti o, se del caso, specificate dalla legge (loc. cit. consid. 6.2.1). In materia di verifica delle firme , il Tribunale federale ha già avuto modo di precisare che la banca non deve prendere misure straordinarie incompatibili con una liquidazione rapida delle operazioni e non deve presumere sistematicamente l'esistenza

di frodi, dovendo per contro procedere a verifiche supplementari in presenza di indizi seri di falsificazione, se l'ordine non verte su un'operazione prevista contrattualmente né usualmente domandata o ancora se circostanze particolari destano dubbi (loc. cit. consid. 6.2.1.1). In relazione all'uso concordato della posta elettronica per la trasmissione degli ordini, l'Alta Corte ha inoltre avuto modo di stabilire che la banca non è obbligata ad adottare misure straordinarie per l'esame della loro autenticità che siano incompatibili con un'evasione rapida delle operazioni, ritenuto che se provengono dall'indirizzo e-mail comunicatole dal cliente essa non deve presumere sistematicamente che tali ordini non siano stati impartiti da lui ma siano il frutto di atti di pirateria informatica (loc. cit., consid. 6.2.1.2). Per tali situazioni il Tribunale federale ha precisato che la banca commette una colpa grave solo se dall'esame a cui essa procede, necessariamente rapido per il tipo di transazioni che è chiamata a effettuare, sorgono seri indizi di usurpazione d'indirizzo e quindi d'identità. Ciò è il caso se deve "balzare all'occhio" a qualsiasi persona ragionevole che l'ordine trasmesso, in virtù del suo indirizzo, testo, contenuto o luogo esotico del bonifico, e tenuto conto della situazione del cliente, non può provenire da quest'ultimo. Per esempio, una colpa grave della banca è stata ammessa nel caso in cui l' account di posta elettronica di un cliente (un avvocato di lingua inglese che si era sempre espresso con un linguaggio accurato) era stato hackerato da sconosciuti che avevano, a sua insaputa, inviato e-mail dall'indirizzo di costui e intercettato quelle inviategli dalla banca, impartendo ordini di bonifico per importi ingenti (l'uno dei quali aveva intaccato il conto per più di un quarto), scritti in un inglese sgrammaticato e approssimativo e in favore di relazioni bancarie a Hong Kong e Singapore, allorché era noto alla banca che il cliente, con cui era in relazione da 20 anni, aveva costantemente incrementato le sue posizioni nell'ottica di una conservazione a lungo termine (loc. cit. con riferimento a STF 4A_386/2016 del 5 dicembre 2016, consid. 2.3 e 2.4).

E. 6.2.1

Costituisce colpa grave la violazione delle elementari regole di prudenza che si imporrebbero a qualsiasi persona ragionevole posta nelle medesime circostanze (DTF 146 III 326 consid.

E. 6.2.2

Trattandosi invece degli ordini di pagamento tramite e-banking non consta – per quanto è dato di vedere – che la giurisprudenza abbia elaborato regole specifiche. Tale metodo di pagamento si caratterizza per le modalità operative, ovvero per il fatto che il sistema informatico del cliente comunica attraverso l'internet con il sistema informatico della banca. Nell' online banking il cliente interviene sul sistema registrando l'ordine di pagamento. Il resto della procedura è automatizzato e si interfacciano esclusivamente macchine con macchine, fermo restando che il sistema informatico del cliente è spesso l'anello debole della catena (Reichart , Betrugsversuche im Zahlungsverkehr im digitalen Zeitalter in: SZW 2019 pag. 401). In tale ambito è reputata agire negligentemente la banca che utilizza un sistema che non è più impiegato dalla maggior parte degli altri istituti e che non raggiunge gli standard di sicurezza dei sistemi più moderni. In altri termini, le misure di sicurezza devono corrispondere allo stato dell'arte, la banca dovendo installare processi d'autenticazione conformi agli usi professionali (loc. cit.; Liégeois/Hirsch , Ordres bancaires frauduleux: discours de la méthode in: SJ 2021 II pag. 147). Alla luce della giurisprudenza testé illustrata (sopra, consid. 6.2.1) v'è da chiedersi in che misura la banca, dando prova della diligenza usuale negli affari, debba riconoscere indizi particolari che

inducono a concludere per un abuso nell' online banking . Siccome un controllo dei singoli ordini di pagamento a opera di un collaboratore della banca non è possibile, il riconoscimento può solo avvenire attraverso sistemi informatici muniti di adeguati filtri o blocchi, quali il profiling o il geoblocking (Reichart , op. cit., pag. 402 seg.) . Considerato il progresso tecnologico in continua evoluzione, non è facile tuttavia dire quale sia la diligenza usuale esigibile dalle banche (Reichart , loc. cit.). Una colpa grave sembrerebbe ammettersi nel caso in cui il sistema informatico avrebbe dovuto rilevare la natura manifestamente insolita dell'ordine (Liégeois/Hirsch , loc. cit.; analogamente Rappo/Stojanovic , E-banking et fraudes informatiques in: Expert Focus 1-2/18 pag. 62).

E. 6.2.3

L'appellante ribadisce che a prescindere dalle modalità operative concordate (immissione di una password e di un codice matrice figurante su un supporto cartaceo: doc. D) alla banca incombeva un obbligo di verifica, viste le particolarità dell'operazione contestata. L'istruttoria avrebbe dimostrato che le parti avevano pattuito un'autorizzazione all'esecuzione di ordini di pagamento di salari, circostanza che si evince dalla convenzione medesima relativa all' e-banking (doc. D) come pure dal proprio scopo sociale (reclutamento, selezione e collocamento di personale). L'ordine di € 74'300.-, modificato in fr. 113'224.14 risultava pertanto palesemente inusuale viste le modalità, gli importi e la destinazione (Lituania in un primo momento e poi Turchia) del bonifico che non corrispondeva alle finalità operative dichiarate della società che oltretutto effettuava unicamente versamenti nazionali dell'ordine di fr. 3'000.-/4'000.- al massimo. Ciò posto, il Pretore non poteva limitarsi a ritenere che nell'estratto conto figuravano anche bonifici senza specifica di sorta. Dandosi un ordine di pagamento inusuale – come ha del resto ammesso lo stesso Pretore – la banca avrebbe dovuto compiere accertamenti supplementari. Non avendolo fatto, quando sarebbe bastato un breve contatto telefonico per avere un riscontro, la convenuta avrebbe commesso una colpa grave. Che la banca non disponesse di un sistema in grado di individuare ordini sospetti non permette a costei di sgravarsi dall'obbligo di verifica ma integra una grave violazione del dovere di diligenza, spettando alla medesima dotarsi delle opportune soluzioni tecnologiche – quali un sistema di logaritmi di analisi – e di organizzazione per adempiere al proprio dovere di diligenza. Senza contare – epiloga l'appellante – che, come si evince dalla deposizione del teste G_____ M_____, la banca sarebbe stata in grado di offrire un sistema di protezione più efficace, ovvero quello tramite codice SMS detto "mTAN" (numero mobile di autorizzazione alla transazione: doc. D), che la convenuta non ha però implementato nei suoi confronti lasciandola così operare con un sistema vulnerabile e meno sicuro (memoriale, pag. 9 a 18, n. 7 e 8).

E. 6.2.4

Da quest'ultima argomentazione va subito sgombrato il campo. Non è la convenuta che ha omesso di implementare nei suoi confronti il sistema di identificazione "mTAN" – già fruibile nel febbraio 2014 (v. Doc. D, pag. 1 n. 3) – ma è l'attrice medesima che – non si sa per quali ragioni – non se ne è avvalsa. D'altronde l'appellante non contesta di avere optato per il sistema di accesso fondato sull'immissione di una password e del codice matrice. Perché poi il sistema d'accesso "mTAN" garantisse una maggiore sicurezza nella tutela contro gli ordini fraudolenti l'interessata non spiega, sicché al riguardo l'appello si rivela finanche irricevibile per carenza di motivazione. Ma quand'anche il sistema di accesso tramite SMS fosse stato effettivamente più sicuro, nulla impediva all'attrice di indicare nella

relativa rubrica (doc. D: "3. Identificazione per l'E-Banking – mTAN") il numero di telefonia mobile cui inviare i codici supplementari, come ha obiettato l'appellata (risposta, pag. 15). L'attrice va rimessa così alle proprie responsabilità.

E. 6.2.5

Per quel che è della pattuizione di un'autorizzazione all'esecuzione di (soli) ordini di pagamento di salari, si rileva anzitutto che la censura è formulata in modo poco chiaro se non contraddittorio, al punto 7.3 del memoriale (pag. 12) l'appellante sembrando revocare o quanto meno relativizzare l'allegazione ("Ora, l'appellata non ha mai sostenuto che con la banca fosse stato concordato che sarebbero stati eseguiti unicamente dei pagamenti di salario. Questo aspetto è comunque del tutto irrilevante in quanto l'esecuzione del pagamento di salari è in concreto l'unica operazione che è stata eseguita sul conto dell'appellante"). A parte ciò, il Pretore ha rilevato che se nella convenzione (al punto 4b "Autorizzazione di accesso ad hoc per i seguenti conti/depositi") risultava effettivamente spuntata la casella "Pagamenti di salari", ciò non significava che l'unica finalità del conto fosse il traffico di pagamenti connessi ai salari, nel medesimo documento essendo vistata anche la rubrica "interrogazioni e ordini" che poteva riferirsi genericamente a pagamenti di altra natura, come confermava del resto l'estratto conto in cui figuravano anche bonifici senza alcuna specifica (sentenza impugnata, pag. 12). E al riguardo l'appellante si limita a contrapporre la propria soggettiva valutazione asseverando – per altro per la prima volta in appello – che il contesto operativo del conto e quindi la natura salariale delle "interrogazioni e ordini" si evincevano dal settore di attività della società senza spiegare perché l'accertamento del primo giudice – fondato su un esame dell'estratto conto – sarebbe erroneo. Al proposito l'appello si dimostra quindi irricevibile per carente motivazione.

E. 6.2.6

Quanto alla censura che alla banca, date le particolarità dell'operazione, incombeva un obbligo di verifica a prescindere dalle modalità di accesso concordate, si conviene con l'appellante – come ha accertato per altro lo stesso Pretore – che l'ordine di pagamento in rassegna era anomalo già solo in ragione degli importi (il conto essendo stato intaccato per il 90% del suo saldo: plico doc. 14, pag. 142 seg. dell'estratto) e della destinazione esotica del bonifico (Lituania e Turchia, allorché gli altri pagamenti, tranne tre, erano limitati al territorio svizzero: plico doc. 14, pag. 3, 117 e 140). Come va dato atto all'attrice che il solo fatto – non contestato – che il sistema operativo della convenuta non fosse in grado di segnalare transazioni insolite non poteva – contrariamente all'opinione del primo giudice – essere decisivo per escludere una colpa grave della banca, quanto meno ove altri istituti finanziari nella stessa situazione della convenuta fossero stati invece in grado, nel periodo in esame (settembre 2016) e valendosi anch'essi dei codici matrice per accedere ai loro sistemi e-banking , di rilevare operazioni sospette. Il problema è che al riguardo manca ogni accertamento e prova che incombeva all'attrice recare, trattandosi di esaminare la diligenza che ci si poteva attendere in virtù degli usi professionali (sopra, consid. 6.2.1; cfr. pure DTF 108 II 314 consid. 4). Senza contare che non sembrerebbero esservi state – comunque sia – chiare direttive che obbligavano le banche nella stessa situazione della convenuta e per le modalità di accesso in esame (che nemmeno l'appellante pretende fossero superate all'epoca dei fatti) a installare, nel settembre 2016, dei programmi suscettibili di analizzare il profilo del cliente e di bloccare o rielaborare manualmente, per esempio tramite callback, ordini che non corrispondevano a un determinato profilo (Reichart , op. cit., pag. 403; analogamente pure Stengel/Rüegg/Sommer/Stäuble/Freund , Kooperationsformen zwischen

Banken und Drittanbietern aus vertrags- und datenschutzrechtlicher Perspektive in: SZW 2022 pag. 23). Non potendosi quindi ammettere, in definitiva, una colpa grave della banca, l'appello vede la sua sorte segnata.

E. 7

Gli oneri processuali d'appello, calcolati su un valore litigioso di fr. 113'224.15, seguono la soccombenza dell'appellante (art. 106 cpv. 1 CPC), che rifonderà alla controparte ripetibili di fr. 4'000.- stabilite sulla base dell'art. 11 RTar.

E. 8

Il valore litigioso determinante ai fini di un'eventuale impugnazione dinanzi al Tribunale federale supera la soglia di fr. 30'000.- prevista dall'art. 74 cpv. 1 lett. b LTF. Per questi motivi, richiamati l’art. 106 CPC, la LTG e il RTar, decide: 1. Nella misura in cui è ricevibile, l’appello 24 agosto 2022 della AP 1 è respinto . 2. Le spese processuali di fr. 6'000.- sono poste a carico dell'appellante che rifonderà alla controparte fr. 4'000.- per ripetibili. 3. Notificazione: - ; - . Comunicazione alla Pretura della giurisdizione di Locarno-Città. Per la seconda Camera civile del Tribunale d'appello Il presidente Il vicecancelliere Rimedi giuridici Nelle cause a carattere pecuniario con un valore litigioso superiore a fr. 30'000.- è dato ricorso in materia civile al Tribunale federale, 1000 Losanna 14, entro 30 giorni dalla notificazione del testo integrale della decisione (art. 100 cpv. 1 LTF). Qualora non sia dato il ricorso in materia civile è possibile proporre negli stessi termini ricorso sussidiario in materia costituzionale (art. 113, 117 LTF). La parte che intende impugnare una decisione sia con un ricorso ordinario sia con un ricorso in materia costituzionale deve presentare entrambi i ricorsi con una sola e medesima istanza (art. 119 LTF).