Sentenza n. 32/2026 pubbl. il 19/03/2026
RG n. 1316/2024
Repert. n. 155/2026 del 19/03/2026
Sentenza n. cronol. 664/2026 del 19/03/2026

N.RG 1316 / 2024

IN NOME DEL POPOLO ITALIANO

UFFICIO DEL GIUDICE DI PACE DI EMPOLI

SENTENZA

vertente tra

Omissis come in atti

-RICORRENTE-

contro

BNL come in atti

-RESISTENTE-

SENTENZA

Il Sig. Omissis con ricorso ex artt. 316 e 281 undecies c.p.c adiva il giudice di pace al fine di ottenere la restituzione della somma di Euro 2.700,00, oggetto di un bonifico fraudolento eseguito il 2 maggio 2023 mediante il proprio conto corrente intrattenuto presso Banca Nazionale del Lavoro S.p.A.

La resistente si costituiva mediante deposito di comparsa di costituzione e risposta.

All'esito dell'istruttoria documentale e del contraddittorio sviluppatosi tra le parti, la causa passava in decisione.

La difesa della Banca, come era suo onere, non è riuscita a dimostrare che il pagamento sia stato autorizzato dal cliente né che lo stesso abbia agito con dolo o colpa grave, unici presupposti che, ai sensi degli artt. 10 e ss. del d.lgs. n. 11/2010, consentirebbero di addossare al prestatore di servizi di pagamento l'esonero da responsabilità.

La ricostruzione di parte resistente viene incentrata sull'asserita imprudenza del Omissis nella navigazione internet e sull'utilizzo di un sito di streaming, non coglie nel segno e appare giuridicamente irrilevante.

Invero, anche a voler ritenere che il ricorrente sia stato vittima di un malware o di un trojan, tale circostanza non equivale affatto a una autorizzazione dell'operazione di pagamento né può essere automaticamente qualificata come colpa grave.

Nel caso di specie, la Banca si è limitata a produrre log informatici e a richiamare l'astratto funzionamento del sistema di autenticazione forte (SCA), senza tuttavia fornire la prova decisiva che l'operazione sia stata consapevolmente autorizzata dal Sig. Omissis

La mera circostanza che il pagamento risulti tecnicamente eseguito tramite le credenziali e il dispositivo del cliente non equivale a dimostrazione dell'autorizzazione, soprattutto in presenza di un contesto di frode informatica che ha consentito a terzi di operare all'insaputa dell'intestatario del conto.

Né può assumere rilievo decisivo l'invio di notifiche push o di SMS alert.

Tali strumenti hanno natura meramente informativa e non possono trasformarsi, a posteriori, in una sorta di presunzione di consenso dell'utente.

La linea difensiva adottata da Banca Nazionale del Lavoro S.p.A. si fonda interamente su un unico pilastro: addossare la responsabilità dell'accaduto al Omissis

Senonché, si tratta di una strategia che tenta di spostare l'attenzione dall'unico elemento rilevante ai fini della decisione: il mancato assolvimento, da parte della Banca, dell'onere probatorio che l'art. 10, comma 1, del D.Lgs. 11/2010 pone espressamente a suo carico.

Nello specifico, il legislatore ha chiaramente stabilito che, in presenza di un'operazione disconosciuta, è la Banca a dover dimostrare che il sistema di pagamento ha funzionato correttamente e che sono state adottate tutte le misure di sicurezza necessarie.

Nel caso di specie, BNL non ha fornito alcuna prova convincente in tal senso.

L'art. 10, comma 1, del D.Lgs. 11/2010 (come modificato dal D.Lgs. 218/2017) è di cristallina chiarezza: "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti".

La norma, dunque, inverte l'onere della prova: non è il cliente a dover dimostrare che non ha autorizzato l'operazione, ma è la Banca a dover provare che l'operazione è stata effettivamente autorizzata dal cliente, che il sistema di autenticazione era sicuro e non vulnerabile e che non vi sono stati malfunzionamenti o inconvenienti nelle procedure.

Nel caso di specie, BNL non ha assolto tale onere probatorio.

Invero, la resistente sostiene testualmente che "l'asserito truffatore tramite una APP terza, alla quale il Omissis consentito l'accesso incautamente sul suo cellulare, ha assunto il controllo del device del correntista potendo così carpire le credenziali di accesso all'home banking e disporre l'operazione in contestazione".

Questa affermazione rappresenta una prova a favore del ricorrente.

La Banca ammette che il truffatore ha "assunto il controllo del device" e "carpito le credenziali".

Ma se ciò è stato possibile, significa che il sistema di autenticazione forte (Strong Customer Authentication - SCA) implementato dalla BNL non era affatto sicuro e non ha impedito la

frode.
In altre parole, la resistente afferma che il proprio sistema di sicurezza è stato aggirato.
E se un sistema di sicurezza può essere aggirato da un malware relativamente comune (i trojan bancari sono purtroppo diffusi), allora quel sistema non è adeguato ai sensi della normativa vigente.
La giurisprudenza è costante nel ritenere che "la mera implementazione di un sistema di autenticazione forte non esonera la banca dalla responsabilità se tale sistema si rivela inefficace nel prevenire le frodi" (Cfr. Cass. Civ., Sez. I, ordinanza n. 29852/2023; Trib. Padova, sentenza n. 2309/2023).
Più nello specifico, la Banca non ha fornito alcuna prova documentale dell'esistenza di sistemi automatizzati di rilevamento delle operazioni anomale, quali algoritmi di intelligenza artificiale o machine learning capaci di identificare transazioni sospette in base ai comportamenti abituali del cliente.
Nel caso di specie, l'operazione fraudolenta presentava molteplici red flags che avrebbero dovuto far scattare immediatamente un allarme: il bonifico è stato disposto alle ore 04:46 del mattino, orario assolutamente inconsueto per qualsiasi operazione bancaria legittima; il beneficiario nuovo: la Sig.ra F Omissis non era mai stata utilizzata come beneficiaria dal Sig. Omissis precedenza; IBAN estero: il conto di destinazione era intestato in Lituania Omissis elemento che avrebbe dovuto imporre controlli rafforzati ai sensi della normativa antiriciclaggio; importo rilevante: Euro 2.700,00 rappresentano una somma significativa per un correntista privato.
Qualsiasi banca dotata di sistemi di sicurezza adeguati avrebbe bloccato automaticamente questa operazione, richiedendo una verifica aggiuntiva al cliente prima di procedere all'esecuzione.
La BNL non lo ha fatto.
La giurisprudenza ha chiaramente affermato che "la banca ha l'obbligo di monitorare l'operatività dei conti correnti e di bloccare preventivamente le operazioni anomale rispetto alle abitudini del correntista"(cfr. Trib. Milano, sentenza n. 5967/2022; Trib. Roma, sentenza n. 16478/2022)"
Nel caso che ci occupa vi è la responsabilità della Banca oltre che per non aver adempiuto all'onere probatorio posto a suo carico in ordine all'adozione di misure atte a prevenire frodi informatiche e all'adeguatezza dei sistemi informatici, anche per non aver altresì "fornito la prova di alcuna specifica condotta dolosa o colposa del cliente alla quale possano ricondursi le operazioni disconosciute dal medesimo.
La BNL ha depositato in atti i cosiddetti "Log del cliente" e l'"SMS alert" , ritenendo evidentemente che questi documenti siano sufficienti a provare l'autorizzazione dell'operazione.
Nulla di più errato.
I log informatici dimostrano unicamente che l'operazione è stata eseguita utilizzando le credenziali del S Omissis li e il suo dispositivo mobile.
Ma questo è esattamente ciò che accade in ogni frode informatica basata su malware, ove il truffatore, una volta ottenuto il controllo del dispositivo della vittima, opera utilizzando le credenziali legittime carpite, facendo apparire l'operazione come se fosse stata autorizzata dal titolare.
Quanto agli SMS alert e alle notifiche push, la Banca sostiene che questi sarebbero stati inviati al Sig. Omissis lle ore 03:30, 04:46 e 05:02 del 2 maggio 2023, e che il cliente avrebbe potuto bloccare l'operazione se avesse prestato attenzione a tali comunicazioni.
Anche questa argomentazione è palesemente pretestuosa.

È la stessa Banca ad ammettere che il malware aveva assunto il controllo del dispositivo del ricorrente. Infatti, se il malware controllava il telefono, controllava anche le notifiche, potendo intercettarle, nasconderle o addirittura approvarle autonomamente senza che il Sig. Omissis fosse consapevole.

Ma vi è un elemento ancora più decisivo: le notifiche sono state inviate in piena notte, quando qualsiasi persona ragionevole si trova nel sonno. Pretendere che il cliente monitorasse il proprio smartphone alle ore 03:30 del mattino è una richiesta assurda e contraria al senso comune.

Sulla pretesa "colpa grave" del ricorrente: una costruzione artificiosa

Consapevole di non poter assolvere l'onere probatorio principale, la Banca tenta di invocare l'art. 12, comma 2, del D.Lgs. 11/2010, il quale prevede che l'utilizzatore risponda delle perdite derivanti da operazioni di pagamento non autorizzate in caso di dolo o colpa grave.

Secondo la resistente, il Sig. Omissis avrebbe agito con colpa grave perché si sarebbe collegato a un "sito illegale" per vedere una partita di calcio in streaming, avrebbe "consentito" l'installazione di un malware sul proprio dispositivo, avrebbe ignorato presunti segnali di pericolo.

Tuttavia la circostanza che il sito fosse “illegale” è una mera supposizione della Banca, che non ha fornita prova in questa sede.

In secondo luogo, il nesso causale tra la visione della partita e l'installazione del malware non è stato provato. La Banca assume che il trojan sia stato scaricato necessariamente dal sito di streaming, ma si tratta di una mera supposizione, anche questa priva di qualsiasi fondamento probatorio.

Invero, i malware possono essere veicolati attraverso molteplici canali: email di phishing, messaggi WhatsApp, pubblicità ingannevoli, applicazioni apparentemente legittime scaricate da siti ufficiali.

Peraltro, la Banca sostiene che il Sig. Omissis avrebbe "consentito" l'installazione del malware, come se si trattasse di una scelta consapevole e volontaria.

Questa ricostruzione non è provata.

Il malware si è presentato come un legittimo aggiornamento dell'applicazione Google Chrome, una delle app più diffuse e attendibili al mondo.

Il Sig. Omissis è stato ingannato da una sofisticata tecnica di social engineering, progettata specificamente per eludere la vigilanza dell'utente e bypassare i sistemi di sicurezza degli smartphone. Non si tratta di negligenza, ma di frode qualificata.

A riprova di ciò, il ricorrente ha immediatamente notato anomalie (icona di Chrome non conforme, richieste di autorizzazione sospette, impossibilità di disinstallare l'app) e ha tentato di rimuovere l'applicazione malevola.

Questo dimostra che il Sig Omissis ha agito con la diligenza che ci si può ragionevolmente attendere da un utente medio, senza competenze tecniche avanzate in ambito informatico.

Da ultimo, la resistente fa leva sul fatto che il Sig. Omissis avrebbe contattato la Banca solo il 4 maggio 2023, ossia due giorni dopo l'operazione fraudolenta del 2 maggio 2023.

Anche questa argomentazione è manifestamente pretestuosa.

Come già ampiamente dimostrato, le notifiche sono state inviate in orario notturno (tra le 03:30 e le 05:02), quando il ricorrente dormiva. È del tutto normale che il cliente non abbia verificato immediatamente il proprio smartphone in piena notte.

Inoltre, il malware aveva assunto il controllo del dispositivo, potendo quindi nascondere o manipolare le notifiche ricevute.

Peraltro, appena il ricorrente ha avuto il sospetto di essere stato vittima di frode, ha immediatamente contattato la Banca richiedendo l'estratto conto. Non vi è stato alcun ritardo colpevole.

Appare, comunque, opportuno precisare che l'operazione fraudolenta, si è consumato e/o concretizzato solo il 2 maggio, pertanto l'eventuale e lamentato ritardo nella segnalazione non è affatto dirimente in quanto non ha prodotto ulteriori danni.
Altro aspetto riguarda gli obblighi di vigilanza.
Il bonifico fraudolento è stato eseguito a favore di un conto corrente lituano (IBAN: I[illegible] intestato a Omissis , soggetto mai utilizzato in precedenza da Omissis come beneficiario.
In presenza di un bonifico transfrontaliero, la Banca è tenuta ad applicare misure di controllo rafforzate ai sensi della Direttiva UE 2018/843 (V Direttiva Antiriciclaggio), che prevede obblighi di adeguata verifica rafforzata per transazioni a rischio elevato, inclusi i bonifici verso paesi extra-UE o verso beneficiari nuovi e sconosciuti e dell'art. 7, commi 3, 4 e 5 lett a) del Regolamento UE 2015/847 (Regolamento sui trasferimenti di fondi), che impone agli intermediari finanziari di verificare l'identità del beneficiario e di monitorare le operazioni sospette, i quali stabiliscono "Nel caso di trasferimenti di fondi superiori a 1 000 euro , indipendentemente dal fatto che tali trasferimenti siano effettuati con una singola operazione o con più operazioni che sembrano collegate, prima di effettuare l'accredito sul conto di pagamento del beneficiario o di mettere a sua disposizione i fondi, il prestatore di servizi di pagamento del beneficiario verifica l'accuratezza dei dati informativi relativi al beneficiario basandosi su documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente, fatti salvi gli obblighi previsti dagli articoli 69 e 70 della direttiva 2007/64/CE."
Nel caso di specie, la BNL ha eseguito il bonifico senza alcuna verifica aggiuntiva, nonostante l'evidente anomalia dell'operazione.
Tanto basta a costituisce una grave violazione degli obblighi di vigilanza imposti dalla normativa europea e rappresenta un'ulteriore prova dell'inadeguatezza dei sistemi di sicurezza implementati dalla resistente. Inoltre la Banca non ha contestato la domanda nella propria comparsa di costituzione, limitandosi a sostenere genericamente che "l'evento dannoso non è imputabile alla condotta della Banca ma esclusivamente alla negligenza del Sig. Omissis
Ciò non fa che confermare l'inadempimento della BNL agli obblighi previsti dal GDPR.
L'art. 32 GDPR impone al titolare del trattamento di "mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" e l'art. 34 stabilisce che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo", fatti salvi i casi in cui tale comunicazione non è richiesta in quanto risulta essere soddisfatta una delle condizioni previste al par. 3 del medesimo articolo, non applicabile al caso in specie in quanto il soggetto leso è uno solo.
Nel caso di specie, è pacifico che i dati personali e finanziari del Sig Omissis (credenziali di accesso, password, informazioni bancarie) sono stati sottratti da terzi non autorizzati.
Ai sensi dell'art. 82 GDPR, "chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento".
Il Regolamento prevede un sistema di responsabilità oggettiva, secondo cui il titolare è esonerato solo se prova "che l'evento dannoso non gli è in alcun modo imputabile".
La giurisprudenza di legittimità ha ripartito l'onere della prova nelle controversie fondate su tale titolo di responsabilità secondo i criteri prescritti dall'art. 15 del D.Lgs. 196/2003, il quale dispone che "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile", con la possibilità per l'istituto di credito di offrire prova liberatoria dalla propria responsabilità dimostrando di aver

adottato tutte le misure idonee ad evitare il danno secondo le conoscenze acquisite in base al progresso tecnico, alla natura dei dati, alle caratteristiche specifiche del trattamento, mediante adozione di misure idonee e preventive per impedire l'accesso o il trattamento non autorizzato ai sensi dell'art. 31 e 36 del D.Lgs. 196/2003. Secondo la Cassazione, infatti, "in base al rinvio all'art. 2050 c.c., operato dall'art. 15 del codice della privacy, l'istituto che svolga un'attività di tipo finanziario o in generale creditizio risponde, quale titolare del trattamento di dati personali, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico del cliente mediante la captazione dei suoi codici di accesso e le conseguenti illegittime disposizioni di bonifico, se non prova che l'evento dannoso non gli è imputabile perché discendente da trascuratezza, errore (o frode) dell'interessato o da forza maggiore". La Cassazione ha, quindi, rilevato che ad analoga conclusione si perviene applicando le disposizioni del D.Lgs. 11/2010, applicabile anche nel presente giudizio. La normativa richiamata sancisce l'obbligo del prestatore del servizio di pagamento di assicurare che i dispostivi personalizzati forniti dai gestori non siano accessibili a soggetti diversi dal legittimo titolare e detta alcune disposizioni specificamente indirizzate a ripartire le responsabilità derivanti dall'utilizzazione del servizio stesso. In particolare, l'art. 8, comma 1, dispone che "Il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7 (che sono: utilizzare lo strumento di pagamento in conformità con i termini che ne regolano l'emissione e l'uso e comunicare senza indugio al prestatore di servizi di pagamento, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza). L'art. 10 prevede, inoltre, che, "qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti"; il comma 2 aggiunge che "quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente". La normativa in esame, quindi, prevede come regola generale una responsabilità dell'istituto di credito in caso di operazione non autorizzata dal cliente, a meno che questa non discenda dal dolo o dalla colpa grave del medesimo, con la precisazione che grava sull'operatore bancario l'onere di provare che l'illecita operatività ad opera di terzi, con riferimento alle disposizioni contestate, sia stata resa possibile dal dolo o dalla colpa grave del cliente. La Corte di Cassazione ha altresì precisato che "in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo" (Cass. n. 2950/2017; v. anche Cass. n. 10638/2016; Cass. n. 9158/2018 e, da

ultimo, Cass. n. 26916/2020 e, da ultimo, Cass. n. 1641/2022):
La Banca non ha fornito alcuna prova in tal senso. Al contrario, ha ammesso che il sistema di sicurezza è stato aggirato, confermando così l'inadeguatezza delle misure adottate.
La responsabilità della BNL ai sensi del GDPR è, pertanto, pienamente configurata.
Quanto alla richiesta di condanna ex art. 12 bis d.lgs. 28/2010 in riferimento all'eccezione di parte resistente che la stessa possa essere formalizzata solo nei confronti della parte soccombente e che, essendo le domande attoree "assolutamente infondate", la BNL non sarà soccombente. Questa obiezione è infondata.
L'art. 12 bis, comma 3, D.Lgs. 28/2010 prevede testualmente che il giudice "nel dare atto del mancato espletamento del procedimento, condanna la parte costituita che, nei casi previsti dall'articolo 5, non ha partecipato al procedimento senza giustificato motivo.
La norma non subordina la condanna alla soccombenza nel merito, ma alla sola mancata partecipazione ingiustificata alla mediazione.
La finalità della disposizione è quella di sanzionare il comportamento non collaborativo della parte, a prescindere dall'esito del giudizio.
Nel caso di specie, la Banca non ha partecipato alla mediazione, né ha fornito alcuna giustificazione per tale comportamento.
Pertanto si condanna parte resistente al pagamento in favore del S Omissis i, di una somma equitativamente determinata in euro 500,00.
Le spese legali seguono la soccombenza e sono liquidate come in dispositivo.

P.Q.M.

Il Giudice di Pace, definitivamente pronunciando

Dichiara la responsabilità di Banca Nazionale del Lavoro S.p.A. e per l'effetto, condannare la resistente alla restituzione, in favore del ricorrente, della somma complessiva di € 2.700,00, oltre interessi legali e la rivalutazione monetaria, dal dì del dovuto all'effettivo soddisfo.

Condanna parte resistente al pagamento di euro 500,00 equitativamente stabilite ai sensi dell'art. 12 bis comma 3 D.lgs. 28/2010 a favore di parte ricorrente.

Condanna parte resistente al pagamento delle spese legali in favore di parte ricorrente in euro 1.500,00 oltre spese generali forfettarie nella misura del 15% sui compensi oltre iva e cap come per legge.

Così deciso in EMPOLI il 18-03-2026

Il Giudice di Pace

Dott. MARIA DORA LANEVE