PAGAMENTI DIGITALI SICURI ED INTELLIGENTI:

*l'impiego di **AI** e **Advanced Analytics** nell'approccio di **Intesa Sanpaolo***

Andrea Claudio Cosentini, *Head of Data Science and Artificial Intelligence*

24 Novembre 2023

Agenda

- ❑ L'Anti Financial Crime Digital Hub: Overview, Mission, «Challenge»
- ❑ L'azione del Centro di Eccellenza AI di Intesa Sanpaolo: un caso d'uso
- ❑ Framework per l'uso dei dati e dell'AI in Banca
- ❑ Utilizzo di AI & Advanced Analytics in ambito di Cyber-sicurezza

L'Anti Financial Crime Digital Hub: Overview

In risposta alle iniziative del Regolatore Europeo per la costituzione della **nuova Authority Europea (AML-A)** per il contrasto al crimine finanziario (***Anti Financial Crime, «AFC»***) e per il contrasto al finanziamento del terrorismo (***«CFT»***), **Intesa Sanpaolo** ha lavorato per la nascita di un **Digital Hub** basato sull'impiego di tecnologie innovative con la collaborazione di **partner scientifici e commerciali**

Anti Financial Crime DIGITAL HUB

INTESA SANPAOLO

Politecnico di Torino

UNIVERSITÀ DI TORINO

INTESA SANPAOLO INNOVATION CENTER

CENTAI

Sede:
Torino, Grattacielo ISP

Costituzione:
16 giugno 2022

L'Anti Financial Crime Digital Hub: Mission

Anti Financial Crime DIGITAL HUB

- L'AFC Digital Hub ha l'obiettivo di **contrastare i crimini finanziari** attraverso l'impiego delle **nuove tecnologie e dell'Intelligenza artificiale**
- **Due principi** guidano le attività: **Innovazione** e **Cooperazione** con partner scientifici e finanziari per incrementare l'efficacia del contrasto al crimine finanziario in ambito bancario con l'aspirazione di contribuire a quella del sistema nazionale ed europeo
- La Società Consortile è quindi **aperta** all'ingresso di **nuovi partner finanziari**

Il ruolo di Intesa Sanpaolo:

- ✓ **Ingegnerizzare** e **industrializzare** le soluzioni sviluppate,
- ✓ **Mettere a disposizione** di altri soggetti del sistema bancario le soluzioni tecnologiche.

Le aree di ricerca AFC Hub e le «challenge»: qualche esempio

	Challenge	Partner	Obiettivo
Funzionali	**Velocity**	ISI Foundation	Evoluzione delle tecniche di transaction monitoring, attualmente basate su algoritmi con accumulatori e soglie di alerting per la ricerca del **red flag di "Velocity"**, usando tecniche di analisi dei **grafi temporali**
Funzionali	**Reduce Expected Detections**	Intesa Sanpaolo *AI Center of Excellence*	Sviluppo di algoritmi di machine learning per **ottimizzare l'effort dedicato dagli analisti del Competence Center di transaction monitoring** alla valutazione degli alert generati dagli applicativi di monitoraggio (Scenario «Carte Prepagate – Persone fisiche» Contante e Traffico Anomalo) per il perimetro delle persone fisiche)
Funzionali	**Hidden Risk**		Identificazione univoca delle controparti (c.d. **entity resolution**) ed identificazione di potenziali scenari di anomalie (c.d. **anomaly detection**), non note a priori
Abilitanti	**Explainable AI**		Sviluppare un prototipo in grado di identificare, con approccio qualitativo, **l'explainer più adeguato in funzione degli algoritmi e dei dati utilizzati**
Abilitanti	**Quantitative Explainable AI**		**Evolvere il prototipo** per l'identificazione degli explainer, **definendo e sviluppando un modello quantitativo** di classificazione degli explainer sulla base delle metriche individuate: effective compactness, fidelity e stability

L'azione del Centro di Eccellenza AI di Intesa Sanpaolo: un caso d'uso

«AI for Behavioural Customer Monitoring»

Lo scopo del progetto è stato quello di sviluppare un motore di intelligenza artificiale in grado di identificare potenziali tentativi di frode sulle transazioni dei clienti (SEPA, IPAY, CLESS, BONEST, RIC). Gli algoritmi analizzano le deviazioni dal profilo finanziario dei comportamenti del cliente al fine di aumentare l'accuratezza e ridurre i falsi positivi dell'attuale motore basato su regole. Il segnale del nostro motore è integrato nell'orchestratore antifrode.

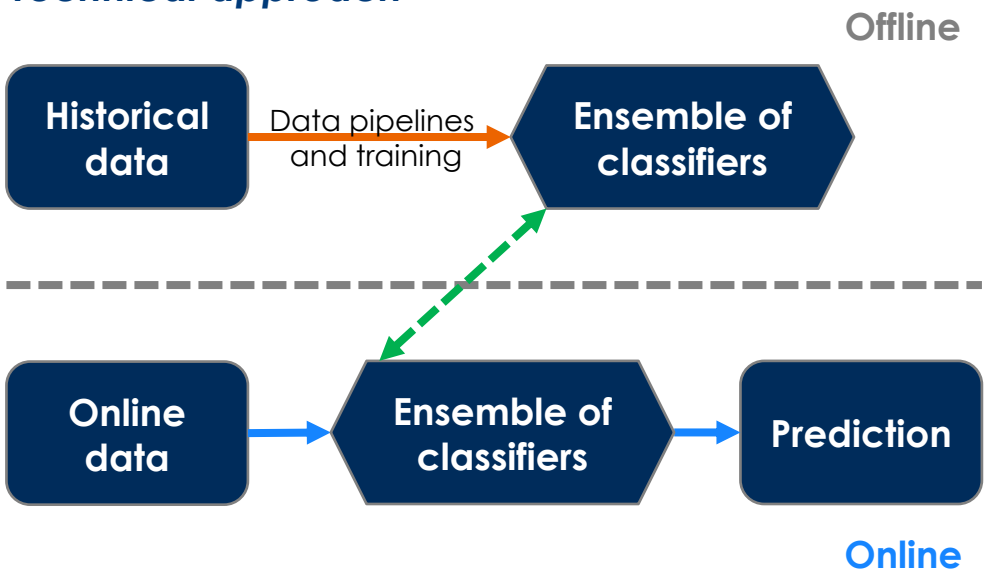
Prima

Il motore della Cybersecurity era costituito da una serie di componenti che seguono regole deterministiche. I colleghi sviluppano regole basate sull'analisi di piccoli sottoinsiemi di dati. Lo sviluppo di queste regole è piuttosto costoso e comporta un gran numero di falsi positivi.

Adesso

Il modulo ML è stato progettato per essere costantemente addestrato su enormi quantità di dati storici ed è in grado di identificare il livello di rischio di una transazione in base alle variazioni rispetto al comportamento abituale del cliente. Il segnale generato viene immesso nell'orchestratore antifrode RBA.

Technical approach



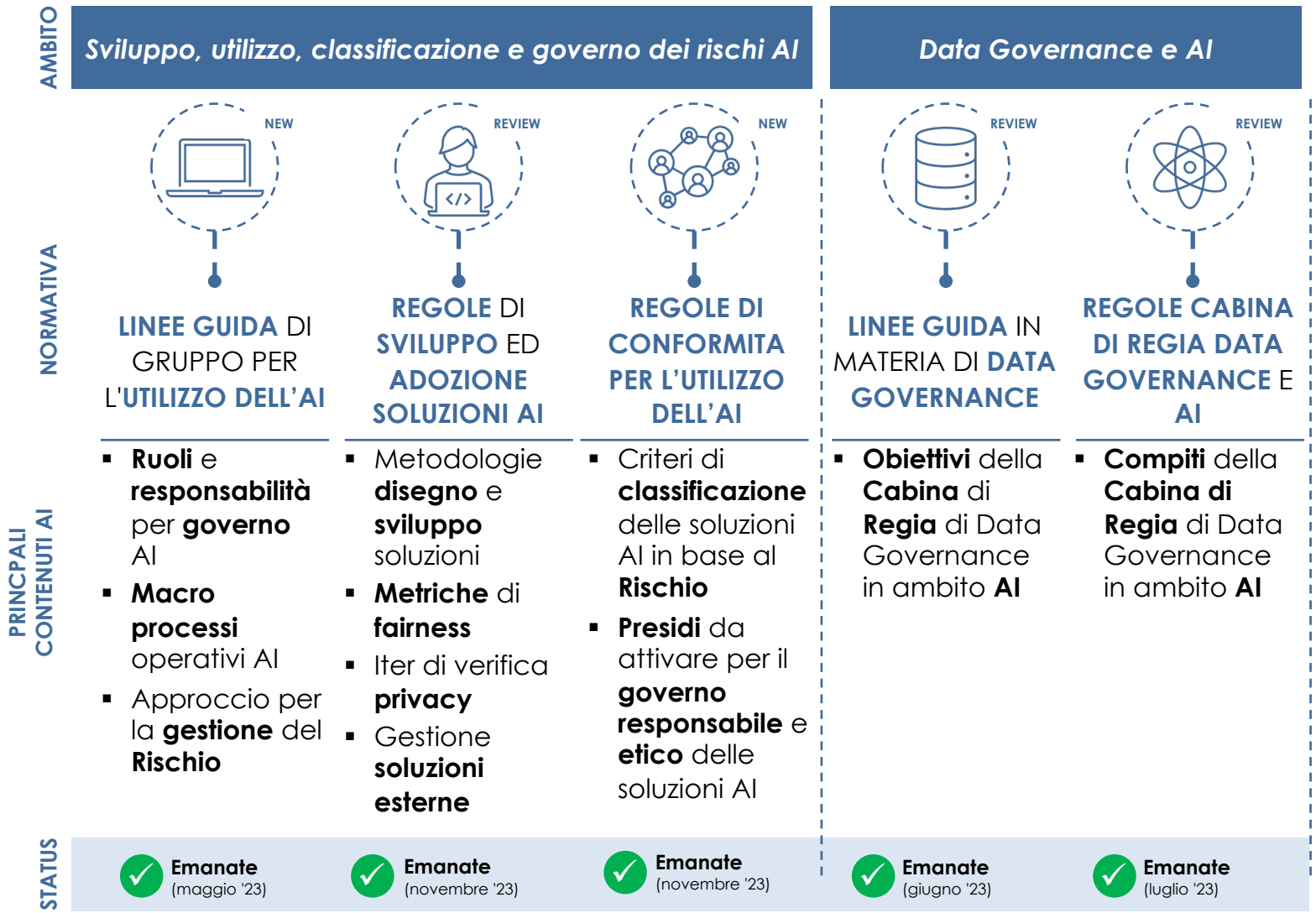
Sfide

- Il contesto è fondamentale per l'azienda.
- A causa dell'elevato volume di dati da elaborare, è necessario prestare particolare attenzione.
- Le previsioni vengono fatte in tempo reale, mentre si verifica la transazione.

Benefici

- Il sistema di apprendimento automatico "ragiona" in base al profilo finanziario del cliente e a tutto lo storico delle transazioni.
- Riduzione del rischio di reputazione.
- Riduzione delle perdite operative grazie al maggior numero di frodi evitate.
- Riduzione dei falsi positivi, con conseguente aumento dell'efficienza (meno FTE per le filiali digitali).

Framework per l'uso dei dati e dell'AI in Banca



In linea con la proposta di regolamento europeo **«Artificial Intelligence Act»** e con i principi di **Trustworthy AI**, Intesa Sanpaolo ha avviato un'attività di **aggiornamento del framework normativo interno**

Framework per l'uso dei dati e dell'AI in Banca: Regole Operative in Intesa Sanpaolo

PRINCIPALI CONTENUTI DELLE REGOLE IN MATERIA DI SVILUPPO E ADOZIONE DI SOLUZIONI A.I

Regole di sviluppo ed adozione soluzioni A.I.


INTESA SANPAOLO

REGOLE IN MATERIA DI SVILUPPO E ADOZIONE DI SOLUZIONI DI INTELLIGENZA ARTIFICIALE (I.A.)

Emanate a ***ottobre 2023***

REGOLE PER DISEGNO, SVILUPPO E ADOZIONE SOLUZIONI A.I.

Metodologie per **progettare**, **sviluppare** e **monitorare** soluzioni **A.I.**

REGOLE PER LA DEFINIZIONE DEL FRAMEWORK DATI

Step di **individuazione**, **raccolta, analisi** e **definizione** del **disegno architetturale** dei **dati**

ITER DI VERIFICA REQUISITI PRIVACY

Processo di **verifica privacy** per l'**avvio** di ogni **Use Case** (Privacy by design)

METRICHE E STRATEGIE DI MITIGAZIONE FAIRNESS

Bias assessment sui dati e Metriche per garantire lo **sviluppo** di **soluzioni non discriminatorie**

REGOLE PER L'ADOZIONE DI SOLUZIONI ESTERNE *Focus slide #47*

Regole operative per l'adozione di **soluzioni** di **terzi** e **checklist**[1] di **verifica** della **fairness**

PRINCIPI GUIDA A.I. RESPONSABILE

Principi per **ispirare** e **guidare** tutte le **iniziative** e i **progetti** relativi all'**A.I.**

Note: 1) La Checklist di verifica della fairness delle soluzioni esterne costituisce un allegato al documento di Regole

Utilizzo di AI & Advanced Analytics in ambito di Cyber-sicurezza

Geolocalizzazione Comportamentale
Definizione delle **aree geografiche trusted** per il singolo cliente. Maggiore protezione per operazioni in aree anomale, maggiore precisione per operazioni dubbie in aree trusted.

Intelligenza Artificiale
Motore di AI in grado di individuare le abitudini finanziarie di ciascun cliente. Maggior precisione grazie all'impiego di **regole non deterministiche** da definire a priori.

Biometria
Introduzione di algoritmi di analisi biometrica GDPR compliant, con l'obiettivo di **rafforzare l'analisi comportamentale** finanziaria ma anche **la protezione del cliente al login**.