DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

La responsabilità della banca per frodi nei servizi di pagamento

Settembre 2026

Margherita Domenegotti, Partner, La Scala Società tra Avvocati
Jessica Cammarano, Managing Associate, La Scala Società tra Avvocati
Chiara Gennaro, Managing Associate, La Scala Società tra Avvocati

Margherita Domenegotti, Partner, La Scala Società tra Avvocati

Jessica Cammarano, Managing Associate, La Scala Società tra Avvocati

Chiara Gennaro, Managing Associate, La Scala Società tra Avvocati

Margherita Domenegotti

Margherita Domenegotti è Partner dal 2017 di La Scala Società tra Avvocati. Dal 2021 è Membro del Consiglio di Amministrazione di La Scala Cerved Società tra Avvocati, realtà specializzata nella gestione giudiziale e stragiudiziale dei crediti di origine bancaria. Assiste primari istituti di credito occupandosi principalmente di diritto bancario, con specializzazione sugli aspetti di gestione del credito. È altresì esperta di procedure esecutive immobiliari e mobiliari, che segue in ogni loro fase. Si occupa della valutazione, gestione individuale, recupero stragiudiziale e giudiziale dei crediti, con particolare riguardo a mutui ipotecari e fondiari, crediti bancari, crediti al consumo e leasing.

1. Introduzione. Le frodi informatiche come banco di prova della disciplina dei servizi di pagamento

L'incremento delle frodi informatiche rappresenta uno dei principali fattori di trasformazione del diritto dei servizi di pagamento. La progressiva digitalizzazione dell'operatività bancaria, l'affermazione dei canali di home banking e mobile banking e la diffusione dei bonifici istantanei hanno certamente accresciuto l'efficienza del sistema dei pagamenti, ma hanno contestualmente ampliato l'esposizione degli intermediari e degli utenti a fenomeni criminali sempre più sofisticati.

La casistica giudiziaria degli ultimi anni evidenzia come il contenzioso non riguardi più esclusivamente l'indebito utilizzo di carte di pagamento o la sottrazione materiale delle credenziali di accesso. Le controversie investono sempre più frequentemente bonifici disposti mediante piattaforme di internet banking all'esito di attacchi di phishing, vishing, smishing o, soprattutto, di infezioni da malware e trojan bancari, idonei ad alterare il funzionamento del dispositivo dell'utente ovvero ad acquisire il controllo dell'intera sessione telematica.

L'evoluzione delle tecniche fraudolente pone interrogativi che trascendono il singolo episodio di illecito e investono la struttura stessa della disciplina dei servizi di pagamento. Il tema non riguarda soltanto la ripartizione del rischio economico tra intermediario e cliente, ma coinvolge la funzione dell'autenticazione forte, il contenuto dell'onere probatorio gravante sul prestatore di servizi di pagamento e, più in generale, il significato da attribuire al concetto di sicurezza nell'attuale ecosistema digitale.

È in questo contesto che si collocano le più recenti pronunce della Corte di Cassazione[1], gli orientamenti dell'Arbitro Bancario Finanziario[2] e alcune significative decisioni della giurisprudenza di merito,

1 Tra le tante, si citano: Cass. sent. n. 2950/2017, Cass. sent. n. 10638/2016, Cass. sent. n. 9158/2018, Cass. sent. n. 26916/2020, Cass. sent. n. 16417/2022, Cass. ordinanza n. 29852/2023, Cass. sent. n. 3780 del 12/02/2024. In particolare, secondo quest'ultima pronuncia: *"essendo la possibilità della sottrazione dei codici al correntista attraverso tecniche fraudolente una eventualità rientrante nel rischio d'impresa, la banca per liberarsi dalla propria responsabilità, deve dimostrare la sopravvenienza di eventi che si collochino al di là dello sforzo diligente richiesto al debitore"*.

2 *Ex multis* si annoverano: Collegio ABF di Milano n. 3501/2025, Collegio ABF di Milano n. 8204/2025; Collegio ABF di Torino n. 8642/2925; Collegio ABF di Napoli n. 772/2026, Collegio ABF di Roma n. 1004/2026, e la recentissima decisione del Collegio ABF di Roma n. 8175 del 9/09/2026 secondo la quale *"la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La*

vedi l'articolo online

accomunate dall'esigenza di verificare se l'adozione di procedure formalmente conformi alla disciplina della Strong Customer Authentication (SCA) sia sufficiente ad escludere la responsabilità dell'intermediario oppure se la valutazione debba estendersi all'intero apparato organizzativo predisposto per prevenire le frodi.

Partendo dall'analisi della più recente evoluzione giurisprudenziale, non emerge un ampliamento dell'ambito della responsabilità bancaria in termini oggettivi, bensì la modifica dell'oggetto dell'accertamento giudiziale. Il giudizio non si concentra più esclusivamente sulla correttezza tecnica dell'autenticazione dell'operazione, ma investe la complessiva adeguatezza del sistema di sicurezza predisposto dal prestatore di servizi di pagamento.

In tale prospettiva, la crescente sofisticazione dei malware bancari ha determinato una progressiva separazione tra autenticazione e autorizzazione, imponendo una rilettura dell'art. 10 del D.Lgs. 27 gennaio 2010, n. 11 alla luce della concreta capacità preventiva degli strumenti di *fraud detection*.

2. Il paradigma della PSD2: autenticazione forte e ripartizione del rischio

La Direttiva (UE) 2015/2366 (PSD2), recepita nell'ordinamento italiano mediante il D.Lgs. 15 dicembre 2017, n. 218, ha profondamente modificato la disciplina dei servizi di pagamento perseguendo due obiettivi strettamente connessi: l'incremento della sicurezza delle operazioni elettroniche e la promozione dell'innovazione nel mercato dei pagamenti.

L'elemento maggiormente innovativo della riforma è rappresentato dall'introduzione dell'obbligo di Strong Customer Authentication (SCA), disciplinato dagli artt. 97 e ss. della Direttiva e specificato dal Regolamento delegato (UE) 2018/389 della Commissione.

L'autenticazione forte (Strong Customer Authentication – SCA) si basa sull'impiego combinato di almeno due fattori di autenticazione tra loro indipendenti, appartenenti a tre distinte categorie: conoscenza, possesso e inerenza. Ai fini dell'autorizzazione di un pagamento o dell'accesso a un servizio di pagamento, il sistema deve verificare che l'utente fornisca almeno due elementi riconducibili a categorie differenti, così da garantire un livello di sicurezza più elevato. In particolare, i fattori di autenticazione possono consistere in:

- **conoscenza**, ossia un elemento noto esclusivamente all'utente, quale una password, un codice PIN o la risposta a una domanda di sicurezza;
- **possesso**, vale a dire un elemento detenuto dall'utente, come uno smartphone, un token hardware, una smart card o un codice OTP (One-Time Password) ricevuto tramite SMS;
- **inerenza**, cioè una caratteristica biometrica dell'utente, quale l'impronta digitale, il riconoscimento facciale o la scansione dell'iride.

L'obiettivo perseguito non consiste soltanto nell'identificazione dell'utilizzatore, ma nella riduzione del rischio sistemico delle frodi informatiche attraverso l'innalzamento degli standard minimi di sicurezza richiesti agli intermediari.

L'introduzione della Strong Customer Authentication non ha tuttavia modificato il criterio fondamentale di allocazione del rischio delineato dalla disciplina dei servizi di pagamento.

Il sistema continua, infatti, a fondarsi su una rigorosa distribuzione dell'onere della prova tra utilizzatore e prestatore dei servizi di pagamento, profilo sotto il quale assumono rilievo decisivo gli artt. 10 e 10-bis del D.Lgs. n. 11/2010.

L'art. 10 stabilisce che, qualora l'utilizzatore neghi di aver autorizzato un'operazione di pagamento già eseguita ovvero sostenga che essa sia stata effettuata in modo inesatto, incombe sul prestatore di servizi di pagamento l'onere di dimostrare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione.

La disposizione assume importanza centrale poiché individua l'oggetto della prova richiesta all'intermediario: il legislatore non si limita a richiedere la dimostrazione della regolare esecuzione tecnica dell'operazione, pretende altresì che il prestatore dimostri l'affidabilità del proprio sistema organizza-

prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente."

tivo, escludendo malfunzionamenti o anomalie che possano avere inciso sulla genesi dell'operazione contestata.

3. La crisi della coincidenza tra autenticazione e autorizzazione

Per comprendere la più recente evoluzione giurisprudenziale è necessario soffermarsi su un presupposto implicito dell'intero impianto normativo della PSD2.

Per lungo tempo, il corretto superamento della procedura di autenticazione è stato considerato un indice particolarmente significativo della volontà del cliente. Se l'operazione risultava eseguita con le credenziali corrette e mediante i fattori di sicurezza previsti, essa veniva normalmente ricondotta all'utilizzatore.

L'evoluzione delle frodi informatiche ha, però, incrinato questa ricostruzione.

Se in passato le principali forme di illecito consistevano nella sottrazione delle credenziali, nel furto dello strumento di pagamento o nell'acquisizione fraudolenta dei codici dispositivi mediante semplici tecniche di phishing, oggi le minacce sono rappresentate da malware bancari di nuova generazione che non mirano necessariamente ad aggirare i sistemi di autenticazione, ma anzi, sempre più spesso, li utilizzano. Si insediano nel dispositivo del cliente, intercettano codici, alterano interfacce, manipolano notifiche e consentono l'esecuzione di transazioni apparentemente regolari, perché fondate su credenziali autentiche.

Ne deriva una separazione concettuale ormai centrale: l'autenticazione attiene alla correttezza della procedura tecnica con cui il sistema identifica l'utente; l'autorizzazione riguarda, invece, la riferibilità dell'operazione a una volontà libera, consapevole ed effettiva del cliente. Le due nozioni, nell'era del malware, non coincidono necessariamente.

È proprio questa dissociazione a spiegare il progressivo spostamento dell'accertamento giudiziale: non basta più chiedersi se la SCA abbia funzionato; occorre verificare se l'intero sistema di sicurezza fosse concretamente idoneo a prevenire, intercettare o bloccare un'operazione anomala.

Deve essere chiaramente distinta la verifica della regolarità tecnica del pagamento dalla dimostrazione della sua effettiva riferibilità al cliente: l'utilizzo delle corrette credenziali dimostra esclusivamente che il sistema di autenticazione ha funzionato secondo le modalità previste, ma non prova necessariamente che l'operazione sia stata voluta da cliente.

La differenza, apparentemente sottile, assume oggi un rilievo decisivo, poiché, come anticipato, i malware bancari di ultima generazione sono progettati proprio per utilizzare credenziali autentiche.

In tale prospettiva cambia anche il contenuto della prova richiesta all'intermediario: non è più sufficiente produrre i log informatici attestanti l'avvenuta autenticazione, ma occorre dimostrare che l'operazione, considerata nel suo complesso, non presenti elementi incompatibili con il normale comportamento del cliente e che il sistema predisposto dall'intermediario fosse concretamente idoneo ad intercettare eventuali anomalie.

4. L'evoluzione della giurisprudenza di legittimità: dall'attività pericolosa all'onere della prova dell'intermediario

L'evoluzione della giurisprudenza della Corte di Cassazione in materia di operazioni di pagamento fraudolente è stata talvolta ricostruita come il passaggio da un orientamento fortemente protettivo dell'utilizzatore con conseguente responsabilità oggettiva in capo alla Banca (Cassazione nn. 10638/2016, 2950/2017 e 9158/2018) ad un approccio maggiormente attento alla condotta del cliente (cfr. *ex multis* Cassazione ordinanza n. 7241/2023, Cassazione n. 3780/2024). Una simile lettura, tuttavia, rischia di semplificare eccessivamente un percorso interpretativo assai più articolato.

L'elemento di continuità che attraversa la giurisprudenza di legittimità non è rappresentato dall'individuazione del soggetto destinato a sopportare il rischio economico della frode, bensì dalla costante valorizzazione della particolare posizione professionale dell'intermediario e del conseguente contenuto del suo obbligo di diligenza.

Le pronunce rese negli anni successivi all'entrata in vigore della prima Direttiva sui servizi di pagamento hanno progressivamente affermato che l'attività bancaria esercitata mediante strumenti elettronici integra un'attività caratterizzata da un elevato rischio tecnologico e che tale rischio, proprio in ragione

della professionalità dell'intermediario, non può essere trasferito automaticamente sull'utilizzatore.[3]

In questa prospettiva la Corte ha ricondotto la responsabilità dell'intermediario nell'ambito dell'art. 2050 c.c., affermando che grava sulla banca l'onere di dimostrare di avere adottato tutte le misure tecnicamente idonee ad evitare il danno.[4]

L'importanza di tale orientamento è duplice.

Da un lato, esso colloca il rischio tecnologico nell'ambito dell'organizzazione imprenditoriale dell'intermediario; dall'altro, impedisce che il semplice verificarsi dell'evento fraudolento possa essere imputato al cliente sulla sola base dell'utilizzo delle sue credenziali di autenticazione.

Ciò non significa, tuttavia, configurare una responsabilità oggettiva dell'intermediario. La banca può andare esente da responsabilità, ma deve dimostrare di avere adottato tutte le misure tecniche, organizzative e procedurali idonee a evitare il danno. In questa prospettiva, l'art. 10 del D.Lgs. n. 11/2010 diventa la norma cardine: non impone soltanto la prova della regolarità del pagamento, ma dell'affidabilità complessiva del sistema predisposto dal prestatore.

Le pronunce recenti valorizzano anche la condotta dell'utilizzatore, escludendo la responsabilità dell'intermediario quando sia provata una grave negligenza del cliente nella custodia delle credenziali, nella comunicazione dei codici o nella tempestiva denuncia dell'uso non autorizzato (Cass. civ., Sez. I, 13.03.2023, n. 7214; Cass. Civ. 8.11.2023, n. 31136; Tribunale di Catania, sentenza n. 1472/2026 del 23.03.2026).

È evidente, infatti, che la valorizzazione degli obblighi organizzativi dell'intermediario non elimina il ruolo della condotta dell'utente. Il sistema dei servizi di pagamento resta fondato su una cooperazione tra banca e cliente: l'utilizzatore deve agire diligentemente e adottare comportamenti prudenti.

Dall'altra parte è innegabile che l'evoluzione delle tecniche di social engineering impone cautela. La colpa grave dell'utilizzatore non può essere desunta dal semplice fatto che lo stesso sia stato raggirato. Occorre verificare se la condotta dell'utente presenti caratteri di macroscopica imprudenza, tali da interrompere il nesso causale tra il rischio professionale dell'intermediario e il danno.

Gli orientamenti richiamati confermano questa impostazione: la responsabilità della banca è stata esclusa nei casi in cui il cliente abbia fattivamente e incautamente cooperato alla frode, ad esempio comunicando credenziali o codici dispositivi a terzi, conservando impropriamente il PIN o denunciando tardivamente l'evento. Al contrario, la responsabilità dell'intermediario è stata affermata in presenza di presidi di sicurezza inadeguati o di truffe particolarmente sofisticate, difficilmente riconoscibili dall'utente medio.

Tuttavia, l'accertamento sulla condotta del cliente non sostituisce quello sull'adeguatezza del sistema bancario: le due verifiche restano autonome e complementari: l'adozione di un sistema SCA costituisce il requisito minimo imposto dalla normativa, ma non esaurisce gli obblighi di diligenza qualificata gravanti sull'intermediario ai sensi dell'art. 1176, comma 2, c.c., specie in presenza di operazioni che presentino indici di anomalia oggettivamente rilevabili (Cass. Civ., Sez. III, ord. 3 novembre 2023, n. 30588; Cass. Civ., Sez. III, ord. 4 dicembre 2024, n. 31052; Trib. Chieti sentenza 247/2026 del 10.06.2026).

La difficoltà sta proprio nel tracciare il confine: non ogni errore dell'utente è colpa grave; non ogni autenticazione regolare è prova di autorizzazione; non ogni frode riuscita è automaticamente imputabile alla banca. Il giudizio resta, inevitabilmente, legato al caso concreto.

Sul punto, ad esempio, l'Arbitro Bancario Finanziario ha contribuito in modo significativo a delineare i

3 Tra le tante è sicuramente degna di nota la già citata Cassazione n. 2950 del 3 febbraio 2017: *"Ne discende che, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema (ciò che rappresenta interesse degli stessi operatori), appare del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore di 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 da parte di terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo".*

4 Emblematica in tal senso è Cassazione n. 10638 del 23/05/2016: *"In tema di ripartizione dell'onere della prova, al correntista abilitato a svolgere operazioni "on line" che, alla stregua degli artt. 15 del d.lgs. n. 196 del 2003 e 2050 c.c., agisca per l'abusiva utilizzazione (nella specie, mediante illegittime disposizioni di bonifico) delle sue credenziali informatiche, spetta soltanto la prova del danno siccome riferibile al trattamento del suo dato personale, mentre l'istituto creditizio risponde, quale titolare del trattamento di dato, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico mediante la captazione dei codici d'accesso del correntista, ove non dimostri che l'evento dannoso non gli sia imputabile perché discendente da trascuratezza, errore o frode del correntista o da forza maggiore."*

contorni dell'onere probatorio gravante sull'intermediario. Dall'elaborazione arbitrale emerge con chiarezza che l'autenticazione rappresenta solo uno degli elementi necessari per escludere la responsabilità del prestatore di servizi di pagamento.

Particolarmente rilevante, sul punto, è la decisione ABF Napoli n. 772 del 28 gennaio 2026, relativa al disconoscimento di bonifici istantanei. In quel caso, il Collegio ha ribadito che la responsabilità del prestatore può essere esclusa solo se quest'ultimo dimostra l'adozione di un sistema di autenticazione forte conforme alla normativa e gli ulteriori presupposti richiesti dalla disciplina speciale, non essendo sufficiente la mera regolarità tecnica dell'operazione.

La decisione è significativa anche per un altro profilo: nel caso concreto, l'intermediario non aveva fornito prova dell'effettiva implementazione del sistema di autenticazione forte. Tale mancanza è stata ritenuta di per sé sufficiente ad accogliere il ricorso del cliente.

Nello stesso senso, anche la recentissima decisione resa dal Collegio ABF di Roma in data 9 settembre 2026, in base alla quale: "*la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un* prius *logico rispetto alla prova della colpa grave dell'utente. Il ricorso dunque merita di essere accolto*"

Il principio che se ne ricava è che la conformità alla SCA non si presume. Essa costituisce un fatto da provare, e non esaurisce comunque la valutazione della diligenza professionale dell'intermediario (conformi anche, tra le tante, ABF Collegio di Milano n. 8204 del 12 settembre 2025 e ABF Collegio di Milano n. 8572 del 29 settembre 2025).

5. La prova tecnica e la prova della volontà del cliente

L'analisi coordinata della giurisprudenza di legittimità e degli orientamenti dell'ABF consente di cogliere un elemento che appare destinato a caratterizzare il futuro contenzioso in materia di bonifici fraudolenti.

La prova dell'intermediario tende progressivamente a scomporsi in due piani distinti.

Il primo riguarda la prova tecnica dell'operazione.

Essa comprende la documentazione relativa ai log di accesso, ai codici OTP, ai sistemi di Strong Customer Authentication, alle registrazioni informatiche e alle evidenze tecniche del pagamento.

Il secondo riguarda invece la prova sostanziale della riconducibilità dell'operazione alla libera volontà del cliente.

È su questo secondo profilo che emergono le più rilevanti difficoltà sul piano probatorio. I malware bancari di nuova generazione sono infatti in grado di riprodurre fedelmente i tratti di un›operazione apparentemente legittima: il sistema registra un impiego corretto delle credenziali, genera log privi di anomalie e documenta il positivo completamento delle procedure di autenticazione. Tali elementi, tuttavia, non escludono che l›operazione sia stata eseguita in assenza di una reale volontà dispositiva del cliente.

La conseguenza è rilevante.

La documentazione tecnica prodotta dall'intermediario continua ad essere necessaria, ma non appare più sufficiente: essa dimostra che il pagamento è transitato correttamente attraverso il sistema informatico, ma non dimostra, da sola, che il sistema fosse immune da vulnerabilità né che il cliente abbia espresso una volontà negoziale libera e consapevole.

È in questa prospettiva che acquistano rilievo crescente le più recenti pronunce della giurisprudenza di merito, chiamate ad affrontare casi nei quali il corretto funzionamento della Strong Customer Authentication coesiste con la presenza di sofisticati attacchi malware.

Saranno proprio tali decisioni a mostrare come l'oggetto dell'accertamento giudiziale si stia progressivamente spostando dalla verifica della correttezza dell'autenticazione alla valutazione dell'effettiva capacità preventiva dell'intero sistema di sicurezza predisposto dall'intermediario.

vedi l'articolo online

6. Il caso Empoli: malware, bonifico fraudolento e vigilanza attiva

La decisione del Giudice di Pace di Empoli del 19.03.2026 n. 32 si inserisce in questo percorso evolutivo e ne rappresentano una significativa applicazione ai casi di frode mediante malware. La vicenda esaminata riguarda un bonifico fraudolento eseguito attraverso un trojan bancario, capace di consentire a terzi il controllo del dispositivo del cliente e di superare i meccanismi di autenticazione.

Il dato centrale non è l'introduzione di un nuovo principio di diritto, bensì l'applicazione rigorosa dell'art. 10 del D.Lgs. n. 11/2010. La banca, per andare esente da responsabilità, non può limitarsi a provare che l'operazione sia stata tecnicamente autenticata: deve dimostrare l'affidabilità complessiva del sistema di pagamento e la sua concreta idoneità a fronteggiare il rischio di frodi evolute.

Il malware, infatti, opera proprio attraverso credenziali autentiche. La correttezza dei log informatici costituisce, in questi casi, il normale effetto del meccanismo fraudolento e non necessariamente la prova della volontà dispositiva del cliente.

La pronuncia assume, inoltre, rilievo per il riferimento agli indicatori di anomalia dell'operazione: orario inconsueto, beneficiario nuovo, IBAN estero, importo rilevante rispetto all'ordinaria operatività del cliente. Tali elementi avrebbero dovuto indurre l'intermediario ad attivare controlli supplementari o a bloccare cautelativamente l'operazione.

È qui che emerge il passaggio dalla sicurezza "passiva" alla sicurezza "attiva": non basta più predisporre credenziali, OTP e notifiche; occorre monitorare il comportamento operativo del cliente, individuare scostamenti anomali e reagire tempestivamente.

In quest'ottica, l'aspetto più innovativo dell'evoluzione in atto riguarda la crescente centralità dei sistemi di cd. *fraud detection*. Per anni, il parametro principale di valutazione dell'operato dell'intermediario è stato rappresentato dalla conformità della procedura di autenticazione ai requisiti normativi. Oggi, la sofisticazione degli attacchi informatici mostra che tale parametro, pur necessario, non è più sufficiente.

La banca dispone di informazioni che il cliente non possiede: storico delle operazioni, ricorrenza dei beneficiari, importi abituali, orari di disposizione, localizzazione, caratteristiche del dispositivo, frequenza e tipologia delle transazioni. La disponibilità di tali dati rende sempre più difficile sostenere che essi siano irrilevanti ai fini della diligenza professionale.

La sicurezza dei pagamenti non coincide più soltanto con la capacità di identificare il cliente, ma comprende anche la capacità di riconoscere operazioni incompatibili con il suo ordinario profilo operativo. In questa prospettiva, la diligenza dell'intermediario, valutata ai sensi dell'art. 1176, comma 2, c.c., assume un contenuto dinamico: cresce con l'evoluzione delle tecnologie disponibili e delle migliori pratiche del settore.

7. La dimensione privacy della frode: gli artt. 24, 32 e 82 GDPR come ulteriori parametri di responsabilità

Un profilo particolarmente interessante emerso nella più recente giurisprudenza riguarda il progressivo dialogo tra la disciplina dei servizi di pagamento e la normativa in materia di protezione dei dati personali. La vicenda esaminata dal Giudice di Pace di Empoli non è stata infatti letta esclusivamente attraverso la lente del D.Lgs. n. 11/2010 e della PSD2, ma anche alla luce degli obblighi che gravano sugli intermediari quali titolari del trattamento dei dati personali dei propri clienti.

La decisione richiama espressamente gli articoli 32 e 82 del Regolamento (UE) 2016/679 (GDPR), valorizzando il fatto che la compromissione delle credenziali bancarie e l'esecuzione del bonifico fraudolento costituiscono un problema di sicurezza sia dei pagamenti che del trattamento dei dati personali.

In questa prospettiva assume anzitutto rilievo l'art. 24 GDPR, che impone al titolare del trattamento di adottare misure tecniche e organizzative adeguate a garantire e dimostrare che il trattamento sia effettuato conformemente al Regolamento. Sebbene la disposizione non individui specifici standard tecnologici, essa impone un obbligo di accountability che richiede una valutazione continua dei rischi e l'adeguamento delle misure di sicurezza all'evoluzione delle minacce informatiche. Nel settore bancario, caratterizzato da un elevato livello di digitalizzazione e da un costante incremento delle frodi informatiche, tale obbligo tende inevitabilmente ad assumere una particolare intensità.

Ancora più centrale è l'art. 32 GDPR, che impone al titolare e al responsabile del trattamento di adottare

misure tecniche e organizzative adeguate al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura dei dati trattati e delle probabilità e gravità dei rischi per i diritti e le libertà degli interessati. Nel contesto dei servizi di pagamento, tale disposizione si traduce nell'esigenza di predisporre non soltanto sistemi di autenticazione robusti, ma anche strumenti di monitoraggio, rilevazione delle anomalie, gestione degli incidenti e prevenzione delle intrusioni informatiche.

È significativo che il Giudice di Pace di Empoli abbia ritenuto che l'efficace azione del malware e la conseguente sottrazione delle credenziali rappresentassero un indice dell'inadeguatezza delle misure di sicurezza predisposte dall'istituto di credito rispetto ai rischi concretamente esistenti. In tale ottica, la vulnerabilità del sistema informatico non rileva soltanto come possibile malfunzionamento della procedura di pagamento ai sensi dell'art. 10 del D.Lgs. n. 11/2010, ma anche come possibile inadempimento degli obblighi di sicurezza imposti dal GDPR.

Completa il quadro l'art. 82 GDPR, che riconosce all'interessato il diritto di ottenere il risarcimento del danno materiale o immateriale subito in conseguenza di una violazione del Regolamento. La disposizione introduce una forma di responsabilità particolarmente incisiva, dalla quale il titolare può liberarsi soltanto dimostrando che l'evento dannoso non gli è in alcun modo imputabile. Nel contesto delle frodi bancarie informatiche, ciò apre uno spazio ulteriore di tutela per il cliente, che può affiancare ai rimedi restitutori previsti dalla disciplina dei servizi di pagamento le pretese risarcitorie derivanti dall'eventuale inadeguatezza delle misure di sicurezza adottate dall'intermediario.

L'interazione tra PSD2 e GDPR appare quindi destinata ad assumere un ruolo crescente nel contenzioso relativo ai bonifici fraudolenti. Se la disciplina dei servizi di pagamento è tradizionalmente orientata alla ripartizione del rischio economico dell'operazione non autorizzata, la normativa privacy introduce una prospettiva ulteriore, concentrata sulla capacità dell'intermediario di proteggere dati, credenziali e identità digitale del cliente. Il risultato è una progressiva convergenza tra obblighi di sicurezza bancaria e obblighi di sicurezza del trattamento, entrambi valutati alla luce di un parametro comune: l'adeguatezza concreta delle misure predisposte rispetto all'evoluzione delle minacce informatiche.

8. I dati di Banca d'Italia e la spinta verso la prevenzione

Il Rapporto Banca d'Italia sulle operazioni di pagamento fraudolente relativo al secondo semestre 2025, pubblicato il 20 luglio 2026 conferma la rilevanza sistemica del fenomeno dei pagamenti fraudolenti. Le frodi sui bonifici, infatti, continuano a presentare importi medi elevati e le frodi da manipolazione del pagatore rappresentano una componente largamente significativa del valore complessivo dei bonifici fraudolenti.

Il Rapporto segnala inoltre il ruolo dei bonifici istantanei, caratterizzati da una maggiore esposizione al rischio rispetto ai bonifici ordinari, sebbene in riduzione anche per effetto del rafforzamento delle misure di prevenzione e dell'introduzione della Verification of Payee prevista dalla nuova normativa europea sui pagamenti istantanei.

In tale prospettiva, la prevenzione assume un ruolo sempre più centrale rispetto alla successiva riparazione del danno.

9. Considerazioni conclusive

L'evoluzione normativa, arbitrale e giurisprudenziale consente di formulare una conclusione di fondo: è in corso una ridefinizione del contenuto della diligenza richiesta all'intermediario.

La Strong Customer Authentication resta un presidio essenziale e imprescindibile. Tuttavia, non può più essere considerata l'unico parametro di valutazione della sicurezza. L'esperienza dei malware bancari dimostra che un'operazione può essere perfettamente autenticata e, nondimeno, non realmente autorizzata dal cliente.

Da questa dissociazione deriva l'ampliamento dell'onere probatorio dell'intermediario: la banca non è chiamata soltanto a provare il corretto funzionamento della procedura di autenticazione, ma l'adeguatezza dell'intero ecosistema di sicurezza predisposto per prevenire la frode. In tale ecosistema rientrano la SCA, i sistemi di monitoraggio comportamentale, gli algoritmi di *fraud detection*, le procedure di rilevazione delle anomalie, la verifica della coerenza dell'operazione rispetto al profilo del cliente e, più in generale, tutte le misure che l'evoluzione tecnologica rende concretamente esigibili da un operatore

vedi l'articolo online

professionale.

È questa la vera direttrice dell'attuale contenzioso in materia di bonifici fraudolenti: il passaggio da una sicurezza meramente formale, misurata sulla regolarità dell'autenticazione, a una sicurezza sostanziale, valutata sulla concreta capacità del sistema bancario di prevenire, intercettare e neutralizzare la frode.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it