Intelligenza artificiale, quali rischi si corrono nei sistemi esperti?

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*

McKinsey, in un recente articolo[1], avverte di possibili rischi nell'uso della Intelligenza Artificiale (AI). Se da una parte riconosce i vantaggi e la positiva percezione da parte degli imprenditori, dall'altra avverte che la AI è come una spada a doppio taglio: può ad esempio provocare – come accaduto in alcuni casi – che, dopo una elaborazione di grandi moli di dati, siano sorti problemi di privacy, svelando dati riservati o trattando i dati senza il preventivo consenso del cliente, o, piuttosto, in un modo non sicuro; in altri casi, si sono ottenute informazioni fuorvianti che hanno originato decisioni errate (ad esempio, derivanti da eccesso di fiducia nelle funzioni predittive della manutenzione; ecc.).

Perché cito questo articolo? Al di là del fatto che ho trovato spunti interessanti, mi ha ricordato una delle mie prime esperienze nella realizzazione di sistemi esperti, finalizzati al trattamento di grandi moli di dati confidenziali. Quella volta mi andò benissimo (un successo inatteso), ma mi suonò come un avvertimento per il futuro (come molti sanno, le banche hanno da lunghissimo tempo delle apposite applicazioni atte ad assistere chi deve controllare la *compliance* alla normativa ed alla regolamentazione corrente).

Racconto brevemente l'episodio.

Il sistema esperto era finalizzato ad individuare eventuali possibili impiegati disonesti (per fortuna sono molto pochi,

ma il danno di immagine che provocano è deleterio). Ciò che giunse inatteso, fu che il risultato fu assai apprezzato dalle filiali per un'altra ragione, diversa dalle finalità originarie!

Ero all'epoca responsabile dell'IT auditing in **BNL** e fra i nostri obiettivi vi era quello di aiutare l'Ispettorato (così si chiamava all'epoca) nell'individuare possibili frodi.

Una delle più antipatiche, vedeva un impiegato (spesso ricattato per il vizio del gioco o per altri vizi) prelevare quanto a lui necessario dai conti di persone anziane o altre che avevano comunque una discreta giacenza e prelevavano il denaro di rado. Il caso tipico era quello della persona pensionata che prelevava il minimo indispensabile, non aveva assegni, non faceva bonifici, ecc..

Dopo aver ascoltato gli ispettori che ci hanno illustrato le modalità operative generalmente seguite, abbiamo disegnato l'applicazione; questa, di notte, consultava tutti gli archivi necessari e, se trovava possibili comportamenti rientranti nelle casistiche a noi descritte, evidenziava la filiale ed il conto potenzialmente interessato.

Il Direttore della prima filiale da noi interpellata, mi chiamò entusiasta! Aveva convocato un cliente il cui conto, normalmente interessato da versamenti e raramente da prelevamenti, da qualche giorno evidenziava cospicui prelevamenti tramite assegno. Tutto combaciava con le caratteristiche di una potenziale frode: aveva cambiato l'indirizzo per l'invio dell'estratto conto; aveva chiesto un carnet di assegni; aveva comunicato i dati di un delegato; e così via. Il quadro rientrava nella casistica da noi ipotizzata.

Il cliente ringraziò per essere stato convocato in quanto la

banca finalmente dimostrava un interesse nella sua persona: ciò non era avvenuto fino ad ora, e, non solo, era stato addirittura maltrattato con il tasso creditore; infatti, gli era stato negato il tasso di interesse promesso e, di conseguenza, lui – per ripicca – aveva aperto il conto in un'altra banca e aveva iniziato a trasferire i soldi!

Una applicazione nata per individuare i ladri era invece ambita dalle filiali per analizzare comportamenti anomali dei clienti.

Da allora sono passati tanti anni, e le applicazioni nell'analisi della clientela hanno fatto passi enormi. Oltre a crescere in numero e qualità, devono affrontare grandissime moli di dati assai diversi, di diversa provenienza, di diversa frequenza di aggiornamento, ecc.

Questa mia breve testimonianza, molto semplice e quindi facilmente comprensibile da tutti, è per affermare che le applicazioni, finalizzate ad assistere il personale operativo e di business, spesso progettate per una determinata finalità, poi possono essere utili anche per altri fini, inizialmente non previsti.

Ma, attenzione! Come ci ricorda McKinsey, si tratta di una spada a doppio taglio: l'altra faccia della spada può essere invece una minaccia alla protezione dei dati personali o alla continuità del business.

Non bisogna quindi trascurare una attenta analisi degli obiettivi e dei possibili output; non bisogna essere presi dalla fretta di mettere l'applicazione in produzione, ma esaminarne i contenuti e le fonti con estrema attenzione coinvolgendo nell'esame tutte le funzioni aziendali potenzialmente interessate.

Anthony.wright@anssaif.it

[1] https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/confronting-the-risks-of-artificial-intelligence

https://www.key4biz.it/intelligenza-artificiale-quali-rischi-si-corrono-nei-sistemi-esperti/256324/