AI GOVERNANCE - AI POLICY

APPROVATA DA

PRYSMIAN S.p.A CONSIGLIO DI AMMINISTRAZIONE

29 OTTOBRE 2025

prysmian

The planet's pathways

Indice

1. SCOPO

Prysmian riconosce il potenziale trasformativo dell'Intelligenza Artificiale (AI) per migliorare le operazioni, i prodotti e i servizi. Questa Policy delinea l'impegno di Prysmian per un uso responsabile dell'AI al fine di garantire che le considerazioni etiche siano rispettate, che i rischi siano gestiti e che sia assicurata la conformità alle normative applicabili. Il documento fornisce un framework per guidare tutte le attività relative all'AI, offrendo linee guida per un uso informato e responsabile dell'AI, e stabilendo principi, istruzioni e regole sui comportamenti accettabili e inaccettabili.

2. APPLICAZIONE

Questa Policy si applica a tutte le entità del Gruppo Prysmian (di seguito il "Gruppo"), incluse le terze parti.

Questa Policy si applica a tutto il personale, sia interno che esterno, coinvolto nella gestione o nell'utilizzo degli AI assets del Gruppo (inclusi i sistemi online/cloud). Copre tutti i Sistemi AI sviluppati o utilizzati dal Gruppo all'interno della sua area di responsabilità.

3. DEFINIZIONI

- Sistema AI - Indica un sistema basato su macchina che è progettato per operare con diversi livelli di autonomia e che può mostrare adattività dopo l'implementazione, e che, per obiettivi espliciti o impliciti, inferisce , dall'input che riceve, come generare outputs come predizioni, contenuti, raccomandazioni o decisioniche possono influenzare ambienti fisici o virtuali.
- Tipologie di AI – Traditional AI, Generative AI, Agentic AI
- Algoritmo – Una serie di istruzioni matematiche utilizzate dagli Sistemi AI per elaborare data e prendere decisioni.
- Bias – Distorsione nei data o negli algortmi che può portare a decisions errate o discriminatorie.
- Proprietà Intellettuale– L'insieme dei diritti legali che proteggono le creazioni della mente umana, come invenzioni, opere letterarie e artistiche, design, simboli, nomi e immagini utilizzati nel commercio.
- Categorizzazione biometrica - Processo attraverso il quale un Sistema AI analizza dati biometrici—come caratteristiche facciali, impronte digitali, voice schemi, o altre caratteristiche fisiologiche e comportamentali—per classificare gli individui in categorie specifiche basate su attributi predefiniti (ad esempio, fascia d'età, genere o etnia).
- Deep Learning – Un approccio di Machine Learning basato su deep neural networks per riconoscere schemi complessi nei data.

- Inferenza – Il processo attraverso il quale un modello AI applica ciò che ha imparato per generare predizioni o decisioni su nuovi dati.
- Allucinazioni - Casi in cui un modello AI genera outputs errati, fuorvianti o interamente fabbricati che non sono basati sui dati di input o su fatti del mondo reale.
- Machine Learning – Un sottoinsieme dell'AI che utilizza algoritmi per imparare dai dati e migliorare le performance senza essere esplicitamente programmato.
- Modello - Implementazione concreta di un algoritmo addestrato su un dataset specifico. Dopo che un algoritmo elabora i data e ottimizza i suoi parametri, il risultato è un modello che può essere utilizzato per fare predizioni, decisioni o condurre azioni.
- Reti Neurali – Modello computazionale che consiste in strati di nodi interconnessi che trasformano gli inputs attraverso connessioni ponderate e funzioni di attivazione.

4. RIFERIMENTI

Riferimenti interni:

1. Codice Etico di Prysmian
2. Codice Etico di Business
3. Policy di Crittografia - PO-HR&O-SEC-013
4. Policy di Data Classification- PO-HR&O-SEC-010
5. Policy di Gestione degli incidenti di Data Breach - OP-HR&O-SEC-006

Riferimenti esterni:

1. Regolamento (EU) 2024/1689 del Parlamento Europeo e del Consiglio del 13 Giugno 2024 relativo alle norme armonizzate sull'intelligenza artificiale ('EU AI ACT' - link]
2. Lergge N. 132/2025, sullo sviluppo, adozione e governance dei sistemi di AI [link]
3. ISO/IEC 42001:2023 - Information technology — Artificial intelligence — Management Sistemi.
4. ISO/IEC 23894:2023 - Information technology — Artificial intelligence — Guidance on risk management.
5. NIST AI 100-1 - Artificial Intelligence Risk Management Framework (AI RMF 1.0).

5. PRINCIPI GENERALI

DEFINIZIONE DI IA E TASSONOMIA

Secondo l'EU AI ACT, un Sistema AI è definito come un sistema basato su macchina che è progettato per operare con diversi livelli di autonomia e che può mostrare adattività dopo l'implementazione, e che, per obiettivi espliciti o impliciti, inferisce, dall'input che riceve, come generare outputs come predizioni, contenuti, raccomandazioni, o decisioni che possono influenzare ambienti fisici o virtuali.

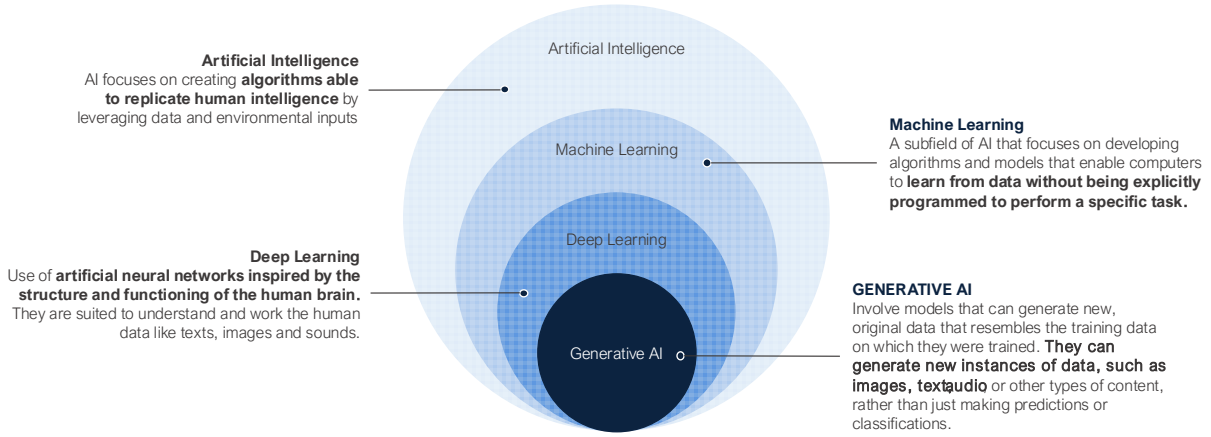

Figura 1: Relazione gerarchica tra le diverse aree dell'IA: Intelligenza Artificiale (IA), Machine Learning, Deep Learning, Gen AI e Agentic AI.

Machine Learning & Deep Learning

Machine Learning e Deep Learning si basano su algoritmi e modelli predefiniti che consentono ai computer di imparare dai data, spesso attraverso l'analisi di datasets e schemi esistenti, anche senza essere esplicitamente programmati per eseguire compiti specifici. Non creano nuovi contenuti ma si concentrano sull'ottimizzazione dei processi e sul decision-making basato sulle informazioni.

Generative AI

L'Artificial Intelligence Generativa (Gen AI) è un ramo dell'AI che si concentra sulla creazione di nuovo contenuti o data da inputs esistenti. A differenza delle forme tradizionali di AI, che si basano principalmente sulla classificazione e l'analisi dei data, la Gen AI può produrre outputs originali in vari formati, come testo, immagini, audio e video, in risposta ai user prompts (inputs).

La Generative AI assume diverse forme ed è utilizzata, ad esempio, per:

- Chatbots

Sfruttare i generative language models per sviluppare chatbots che forniscano risposte accurate e dettagliate basate su un corpus di documenti interni ufficiali, incluse policy aziendali, procedure operative, istruzioni tecniche e manuali di istruzioni per software.

- Agentic AI

L'Agentic AI opera attraverso Large Action Models (LAMs) o architetture simili che integrano capacità di percezione, ragionamento ed esecuzione. Questi Sistemis possono pianificare attività a più fasi, interagire con altri agents o umani e adattare le loro strategie in base al feedback e al contesto.

La Generative AI offre nuovi modi per gli utenti di creare, riassumere, modificare ed eseguire in modo efficiente compiti che coinvolgono la produzione di contenuti.

Adozione dei Sistemi AI

L'adozione degli Sistemi AI porta indubbiamente vantaggi significativi, come maggiore efficienza, automazione e capacità di data processing. Tuttavia, per massimizzare questi benefici, è fondamentale valutare attentamente i rischi associati, inclusa la potenziale per decisioni erronee, la ridotta transparenza nei processi di decision-making e le implicazioni etiche dell'uso dei dati. Questi rischi includono anche possibili impatti sulle operazioni di Prysmian, sulla conformità con le normative vigenti e sulla reputazione dell'azienda.

6. RISCHI E SFIDE DELL'AI

È importante riconoscere che l'uso delle tecnologie di intelligenza artificiale può esporre Prysmian a molteplici sfide e rischi. Alcuni dei principali rischi, allineati con lo standard NIST AIRMF (Artificial Intelligence Risk Management Framework), sono elencati di seguito.

- Data Privacy and Security

  I Sistemi AI sono generalmente basati su modelli "black box" addestrati su vasti dataset disponibili da numerose fonti, il che rende complesso tracciare chiaramente l'origine e le politiche sull'utilizzo dei dati. Inoltre, la condivisione di informazioni confidenziali durante l'addestramento o l'utilizzo di un Sistemi AI potrebbe portare al rilascio di tali informazioni a soggetti non autorizzati. Infine, la raccolta di input di clienti e dipendenti solleva diverse preoccupazioni riguardo ai diritti di utilizzare tali data per l'addestramento dei modelli.

In questo contesto, è cruciale tenere in considerazione le normative sulla privacy e sulla data protection. In particolare, qualsiasi processamento di dati personali eseguito da o in connessione con Sistemi AI deve essere conforme ai principi e agli obblighi stabiliti nel GDPR, inclusi ma non limitati a legalità, equità, trasparenza, finalità, data minimization, integrità, confidenzialità, e accountability. Inoltre, l'uso degli Sistemi AI e qualsiasi attività correlata di data processing devono aderire alle disposizioni delle Policy aziendali applicabili, incluse quelle che regolano la privacy governance e l'uso degli strumenti aziendali.

Esempio: Addestrare Sistemi AI con informazioni aziendali confidenziali o dati personali per scopi diversi da quelli indicati nelle informative fornite ai dipendenti Prysmian, può comportare il rischio di esporre tali informazioni a utenti non autorizzati attraverso richieste specifiche.

- Proprietà Intellettuale

Esiste un rischio che la GenAI possa generare contenuti basato su materiale preesistente protetto da proprietà intellettuale, violando così copyrights o brevetti.
Inoltre, non è sempre chiaro chi sia l'autore effettivo del contenuti generato dagli Sistemi GenAI - ad esempio, si potrebbe sostenere che l'autore dell'output di un Sistemi AI sia l'autore del prompt da cui è stato generato o, al contrario, l'azienda che sviluppa il Sistemi AI.

Esempio: Utilizzare immagini generate da strumenti che non garantiscono l'addestramento su data liberi da copyright in documenti che saranno resi pubblici, con il rischio di violazione del copyright.

- Bias

I data utilizzati per addestrare il model potrebbero non essere pienamente rappresentativi e potrebbero contenere bias verso determinati gruppi di individui. Ciò potrebbe generare e amplificare la discriminazione nei risultati generati, perpetuando possibilmente negative effetti sugli utilizzatori finali.

Esempio : Escludere i CV di candidate donne, alimentando un gender bias e rendendo più difficile per le donne l'ingresso in azienda, anche se potrebbero avere qualifiche e skills appropriate.

- Precisione ed Affidabilità

I Sistemi AI possono produrre errori durante l'utilizzo. L'Artificial Intelligence può talvolta produrre contenuti inaccurato o irrealistico, o persino generare allucinazioni, dove i risultati possono sembrare coerenti ma mancano di una base di veridicità. La qualità delle risposte generate dall'Artificial Intelligence deve essere verificata prima che vengano utilizzate.

Esempio: Una demand forecast inaccurata potrebbe portare a una sovrapproduzione, aumentando i costi di storage, o a una sottoproduzione, con conseguenti ritardi nelle consegne ai clienti.

- Conformità alle normative vigenti

L'EU AI ACT, la prima regolamentazione sull'Artificial Intelligence, è stata approvata a marzo 2024 ed è entrata in vigore nell' agosto 2024. Il rischio di mancata conformità all'EU AI ACT può portare a conseguenze significative per l'organizzazione, incluse sanzioni legali e danno reputazionale

.

Esempio: Lo sviluppo o l'uso di un Sistema AI che rientra negli scopi proibiti definiti dalla regolamentazione può comportare la comminazione di multe per l'azienda.

Inoltre, la Legge Italiana n. 132/2025 è stata approvata il 25 settembre 2025 ed è entrata in vigore il 10 ottobre 2025. Questa legge stabilisce il framework nazionale per lo sviluppo, l'adozione e la governance degli Sistemi AI, in linea con l'EU AI ACT europeo. Il rischio di mancata conformità con la Legge Italiana sull'AI può portare a ulteriori rischio legali e danni reputazionali per l'organizzazione.
Esempio: L'uso di Sistemi AI nei processi di assunzione senza fornire ai lavoratori le informazioni richieste, come stabilito dall'Articolo 11 della legge, può portare a violazioni di conformità e rischi reputazionali per l'Azienda.

- Sostenibilità

L'addestramento degli modelli AI richiede l'uso di enormi quantità di risorse computazionali, poiché i processi di machine learning sono altamente complessi e richiedono processamento intensivo dei dati per analizzare e gestire grandi volumi di data. Questo uso significativo di potere computazionale porta a un elevato dispendio energetico, che non solo influisce sugli costi operativi delle infrastrutture IT, ma ha anche un notevole impatto ambientale. Infatti, gli elevati requisiti enegetici associati a queste operazioni contribuiscono all'aumento delle

emissioni di Co2 ed alla pressione sulle risorse naturali, sollevando importanti problematiche di sostenibilità nello sviluppo e nell'implementazione delle tecnologie AI.
Esempio: L'uso di server ad alta performance, cloud computing, o data centres che consumano una quantità significativa di energia e contribuiscono alle emissioni di Co2.

- Trasparenza e Spiegabilità

La mancanza di trasparenza nei Sistemi AI potrebbe portare gli utenti a interpretare erroneamente le informazioni ricevute dal Sistemi, così come il modo in cui i dati personali e non, sono elaborati dai Sistemi. Inoltre, la complessità di alcuni modelli AI potrebbe portare a un'incapacità di fornire agli stakeholders spiegazioni adeguate per comprendere e giustificare le decisioni prese dai Sistemi.
Esempio: Utilizzare e rendere pubblico, ad esempio sui social media, contenuti generati da Sistemi AI senza indicare che il contenuti è stato prodotto da Sistemi AI.

- Salute e Sicurezza

I Sistemi AI, a causa di possibili problemi di precisione e robusezza, possono introdurre rischi significativi per la sicurezza delle persone, nonché per la loro salute mentale e fisica.

Esempio: Se il Sistema di Machine Vision di un veicolo self-driving non è in grado di rilevare correttamente un pedone che attraversa la strada o un altro veicolo, il risultato potrebbe essere un incidente.

7. PRINCIPI E REGOLE PER UN USO RESPONSABILE DELL'AI

PRINCIPI DI RESPONSIBLE AI

Nel trattare il tema dell'Artificial Intelligence, l'etica gioca un ruolo cruciale nel determinare come questa nuova tecnologia debba essere sviluppata, utilizzata e integrata in Prysmian nel rispetto dei valori umani e dei diritti fondamentali in modo che la tecnologia contribuisca positivamente al benessere umano. A tal fine, Prysmian definisce e adotta i Ethical Principles for Responsible AI, che derivano dal Code of Ethics del Gruppo.

Figure 2: Principles for Responsible AI

- Legalità

I sistemi di intelligenza artificiale devono essere utilizzati in conformità con la legislazione applicabile, in particolare quella relativa alla proprietà intellettuale (IP), alla privacy e alla protezione dei dati personali, nonché con qualsiasi legge specifica che disciplini l'intelligenza artificiale.

- Precisione e Responsabilità

I sistemi di IA devono produrre risultati precisi, coerenti e affidabili, riducendo al minimo errori e distorsioni per garantire prestazioni elevate e l'allineamento con lo scopo previsto. L'intelligenza artificiale ha lo scopo di migliorare le decisioni umane, non di sostituirle.

- Trasparenza

L'uso dei sistemi di intelligenza artificiale deve garantire che gli individui siano consapevoli quando interagiscono con la tecnologia IA e ricevano informazioni sufficienti per comprendere i criteri principali, il ragionamento e i processi alla base dei risultati o delle decisioni del sistema.

- Etica, equità e non discriminazione

I sistemi di intelligenza artificiale devono essere utilizzati in modo responsabile ed etico, nel rispetto della dignità, della libertà e della diversità delle persone, evitando impatti discriminatori e pregiudizi ingiusti.

- Robustezza, sicurezza e salute

I sistemi di intelligenza artificiale devono funzionare in modo robusto, sicuro e protetto per tutta la loro durata di vita, e i potenziali rischi devono essere costantemente valutati e gestiti.

- Supervisione umana

I sistemi di intelligenza artificiale devono essere utilizzati in modo tale da garantire sempre la supervisione umana dei loro risultati, anche al fine di prevenire conseguenze che potrebbero avere ripercussioni sugli individui, nonché risultati errati, distorti o parziali.

- Accountability

Tutti gli attori devono essere responsabili dell'uso dei sistemi di IA e del rispetto dei principi sopra indicati, in base ai loro ruoli, al contesto e in linea con lo stato dell'arte.

8. REGOLE PER UN UTILIZZO RESPONSABILE DELL'AI

Quando si utilizza l'IA, è fondamentale assicurarsi di farlo in modo responsabile ed etico. Ciò implica che si dovrebbe sempre valutare se sia appropriato utilizzare l'IA per uno scopo specifico e, se si decide di utilizzarla, che vengano rispettate le seguenti linee guida:

Comportamenti proibiti

Come previsto dall'AI ACT dell'UE, sono vietate le pratiche di IA proibite, quali:

i. Sistemi di IA che utilizzano tecniche manipolative, subliminali o ingannevoli;
ii. Sistemi di IA che sfruttano le vulnerabilità delle persone;
iii. Sistemi di IA che valutano e classificano le persone sulla base del comportamento sociale e delle caratteristiche personali, determinando un trattamento pregiudizievole

o sfavorevole in contesti sociali non correlati a quello in cui i dati sono stati raccolti e/o ingiustificato o sproporzionato rispetto al comportamento;

iv. Sistemi di IA per valutare il rischio di commissione di reati penali da parte di persone fisiche;

v. Sistemi di IA per creare o ampliare banche dati di riconoscimento facciale mediante la raccolta indiscriminata di immagini facciali da Internet o da filmati di telecamere a circuito chiuso;

vi. Sistemi di IA per dedurre le emozioni di una persona fisica sul posto di lavoro, tranne nei casi in cui l'uso del sistema di IA sia destinato ad essere utilizzato o immesso sul mercato per motivi di sicurezza;

vii. Sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici al fine di trarre deduzioni o conclusioni sulla razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale;

viii. L'uso di sistemi di identificazione biometrica a distanza "in tempo reale" in aree accessibili al pubblico a fini di applicazione della legge.

È inoltre obbligatorio rispettare tutti gli obblighi normativi applicabili in base al livello di rischio identificato in relazione al sistema di IA e al ruolo svolto da Prysmian in relazione a ciascuna singola soluzione/sistema di IA.

Inoltre, in conformità con il principio di responsabilità, è vietato:

a) utilizzare dispositivi, credenziali, indirizzi e-mail o numeri di telefono aziendali per accedere a strumenti di IA disponibili al pubblico (ad esempio Chat GPT);

b) installare interfacce di programmazione di applicazioni, plug-in, connettori o software relativi all'IA non approvati;

c) implementare o utilizzare, in qualsiasi modo, codici generati da GenAI sui sistemi aziendali;

d) utilizzare strumenti di IA, in attività/progetti che coinvolgono terzi, senza che entrambe le parti abbiano condiviso/approvato il loro utilizzo e senza specifiche clausole contrattuali in materia.

- Modalità e finalità di uso

I Sistemi AI devono essere utilizzati solo per lo scopo per cui sono stati progettati e in conformità con le istruzioni per l'utilizzo fornite dal fornitore.
Garantire che i Sistemi AI siano utilizzati in conformità con le istruzioni per l'uso definite dal fornitore è cruciale sia in termini di sicurezza, poiché il Sistemi potrebbe non essere ottimizzato o sicuro per un uso diverso dalla sua finalità predefinita, sia in termini di conformità normativa, poiché un uso errato può esporre Prysmian a multe e sanzioni.

- Esportazione di dati verso Sistemi AI non autorizzati

È proibito esportare, trasferire o condividere dati aziendali con sistemi AI di terze parti che non siano stati esplicitamente approvati dal C.D.A. dell'Azienda e dal Security & AI Committee. L'uso di Sistemi AI autorizzati è l'unica opzione consentita per il processamento di informazioni interne, e qualsiasi uso di un sistema AI esterno deve essere pre autorizzato.

- Dati Personali ed informazioni di business

Salvo specifica autorizzazione, in conformità con i principi di legalità e minimizzazione, non devono essere condivise informazioni aziendali confidenziali, sensibili e riservate, inclusi i dati personali dei dipendenti e di altri parti di business. In particolare, come stabilito nel documento "Data Classification Policy":

  - CONFIDENTIAL RESTRICTED – Questo è il livello di classificazione più alto e identifica informazioni estremamente confidenziali e business critical. La diffusione non autorizzati al di fuori dell'ambito di distribuzione consentito, la perdita, l'uso non conforme e la manomissione rappresentano un rischio grave, in alcuni casi irreversibile, per il Gruppo stesso, i suoi dipendenti o terze parti.
  - CONFIDENTIAL – Questo livello identifica informazioni del Gruppo Prysmian altamente sensibili. Un accesso non autorizzato o rilascio di questo tipo di informazioni pone un rischio medio sul Gruppo e sui suoi stakeholders.
  - INTERNAL – Questo livello identifica informazioni che non appartengono ai livelli precedenti e il cui accesso non autorizzato pone un rischio basso sul Gruppo.
  - PUBLIC – La diffusione non autorizzata delle informazioni al di fuori del Gruppo Prysmian non pone alcun rischio. Informazioni di questo tipo sono accessibili a tutti gli utenti senza restrizioni e/o divulgate pubblicamente dal Gruppo.

È obbligatorio:

- Prima di caricare documenti (incluse registrazioni di riunioni e transcription) su Sistemi AIs, verificare se contengono personal data o informazioni commerciali/aziendali confidenziali.
- Per qualsiasi domanda o chiarimento riguardante la documentazione e i materiali che possono essere caricati su Sistemi AIs, inclusa la verifica della presenza di personal data o informazioni commerciali/aziendali confidenziali, si prega di contattare il Data Protection Officer (DPO) di Prysmian.
- Per qualsiasi domanda riguardante ciò che può costituire personal data e/o informazioni commerciali/aziendali confidenziali, e in generale riguardante le data protection issues, si prega di contattare il DPO.

Quando l'AI è implementata o ospitata da una terza parte, qualsiasi input rappresenterà una "disclosure" di informazioni a una terza parte. Non solo la terza parte avrà accesso all'input fornito, ma questo input potrebbe essere utilizzato per addestrare il model e generare risposte per altri utenti. Infatti, gli modelli AI possono imparare e riprodurre le informazioni nei training data. Ciò può portare alla generazione di outputs contenenti informazioni confidenziali che, se condivise o rese pubbliche, potrebbero compromettere la confidenzialità e la sicurezza.

Ciò significa che qualsiasi cosa venga inserita nei Sistemi AI, in particolare per quanto riguarda i dati personali, deve essere trattata come una diffusione di tali informazioni a una terza parte, soggetta ai requisiti delle leggi applicabili sulla privacy e sulla data protection. Lo stesso principio si applica anche alle informazioni commerciali e aziendali di Prysmian, incluse le informazioni che rientrano nella categoria dei segreti aziandali, che devono essere mantenute private e confidenziali, o informazioni di terze parti per le quali Prysmian ha obblighi di confidenzialità.

Inoltre, va notato che l'inclusione di dati personali e informazioni aziendali e societarie nei Sistemi AI potrebbe comportare rischi significativi per gli individui interessati e per Prysmian, in caso di perdita di dati o incidenti di sicurezza.
Il personale del Gruppo Prysmian, pertanto, deve sempre prestare grande attenzione al tipo di data e informazioni che vengono inseriti nei Sistemi di AI.

- Verifica degli output

In conformità con il principio di sorveglianza umana, l'AI output non deve essere utilizzato per automatizzare completamente un processo di decision-making, ad eccezione degli outputs degli Sistemi AI la cui precisione Prysmian ha verificato o confermato.
Oltre a ciò, in conformità con il GDPR, è vietato automatizzare, con la rimozione dell'operatore umano, processi che utilizzano dati personali e che possono avere un impatto significativo sugli individui, riguardo a decisioni che producono effetti legali o che influenzano significativamente la loro sfera personale o professionale.

È obbligatorio:

- Verificare sempre l'accuracy delle informazioni ricevute quando si utilizzano gli Generative Sistemi AIs;
- Coinvolgere domain experts per verificare l'accuracy delle predictions o recommendations fornite dagli Sistemi AIs, ad eccezione dei casi precedentemente menzionati;
- Prima di utilizzare gli outputs, correggerli se le verifiche rivelano errors o inaccuracies, o violation della privacy e/o inclusione di informazioni/materiale protetto da copyright o intellectual property di terze parti o informazioni/materiale non in linea con i principi del Gruppo Prysmian.

È proibito:

- Utilizzare gli outputs il cui contenuti è inappropriato, discriminatorio (sulla base di razza, religione, genere, origine, età, disability, stato civile, affiliazione politica o sexual orientation) o altrimenti harmful per il Gruppo Prysmian e i suoi stakeholders;
- Utilizzare Gen AI tools per creare testo, audio o visual contenuti per scopi fraudolenti o per travisare l'identità di un individuo;

L'output dell'Artificial Intelligence si basa su modelli statistici-probabilistici e include un fattore randomico integrato. Ciò implica che l'output, sebbene plausibile, può essere inaccurato o inaffidabile, manifestandosi in quella che viene chiamata 'allucinazione'. Inoltre, per i Sistemi AI generativi, anche utilizzando inputs identici, l'output non sarà sempre identico.
È una limitazione conosciuta che i Sistemi AI possano produrre risultati dannosi, biased, incompleti, obsoleti o falsi, presentando questi risultati con un tono apparentemente sicuro, cioè come se fossero certi o pienamente reliable. In questo contesto, gli utenti possono

riporre completa fiducia in outputs errati, allucinati o biased, e prendere decisions e azioni basate su informazioni inaccurate o false.
Pertanto, è cruciale non utilizzare mai qualcosa prodotto dall'Artificial Intelligence senza prima rivedere e verificare la precisione dell'output. L'Artificial Intelligence è destinata a migliorare il human decision-making e a rendere alcune azioni aziendali più efficienti, mai a sostituirlo.

Proprietà Intellettuale

Salvo specifica autorizzazione, gli asset aziendali proprietari non devono essere forniti come input a un Sistemi AI, né output che possano violare il copyright di altri.
È essenziale non utilizzare o riprodurre contenuti soggetto a copyright di terze parti o diritti di proprietà intellettuale senza un'appropriata licenza. Comprendere e rispettare le leggi sul copyright applicabili ed i licence agreements è essenziale quando si impiegano materiali preesistenti, come immagini, testo o musica, come input per l'AI. Poiché le soluzioni AI sono addestrate utilizzando manufatti originali creati da esseri umani, l'output può violare i diritti di terze parti se è sufficientemente simile a materiali esistenti. Esempi particolarmente rischiosi includono manufatti grafici, come i loghi.

- Utilizo etico e whistleblowing

L'uso dell'AI deve essere conforme ai principi etici stabiliti in questo documento ed ai valori del Gruppo stabiliti nel Codice Etico. Se c'è un sospetto di uso non conforme a questi principi (ad esempio, discriminazione di genere nella selezione del personale), deve essere fatta una segnalazione attraverso il calane del DPO.
Inoltre, qualsiasi sospetto di malfunzionamento o interruzione dell'operazione del Sistemi (ad esempio, perdita di accesso al Sistemi, diffusione di dati personali non necessari) deve essere immediatamente segnalato a privacy@prysmian.com e/o al DPO, in linea con le disposizioni delle procedure su security e privacy incidents, come descritto nel documento di "Data Breach Incident Management".
È essenziale riconoscere che qualsiasi condotta non etica o impropria, che non rispetti la dignità umana e la libertà degli individui, e che non sia in accordo con i principi e i valori promossi da Prysmian, non è né approvata né supportata da Prysmian. Tale condotta potrebbe mettere a repentaglio la reputazione e l'affidabilità di Prysmian, generando conseguenze negative per l'Azienda, inclusi potenziali impatti finanziari.

- Trasparenza nell'uso dei Sistemi AI

È necessario garantire la massima trasparenza, all'interno e all'esterno del Gruppo Prysmian, su come l'AI viene utilizzata per supportare il business.

È obbligatorio:

- Informare il proprio manager prima di utilizzare un AI tool per l'esecuzione di un'attività lavorativa
- Attribuire chiaramente qualsiasi output utilizzato per scopi lavorativi all'AI tool che lo ha generato (ad esempio, tramite una footnote o altri mezzi visibili al lettore, indicando che il contenuti è stato generato tramite un AI tool e specificando il name di quel tool).

È cruciale non presentare mai contenuti prodotto dall'AI, né all'esterno né all'interno di Prysmian, senza dichiarare chiaramente il ruolo dell'AI nella creazione di tale contenuti. Ciò include, quando necessario, un'indicazione della specifica soluzione AI utilizzata.

Inoltre, se la Generative AI viene utilizzata per generare o manipolare visual, audio o video contenuti, deve essere reso chiaro che tale contenuti è stato artificialmente generato o modificato.

9. MODELLO OPERATIVO

AI Governance and Compliance Framework

In linea con questa Policy, devono essere definiti processi e procedure per supportare l'efficace management delle attività relative ai Sistemi AI.

Identificazione e Catalogazione dei Sistemi AI

L'identificazione dei Sistemi AI si riferisce al processo di riconoscere un Sistema come appartenente a uno delle varie tipologie di AI, tenendo conto di fattori distinti come caratteristiche tecniche, finalità specifiche, ed applicazione pratiche. Questo processo richiede un'analisi approfondita delle capacità operative del Sistema, del livello di autonomia, dei modalità di apprendimento, e delle tecnologie sottostanti, al fine di comprendere come il Sistema opera e quali rischi può comportare.

Il catalogo dei Sistemi AI rappresenta un componente centrale di un AI Governance framework. È un repository strutturato e completo che registra tutti i Sistemi AI in uso o in sviluppo all'interno dell'organizzazione.

Classificazione dei Sistemi AI secondo l'EU AI Act

L'AI ACT dell'UE introduce una classificazione basata sul rischio per i sistemi di IA a seconda del loro potenziale impatto sui diritti fondamentali, sulla sicurezza e sulla salute umana, con l'obiettivo di garantire uno sviluppo e un utilizzo sicuro, equo e trasparente dell'IA. Il processo di classificazione determina la categoria di rischio del sistema di IA, che definisce i corrispondenti obblighi normativi.

- Gestione del rischio AI

Il processo di gestione dei rischi legati all'IA identifica e valuta le minacce e i rischi associati allo sviluppo, all'implementazione e all'uso dei sistemi di IA. Vengono definiti e implementati dei controlli per mitigare tali rischi. Il processo mira a garantire che i sistemi di IA funzionino in modo sicuro, etico e conforme alle normative, riducendo al minimo gli impatti negativi su individui, organizzazioni e società nel suo complesso.

- Conformità normativa

A seconda della classificazione di rischio del sistema di IA, devono essere attuate misure adeguate e proporzionate per garantire il pieno rispetto degli obblighi delineati nell EU AI Act, nonché in altre normative applicabili. Tali misure dovrebbero essere in linea con la natura e la gravità del rischio identificato, al fine di garantire che lo sviluppo, l'implementazione e l'uso dell'IA avvengano in modo sicuro, equo e trasparente, proteggendo al contempo i diritti fondamentali, la sicurezza e la salute umana.

Le azioni di protezione, attuate attraverso processi e procedure definiti, devono essere applicate in modo proporzionale al valore e al livello di rischio associati ai sistemi di IA, in conformità con il quadro normativo applicabile.

Per garantire una gestione sicura ed etica dei sistemi di IA, i processi stabiliti devono garantire che:

- I dipendenti e le parti interessate coinvolti nell'implementazione e nell'uso dei sistemi di IA agiscano in conformità con il quadro di governance responsabile dell'IA dell'azienda;
- Il miglioramento continuo della gestione dei sistemi di IA, con particolare attenzione alla trasparenza, all'equità e alla mitigazione dei rischi.

Nel complesso, Prysmian garantisce che i sistemi di Intelligenza Artificiale siano sviluppati e gestiti in linea con i principi di cui sopra e in conformità con tutte le normative e disposizioni applicabili in materia di governance dell'IA.

- Sostenibilità, Impatto e Considerazioni sull'utilizzo dell'AI

L'addestramento dei modelli di IA richiede l'uso di enormi quantità di risorse computazionali, poiché i processi di apprendimento automatico sono molto complessi e richiedono un'elaborazione intensiva per analizzare e gestire grandi volumi di dati. Questo uso significativo di potenza di calcolo comporta un elevato consumo energetico, che non solo incide sui costi operativi delle infrastrutture IT, ma ha anche un notevole impatto ambientale. Infatti, l'elevato fabbisogno energetico associato a queste operazioni contribuisce all'aumento delle emissioni di carbonio e alla pressione sulle risorse naturali, sollevando importanti questioni di sostenibilità nello sviluppo e nell'implementazione delle tecnologie di IA.

10. MODELLO ORGANIZZATIVO

Nell'ambito della governance dei sistemi di IA, vengono identificate le principali funzioni aziendali coinvolte e vengono definiti i loro ruoli e responsabilità nella gestione dell'IA.

Principali Attività di Gestione dei Sistemi AI

DPO & Compliance

- Identificazione delle normative nazionali e internazionali in materia di IA (ad esempio, EU AI ACT, GDPR, normative nazionali di attuazione);
- Responsabile di garantire la conformità dei processi e della documentazione di riferimento alla legislazione vigente in materia di IA e protezione dei dati;
- Supporta l'Ufficio dei CIO nell'identificazione della classificazione dei rischi dei sistemi di IA, in conformità con i requisiti dell'EU AI ACT;
- Valutazione dell'impatto per la conformità normativa e i diritti fondamentali, in particolare per i sistemi ad alto rischio;
- Supporta i dipartimenti nella segnalazione di incidenti gravi, in particolare quelli relativi a sistemi ad alto rischio.
- Fornisce formazione specifica a tutto il personale coinvolto nell'uso dei sistemi di IA e prepara e aggiorna i materiali di formazione sui sistemi di IA, la governance dell'IA e la legislazione applicabile.
- Collabora con altre funzioni aziendali (ad esempio, legale, gestione dei rischi, risorse umane, IT, sicurezza) per garantire una governance integrata e l'allineamento tra la protezione dei dati e i requisiti di conformità dell'IA.

Information & Cybersecurity

- Identificazione e valutazione dei rischi per la sicurezza informatica connessi all'implementazione e all'uso dell'IA, garantendo una gestione adeguata, in particolare per i sistemi ad alto rischio;
- Esecuzione di test e audit indipendenti per verificare la conformità ai requisiti di sicurezza, in particolare per i sistemi ad alto rischio (ad esempio, analisi delle vulnerabilità, simulazioni di attacchi, controlli dell'integrità dei dati);
- Definizione di un piano di risposta agli incidenti specifico per l'IA, mirato in particolare alle vulnerabilità dei sistemi ad alto rischio;

- Promozione della consapevolezza dei rischi per la sicurezza informatica legati all'IA tra le parti interessate coinvolte in progetti di IA;
- Supervisione e coordinamento dei processi di risposta agli incidenti legati all'IA per garantire una risoluzione tempestiva e un miglioramento continuo;
- Promozione dell'alfabetizzazione organizzativa in materia di IA attraverso lo sviluppo di iniziative di formazione e risorse che migliorino la comprensione e l'uso responsabile delle tecnologie di IA.

Risorse Uman

- ·Supervisione del potenziale dell'IA per la forza lavoro;
- Garantire che l'uso dell'IA sia in linea con i valori etici aziendali, promuovendo un'applicazione equa e non discriminatoria;
- Promuovere iniziative di formazione sull'uso responsabile dell'IA.

Ufficio Acquisti

- Responsabile della revisione dei processi di qualificazione e contrattazione con i fornitori di soluzioni o servizi di IA al fine di includere misure di salvaguardia contro rischi legali, questioni relative alla proprietà intellettuale e limitazioni di responsabilità;
- Responsabile di informare l'Ufficio Legale e Affari Societari qualora vengano individuati appalti che coinvolgono soluzioni di IA.

Ufficio dei CIO aziendali e governance IT

- Responsabile della verifica della conformità delle soluzioni AI e dei processi di sviluppo alle Linee guida Prysmian per lo sviluppo responsabile dell'intelligenza artificiale;
- Integrazione della gestione dei rischi legati all'intelligenza artificiale nel sistema di gestione dei rischi aziendali (ad esempio, identificazione delle aree di conformità interessate, definizione di nuovi controlli);
- Responsabile della definizione e del monitoraggio delle metodologie e degli strumenti di governance dei dati, in particolare per quanto riguarda l'analisi dei set di dati di formazione e operativi per i sistemi ad alto rischio, identificando problemi di qualità, rappresentatività o distorsione;
- Responsabile dell'archiviazione, della gestione e della facile recuperabilità di tutta la documentazione tecnica relativa ai sistemi di IA;
- Responsabile dell'implementazione di sistemi di registrazione automatica che registrano in modo continuo e sistematico le operazioni o le situazioni che

comportano potenziali rischi per i sistemi di IA, in particolare per i sistemi ad alto rischio, garantendo l'accessibilità ai fini di audit;
- Responsabile della manutenzione dell'inventario dei sistemi di IA.

Proprietà Intellettuale

- Protezione dei diritti di proprietà intellettuale di Prysmian, con particolare attenzione alla salvaguardia dei dati, dei contenuti e delle opere aziendali che potrebbero essere utilizzati per addestrare i sistemi di intelligenza artificiale;
- Prevenzione dell'uso non autorizzato di dati, opere o contenuti protetti da copyright di terzi nello sviluppo, nell'addestramento o nell'implementazione di sistemi di IA;
- Conformità alle leggi applicabili e alle politiche aziendali in materia di copyright, brevetti, marchi commerciali e modelli di utilità, in coordinamento con le funzioni legali competenti.

AI Governance Committee

Data la natura interfunzionale dei rischi e delle opportunità legati all'IA, il Comitato di governance dell'IA di Prysmian opera in modo cooperativo e interdisciplinare tra i dipartimenti sopra citati. Ha il compito di:

- Valutare le proposte relative all'IA da una prospettiva olistica, includendo gli aspetti tecnici, operativi, legali ed etici. Ciò comprende la fattibilità tecnica, il ritorno economico e gli impatti etici/reputazionali. Il comitato raccoglie i contributi dei vari dipartimenti e fornisce indicazioni sulla gestione dei rischi, esprimendo un parere sull'opportunità di procedere con un'iniziativa di IA o individuando le questioni critiche da affrontare;
- Fungere da punto di riferimento o di escalation per segnalazioni, reclami o controversie relative all'IA, in particolare quelli che richiedono una valutazione imparziale e multidisciplinare. Valuta i rischi associati e raccomanda azioni correttive, promuovendo la trasparenza e la fiducia nei sistemi di IA;
- Promuovere un approccio responsabile durante tutto il ciclo di vita del sistema di IA definendo linee guida generali per lo sviluppo, il collaudo, l'implementazione, il monitoraggio e l'approvvigionamento. Queste garantiscono che l'utilizzo dell'IA sia in linea con i valori aziendali e i principi di trasparenza e sostenibilità.

11. CONSEGUENZE IN CASO DI VIOLAZIONE

In qualità di dipendente Prysmian o terza parte, l'utente accetta di sostenere il nostro impegno nei confronti della condotta etica e dell'integrità e di rispettare il nostro Codice Etico. I dipendenti Prysmian che violano tale impegno o non rispettano la presente Politica saranno soggetti a procedimenti disciplinari, compreso il possibile licenziamento, e a qualsiasi altra azione legale necessaria a proteggere gli interessi e la reputazione di Prysmian. La Società si riserva il diritto, a sua esclusiva discrezione, di divulgare informazioni relative a violazioni della legge da parte di dipendenti Prysmian alle autorità di regolamentazione competenti.

I partner commerciali e le terze parti che agiscono per conto della Società che violano la presente Politica saranno soggetti a conseguenze finanziarie e legali, ove applicabile, tra cui la risoluzione del contratto e il divieto di intrattenere rapporti commerciali con il Gruppo Prysmian.

12. SEGNALAZIONI IN CASO DI VIOLAZIONE

In qualità di dipendente Prysmian, sei tenuto a segnalare qualsiasi violazione della presente Politica a:

a) la **IF Helpline**, oppure

b) il tuo Team di conformità regionale o gli altri soggetti designati menzionati nella presente Politica.

13. AUDIT E MONITORAGGIO

Utilizzando un approccio basato sul rischio, la Funzione Compliance del Gruppo e la Direzione Internal Audit possono svolgere periodicamente, rispettivamente, attività di monitoraggio o di audit volte a verificare la corretta applicazione della presente Politica all'interno dell'organizzazione.

14. REVISIONE

L'intelligenza artificiale è un settore in continua e rapida evoluzione, caratterizzato da progressi significativi e innovazioni costanti. In questo contesto, Prysmian si impegna a rivedere periodicamente la presente politica per garantire che rimanga pertinente e aggiornata rispetto alle ultime tendenze e agli sviluppi nel settore dell'IA. È essenziale consultare regolarmente la presente politica, poiché contiene indicazioni preziose e aggiornamenti cruciali per garantire un uso responsabile e conforme delle tecnologie di IA

all'interno dell'organizzazione. Questo approccio proattivo consentirà a Prysmian di affrontare le sfide emergenti e di sfruttare al massimo le opportunità offerte dall'IA.

15. DOCUMENTI CORRELATI

I seguenti documenti sono correlati alla presente Politica e devono essere consultati da tutti i Dipendenti Prysmian per ulteriori indicazioni. Parte di tali documenti è disponibile sulla homepage Prysmian Ethics & Integrity della **Intranet** della nostra Società ed è anche accessibile al pubblico nella sezione corrispondente del nostro **sito web aziendale**.

a) Codice Etico;

b) Politica sulla Helpline.