protiviti | Insights | Face the Future with Confidence

Luglio | COMPLIANCE | 2021

a cura di / **Tamara Devalle**
Director Protiviti

INTELLIGENZA ARTIFICIALE: CHE COSA FARE IN VISTA DEL REGOLAMENTO UE

La Commissione Europea ha da poco pubblicato una proposta per regolamentare l'uso dei sistemi d'Intelligenza Artificiale (IA).

La Commissione Europea ha da poco pubblicato una proposta per regolamentare l'uso dei sistemi d'Intelligenza Artificiale (IA). I tempi di approvazione e applicazione non sono ancora certi ma, intanto, la bozza ha generato numerose domande sull'applicazione e l'impatto che coinvolgono diverse funzioni manageriali, a cominciare da Risk Management e Compliance:

- quanto sono note e condivise nelle imprese applicazioni e criticità dell'IA?
- quali rischi sono stati identificati e quali sono le misure di gestione più appropriate?
- come dovranno strutturarsi le imprese per adeguarsi al Regolamento?
- che cosa fare nel caso di un incidente?

In questo *Insights* entreremo nel merito delle indicazioni contenute nel testo della Commissione e degli interventi che le imprese dovrebbero valutare fin da ora per rispondere allo spirito del testo: responsabilizzarsi sui possibili impatti delle soluzioni di IA e mantenere alto il monitoraggio.

Il Regolamento si applica a tutte le società che offrono, attivano e/o utilizzano sistemi d'IA, definizione *ombrello* sotto la quale ricadono tecnologie con funzionalità diverse: dalla manutenzione predittiva al monitoraggio della qualità fino al riconoscimento facciale e agli assistenti virtuali.

Il testo configura quattro livelli di rischio (inaccettabile, alto, limitato, minimo), dettando le regole per gestirli in ambiti diversi (risk management, testing dei sistemi, trasparenza, data governance, requisiti tecnici specifici, supervisione umana).

Oltre a indicazioni in ambito di Risk Management, Governance e gestione incidenti, si chiede alle imprese di tutelarsi verso i fornitori/sviluppatori e adottare adeguata trasparenza verso gli utenti/clienti finali.

Sono previste procedure di valutazione della conformità in linea con quanto avviene per altri prodotti regolamentati a livello europeo (dispositivi medici, apparecchiature elettroniche, ...): in alcuni casi, sarà lo sviluppatore dei sistemi a valutare autonomamente la conformità, in altri bisognerà coinvolgere un organismo esterno. La valutazione sarà in ogni caso facilitata dagli standard di riferimento per le categorie di sistemi di IA degli enti di normazione quali ISO e CEN. In caso di difformità, le sanzioni amministrative possono arrivare fino a 30 milioni di euro o al 6% del fatturato annuo.

Contesto di riferimento

Mercoledì 21 aprile la Commissione Europea ha pubblicato una proposta per la regolamentazione dell'utilizzo dei sistemi di Intelligenza Artificiale (IA) - "*Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*". Un nuovo approccio europeo che fa seguito ad una serie di iniziative intraprese negli ultimi anni[1] con lo scopo di indicarne gli usi consentiti e quelli proibiti e fare in modo che l'uso della IA avvenga nel rispetto dei diritti fondamentali e dei valori europei.

L'iniziativa della Commissione copre diversi ambiti e applicazioni della IA. Il Regolamento, nella sua versione in bozza, si applica a tutte le società che immettono sul mercato, mettono in servizio e/o utilizzano "sistemi di IA".

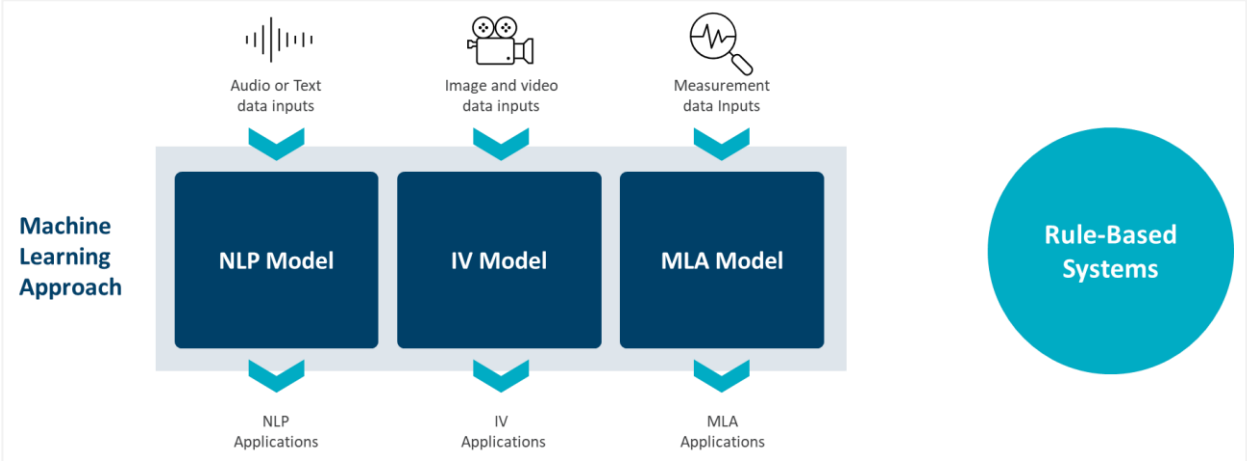
Forti della nostra esperienza nel recepire e riflettere nella nostra gamma di servizi (sia metodologici che tecnologici) questo tipo di soluzioni, vi presentiamo una sintesi dei requisiti e le nostre riflessioni sugli impatti in ambito Compliance/Risk Management.

Cosa si intende per Intelligenza Artificiale (IA)?

Nonostante le molteplici definizioni di Intelligenza Artificiale, questa appare ancora come un concetto sfocato. Nel comune dibattito aziendale un vasto numero di tecnologie rientra in questo termine a partire dalla manutenzione predittiva, al monitoraggio della qualità, fino al riconoscimento facciale e agli assistenti virtuali.

[1] La consultazione pubblicazione del 19 febbraio 2020 - White Paper sull'Intelligenza Artificiale (COM 2020) 65 final; Le Linee guida etiche finali per un'intelligenza artificiale affidabile – pubblicazione dell'8 aprile 2019; Il Rapporto sulla responsabilità per l'Intelligenza Artificiale e altre tecnologie emergenti, pubblicato il 21 novembre 2019;

Tutte queste tecnologie sono comunemente considerate IA. Per classificarle meglio vi proponiamo la tassonomia del ***DEVO Lab*** secondo la quale **l'IA è un *cluster* tecnologico composto da tre principali tecnologie**[2]:



a. **Natural Language Processing (NLP):** tecnologia basata su algoritmi che consentono l'analisi e quindi la comprensione dei "linguaggi naturali" fornita dagli utenti tramite testo / voce (NLU), così come la generazione del linguaggio naturale (NLG), basato su apprendimento autonomo che non richiede una specifica e puntuale programmazione. I servizi *text-to-speech* sono un esempio di questa tecnologia;
b. **Intelligent Vision (IV):** tecnologia basata su algoritmi che consentono alle macchine di imparare come riconoscere e classificare gli input visivi, classificare il loro contenuto per migliorare la loro precisione nel tempo, senza la necessità per una programmazione completa basata su regole puntuali. Servizi di riconoscimento facciale e la classificazione automatica di frame nei video sono esempi di questa tecnologia;
c. **Machine Learning Analytics (MLA):** tecnologia basata su algoritmi che consentono l'elaborazione statistica di dati numerici e il miglioramento autonomo nell'accuratezza dell'analisi senza necessità di implementare specifiche regole di programmazione. I consigli automatici presenti all'interno di una chat e basati sul comportamento online dei clienti sono un esempio di questa tecnologia.

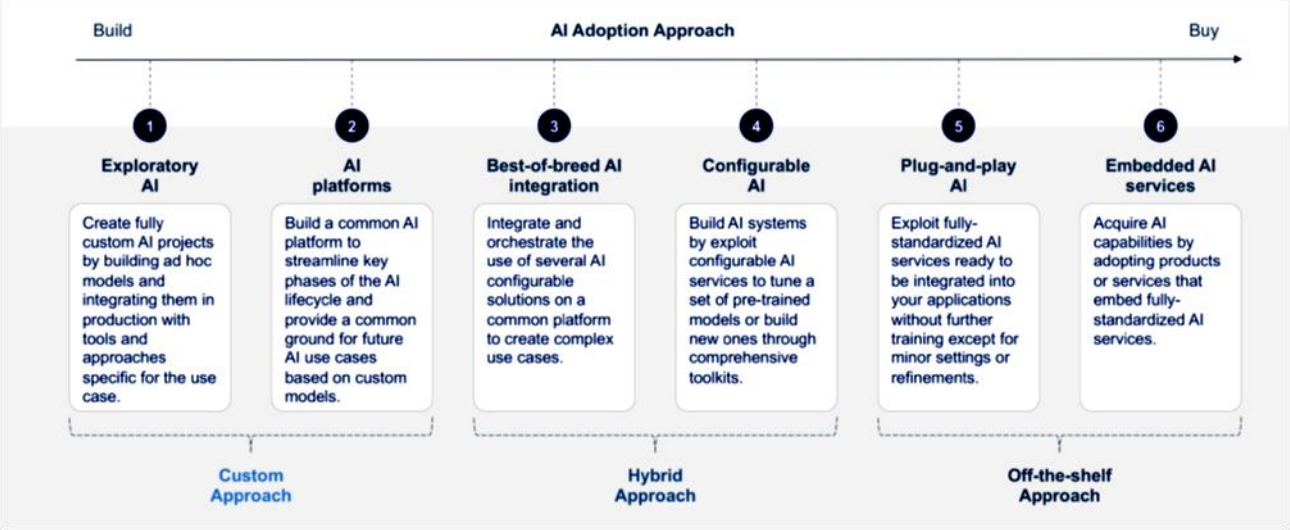
I sistemi di IA possono essere abilitati da una singola tecnologia o essere il prodotto della combinazione di due o più di loro. Ad esempio, mentre gli assistenti virtuali si basano sulla tecnologia della NLP, altre applicazioni complesse - come le "*automobili autonome*" piuttosto che i sistemi di monitoraggio basati su input visivi e uditivi - tendono a sfruttare varie combinazioni di differenti tecnologie come NLP, IV e MLA.

Una possibile clusterizzazione delle varie soluzioni di IA

Le soluzioni di Intelligenza Artificiale possono essere adottate dalle società secondo approcci estremamente differenti che spaziano dalla creazione *in-house* delle

[2] DEVO Lab (2021), The AI Democratization: the myths and reality of adopting Artificial Intelligence, SDA Bocconi School of Management.

applicazioni necessarie, all'acquisto di applicazioni *plug-and-play* già presenti sul mercato.



Il framework[3] qui rappresentato, che sintetizza 3 diversi "*adoption approaches*" per l'implementazione e la gestione nel continuo delle diverse soluzioni di Intelligenza Artificiale, è stato sviluppato proprio analizzando e raggruppando le principali modalità con cui le aziende implementano soluzioni di IA:

a. **Approccio personalizzato:** strategie che consentono di "*costruire*" un'ampia varietà di applicazioni di IA con alti livelli di personalizzazione e in grado di indirizzare vasti casi d'uso. La realizzazione di queste soluzioni richiede decisioni puntuali sui requisiti tecnici e commerciali del sistema. A seconda dei casi, l'implementazione di soluzioni personalizzate può avvenire sia attraverso la creazione "*ad hoc*" di modelli e strategie di *deployment* (archetipo **Exploratory AI**) sia attraverso la creazione di un'architettura comune in cui è possibile costruire più casi d'uso personalizzati (archetipo **AI platforms**);

b. **Approccio Ibrido:** opzioni intermedie che sfruttano processi di sviluppo guidato e soluzioni configurabili per creare applicazioni. Ciò può avvenire attraverso l'integrazione di numerosi servizi di IA su una piattaforma comune, sfruttando singole soluzioni per diversi casi d'uso (archetipo **AI best-of-breed**) o adottando singoli *toolkit* di IA completi che vengono poi personalizzati in base alle specifiche esigenze del progetto (Archetipo **AI configurabile**);

c. **Approccio Off-the-shelf**: casi in cui il focus è sull'"*acquisizione*" dell'Intelligenza Artificiale, secondo una prospettiva *full-buy*. Qui, l'ambito dei casi d'uso potenziati dai sistemi di Intelligenza Artificiale è molto più limitato e può essere realizzato grazie a servizi di IA completamente standardizzati e da integrare in applicazioni software (archetipo IA **plug-and-play**) o attraverso l'acquisizione di prodotti/servizi che vengono forniti con funzionalità IA già integrate (archetipo **Embedded AI Services**).

Qualunque sia l'approccio scelto, le aziende che adottano sistemi di IA dovranno rispondere ai requisiti del nuovo Regolamento.

[3] DEVO Lab (2021), The AI Democratization: the myths and reality of adopting Artificial Intelligence, SDA Bocconi School of Management.

Che cosa dice il Regolamento

Regolamentazione basata su una scala di rischio

La Commissione Europea propone una regolamentazione dell'IA basata su 4 livelli di rischio:

a. **Rischio Inaccettabile**: usi dell'IA che rappresentano una minaccia per i cittadini UE, in quanto violano i diritti fondamentali. Sistemi di social scoring, identificazione biometrica da remoto, sistemi che sfruttano vulnerabilità delle persone per distorcerne il comportamento **sono vietati**;

b. **Rischio Alto:** sistemi di IA che possono avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali: ad esempio destinati ad essere utilizzati come componenti di sicurezza di dispositivi medici, apparecchiature radio, ascensori, giocattoli, e da utilizzare per la selezione del personale, valutare la solvibilità delle persone, e sistemi di polizia predittiva. Per tali sistemi, il Regolamento prevede **specifici requisiti** (tali requisiti riguardano la qualità dei set di dati utilizzati, la documentazione tecnica e la conservazione dei dati, la trasparenza e la fornitura di informazioni agli utenti, la sorveglianza umana, la robustezza, l'accuratezza e la cyber security);

c. **Rischio Limitato:** sistemi di IA destinati ad interagire con persone fisiche, di riconoscimento delle emozioni (es. apparati promozionali del tipo "*digital signage*"), e usati per la manipolazione di video e immagini di persone fisiche. Per tali sistemi il Regolamento prevede specifici **obblighi di trasparenza** (es. *chatbot*: gli utenti devono essere consapevoli del fatto che stanno interagendo con una macchina);

d. **Rischio Minimo:** tutti i sistemi di IA possono essere sviluppati e utilizzati nel rispetto della legislazione vigente senza ulteriori obblighi giuridici. La grande maggioranza dei sistemi di IA attualmente utilizzati nell'UE rientra in questa categoria. I fornitori di tali sistemi possono scegliere di applicare, su base

volontaria, i requisiti per un'IA affidabile e aderire a codici di condotta volontari.

Regole specifiche per i sistemi a rischio alto

CREARE E MANTENERE ATTIVO UN SISTEMA DI RISK MANAGEMENT

Vale a dire un processo iterativo che copra l'intero ciclo di vita di un sistema ad alto rischio e che preveda:

- identificazione e analisi dei rischi noti e prevedibili associati a ciascun sistema;
- stima e valutazione dei rischi che possono emergere quando il sistema viene utilizzato conformemente allo scopo previsto e in condizioni di uso improprio ragionevolmente prevedibile;
- valutazione di altri rischi derivanti sulla base dell'analisi dei dati raccolti dal sistema di monitoraggio post-adozione;
- adozione di apposite misure di gestione del rischio.

TESTING DEI SISTEMI

I sistemi di IA ad alto rischio devono essere testati al fine di garantire che funzionino in modo coerente per lo scopo previsto e siano conformi ai requisiti stabiliti dal regolamento. Il testing deve:

- essere idoneo a conseguire lo scopo previsto e non deve andare oltre quanto necessario per conseguire tale obiettivo;
- essere effettuato prima dell'immissione sul mercato o della messa in servizio;
- essere effettuato sulla base di metriche definite in via preliminare e di soglie probabilistiche adeguate allo scopo previsto;

Inoltre, nell'attuazione del sistema di gestione dei rischi, si deve tenere conto in modo specifico se è probabile che il sistema sia accessibile o abbia un impatto sui bambini.

TRASPARENZA

Sussistono specifici obblighi di trasparenza e l'obbligo di garantire l'attendibilità, accuratezza e sicurezza di tali sistemi che devono essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare i risultati del sistema e utilizzarli in modo appropriato.

DATA GOVERNANCE

I sistemi che fanno uso di tecniche che implicano l'addestramento di modelli con dati devono essere sviluppati sulla base di set di dati di addestramento, convalida e test che soddisfano i seguenti criteri di qualità:

- devono essere soggetti a adeguate pratiche di data governance e data management (es. data collection, data preparation, assunzioni di base, bias, …);
- i data set utilizzati per il training, la convalida e il testing devono essere rappresentativi, senza errori e completi, rilevanti per il fine del Sistema (tenendo in considerazione gli aspetti geografici, di comportamento o funzionali per gli obiettivi del Sistema);
- categorie speciali di dati personali possono essere trattati fatte salve adeguate garanzie per i diritti e le libertà fondamentali delle persone fisiche.

REQUISITI TECNICI SPECIFICI

- I sistemi di IA ad alto rischio devono essere sviluppati seguendo una serie di specifici criteri, quali:
- adeguato set di log per assicurare, nell'operatività, che stia funzionando come previsto dal suo scopo;
- il livello di accuratezza raggiunto dal sistema deve essere dichiarato all'interno delle istruzioni;
- resilienza in relazione a errori, guasti o incongruenze;
- garanzia che gli output eventualmente distorti a causa degli output utilizzati come input per le operazioni future (`` feedback loops '') siano debitamente gestite con adeguate misure di mitigazione;
- cyber security. I sistemi devono resistere ai tentativi di terzi non autorizzati di alterarne l'uso o le prestazioni sfruttando le vulnerabilità. Occorre prevedere adeguate misure tecniche per garantire la sicurezza del sistema.

SUPERVISIONE UMANA

I sistemi devono essere progettati e sviluppati in modo tale da poter essere efficacemente controllati dalle persone durante il periodo in cui il sistema di intelligenza artificiale è in uso. La supervisione umana deve mirare a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando il sistema è utilizzato sia conformemente allo scopo previsto o in condizioni di uso improprio ragionevolmente prevedibile. La supervisione umana deve poter:

- comprendere appieno le capacità e le limitazioni del sistema ed essere in grado di monitorarne adeguatamente il funzionamento, in modo che i segni di anomalie, disfunzioni e prestazioni impreviste possano essere rilevati e affrontati il prima possibile;
- rimanere consapevoli della possibile tendenza a fare affidamento o affidamento eccessivo sui risultati prodotti (``automation bias''), in particolare per i sistemi utilizzati per fornire informazioni o raccomandazioni a supporto di decisioni assunte da persone fisiche;
- essere in grado di interpretare correttamente i risultati;
- essere in grado di decidere di non utilizzare il sistema o altrimenti ignorare o modificare l'output del sistema;
- essere in grado di intervenire sul funzionamento del sistema o interromperne il funzionamento nel caso serva.

Verifica, Monitoraggio e sanzioni

La **verifica** del rispetto dei requisiti avverrà attraverso procedure di valutazione della conformità, in linea con quanto previsto per altri prodotti regolamentati a livello europeo (dispositivi medici, apparecchiature elettroniche, ...).

In alcuni casi, sarà il produttore (inteso anche come sviluppatore) a valutare in maniera autonoma la conformità ai requisiti del Regolamento, mentre in altri sarà necessario coinvolgere un organismo esterno. Questo sistema di *conformity assessment* sarà facilitato dall'adozione di appositi standard di riferimento (per categorie di sistemi di IA) da parte degli enti di normazione quali ISO e CEN.

Una volta effettuata con successo la "procedura di valutazione della conformità", i sistemi di IA dovranno essere marcati CE. Alcuni sistemi dovranno, inoltre, essere registrati in un database accessibile al pubblico. Solo a questo punto, potranno essere immessi sul mercato.

I fornitori di soluzioni di IA sono tenuti ad implementare sistemi volti a monitorare l'uso di ciò che immettono sul mercato, per verificare se tali soluzioni rimangono conformi al Regolamento nel corso del proprio ciclo di vita. Sono, inoltre, tenuti a segnalare alle autorità competenti eventuali malfunzionamenti e incidenti che dovessero ricontrare

attraverso tale attività di monitoraggio.

Le sanzioni amministrative possono arrivare fino a 30 milioni di euro o al 6% del fatturato annuo.

Come prepararsi? I nostri suggerimenti

La lettura della proposta di Regolamento fa emergere alcune domande:

- all'interno delle aziende, quanto sono note e condivise le applicazioni dell'IA e la loro criticità?
- quali rischi e quali misure di gestione più appropriate sono stati identificati?
- come devono strutturarsi le aziende per adeguarsi a questo nuovo Regolamento?
- cosa fare in caso si registri un *incident*?

L'attuazione di quanto richiesto dal Regolamento, in ottica di impostazione di una sana governance, impone alle aziende di responsabilizzarsi sui possibili impatti derivanti dall'adozione di soluzioni di IA e di mantenere alto il livello di monitoraggio (azione indispensabile in ambiti come questi in cui la tecnologia evolve rapidamente).

Conoscere: i primi step fondamentali per la gestione del rischio

Le funzioni Risk Management e Compliance saranno le prime chiamate a svolgere gli step fondamentali per l'adeguamento al nuovo Regolamento, vale a dire:

a. Mappatura di tutte le soluzioni di IA presenti in azienda e successivo Risk Assessment per l'identificazione di minacce specifiche e per la classificazione delle stesse secondo i livelli di rischio definiti dal Regolamento (i.e. inaccettabile, alto, limitato, minimo);
b. Qualora fossero identificate soluzioni a rischio inaccettabile, definizione di una strategia di dismissione;
c. Per le soluzioni a rischio alto, elaborazione di una gap analysis tra attuali presidi in essere e requisiti richiesti dal Regolamento;
d. Definizione di un piano che preveda l'implementazione di specifici remediation plan per garantire l'adeguamento ai requisiti richiesti dal Regolamento (per le soluzioni a rischio alto o limitato).

In questa fase ancora "*embrionale*" per l'implementazione delle soluzioni di IA nelle aziende, risulta fondamentale la costruzione di un Risk Assessment per identificare i rischi cui è esposta l'azienda e le misure di mitigazione più appropriate.

Gli effetti dell'IA dipendono da come viene progettata e da quali dati vengono immessi nel sistema: questo processo, però, può anche essere "manomesso" intenzionalmente. Se non programmata correttamente, l'IA potrebbe influenzare le decisioni riguardo a un'offerta di lavoro o all'offerta di prestiti.

L'IA può anche minacciare la protezione dei dati e il diritto alla vita privata: può essere usata infatti su dispositivi per il riconoscimento facciale o per la profilazione di utenti e clienti finali (senza che questi ne siano stati adeguatamente informati). Può anche

essere usata per creare immagini, video e audio falsi ma estremamente realistici (noti come ***deepfake***), che possono essere usati per truffare, rovinare la reputazione e mettere in dubbio la fiducia nei processi decisionali. Le disuguaglianze nell'accesso alle informazioni potrebbero essere sfruttate a discapito degli utenti: sulla base di un comportamento in rete di una persona, un fornitore di servizi potrebbe prevedere quanto questa sia disposta a pagare per un servizio.

Per tutti questi motivi (e molti altri), è importante che le aziende sappiano come utilizzare queste soluzioni e siano soprattutto in grado di implementare le adeguate misure di sicurezza a presidio dei rischi sopra elencati, prevedendo anche eventuali "*piani B*" per gli scenari in cui la soluzione di IA scelta risulti inaccettabile.

Gestire nel continuo: la governance al centro

Considerata la rapida evoluzione degli aspetti tecnologici, è fondamentale mantenere aggiornata nel continuo la mappatura delle soluzioni e il relativo risk assessment. Poiché il Regolamento IA ha un'impostazione analoga alla normativa privacy (GDPR), è auspicabile capitalizzarne il framework e integrarlo rispetto a quanto di più specifico richiesto per l'IA (es. registro delle attività di trattamento, risk assessment, …) e quindi:

a. definire un **modello di gestione delle soluzioni di Intelligenza Artificiale** in grado di (i) tutelare le informazioni e i dati ivi contenuti per tutto il loro ciclo di vita, (ii) garantire una corretta applicazione del Regolamento e (iii) identificare correttamente, all'interno dell'azienda, ruoli e relative responsabilità attraverso l'elaborazione di **Linee Guida** e **Procedure Operative.** In considerazione della dinamicità e della continua evoluzione dell'IA, si suggerisce anche di strutturarsi identificando responsabilità "*ad hoc*", dedicate nell'organizzazione aziendale alla gestione di tematiche di IA (sia di compliance che operative);

b. costruire un adeguato **processo di Data/IT Governance** che permetta, una volta mappate le soluzioni di IA, d'identificare le tipologie di dato trattato e che ne definisca i limiti e le modalità di storicizzazione. Per ogni tipologia identificata, dovranno essere poi implementate adeguate misure di sicurezza e dovrà essere garantito un processo di monitoraggio delle stesse nel continuo: tale processo, dovrà essere supportato da specifiche procedure di ***Disaster Recovery*** e di ***Gestione degli Incidenti***. Data la complessità e anche la possibile vulnerabilità di queste soluzioni si suggerisce di elaborare anche un processo alternativo per le soluzioni di IA a rischio alto, al fine di garantire la **continuità operativa** dell'azienda.

c. considerare le nuove **vulnerabilità** introdotte in azienda dall'adozione di soluzioni di IA (sia in termini di prevenzione che di Business Continuity, già considerata nel punto precedente). L'IA potrà essere utilizzata in modo malevolo, per far evolvere i Cyber Attack, che diventeranno sempre più sofisticati. Occorrerà, quindi, comprendere come attrezzarsi per difendersi da queste nuove minacce (approcci tradizionali vs. innovativi). Questo aspetto è confermato da una ricerca Protiviti[4] che inserisce le preoccupazioni del Top Management in merito alla

[4] Protiviti – Competing in the Cognitive Age: ricerca svolta in collaborazione con ESI ThoughtLab che riporta l'esito di più di 300 interviste a Top Management di tutto il mondo, operanti in diverse funzioni e in aziende di varie dimensioni e settori (sanità, tecnologia, servizi finanziari e prodotti di consumo, ...).

Data Privacy e agli aspetti legati alla Cyber in cima alla lista dei principali ostacoli all'adozione dell'IA. La stessa ricerca evidenzia anche l'utilizzo dell'IA come motore evolutivo delle tecnologie per la detection e la protezione dai Cyber Risk, sfruttando l'abilità di individuare trend e anomalie in grosse moli di dati. L'IA sarà, quindi, comunque anche un'arma a disposizione dei meccanismi di difesa che potranno diventare sempre più "intelligenti".

Reagire: come comportarsi in caso di Incident

Cosa è un *incident*? Quando si verifica? Come deve essere gestito? Come coinvolgere i diversi attori (produttori, configuratori, clienti)? Queste sono solo alcune delle domande che sorgono spontanee quando si parla di Intelligenza Artificiale e Incidenti.

L'Art. 3 par. 44) del Regolamento attribuisce una prima descrizione al termine "***incidente grave***": *"qualsiasi incidente che, direttamente o indirettamente, causa, può aver causato o può causare una delle seguenti conseguenze:*

a) *il decesso di una persona o gravi danni alla salute di una persona, alle cose o all'ambiente,*
b) *una perturbazione grave e irreversibile della gestione e del funzionamento delle infrastrutture critiche."*

L'Art. 62, invece, descrive il processo per la segnalazione di incidenti e malfunzionamenti: *"I fornitori[5] di sistemi di IA ad alto rischio immessi sul mercato dell'Unione segnalano qualsiasi incidente grave o malfunzionamento di tali sistemi che costituisca una violazione degli obblighi previsti dal diritto dell'Unione intesi a tutelare i diritti fondamentali alle autorità di vigilanza del mercato degli Stati membri in cui tali incidenti o violazioni si sono verificati. Tale notifica è effettuata immediatamente dopo che il fornitore ha stabilito un nesso causale tra il sistema di IA e l'incidente o il malfunzionamento o quando stabilisce la ragionevole probabilità di tale nesso e, in ogni caso, non oltre 15 giorni dopo che è venuto a conoscenza dell'incidente grave o del malfunzionamento."*

Il Regolamento prevede che sia necessario adottare un sistema di monitoraggio successivo all'immissione sul mercato, per *migliorare i sistemi e il processo di progettazione e sviluppo o adottare tempestivamente eventuali misure correttive, tenendo in considerazione l'esperienza sull'uso di sistemi di IA ad alto rischio. Tale sistema è altresì fondamentale per garantire che i possibili rischi derivanti dai sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio possano essere affrontati in modo più efficiente e tempestivo.*

Su questo punto, è importante definire la ripartizione degli obblighi e delle **responsabilità** tra gli operatori economici coinvolti sin dai primi passi dell'adozione di una soluzione: il ciclo di vita di un sistema di IA, infatti, coinvolge numerosi operatori tra cui lo sviluppatore, il soggetto che lo applica, il "deployer" - ossia la persona che utilizza un prodotto o servizio dotato di IA e potenzialmente altri soggetti (es. il produttore, il distributore o l'importatore, i prestatori di servizi, gli utenti professionali o privati).

[5] Art. 3 del Regolamento - "fornitore": *una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o che fa sviluppare un sistema di IA al fine di immetterlo sul mercato o metterlo in servizio con il proprio nome o marchio, a titolo oneroso o gratuito*

Conclusioni

Ricapitolando, oltre ai suggerimenti forniti in ambito Risk Management, Governance e Gestione Incidenti e Responsabilità, suggeriamo alle aziende di valutare adeguate tutele:

- **verso i fornitori / sviluppatori:** partecipando attivamente alla definizione di tutti i requisiti tecnici e funzionali per la soluzione di IA che si vuole implementare e richiedendo agli stessi evidenze puntuali circa le misure di sicurezza attivate;
- **verso gli utenti / clienti finali**: garantendo adeguata informativa circa le operazioni di trattamento del dato effettuate tramite soluzioni di IA e incrementando il livello di awareness interno all'organizzazione, al fine di assicurare correttezza e massima trasparenza nei trattamenti effettuati.

Ci aspettiamo che le funzioni di Risk Management e Compliance svolgano un ruolo centrale nel processo di adeguamento delle aziende al nuovo Regolamento nonché nella gestione delle tematiche legate all'analisi diretta delle soluzioni di Intelligenza Artificiale.

CONTATTI

— **Tamara Devalle** / Director Protiviti / **tamara.devalle@protiviti.it**