

Pagamenti. Data analytics e algoritmi permettono di rendere sempre più sicure le transazioni e prevenire potenziali frodi. Ma abilitano anche nuovi servizi, dal marketing alla comparazione delle performance, a disposizione dell'intero ecosistema

Intelligenza artificiale da open banking

Pierangelo Soldavini

È successo non molto tempo fa. Sul deep web è stato intercettato un pacchetto di carte di credito rubate via phishing online in attesa di compratori: i motori che scandagliano la parte del web non indicizzata e quindi non raggiungibile con i sistemi tradizionali di ricerca l'hanno individuato e segnalato alle autorità di sicurezza della rete. Così anche nella fase successiva al furto dei dati sensibili delle carte è stato possibile intervenire per prevenire danni maggiori per i consumatori.

Grazie agli algoritmi di intelligenza artificiale allenati quotidianamente a suon di *machine learning* è oggi possibile infatti garantire una copertura di sicurezza che copra l'intero spettro delle casistiche, sia in fase preventiva, non appena si possano evidenziare i presupposti di una frode, sia durante l'atto criminoso, riducendone al minimo l'impatto, che nella fase successiva, quando i dati sono "pacchettizzati" e venduti all'ingrosso nel web "profondo". «Oggi possiamo affermare con sufficiente sicurezza che c'è una maggior probabilità di furto fisico del portafoglio rispetto all'ipotesi di frode digitale. Anzi più si utilizza la carta per i pagamenti e più aumenta la sicurezza perché l'intelligenza artificiale arriva a delineare meglio il profilo del singolo consumatore e quindi i casi in cui l'utilizzo della carta stessa si discosti dai comportamenti usuali dell'utilizzatore», spiega Roberto Catanzaro, responsabile Business development di Nexi, il gruppo italiano dei pagamenti che gestisce ogni anno 2,9 miliardi di transazioni tramite Pos, Atm e negozi convenzionati.

In una prima fase la singola transazione viene analizzata confrontandola con le regole sulla base della casistica del passato, ma l'intelligenza artificiale interviene soprattutto nella

fase previsionale di potenziali frodi: macinando i dati delle transazioni gli algoritmi imparano a profilare ogni persona sulla base dei dispositivi utilizzati, della geolocalizzazione e dei comportamenti usuali. Ogni azione può essere così elaborata in tempo reale con la segnalazione di qualsiasi anomalia: un dispositivo o un luogo diverso, ma anche una serie di scommesse online per un utente solitamente prudente, fanno immediatamente scattare l'allarme rosso e l'eventuale blocco della transazione. Vengono anche analizzati i cluster di comportamenti nella loro evoluzione: per esempio nella fase attuale di emergenza sanitaria e di minor frequenza degli acquisti fisici, sono in qualche modo allargate le maglie per quanto riguarda la spesa online.

«Il 99,5% dei tentativi di frode riesce a essere bloccato prima che il cliente se ne accorga, solo una quota marginale dello 0,5% arriva a essere segnalata. D'altra parte la fiducia dell'utente è fondamentale per la sicurezza e per accelerare la digitalizzazione delle transazioni in un paese come l'Italia», prosegue il manager di Nexi, che figura tra i primi tre player antifrode in Europa. Il gruppo ha iniziato a scommettere sull'intelligenza artificiale fin dal 2016, in occasione della transizione da CartaSi e oggi può contare su un gruppo di 60 professionisti dedicati con skills diversificate e su investimenti annui per una trentina di milioni di euro sui 170 totali puntati sull'innovazione.

Tutte risorse che non si concentrano solo sulla sicurezza ma che abilitano nuove opportunità. A partire dal tradizionale utilizzo dei dati per l'elaborazione di campagne di marketing e di pricing tagliate su misura e per il miglioramento del servizio ai clienti, attraverso la semplificazione delle operazioni. Ma il processo di data analytics si concretizza anche in servizi innovativi. L'app Nexibusiness permette

così di analizzare tutte le transazioni del singolo esercente, mettendole a confronto con i concorrenti della stessa categoria merceologica sulla base del livello di spesa e dello scontrino medio, delle vendite, delle tipologie di clienti e di carte. Si tratta di uno strumento su cui la grande distribuzione può contare con mezzi propri, ma che manca al piccolo esercente. E che può diventare essenziale per il business: un ristorante ha scoperto così che il suo business era severamente penalizzato dall'assenza del *food delivery*, che in alcune aree arriva a fare una differenza fino a un terzo del giro d'affari.

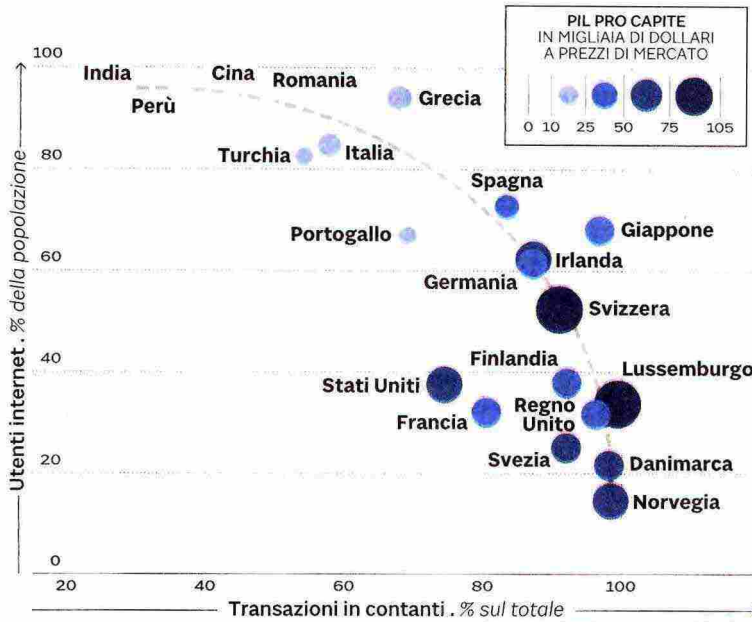
Queste opportunità sono poi condivise con il sistema bancario in ottica di *open banking*. Così come la ricerca di innovazione. «In prospettiva l'utilizzo dell'intelligenza artificiale potrà abilitare la semplificazione degli adempimenti normativi di *know your customer* e anti *money laundering* per i processi di *onboarding* e rendere l'esperienza di interazione del tutto customizzata sulla base delle esigenze e dei comportamenti delle singole persone, quello che io chiamo "segment of one"». L'analisi delle transazioni potrà quindi arrivare all'elaborazione automatica dello *scoring* creditizio sulla base delle operazioni e dei conti e alla contestualizzazione dei servizi sempre su base profilata. In logica di *open banking* la stessa Nexi è *founding partner* insieme a UniCredit del nuovo polo del fintech creato in Italia dalla piattaforma globale di *open innovation* Plug and Play.

Dopo l'avvio della Psd2 diverse banche, recentemente Banca Sella e Intesa Sanpaolo, hanno introdotto servizi di aggregazione dei dati per i clienti che hanno conti correnti su più banche. Ma già si sta pensando all'aggregazione degli investimenti, in modo da poter arrivare a raccomandazioni di investimento robotizzate. Sempre profilate sulla base delle esigenze del singolo.

© RIPRODUZIONE RISERVATA

Più internet, meno contanti

Tasso di penetrazione di internet a confronto con le transazioni in contanti. Dati 2016. *In percentuale*



Fonte: The Economist; Bank of England; World Bank

