"*HOME BANKING*" E LA RESPONSABILITÀ DELL'ISTITUTO DI CREDITO: IL RECENTE ORIENTAMENTO DELLA SUPREMA CORTE

di MARIA FRANCESCA LUCENTE

Con la presente nota, si intende operare un'interessante ricostruzione del recente orientamento della giurisprudenza di legittimità in tema di responsabilità della banca per le operazioni elettroniche poste in essere abusivamente da terzi, a danno di clienti titolari di conti correnti e di carte di credito.

Nel caso di operazioni effettuate con strumenti elettronici (*home banking*), spetta all'istituto di credito verificare la riconducibilità delle stesse alla volontà del cliente. L'eventuale uso dei codici di accesso al sistema da parte dei terzi rientra nel rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure tecniche, volte a verificare la riferibilità delle operazioni suddette alla volontà del correntista. La banca non risponde del danno patito dal cliente, solo qualora dimostri che il fatto sia attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo[1].

Ciò è quanto statuito recentemente dalla Suprema Corte in un'ordinanza, la n. 9158 del 2018, la quale richiama un principio anche più volte ribadito dalla stessa Corte (si consideri Cass., sent. n. 2950/2017)[2], secondo cui è onere della banca fornire la prova della riconducibilità di ogni singola operazione al cliente, titolare del conto o della carta di credito. La diligenza richiesta alla banca nello svolgimento delle sue attività è una diligenza di

[1] Cass. Civ. Ordinanza n. 9158/2018.

[2] Si vedano *ex plurimus*: Cass. Civ. n. 2950/2017; Cass. Civ. n. 806/2016; Cass. Civ. N. 10638/2016; Cass. Civ. N. 13777/2007.

natura tecnico-professionale, parametrabile sullo stereotipo del c.d. "accorto banchiere".

Ma cos'è la "*Home Banking*"[3]?

L'Home Banking è un servizio utile e vantaggioso che la diffusione di Internet ha portato. **Grazie a questo sistema è possibile fare bonifici, accedere al proprio conto e fare altre operazioni da casa o dallo smartphone.** *Con Internet però sono arrivati anche gli hacker e i furbi della rete, che hanno messo a repentaglio la sicurezza dell'Home Banking. Oggi però si utilizzano i Token OTP, un metodo di sicurezza informatica efficiente, che ha ripristinato la situazione.* **Ogni persona ha un sistema che fornisce istantaneamente una password che può essere utilizzata una sola volta.** Questo codice è numerico o alfanumerico ed è sostanzialmente usa e getta, disponibile solo in quel momento. Questo sistema ha il vantaggio di non poter essere intercettato, di conseguenza non è possibile decrittare la password OTP e accedere al Home Bank. In sostanza quindi l'utente si collega al portale della banca, inserisce *id e password* personali, richiede la *password* OTP e inserisce il codice fornito sul portale. Ecco che allora viene reindirizzato al proprio conto bancario *online*.

Premesso ciò, è bene ribadire che i prestatori dei servizi di pagamento che forniscono gli strumenti di *home banking*, dispongono dei dati sensibili dei clienti, ed infatti trova piena applicazione il *Codice in materia di protezione dei dati personali*. In particolare, l'art. 15 prevede che chiunque cagioni un danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'**art. 2050 c.c.** (esercizio di attività pericolose). L'art.31 dello stesso Decreto, dispone che i dati personali oggetto di trattamento siano custoditi e controllati in modo da ridurre al minimo, **mediante l'adozione di idonee e preventive misure di sicurezza**, i rischi di distruzione o perdita

[3] Con la locuzione inglese *home banking* o *internet banking* (letteralmente "banca da casa"), in italiano telebanca o banca a domicilio, si definiscono quei servizi bancari che consentono al cliente di effettuare operazioni bancarie da casa o dall'ufficio, mediante collegamento telematico. Anche detta banca online o banca via internet, prevede che le operazioni bancarie siano effettuate dai clienti degli istituti di credito tramite una connessione remota con la propria banca, funzionalità resasi possibile con la nascita e lo sviluppo di internet e delle reti di telefonia cellulare.

dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Alla luce di quanto sopra, l'intermediario, quindi, ha l'obbligo di adottare degli accorgimenti adeguati a prevenire l'illecita captazione di dati, onde evitare accessi non autorizzati. L'adeguatezza dei sistemi impiegati dall'istituto di credito viene valutata avendo riguardo alle **conoscenze acquisite in base al progresso tecnico.** Qualora si verifichi un accesso non autorizzato o l'impiego dei dati raccolti per finalità non conformi alla legge, il gestore risponde *ex* art. 2050 c.c.. Si tratta di una forma di responsabilità oggettiva "aggravata", in cui il prestatore del servizio, per andare esente da responsabilità, non deve solo dimostrare di aver adottato tutte le misure idonee ad evitare il danno (cosiddetta "prova liberatoria"), ma è tenuto a fornire la prova positiva di una causa esterna. Può trattarsi di fatto naturale, di fatto del terzo o di fatto dello stesso danneggiato che, per imprevedibilità ed inevitabilità, sfugge alla sfera di controllo dell'esercente l'attività pericolosa[4].

Ciò non esclude che, nel caso di erogazione del servizio di *home banking*, la banca debba garantire uno *standard* di sicurezza adeguato nell'effettuazione dei pagamenti al fine di precludere l'accesso a soggetti non abilitati al sistema. La diligenza richiesta, in tale circostanza, come già sopra anticipato, ha natura tecnica e «*deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed* ***assumendo quindi come parametro la figura dell'accorto banchiere***».

A questo punto, rileva evidenziare che nell'ambito delle operazioni telematiche, prima richiamate, ricorrente è l'espressione "*phishing*[5]" con la quale si fa riferimento ad una truffa, operata tramite Internet, caratterizzata dall'invio di messaggi di posta elettronica mendaci, che imitano perfettamente la grafica di istituti di credito e postali. Tali e-mail inducono in errore l'utente, il quale ritiene di essere stato contattato dalla propria banca,

[4] Cfr. P.Perlingieri, Manuale di diritto civile, ESI, ed. 2018

[5] Il termine phishing è una variante di *fishing* (letteralmente "pescare" in lingua inglese, probabilmente influenzato da *phreaking* e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente. La parola può anche essere collegata al linguaggio leet, nel quale la lettera f è comunemente sostituita con ph. La teoria popolare è che si tratti di un portmanteau di *password harvesting*, è un esempio di pseudo-etimologia.

ignaro del fatto che l'e-mail incriminata, contiene un *link* che rinvia ad un sito-truffa, in apparenza del tutto simile all'originale. Lo scopo dei cyber-criminali, si sostanzia nel carpire le credenziali del correntista (*user id* e *password*), per poi impiegarle fraudolentemente, al fine di sottrarre liquidità.

Varie pronunce dell'ABF (Arbitro Bancario Finanziario) – organismo deputato a risolvere in via stragiudiziale le controversie insorte tra clienti e operatori finanziari – hanno statuito che sia gravemente colposa la condotta del correntista che inserisca le proprie credenziali, qualora l'e-mail truffaldina sia stata redatta con errori marchiani e lessico inadeguato, rendendo evidente lo scopo fraudolento. Parimenti, è responsabile il cliente che cada reiteratamente in errore, continuando ad inserire i propri dati di accesso in risposta a e-mail palesemente "false".

Tuttavia, al di là di tali casi, l'orientamento dominante è volto a tutelare il correntista e ad ascrivere la responsabilità alla banca, in quanto l'eventualità di sottrazione delle credenziali rientra nel rischio professionale dell'erogatore dei servizi di pagamento.

Ciò posto, a proposito dell'*onus probandi*, la giurisprudenza ritiene che «*la sottrazione dei codici del correntista, attraverso tecniche fraudolente, rientra nell'area del rischio di impresa, destinato ad essere fronteggiato attraverso l'adozione di misure che consentano di verificare, prima di dare corso all'operazione, se essa sia effettivamente attribuibile al cliente*».

Più in particolare, non è sufficiente che nell'eseguire l'operazione bancaria vengano inserite le credenziali per garantire la volontarietà dell'azione ma è necessario un *quid pluris* per consentire alla banca di acclarare l'effettiva volontà del correntista di dar luogo alla disposizione patrimoniale. Il D.Lgs. 11/2010, attuativo della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, all'art. 10 si occupa della "*prova di autenticazione ed esecuzione delle operazioni di pagamento*". In particolare, dispone che se il correntista (definito "utilizzatore di servizi di pagamento") nega di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dalla banca ("prestatore di servizi di pagamento" nel linguaggio del legislatore) non è di per sé sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento. La legge pone in

capo all'istituto di credito l'obbligo di risarcire il correntista truffato (art. 12, D.Lgs. 11/2010), il quale risponde personalmente della perdita subita sino a 150 euro. Se l'istituto di credito vuole andare esente da responsabilità, ha l'onere di dimostrare la legittimità dell'operazione *on line* non autorizzata e la violazione, da parte del cliente, degli obblighi nascenti dal contratto. In altri termini, deve provare che il fatto sia stato cagionato dalla condotta colposa del danneggiato.

Quali sono i rimedi a cui ricorrere per arginare i rischi connessi alla Home Banking?

Tra le misure che riducono i rischi legati alle operazioni telematiche della Home Banking, vi è l'OTP, ossia *One Time Password* , che consiste nella doppia autenticazione e nella conferma dell'operazione con un pin inviato tramite *sms* al titolare del conto**.** In particolare**, il sistema OTP più utilizzato è quello dei Token OTP.** Questo codice può essere fornito anche sul telefono cellulare o con un'apposita app, tuttavia il metodo più diffuso e sicuro è fornire all'utente un piccolo device, dotato di un minischermo LCD, il Token. Questo apparecchio è anche chiamato Ge.Co., ovvero Generatore di Codici. Si tratta di un dispositivo piccolo e pratico che permette, attivandolo semplicemente con un pulsante, di avere istantaneamente la password OTP di solito di 6 cifre.

Il Token al suo interno ha un quarzo che scandisce il tempo e un codice seriale identificativo preciso. **La banca sostanzialmente riconosce quel seriale, la temporizzazione e il conto a cui è collegato.** Il sistema della banca ha la stessa temporizzazione, di conseguenza il sistema online richiede in quel momento, per quel conto, quel codice preciso. Proprio per questo il codice è affidabile, ha una sicurezza molto elevata, anche perché è a disposizione solo fisicamente dell'utente che lo richiede. La password temporanea è praticamente inviolabile, non si può calcolarla e nemmeno tirare a indovinare, dal momento che trovare un codice di sei cifre vuol dire indovinare un numero preciso su un milione.

Concludendo, dal breve *excursus* condotto, deriva un importante corollario: nell'ambito dei pagamenti *online* è ragionevole l'affidamento, in termini di sicurezza, che il titolare di un conto corrente *online* ripone nel prestatore del servizio di pagamento,

dal momento che la riconducibilità alla volontà del cliente delle operazioni compiute mediante il servizio, rientra nel rischio d'impresa che il prestatore deve sopportare e fronteggiare, anticipando il potenziale utilizzo fraudolento dei codici segreti che autorizzano le suddette operazioni. Nonostante tale principio[6] rappresenti la base necessaria per una generale e diffusa fiducia degli utenti nella sicurezza dei sistemi di pagamento *online*, ciò non toglie, comunque, che il titolare del conto ha l'obbligo di custodire con diligenza i propri codici segreti, contribuendo così al mantenimento di un sistema di transazioni di denaro più sicuro.

[6] Trattasi del principio di diritto espresso dalla Suprema Corte di Cassazione in più pronunce, già ivi richiamate.