Il Fin-tech: ricerca e sviluppo tecnologico nella nuova tecno-finanza. Opportunità e nuovi rischi

Author : Maria Cristina Leone

Date : 25 Ottobre 2019

All’interno di una realtà tecnologica ormai globalizzata, l’attuale frontiera dell’economia vede l’utilizzo di nuovi strumenti e nuove modalità di fruizione dei servizi, che si vanno delineando sotto il nome di Fintech.

Cos’è il Fin-tech?

Viene considerato Fintech (abbreviazione di **Financial Technology**) qualsiasi innovazione tecnologica dei servizi finanziari, che utilizza soprattutto elementi di *tecnologia diffusa*, come ad esempio le App ed i software più complessi che si basano su Big data e Intelligenza Artificiale.

Il fintech è legato quindi a un diverso modello di sviluppo che vede come fulcro un sistema che lega A.I., Big data e tecnologia.

A livello internazionale i mercati finanziari hanno visto il progressivo surclassamento, accentuato dalla Brexit, del riferimento economico del polo londinese, che fino a pochi anni fa poteva considerarsi leader indiscusso, in favore delle potenze asiatiche rappresentate *in primis* da Hong Kong e Singapore, potenze che hanno fatto importanti investimenti negli ultimi anni in questo nuovo settore della tecnologia.

La Cina e l’Asia hanno investito in tecnologie che modificano e innovano fortemente le infrastrutture economiche. Il sistema infrastrutturale europeo, al contrario, fa fatica ad affrontare il cambiamento soprattutto in ambito bancario e perde, così, di competitività.

L’innovazione tecnologica cinese per il settore finanza rivoluziona il modello tradizionale di banca e sposta il modello di business non più sul processo ma sull’utente attraverso la ***user experience***.

La fruizione del servizio da parte dell’utente mediante l’uso di **device** diventa centrale.

L’utente ha la possibilità di controllare in tempo reale la propria posizione bancaria, può effettuare modifiche da smartphone e, attraverso questa interazione, produce una grossa quantità di dati che possono essere quindi sottoposti ad analisi.

L’analisi dei dati, il *data mining*, porta a sua volta a valutare quali sono le preferenze ed esigenze dell’utente e sulla base di queste si possono quindi formulare nuove proposte per migliorare l’offerta di prodotto.

L’obiettivo è creare un circolo virtuoso che punta alla maggior soddisfazione del cliente attraverso il miglioramento sia dell’offerta che dell’efficienza del servizio, seguendo le personali e specifiche esigenze.

La Fintech si occupa soprattutto dei settori relativi al *sistema di pagamenti* (in Cina ad esempio non si utilizza più la carta di credito, dal momento che le operazioni si effettuano unicamente via smartphone) e *prestiti*, che avvengono sempre più via *mobile*.

Mentre i dati in Cina sono condivisi e visibili, quindi sono tutti analizzabili e processabili, nel sistema occidentale non è così.

Secondo gli esperti il modello Fintech, che si basa sull’accesso diretto da parte dell’utente e sulla eliminazione degli intermediari, risulterà predominante già nell’immediato futuro rispetto ai modelli finanziari classici.

Se da un lato l’eliminazione di intermediari porta vantaggi in termini di risparmio economico e velocità, dall’altro aumenta i rischi derivanti dall’assenza di adeguato controllo.

La gestione dei dati coinvolti nelle operazioni genera una *problematica di sicurezza e di privacy* relativa ai dati stessi, e la mancanza di istituzioni o enti preposti alla tutela e al controllo offre minori garanzie rispetto alla corretta esecuzione del servizio.

Quali sono le organizzazioni interessate al Fintech?

Il tipo di organizzazioni coinvolte nel settore è eterogeneo e va dalle Start-up (che vogliono conquistare i mercati attraverso l'innovazione) agli istituti di credito tradizionali come banche e assicurazioni (che cercano di non perdere quote di mercato).

La velocità e gli impatti dei cambiamenti introdotti dalla nuova forma di finanza causano nuovi rischi e timori.

Relativamente ai ***rischi***, i possibili danni provenienti dall'utilizzo del Fintech coinvolgono attori quali:

- *consumatori e investitori,* soggetti al rischio di possibili mis-selling di prodotti e servizi, violazioni della privacy, esfiltrazione di dati, circolazione di informazioni non sicure;
- *intermediari finanziari,* che rischiano l'utilizzo di un modello di business non sostenibile, il che comporta fronteggiare un rischio tecnologico della governance e la tematica di resilienza operativa in caso di attacco, nonché la gestione dei dati e l'antiriciclaggio;
- *stabilità finanziaria,* per il rischio che si creino mercati paralleli alternativi incontrollati di intermediazione finanziaria attraverso crypto asset.

Le problematiche fondamentali che si pongono dovendo far fronte alle esigenze di protezione del settore sono legate a fattori quali:

- un *aumento* esponenziale *della superficie di* eventuale *attacco*, dato che la tecnologia utilizza processi on line.

Aumentano i possibili punti di accesso per frodi relative all'identità digitale, che sfruttano le vulnerabilità presenti nella rete nei sistemi di identificazione ed autenticazione.

- la *mancanza di information sharing* tra le organizzazioni coinvolte, che ha come conseguenza una difficoltà di risposta in termini di contromisure a livello di contenimento e messa in sicurezza a seguito degli attacchi.

La mancata cooperazione, anche se gli strumenti e le piattaforme di interscambio esistono, è dovuta spesso a motivazioni di tipo concorrenziale o reputazionale.

- *Rischio di effetto domino tra mercati in caso di attacco.*

I mercati in cui interagiscono i servizi finanziari sono sempre più interdipendenti ed interconnessi e richiedono così la messa in sicurezza delle infrastrutture utilizzate come quelli per le transazioni finanziarie, i pagamenti, la gestione dell'identità digitale.

- *Difficile gestione nell'utilizzo dei Big Data*.

Data Collection e Analytics sono tematiche nuove per molte aziende e la loro regolamentazione risulta ancora in evoluzione.

La natura del nuovo settore per quanto riguarda le transazioni è di fatto *ibrida*, ovvero coesiste una parte fisica e una virtuale.

Le transazioni possono infatti avvenire:

- solo digitalmente, ad esempio tramite home banking online
- in parte digitalmente e in parte fisicamente, come per il prelievo bancomat.

Anche quando le transazioni avvengono solo digitalmente c'è il rischio che i data center degli istituti finanziari siano soggetti ad esfiltrazione di dati sia da parte di hakers esterni che di insider, ovvero attaccanti interni che possono istallare strumenti di rilevazione per *skimming attack.*

Cos'è uno *skimming attack*?

È un metodo utilizzato dai ladri di identità per acquisire informazioni da un titolare della carta mediante l’istallazione un piccolo dispositivo chiamato skimmer.

Gli skimmer sono dispositivi tecnologici che possono essere costruiti adattandoli all' uso ed utilizzati in molte sedi fisiche.

Sedi preferenziali sono ad esempio i bancomat e le stazioni di rifornimento carburante, dal momento che i lettori di schede sono spesso all'esterno del distributore e separati da una cassa, ma gli obiettivi appetibili possono essere di svariato genere.

Nei bancomat può essere istallato un piccolo skimmer che consente di ottenere informazioni dallo scorrimento della banda magnetica della carta.

Alcuni skimmer possono anche includere un touchpad da sovrapporre a quello esistente, oppure una telecamera, o un apparecchio per foto digitali, per acquisire singoli numeri identificazione personale ed effettuare, ad esempio:

- *Transazioni fraudolente* mediante PIN;

- *Dumping* delle carte di credito: crea una carta di credito falsa a partire dalla copia digitale non autorizzata dalla lettura della striscia magnetica;

- *Carding forum*, scambio di informazioni e dati di carte e sharing dei metodi fraudolenti, operazioni che avvengono all’interno di siti del dark web.

Questo fa capire come sia importante per le società di carte di pagamento e quelle finanziarie

adottare soluzioni per la sicurezza e prevenzione che vadano di pari passo con le evoluzioni tecnologiche delle tecniche di frode.

Per aumentare la sicurezza e mitigare le informazioni sui dati compromessi è utilissimo ottenere maggiori informazioni e feedback da parte dei clienti, anche tramite risorse online.

La **superficie di attacco** da difendere vede un perimetro sempre più ampio, digitale, fisico e ibrido, che comporta che gli istituti finanziari adottino un atteggiamento prudente sia nei confronti di attaccanti esterni che interni.

In questo contesto sarebbe quindi conveniente un atteggiamento di apertura e comprensione dell' inevitabile sviluppo tecnologico in cui siamo già inevitabilmente immersi e in cui dobbiamo adottare contromisure adeguate ai tempi, investendo in ricerca e sviluppo, in cyberintelligence e cybersecurity, e favorendo l'*information sharing* tra gli attori interessati per comprendere meglio criticità e vulnerabilità.

Articolo a cura di **Maria Cristina Leone**