OSSERVATORIO
CORPORATE LEADERS

DOCUMENTO PROGRAMMATICO

PROPOSTE PER UNA GOVERNANCE DELL'INTELLIGENZA ARTIFICIALE NELLE IMPRESE

2026

in collaborazione con
assonime
L'associazione delle imprese

OSSERVATORIO CORPORATE LEADERS

Direttore Scientifico
Michele Carpagnano

Comitato Scientifico
Alessandro Nespoli, Domenica Lista
e Valentina Ranno

Collaborano con l'Osservatorio Corporate Leaders:

Francesco Lamanna, Angela Raffaele
e Adelaide Zorzettig.

www.the-experts-talk.com

info@the-experts-talk.com

Piazza Vicenza n. 8
38122 Trento

INDICE

ABSTRACT

Il presente documento, elaborato dal gruppo di lavoro Experts Talk Corporate Leaders in collaborazione con Assonime, propone un quadro strategico integrato per supportare i vertici aziendali nella *governance* dell'intelligenza artificiale e nella gestione delle trasformazioni che essa sta determinando nei modelli di *business*, nei processi decisionali e negli assetti organizzativi delle imprese.

Muovendo dall'analisi delle principali sfide emerse nei percorsi di adozione dell'IA, il documento individua indirizzi operativi, modelli di *governance* e *best practices* fondati su un approccio multidisciplinare che integra profili giuridici, tecnologici, organizzativi, manageriali ed etico-sociali.

Le raccomandazioni si sviluppano lungo quattro direttrici strategiche:

- il rafforzamento della governance e dei sistemi di gestione del rischio;
- l'integrazione tra intelligenza artificiale, sostenibilità e responsabilità sociale d'impresa;
- la promozione della resilienza digitale e della sicurezza geopolitica delle catene del valore;
- la tutela della concorrenza e dei consumatori nei mercati digitali.

L'obiettivo è fornire ai *corporate leaders* strumenti concreti per governare l'innovazione in modo responsabile, favorendo la competitività delle imprese, la creazione di valore sostenibile e la tutela dei diritti fondamentali, in coerenza con l'evoluzione del quadro normativo europeo e con le crescenti aspettative degli *stakeholders*.

Il documento rappresenta il risultato del lavoro congiunto di ventinove esperti provenienti dal mondo dell'impresa, delle istituzioni, dell'accademia e delle professioni, e recepisce gli sviluppi normativi, tecnologici e applicativi maturati a livello nazionale ed europeo fino a maggio 2026[1].

---

1 Tra gli Esperti che hanno partecipato alla prima edizione di Experts Talk Corporate Leaders tenutasi a Madonna di Campiglio dal 3 al 5 dicembre 2025, in ordine alfabetico: Patrizia Ballardini, Daniele Bobba, Tommaso Buganza, Fabrizio Caretta, Francesca Carpagnano, Michele Carpagnano, Rosy Cinefra, Sara Citterio, Fabrizia Fiandaca, Stefano Firpo, Fabio Orlando Fiumanò, Domenica Lista, Tiziana Lombardo, Giulia Marinelli, Jessica Meloni, Alessandro Musella, Maurizio Napolitano, Alessandro Nespoli, Niccolò Pallesi, Nicola Polito, Oreste Pollicino, Maria Pratesi, Paolo Quaini, Valentina Ranno, Sara Rolandi, Ernesto Tammaro, Pietro Tredici, Rosanna Volpe e Francesco Wembagher.

Tra gli Esperti che hanno contribuito alla redazione del Documento Programmatico Corporate Leaders 2026: Daniele Bobba, Tommaso Buganza, Fabrizio Caretta, Francesca Carpagnano, Michele Carpagnano, Rosy Cinefra, Sara Citterio, Fabrizia Fiandaca, Stefano Firpo, Fabio Orlando Fiumanò, Domenica Lista, Tiziana Lombardo, Giulia Marinelli, Jessica Meloni, Alessandro Musella, Maurizio Napolitano, Alessandro Nespoli, Niccolò Pallesi, Oreste Pollicino, Maria Pratesi, Paolo Quaini, Valentina Ranno, Sara Rolandi, Ernesto Tammaro, Pietro Tredici, Rosanna Volpe e Francesco Wembagher.

Maggiori informazioni su Experts Talk Corporate Leaders sono disponibili al seguente link: https://www.the-experts-talk.com/it/experts-talk-corporate-leaders-2/

Si ringrazia Prysmian in qualità di Main Partner e Deloitte, in qualità di Partner, per aver condiviso il progetto e l'approccio metodologico Experts Talk.

Si ringrazia Assonime per la collaborazione nella redazione del Documento Programmatico.

SEZIONE I
PREMESSA METODOLOGICA

1. Obiettivi e finalità del Documento Programmatico Corporate Leaders 2026

Il Documento Programmatico Corporate Leaders 2026 nasce a Madonna di Campiglio in occasione della prima edizione di *The Experts Talk Corporate Leaders* in cui 29 selezionati esperti si sono riuniti dal 3 al 5 dicembre 2025 per confrontarsi sulle sfide e le opportunità connesse alla progressiva integrazione dell'intelligenza artificiale nelle imprese e nelle attività di impresa.

Il Documento Programmatico Corporate Leaders 2026 è un lavoro corale volto a mettere a disposizione degli *stakeholders*, dei vertici aziendali e della collettività un orientamento strategico che parta dallo *status quo* e guardi al futuro.

In un contesto caratterizzato da una crescente interazione tra innovazione tecnologica, regolazione giuridica e dinamiche geopolitiche, il Documento Programmatico si propone di:

- fornire una lettura integrata delle trasformazioni in atto;
- individuare modelli operativi e *best practices* idonei a supportare le imprese nella gestione del rischio e nella definizione delle strategie;
- contribuire al dibattito istituzionale e sociale attraverso proposte concrete.

Il Documento Programmatico non si limita a un approccio teorico ma intende offrire strumenti decisionali per i *Corporate Leaders* chiamati a operare quotidianamente in contesti di crescente complessità.

2. Metodo di lavoro Experts Talk

Il Documento Programmatico Corporate Leaders 2026 è il risultato di un lavoro corale di 29 esperti.

Partendo dalle sessioni di lavoro in alta quota, in una *board room* allestita per l'occasione a 2.100 mt. di altitudine, a Madonna di Campiglio, nel mese di dicembre 2025, è continuato fino al 5 maggio 2026 attraverso riunioni periodiche e momenti di confronto informale culminati nella sessione plenaria di *drafting session* tenutasi a Milano il 5 maggio 2026, che ha condotto ad un processo di elaborazione articolato, fondato sul confronto tra esperti provenienti da ambiti differenti (impresa, istituzioni, accademia, professioni).

Il metodo adottato si basa su alcuni elementi distintivi:

- dialogo strutturato tra pari;
- valorizzazione dell'esperienza concreta dei partecipanti, attraverso il confronto su casi reali e scenari applicativi;
- sviluppo progressivo dei contenuti, a partire dalle sessioni di lavoro bisettimanali Experts Talk fino alla *drafting session*.

In tale prospettiva, il Documento Programmatico rappresenta una tappa di un percorso continuo, destinato a evolversi attraverso ulteriori contributi e momenti di confronto[2].

3. Metodo di analisi: dallo *status quo* alle *best practices* operative

L'analisi sviluppata nel Documento Programmatico segue una struttura omogenea, articolata in due livelli:

- analisi dello *status quo*, volta a identificare criticità, *trend* evolutivi e principali rischi;

2 Il presente documento è stato elaborato dal gruppo di lavoro *Experts Talk Corporate Leaders*. Il quadro analitico, le posizioni sostanziali, le proposte operative e l'impostazione argomentativa complessiva riflettono esclusivamente il giudizio indipendente degli esperti, cui spetta la piena responsabilità editoriale e intellettuale del contenuto.

Strumenti di intelligenza artificiale sono stati utilizzati come supporto alla stesura del documento, in particolare per assistere nella strutturazione, nella formulazione e nella coerenza redazionale tra le sezioni. Tutti i contenuti analitici, le valutazioni e le raccomandazioni sono stati concepiti, indirizzati e validati dagli esperti. I riferimenti normativi, le fonti e i dati fattuali sono stati verificati in modo indipendente.

Il ricorso a strumenti di redazione assistita da intelligenza artificiale non incide sull'indipendenza delle posizioni espresse, che sono quelle del gruppo di lavoro e non rappresentano le opinioni di alcuna impresa, studio professionale o autorità con cui gli esperti hanno rapporti.

Le opinioni e le valutazioni espresse nel presente documento programmatico non riflettono necessariamente le posizioni delle istituzioni o organizzazioni di appartenenza dei singoli esperti che hanno contribuito al gruppo di lavoro.

- proposte operative, formulate in termini di *best practices*, modelli organizzativi e strumenti di *governance*.

Questo approccio consente di superare una lettura meramente descrittiva, per offrire indicazioni concrete, implementabili e verificabili, in linea con le esigenze delle imprese.

Particolare attenzione è dedicata all'integrazione tra cinque dimensioni: i) giuridica; ii) tecnologica; iii) organizzativa; iv) di impresa ed v) etica e sociale.

4. Prospettiva degli *stakeholders*

Il Documento Programmatico adotta una prospettiva di analisi multilivello, che tiene conto delle esigenze e delle aspettative di:

- imprese e *corporate leaders*;
- autorità regolatorie e istituzioni pubbliche;
- mercato e operatori economici;
- consumatori e società civile.

L'obiettivo è favorire un equilibrio tra:

- innovazione e tutela dei diritti;
- competitività e sostenibilità;
- autonomia imprenditoriale e responsabilità sociale.

SEZIONE II
INTELLIGENZA ARTIFICIALE ED ETICA AZIENDALE

1. *Governance* e regolamentazione, valutazione e gestione del rischio

STATUS QUO 2026

L'integrazione di sistemi di intelligenza artificiale (IA) nei processi decisionali aziendali incide non solo sull'efficienza operativa ma anche sulla distribuzione delle responsabilità e sugli assetti di *governance*. In particolare, l'utilizzo di sistemi di IA basati su modelli avanzati e generativi comporta una crescente opacità nei processi decisionali e rende più complessa l'attribuzione delle responsabilità connesse agli *output* prodotti.

Il quadro normativo europeo, con l'entrata in vigore dell'AI Act, introduce un sistema articolato di classificazione dei rischi e obblighi differenziati, imponendo un significativo rafforzamento delle capacità di gestione del rischio tecnologico.

Nella prassi, tuttavia, l'adozione dell'IA viene spesso affrontata come una questione di carattere tecnico o informatico, senza un adeguato coinvolgimento dei vertici aziendali e senza un'integrazione nei sistemi di *governance* e di controllo interno.

Ne consegue il rischio di un crescente disallineamento tra:

- la velocità di adozione dell'IA;
- la capacità organizzativa e gli assetti di governo societario;
- gli obblighi di conformità normativa e di gestione del rischio.

PROPOSTA

(i) Integrazione sistemica nel *risk management* e mappatura dei rischi

Integrare i sistemi di IA nei modelli di Enterprise Risk Management (ERM) prevedendo specifici indicatori di rischio, quali rischio algoritmico, rischio *bias*, rischio reputazionale.

(ii) Centralità del CdA e dei comitati endoconsiliari

Assicurare il coinvolgimento del CdA e, ove presenti, dei comitati endoconsiliari (in particolare quelli competenti in materia di controllo interno, rischi e sostenibilità) attribuendo loro la definizione delle politiche aziendali in materia di IA e la supervisione della relativa attuazione.

(iii) *Accountability* diffusa

Promuovere una chiara attribuzione di responsabilità lungo tutta la struttura operativa.

(iv) *Framework* di classificazione dei sistemi di IA

Adottare modelli interni di classificazione coerenti con l'approccio *risk-based* dell'AI Act, garantendo l'aggiornamento continuo in funzione dell'evoluzione tecnologica e normativa.

(v) Sistemi di tracciabilità e documentazione

Implementare adeguati sistemi di tracciabilità delle decisioni e degli *output* generati dai sistemi di IA al fine di assicurare *audit trail* efficaci e verificabili.

(vi) Funzioni di controllo indipendenti

Prevedere verifiche periodiche attraverso *audit* interni o esterni, volti a valutare la conformità e l'affidabilità dei sistemi di IA adottati.

2. Strategia, sostenibilità e responsabilità sociale

STATUS QUO 2026

La *governance* digitale non è soltanto uno strumento di controllo delle tecnologie: è strettamente connessa alla strategia sociale dell'impresa, ossia alle modalità con cui l'organizzazione interagisce con i propri *stakeholders*, tra cui clienti, fornitori e terze parti.

Mentre la *governance* digitale definisce regole, responsabilità e processi per lo sviluppo, l'adozione e l'utilizzo delle tecnologie, la strategia sociale orienta tali scelte verso obiettivi di equità, inclusione e tutela dei diritti.

In questo contesto, l'integrazione dell'intelligenza artificiale nei processi decisionali aziendali rappresenta un'evoluzione centrale della *governance* contemporanea, all'interno della quale la componente tecnologica si intreccia con profili giuridici, organizzativi ed etici, incidendo sulle modalità attraverso le quali l'impresa assume decisioni, attribuisce responsabilità, gestisce i rischi e tutela i diritti dei soggetti coinvolti.

L'intelligenza artificiale assume pertanto il ruolo di fattore strategico di trasformazione organizzativa, in grado di accelerare l'integrazione dei principi ESG nel contesto aziendale. Le imprese sono chiamate non solo ad integrare tali principi nei propri piani strategici, ma anche ad incorporarne i valori nella cultura aziendale e nei processi decisionali, in coerenza con l'evoluzione del quadro normativo e con le crescenti aspettative degli *stakeholders*.

In questo contesto, la responsabilità sociale d'impresa non può essere limitata alle tradizionali dimensioni ambientali e sociali, ma deve estendersi alla capacità di progettare, implementare e governare sistemi di IA secondo criteri di equità, trasparenza, *accountability* e tutela dei diritti fondamentali.

Strategia aziendale e integrazione dei principi ESG

L'integrazione tra *governance* digitale e strategia sociale si manifesta con particolare evidenza con riferimento all'utilizzo di tecnologie in grado di incidere sui processi decisionali, sugli assetti organizzativi e sulle relazioni dell'impresa con i propri *stakeholders*.

L'utilizzo di sistemi algoritmici e di IA può incidere su decisioni riguardanti il lavoro, l'accesso ai servizi, la valutazione delle *performance* e l'attribuzione di opportunità. Ne deriva l'esigenza di adottare adeguati presidi volti a prevenire discriminazioni ed effetti distorsivi.

L'adozione di sistemi di IA pone inoltre il tema della attribuzione delle responsabilità all'interno dell'organizzazione. La crescente automazione dei processi decisionali richiede di individuare i soggetti responsabili delle decisioni assunte con il supporto dei sistemi di IA, delle modalità di utilizzo di tali sistemi e della gestione dei relativi rischi.

La trasparenza assume un ruolo centrale quale presupposto necessario per rafforzare la fiducia nei rapporti con gli *stakeholders*. Una *governance* digitale efficace contribuisce a tale obiettivo attraverso la comprensibilità delle regole che governano l'utilizzo dei dati e dei sistemi algoritmici.

In tale contesto, la *governance* dell'IA diviene parte integrante della dimensione sociale delle politiche ESG, poiché temi quali diritti fondamentali, equità, inclusione e condizioni di lavoro risultano sempre più strettamente connessi alle modalità con cui le imprese sviluppano e utilizzano le tecnologie digitali.

PROPOSTA

Si propone di integrare l'IA nei *framework* esistenti di gestione del rischio, *compliance* e responsabilità degli organi societari.

A tal fine, si individuano le seguenti *best practices* operative:

(i) *Governance* e supervisione del CdA

L'attenzione del Consiglio di Amministrazione e dei comitati endoconsiliari competenti (quali ad esempio i comitati rischi e sostenibilità) dovrà concentrarsi su profili quali l'attribuzione della responsabilità per gli *output* generati dai sistemi di IA, la tracciabilità delle decisioni automatizzate, la prevenzione dei c.d. *bias* (intesi quali pregiudizi) e fenomeni discriminatori, nonché la gestione dei rischi reputazionali e di *compliance*.

In tal contesto, la supervisione da parte di figure dotate di adeguate competenze tecniche e giuridiche assume un ruolo fondamentale. Le attività di vigilanza e controllo devono essere reinterpretate alla luce delle nuove dinamiche introdotte dall'automazione decisionale, garantendo che i processi decisionali automatizzati siano comprensibili, verificabili e coerenti con gli obiettivi aziendali e con i requisiti normativi.

L'IA diventa quindi materia di governo societario, con rilevanti implicazioni in termini di doveri fiduciari degli amministratori, responsabilità nei confronti degli azionisti e aspettative degli investitori.

La supervisione degli esperti e di coloro che sono deputati a controllare tali *output* alla luce di una nuova declinazione dei concetti di vigilanza e controllo devono restare fondamentali. In questo senso, l'AI diventa materia di governo societario, con ricadute sui doveri fiduciari degli amministratori, sulla responsabilità verso gli *shareholders* e sulle aspettative degli investitori.

(ii) Ruolo dei *corporate leaders*

L'adozione di sistemi di IA richiede un approccio interdisciplinare che integri competenze giuridiche, tecnologiche, organizzative e di *risk management*, attraverso:

- la definizione di *policy* interne sull'utilizzo di sistemi di IA, secondo criteri etici e giuridici chiaramente individuati;
- la valutazione preventiva dei rischi mediante strumenti quali gli *AI impact assessments* e le *algorithmic risk reviews*;
- l'istituzione ed il coordinamento di comitati di supervisione interdisciplinari;
- la definizione di processi di responsabilità interna attraverso i modelli di *accountability* documentati e verificabili.

In questo modo, i *corporate leaders* assumono una funzione di garanzia nella *governance* dell'IA, assicurando coerenza tra innovazione tecnologica, strategie di investimento, obblighi normativi e valori aziendali. A tale funzione si affianca un ruolo di indirizzo culturale, volto a promuovere trasparenza, formazione, consapevolezza del rischio e procedure organizzative che preservino la centralità della persona anche nell'era dell'automazione.

Strategia aziendale, sostenibilità e intelligenza artificiale

La strategia aziendale è orientata, soprattutto nel medio-lungo termine, alla definizione delle linee di sviluppo dell'impresa e delle azioni necessarie al conseguimento degli obiettivi di crescita, competitività e posizionamento sul mercato. In tale contesto, la sostenibilità assume un ruolo sempre più centrale nella pianificazione strategica e nei processi decisionali.

L'integrazione tra sostenibilità ed intelligenza artificiale rappresenta un *driver* di trasformazione organizzativa, in grado di accelerare l'implementazione dei principi ESG nel contesto aziendale. Le tecnologie basate sull'intelligenza artificiale possono infatti supportare il monitoraggio delle *performance* ESG, l'ottimizzazione dei processi aziendali, la gestione dei rischi e l'assunzione di decisioni maggiormente informate e sostenibili.

In tale prospettiva, sempre più di frequente le imprese orientano le proprie strategie verso lo sviluppo di modelli organizzativi ed operativi conformi ai principi ESG e supportati dall'utilizzo dell'IA. Tale percorso richiede una preliminare analisi del contesto aziendale, finalizzata a comprendere le caratteristiche dell'organizzazione, il posizionamento competitivo, il modello di *business*, le risorse disponibili ed il quadro normativo di riferimento.

Un passaggio fondamentale consiste nella definizione di obiettivi ESG chiari, misurabili e coerenti con le caratteristiche dell'impresa e con gli *standard* internazionali di riferimento, tra cui il *Global Reporting Initiative* (GRI) ed i *Sustainable Development Goals* (SDGs). Tali obiettivi devono inoltre essere allineati alle aspettative degli *stakeholders* ed all'evoluzione del quadro normativo applicabile.

PROPOSTA

Si propone di strutturare l'implementazione dei modelli AI-ESG attraverso un approccio integrato che coinvolga *governance*, pianificazione strategica e valutazione degli impatti.

(i) Coinvolgimento degli *stakeholders*

Il dialogo con investitori, dipendenti e fornitori rappresenta elemento essenziale per l'efficace integrazione dei principi ESG nei processi di adozione dell'intelligenza artificiale. A tal fine, è opportuno promuovere forme di comunicazione trasparente e continua, favorendo il coinvolgimento degli *stakeholders* nelle decisioni strategiche e nei processi di trasformazione organizzativa maggiormente rilevanti.

(ii) Definizione di una *roadmap* AI-ESG

L'implementazione di modelli AI-ESG richiede la predisposizione di una *roadmap* strutturata che individui obiettivi, priorità, tempistiche e responsabilità. La *roadmap* dovrebbe articolare il percorso di implementazione in fasi progressive, prevedendo obiettivi di breve, medio e lungo periodo, nonché meccanismi di monitoraggio e revisione periodica dei risultati conseguiti.

(iii) Integrazione della FRIA nei processi di *governance*

Si propone di strutturare la Fundamental Rights Impact Assessment (FRIA) non come un adempimento documentale isolato bensì come uno strumento integrato nel sistema di *governance* dell'IA. In tale prospettiva, la FRIA dovrebbe essere coordinata con i processi di *risk management* previsti dall'art. 9 AI Act[3] e con la Data Protection Impact Assessment (DPIA) di cui all'art. 35 GDPR[4], attraverso un percorso articolato nelle fasi di mappatura del sistema, individuazione dei diritti coinvolti, analisi del rischio e valutazione di proporzionalità delle misure adottate. La valutazione dovrebbe concludersi con l'individuazione di misure di mitigazione verificabili e obblighi di revisione periodica, affinché la tutela dei diritti fondamentali divenga un elemento strutturale della *governance* dei sistemi di IA ad alto rischio.

Responsabilità sociale

La responsabilità sociale dell'intelligenza artificiale riguarda la capacità delle organizzazioni di sviluppare ed utilizzare tali tecnologie secondo principi etici, di trasparenza e sostenibilità, assicuran-

3 Regolamento (UE) 2024/1689 (AI Act), art. 9: 1. In relazione ai sistemi di IA ad alto rischio è istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi. 2. Il sistema di gestione dei rischi è inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici. [...].

4 Regolamento (UE) 2016/679 (GDPR), art. 35: 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.[...].

do un adeguato bilanciamento tra innovazione, tutela delle persone e gestione dei rischi connessi a *bias* e fenomeni discriminatori.

L'adozione dell'intelligenza artificiale produce effetti che vanno oltre la dimensione tecnologica, incidendo sui processi organizzativi, sulle competenze professionali e sulle modalità di interazione con gli *stakeholders*. In tale contesto, è essenziale per le organizzazioni l'adozione di adeguati strumenti di *governance*, formazione e gestione del cambiamento, al fine di favorire un utilizzo responsabile e sostenibile delle nuove tecnologie.

PROPOSTA

Si propone un approccio equilibrato che preveda la formazione della forza lavoro, nonché politiche di supporto per la transizione verso un'economia automatizzata.

(i) Il divario nell'adozione dell'AI rischia di amplificare le disuguaglianze economiche esistenti tra grandi imprese, PMI e microimprese. Chi dispone di maggiori risorse economiche, infrastrutture tecnologiche avanzate e competenze specializzate può investire massicciamente nella tecnologia, creando un *gap* competitivo che rischia di marginalizzare ulteriormente alcune realtà di mercato, con un fenomeno di concentrazione del potere economico che riduce la competitività delle PMI e delle microimprese e aumenta le disuguaglianze nel tessuto produttivo.

(ii) È fondamentale promuovere politiche di incentivazione e supporto per l'adozione dell'IA nelle PMI e nelle microimprese, fornendo accessi agevolati a infrastrutture tecnologiche, formazione mirata e consulenza per la strutturazione dei dati. Solo attraverso un ecosistema inclusivo sarà possibile garantire che i benefici dell'intelligenza artificiale siano ampiamente accessibili.

3. Analisi della struttura aziendale, dei dati e del personale *accountable* per *step*

STATUS QUO 2026

Il grado di integrazione tra i dipartimenti aziendali costituisce uno degli indicatori principali del livello di maturità organizzativa di un'impresa. Nella prassi, tuttavia, le diverse funzioni aziendali operano spesso in modo non pienamente coordinato: organigrammi poco chiari, responsabilità non adeguatamente definite e carenze nei flussi di comunicazione interna rappresentano criticità strutturali ricorrenti.

L'introduzione di sistemi di intelligenza artificiale in contesti aziendali caratterizzati da una limitata maturità organizzativa può amplificare tali criticità, esponendo l'impresa a rischi operativi, organizzativi e reputazionali che possono compromettere i benefici attesi dall'adozione delle nuove tecnologie.

In tale contesto, la capacità dell'organizzazione di individuare con chiarezza ruoli, responsabilità, processi decisionali e flussi informativi assume un rilievo centrale ai fini di una *governance* efficace dell'intelligenza artificiale.

L'integrazione dell'intelligenza artificiale all'interno delle strutture organizzative richiede un percorso di adeguamento complesso e progressivo.

In questa prospettiva, occorre definire il posizionamento dei sistemi di IA all'interno dell'organizzazione, i livelli di autonomia ad essi attribuiti e le responsabilità associate alle diverse fasi del processo decisionale. Assume particolare rilievo l'individuazione dei punti nei quali il controllo umano continua ad essere esercitato, definendo con chiarezza le attività di supervisione, validazione e intervento affidate alle persone.

La definizione della *governance* dell'IA presuppone una preventiva mappatura della struttura aziendale, dei processi, dei dati e delle funzioni coinvolte. Tale attività non rappresenta un mero adempimento formale, ma costituisce il presupposto metodologico per una conoscenza approfondita e verificabile dell'organizzazione e dei rischi associati all'utilizzo dei sistemi di IA.

La complessità di tale percorso varia in funzione del livello di automazione già presente nell'impresa e del ruolo che i sistemi di IA rivestono nei processi decisionali. A ciò si aggiunge la necessità di assicurare coerenza tra le scelte tecnologiche adottate, i valori dell'organizzazione e gli obiettivi perseguiti.

In ogni caso, il presidio umano rimane un elemento imprescindibile della *governance* dell'intelligenza artificiale. I sistemi algoritmici possono infatti essere soggetti a errori, *bias* derivanti dai dati di addestramento o risultati inadeguati in contesti diversi da quelli originariamente previsti. Le decisioni strategiche e la responsabilità delle scelte organizzative restano pertanto in capo alle persone e non possono essere integralmente delegate a sistemi automatizzati.

PROPOSTA

(i) Definizione dell'approccio di mappatura

La scelta dell'approccio alla mappatura dei sistemi di IA dovrebbe essere sviluppata secondo un approccio coerente con la cultura organizzativa dell'azienda e del livello di maturità dell'impresa. È possibile individuare due alternative principali.

Un primo approccio, di tipo **processo-centrico**, parte dall'analisi dei processi aziendali già esistenti e risulta particolarmente adatto alle organizzazioni che intendono integrare l'IA all'interno di modelli operativi già consolidati.

Un secondo approccio, basato sui **casi d'uso** (*use-cases*), muove invece dall'identificazione degli specifici impieghi dell'IA e dei relativi livelli di rischio. In tale prospettiva, si ritiene preferibile una lettura per livelli di rischio, che consenta di differenziare i presidi organizzativi in funzione dell'impatto che ciascun sistema può avere sui diritti della persona sui processi decisionali e sulle attività aziendali.

(ii) Registro dei sistemi di IA

Si propone l'adozione di un registro dei sistemi di intelligenza artificiale volto a censire i sistemi già utilizzati o in fase di implementazione, documentando i profili descritti di seguito:

- il ruolo ricoperto dall'organizzazione ai sensi dell'AI Act (*provider*, *deployer*, *importer* o altro soggetto rilevante);
- la finalità del sistema;
- le categorie di dati trattati;
- il livello di rischio attribuito secondo la classificazione prevista dall'AI Act;
- le misure di sicurezza e di controllo adottate.

(iii) *Vendor* e *Internal risk assessment*

Particolare attenzione deve essere dedicata ai rapporti con i fornitori esterni di sistemi di IA. La valutazione effettuata dal *provider* ai sensi dell'AI Act non esaurisce infatti le responsabilità dell'impresa utilizzatrice (*deployer*).

Si propone pertanto che ogni sistema IA sia sottoposto ad una duplice valutazione:

- *vendor risk assessment*: a cura del fornitore;
- *internal risk assessment*: a cura dell'organizzazione utilizzatrice, tenendo conto delle specificità dei dati trattati, delle finalità perseguite e dell'impatto sui processi decisionali interni.

(iv) Matrice organizzativa

Si propone l'adozione di una matrice organizzativa che consenta di individuare chiaramente ruoli, responsabilità, funzioni di controllo e livelli di autorizzazione associati ai sistemi di IA, assicurando la tracciabilità delle decisioni e l'effettività dei meccanismi di *governance*.

(v) Sistemi ad alto rischio e adempimenti normativi

I sistemi classificati come ad alto rischio ai sensi dell'AI Act richiedono l'adozione di presidi specifici. In particolare, è opportuno:

- identificare i sistemi ad alto rischio presenti nel contesto operativo dell'organizzazione;
- verificare gli obblighi previsti dalla normativa applicabile e le relative tempistiche di adempimento;
- adottare tempestivamente le misure necessarie per garantire la conformità ai requisiti normativi.

4. Coordinamento con altri *framework* aziendali ed organizzativi

STATUS QUO 2026

L'AI incide trasversalmente su numerosi ambiti normativi e organizzativi, tra cui protezione dei dati personali, *cybersecurity*, *compliance*, *risk management*, sostenibilità e sistemi di controllo interno. Nella prassi, tuttavia, tali dimensioni sono spesso gestite in modo separato, secondo approcci a silos che possono determinare incoerenze nelle *policy* aziendali, duplicazioni delle attività di controllo e rischi di non conformità.

La crescente complessità del quadro normativo e regolatorio richiede pertanto un approccio maggiormente integrato, capace di coordinare i diversi presidi organizzativi e di assicurare una gestione coerente dei rischi connessi all'utilizzo dell'intelligenza artificiale.

L'intelligenza artificiale non costituisce un ambito regolatorio autonomo e isolato, ma si colloca all'intersezione di una pluralità di discipline e sistemi di *governance* già presenti nelle organizzazioni. L'adozione di sistemi di IA può infatti incidere, a seconda dei casi, sulla protezione dei dati personali, sulla *cybersecurity*, sulla gestione dei rischi, sui sistemi di controllo interno, sugli obblighi di *compliance* e, più in generale, sulle politiche di sostenibilità e responsabilità aziendale.

In tale contesto, la creazione di presidi organizzativi dedicati all'IA non dovrebbe tradursi nella costruzione di strutture parallele rispetto a quelle già esistenti. Un approccio frammentato rischia infatti di generare sovrapposizioni di competenze, duplicazioni dei controlli e inefficienze nei processi decisionali.

Assume pertanto particolare rilievo la capacità dell'organizzazione di integrare la *governance* dell'IA all'interno dei *framework* già esistenti, valorizzando le funzioni aziendali coinvolte e favorendo il coordinamento tra le diverse competenze. La sfida non consiste soltanto nell'assicurare la conformità ai nuovi obblighi normativi, ma anche nel costruire modelli organizzativi coerenti, sostenibili e in grado di adattarsi all'evoluzione del quadro regolatorio.

In questa prospettiva, il coordinamento tra le diverse funzioni aziendali rappresenta un elemento essenziale per garantire una gestione efficace dei rischi, una corretta allocazione delle responsabilità e una maggiore efficienza complessiva dei processi di *governance*.

PROPOSTA

(i) Coordinamento e integrazione delle *policy* aziendali

Si propone di adottare un approccio unitario nella definizione delle *policy* aziendali, assicurando il coordinamento tra i diversi requisiti normativi e la loro integrazione con riferimento all'utilizzo dei sistemi di IA.

(ii) Coordinamento interfunzionale

Favorire il coordinamento tra le funzioni aziendali coinvolte, tra cui legal, IT, HR, *compliance*, *risk management* e *cybersecurity*, anche attraverso l'istituzione di comitati o gruppi di lavoro dedicati.

(iii) Monitoraggio del quadro normativo e delle prassi applicative

Istituire presidi dedicati al monitoraggio delle evoluzioni normative, regolatorie, giurisprudenziali e delle prassi di mercato, al fine di garantire un costante aggiornamento dei modelli organizzativi e delle *policy* aziendali.

5. *Training* e formazione interna

STATUS QUO 2026

La formazione in materia di intelligenza artificiale costituisce uno strumento essenziale per favorire un'integrazione responsabile dell'IA nei processi aziendali e decisionali. Una formazione adeguata contribuisce a: (i) ridurre i rischi etici, legali e reputazionali; (ii) diffondere competenze e consapevolezza organizzativa; (iii) allineare l'uso dell'IA ai modelli di *governance* ed agli obiettivi strategici dell'impresa; (iv) supportare i processi di *reskilling* e *upskilling* della forza lavoro.

La formazione rappresenta uno dei principali strumenti attraverso cui le organizzazioni possono garantire un utilizzo responsabile dell'intelligenza artificiale e favorire l'effettiva attuazione dei modelli di *governance* adottati. L'introduzione di sistemi di IA non richiede soltanto nuove competenze tecniche, ma comporta anche l'acquisizione di una maggiore consapevolezza in relazione ai profili etici, organizzativi, normativi e di gestione del rischio.

In tale contesto, la scelta del modello formativo assume una rilevanza strategica. La questione non riguarda tanto l'introduzione di nuovi strumenti di formazione, quanto l'individuazione dell'approccio più idoneo a garantire un equilibrio tra diffusione della cultura dell'IA, specializzazione delle competenze e applicabilità operativa.

Approccio olistico

Un primo modello è rappresentato dall'approccio olistico, fondato sulla diffusione di conoscenze e principi comuni all'intera organizzazione. Tale impostazione favorisce la costruzione di un linguaggio condiviso, la diffusione di una cultura aziendale coerente e l'allineamento dei comportamenti ai principi di *governance* dell'IA. Il principale limite consiste nel rischio che i contenuti formativi risultino eccessivamente generici rispetto alle esigenze operative delle singole funzioni.

Approccio settoriale

Un secondo modello è rappresentato dall'approccio settoriale, che prevede percorsi differenziati in funzione dei ruoli e delle responsabilità aziendali. Tale impostazione consente di affrontare casi d'uso concreti, rischi specifici e responsabilità direttamente connesse alle attività svolte, ma può determinare una frammentazione delle competenze e una ridotta uniformità nella comprensione dei principi generali che governano l'utilizzo dell'IA.

Approccio ibrido

L'approccio ibrido combina i punti di forza dei due modelli precedenti, prevedendo una base comune di conoscenze e principi destinata all'intera popolazione aziendale e percorsi specialistici calibrati sulle specifiche esigenze delle diverse funzioni. Tale soluzione favorisce la diffusione di una cultura condivisa dell'IA, mantenendo al contempo un elevato livello di rilevanza operativa e di responsabilizzazione delle singole strutture organizzative.

PROPOSTA

(i) Struttura della formazione e del *training*

Le organizzazioni dovrebbero definire una strategia formativa chiara e continuativa, articolata secondo le seguenti linee direttrici:

- mappatura delle competenze in materia di IA presenti nelle diverse funzioni aziendali, con individuazione delle conoscenze di base che l'intera popolazione aziendale dovrebbe possedere e tempestiva identificazione degli eventuali *gap* formativi;
- sviluppo di programmi di formazione ed aggiornamento continuo, personalizzati in funzione dei ruoli e periodicamente aggiornati alla luce dell'evoluzione tecnologica, normativa ed organizzativa (es. "*real time training*");
- diffusione della conoscenza delle *policy* aziendali in materia di IA, delle regole relative all'utilizzo dei dati, dei sistemi di IA generativa e dei relativi presidi organizzativi;
- preparazione agli scenari evolutivi dell'intelligenza artificiale, inclusi i modelli di IA agentica e le relative implicazioni organizzative e di *governance*;
- definizione e comunicazione di ruoli, responsabilità e presidi organizzativi connessi all'utilizzo dell'IA, anche attraverso l'individuazione di referenti interni o figure di supporto al cambiamento (ad es. "AI Champion");
- predisposizione di percorsi di *reskilling* e *upskilling* mirati in funzione delle specificità dell'azienda e dell'evoluzione delle competenze richieste.

(ii) Requisiti di qualità della formazione

È essenziale integrare i percorsi formativi con i processi aziendali e progettati in modo da favorire un apprendimento concreto, continuativo e misurabile. A tal fine, appare opportuno privilegiare metodologie innovative e ad elevato coinvolgimento, in grado di tradurre i principi generali in comportamenti operativi.

Esempi di frontiere formative innovative possono includere:

- soluzioni digitali di supporto (*chat box* interattivi) in grado di segnalare potenziali criticità operative, di *compliance* o di natura etica nello svolgimento delle attività lavorative;
- simulazioni, esercitazioni e modelli di apprendimento basati su casi pratici, finalizzati a favorire una maggiore consapevolezza dei rischi e delle responsabilità connesse all'utilizzo dell'IA.

(iii) Approccio metodologico consigliato

Si ritiene preferibile adottare un approccio ibrido, che combini una base comune di conoscenze e principi destinata all'intera popolazione aziendale con percorsi specialistici calibrati sulle esigenze delle diverse funzioni. Tale modello consente di:

- evitare sia il rischio di formazione eccessivamente generica sia la frammentazione derivante da approcci esclusivamente settoriali;
- promuovere la diffusione di un linguaggio e di principi comuni all'interno dell'organizzazione;
- garantire competenze specialistiche adeguate ai diversi ruoli e livelli di responsabilità;
- favorire la collaborazione interfunzionale e la coerenza dei processi decisionali;
- rafforzare i meccanismi di *accountability* individuale ed organizzativa.

SEZIONE III

CAMBIAMENTI GLOBALI: ESG, COMPLIANCE, POLITICHE ECONOMICHE E GEOPOLITICA – IL RUOLO DEI CORPORATE LEADERS

1. Scenari di innovazione e concorrenza: impatto sugli operatori economici

STATUS QUO 2026

L'intelligenza artificiale sta ridefinendo in modo strutturale i modelli di *business* e i processi produttivi delle imprese. L'automazione delle attività operative e analitiche più ripetitive, l'utilizzo avanzato dei dati come risorsa strategica per la personalizzazione dell'offerta, e l'adozione di nuovi modelli digitali, dalle piattaforme algoritmiche ai servizi *on-demand*, stanno modificando le modalità di creazione del valore e la struttura interna delle organizzazioni. In questo contesto, dati e competenze tecnologiche si affermano come *asset* competitivi determinanti, in analogia con il ruolo che le risorse fisiche hanno avuto nell'economia industriale tradizionale.

Questa trasformazione genera dinamiche competitive asimmetriche. Le imprese che integrano tempestivamente sistemi di IA nei propri modelli operativi acquisiscono vantaggi in termini di efficienza, capacità decisionale e innovazione di prodotto, mentre i ritardi nell'adozione possono determinare un progressivo indebolimento della posizione di mercato. Il divario risulta particolarmente evidente tra grandi operatori, PMI e microimprese: i primi dispongono di grandi *dataset* e competenze specialistiche che le imprese di minori dimensioni difficilmente riescono a replicare autonomamente, con il rischio di consolidare barriere all'ingresso strutturali.

In tale scenario, la capacità competitiva delle imprese dipende sempre più dalla possibilità di accedere alle tecnologie emergenti e di integrarle efficacemente nei processi aziendali. L'intelligenza artificiale non rappresenta soltanto uno strumento di efficientamento operativo, ma un fattore in grado di incidere sulla capacità di innovazione, sulla rapidità di adattamento ai cambiamenti del mercato e sullo sviluppo di nuovi modelli di *business*.

La trasformazione in atto richiede pertanto un approccio multidimensionale che coinvolga investimenti in infrastrutture tecnologiche e dati, programmi di sviluppo delle competenze e modelli organizzativi in grado di favorire la sperimentazione e l'innovazione. Allo stesso tempo, assume rilievo la creazione di ecosistemi collaborativi che consentano anche agli operatori di minori dimensioni di accedere a competenze, tecnologie e risorse che difficilmente potrebbero sviluppare autonomamente.

In questa prospettiva, la collaborazione tra imprese, università, centri di ricerca, startup e associazioni di categoria può rappresentare un fattore strategico per favorire la diffusione dell'innovazione, ridurre le barriere all'accesso e promuovere una crescita più equilibrata del sistema economico.

PROPOSTA

In un'ottica di competitività sistemica, le imprese, ed in particolare le microimprese, dovrebbero perseguire modelli di cooperazione tecnologica fondati su paradigmi di *open innovation*. L'attivazione di sinergie con associazioni di categoria, *startup*, poli universitari e centri di eccellenza consente l'internalizzazione di *asset* tecnologici di frontiera, mitigando l'onere finanziario connesso alle attività di ricerca e sviluppo.

2. Condizioni “eque” di accesso ai dati, all’infrastruttura digitale, alle capacità computazionali ed alle filiere strategiche critiche (*cloud* sovrano)

STATUS QUO 2026

Il presidio dei dati e delle infrastrutture digitali rappresenta un fattore determinante per il potere economico, la competitività delle imprese e la resilienza delle filiere produttive e la sicurezza economica degli Stati.

Il mercato globale del *cloud computing* e delle infrastrutture digitali è oggi caratterizzato da una forte concentrazione in capo ad un numero limitato di operatori (*hyperscaler*) internazionali. Tale fenomeno può generare situazioni di dipendenza tecnologica e *lock-in*, in particolare quando l'architettura digitale di un'organizzazione viene sviluppata all'interno di ecosistemi proprietari che rendono complessa la migrazione verso soluzioni alternative.

A ciò si aggiungono criticità connesse all'accesso ed alla condivisione dei dati, spesso ostacolate da limitati livelli di interoperabilità tra sistemi, da frammentazioni organizzative e da difficoltà operative nella circolazione sicura delle informazioni.

La dipendenza dell'Europa da operatori extraeuropei nei settori del *cloud computing*, delle infrastrutture digitali, delle capacità computazionali e dell'intelligenza artificiale assume una crescente rilevanza strategica. Le restrizioni all'esportazione di componenti *hardware* avanzati per l'intelligenza artificiale introdotte dagli Stati Uniti hanno reso evidente la rilevanza geopolitica delle *supply chain* tecnologiche e la necessità di rafforzare la resilienza delle infrastrutture critiche e delle filiere strategiche, nonché la necessità di ricostruire filiere rientranti nel perimetro di autonomia strategica.

L'accesso ai dati, alle infrastrutture digitali e alle capacità computazionali non rappresenta più soltanto una questione tecnologica, ma costituisce un elemento centrale delle strategie di competitività e gestione del rischio delle imprese.

La crescente dipendenza da fornitori esterni per servizi *cloud*, capacità di elaborazione e strumenti di intelligenza artificiale rende necessario valutare con maggiore attenzione gli impatti che tali scelte possono avere sulla continuità operativa, sulla portabilità delle soluzioni adottate e sulla capacità dell'organizzazione di mantenere nel tempo un adeguato livello di autonomia decisionale.

Parallelamente, la valorizzazione del patrimonio informativo assume un ruolo sempre più rilevante. La disponibilità di dati di qualità rappresenta infatti uno dei principali fattori abilitanti per lo sviluppo e l'utilizzo efficace dei sistemi di IA. Ciò richiede una maggiore consapevolezza in merito alla localizzazione dei dati, alle modalità di utilizzo da parte di soggetti terzi e ai rischi connessi alla circolazione delle informazioni all'interno di ecosistemi digitali complessi.

In tale prospettiva, la resilienza digitale delle organizzazioni dipende dalla capacità di coniugare efficienza tecnologica, sicurezza, portabilità e governo del patrimonio informativo.

PROPOSTA

Al fine di rafforzare la resilienza digitale, le imprese dovrebbero adottare una serie di misure strutturate lungo le seguenti direttrici.

(i) Mitigazione del rischio di dipendenza tecnologica

Le imprese dovrebbero progettare le proprie architetture digitali secondo logiche orientate all'interoperabilità ed alla portabilità fin dall'origine, limitando il rischio di dipendenza da un singolo fornitore e favorendo, ove possibile, l'adozione di modelli *multi-provider*. A tal fine, assume particolare rilievo la possibilità di migrazione tra piattaforme con costi ed impatti organizzativi contenuti, evitando la necessità di una sostanziale riprogettazione dell'architettura applicativa[5].

(ii) Valorizzazione e censimento del patrimonio informativo

Si propone di censire e classificare il patrimonio informativo aziendale attraverso una *data strategy* che identifichi gli *asset* informativi di maggiore valore strategico, le relative modalità di utilizzo ed i livelli di protezione necessari in funzione della loro rilevanza.

(iii) Protezione del patrimonio informativo

Le imprese dovrebbero sviluppare una maggiore consapevolezza in merito alla localizzazione, alla circolazione e all'utilizzo dei dati impiegati nei sistemi di IA, con particolare riferimento ai casi in cui tali informazioni possano essere trasferite al di fuori del perimetro aziendale (e potenzialmente dell'Unione europea). A tal fine, appare necessario adottare misure proporzionate alla sensibilità dei dati, quali tecniche di anonimizzazione o pseudonimizzazione, soluzioni di *cloud* privato e, ove opportuno, modelli IA implementati in ambienti *on-premise*.

5 La partecipazione a *data spaces* settoriali, promossi dalla Strategia europea per i dati e da iniziative come GAIA-X nei settori dell'industria, della sanità, dell'energia e della mobilità, rappresenta un'opportunità di sviluppo competitivo e contribuisce al rafforzamento dell'ecosistema digitale europeo.

3. Quale ruolo per i *corporate leaders* nelle scelte aziendali in un contesto geopolitico complesso?

STATUS QUO 2026

Il sistema economico globale sta attraversando una fase di profonda trasformazione nella quale la sicurezza economica e tecnologica assume un ruolo sempre più centrale nelle politiche pubbliche e nelle strategie di impresa. La crescente competizione tra grandi potenze economiche sta ridisegnando gli equilibri internazionali, rendendo i mercati al contempo più interconnessi e più esposti a fenomeni di frammentazione geopolitica.

In questo contesto, strumenti giuridici quali sanzioni economiche, *screening* degli investimenti esteri e restrizioni all'esportazione di tecnologie critiche hanno assunto un ruolo centrale nella definizione delle dinamiche competitive e delle strategie industriali.

Le crisi globali degli ultimi anni hanno inoltre evidenziato la vulnerabilità delle catene di approvvigionamento e delle infrastrutture critiche, dimostrando come la dipendenza da specifiche aree geografiche, fornitori o tecnologie possa tradursi in un fattore di rischio strategico per le imprese.

Ne consegue che il ruolo dei *corporate leaders* non può più limitarsi alla gestione di *performance* economica e finanziaria, ma deve necessariamente estendersi alla comprensione ed alla gestione dei rischi geopolitici, regolatori e tecnologici, che incidono sulla capacità dell'impresa di operare e competere nel lungo periodo.

Le decisioni relative all'adozione dell'intelligenza artificiale, alla gestione dei dati, alla selezione dei fornitori tecnologici e all'utilizzo delle infrastrutture digitali non possono più essere considerate scelte esclusivamente tecniche o operative. Tali decisioni incidono infatti sull'autonomia strategica dell'impresa, sulla resilienza delle sue attività e sulla sua esposizione a rischi normativi, geopolitici e reputazionali.

La crescente interdipendenza tra rischio geopolitico, rischio tecnologico e rischio di *compliance* richiede un approccio integrato alla *governance* aziendale. In questo scenario, i *corporate leaders* sono chiamati a sviluppare una visione sistemica che consenta di valutare non soltanto i benefici economici immediati delle scelte adottate, ma anche le loro implicazioni nel medio e lungo periodo.

Assume pertanto particolare rilievo la capacità di anticipare l'evoluzione dei contesti normativi, tecnologici e geopolitici, integrando tali fattori nei processi decisionali, nei sistemi di gestione del rischio e nelle strategie di sviluppo dell'impresa.

PROPOSTA

Si propone l'adozione di un protocollo di *best practices* per integrare il rischio geopolitico nei processi di Enterprise Risk Management.

A tal fine, si individuano i seguenti ambiti prioritari di intervento.

(i) *Geopolitical risk assessment* e *scenario planning*

Le organizzazioni dovrebbero sviluppare processi strutturati di valutazione del rischio geopolitico, basati sull'analisi degli scenari e sull'identificazione delle principali vulnerabilità relative a fornitori strategici, infrastrutture critiche, mercati di riferimento e dipendenze tecnologiche.

(ii) Resilienza delle filiere e diversificazione delle dipendenze strategiche

Al fine di ridurre l'esposizione a rischi geopolitici e operativi, appare opportuno limitare la dipendenza da singole aree geografiche, fornitori o tecnologie critiche. In tale prospettiva, strategie di *reshoring*, *nearshoring*, *friend-shoring* e diversificazione delle *supply chain* possono contribuire a rafforzare la resilienza complessiva dell'organizzazione, pur comportando, in alcuni casi, maggiori costi nel breve periodo.

(iii) Dialogo istituzionale e monitoraggio regolatorio

Il dialogo con istituzioni pubbliche, autorità, organizzazioni internazionali e associazioni di categoria non dovrebbe essere considerato un mero adempimento di *compliance*, bensì uno strumento di presidio strategico finalizzato a comprendere tempestivamente l'evoluzione del contesto normativo e a ridurre l'incertezza operativa.

(iv) Formazione continua dei *corporate leaders*

La formazione continua dei vertici aziendali sui temi della geopolitica economica, della sicurezza tecnologica, del commercio internazionale e della *governance* dell'intelligenza artificiale costituisce un elemento essenziale per rafforzare la capacità dell'organizzazione di anticipare i cambiamenti e adattarsi a contesti caratterizzati da elevata complessità e volatilità.

SEZIONE IV
CONSUMATORI DEL FUTURO, ANTITRUST E NUOVI MERCATI

1. Pressioni competitive nei mercati digitali, *upstream* e *downstream*: concorrenza, innovazione e ruolo del diritto antitrust

STATUS QUO 2026

Nei mercati digitali, la competizione si sviluppa secondo logiche profondamente diverse rispetto ai modelli tradizionali, ponendo nuove sfide per il diritto della concorrenza e per gli strumenti di regolazione pubblica. In tale contesto, il dato rappresenta una risorsa strategica di primaria importanza, che consente agli operatori di comprendere i comportamenti degli utenti, migliorare i servizi offerti e rafforzare il proprio posizionamento sul mercato.

La disponibilità e il controllo di grandi volumi di dati (c.d. *dataset*) consentono infatti di sviluppare capacità analitiche, tecnologiche e commerciali difficilmente replicabili da operatori concorrenti e rappresentano pertanto un fattore di vantaggio competitivo. In presenza di significative asimmetrie informative e tecnologiche, tali risorse possono contribuire alla creazione di barriere all'ingresso e, in taluni casi, sollevare questioni riconducibili alla c.d. *essential facility doctrine*, laddove l'accesso a determinate risorse risulti indispensabile per competere sul mercato[6].

6 La *essential facility doctrine* è un principio del diritto della concorrenza in forza del quale l'impresa dominante che controlli un'infrastruttura o una risorsa indispensabile per operare in un determinato mercato può essere tenuta a consentirne l'accesso a condizioni eque e non discriminatorie, ove il rifiuto sia idoneo ad eliminare la concorrenza nel mercato a valle e non risulti oggettivamente giustificato. Elaborato dalla giurisprudenza statunitense, tale principio ha trovato applicazione anche nell'ordinamento europeo, dove trova il proprio fondamento nell'art. 102 TFUE. I suoi contorni applicativi sono stati delineati dalla Corte di Giustizia nelle sentenze Magill, Bronner e IMS Health (Magill: Causa C-241/91; Bronner C-7/97; IMS C-418/01).

Le dinamiche concorrenziali nei mercati digitali sono inoltre influenzate dagli effetti di rete, dalle economie di scala e di scopo e dalla crescente integrazione in ecosistemi digitali complessi, fattori che tendono a favorire la concentrazione del potere di mercato su pochi grandi operatori.

In tale contesto, gli strumenti tradizionali del diritto antitrust hanno manifestato alcuni limiti, derivanti in particolare dalla loro natura prevalentemente *ex post*, che può risultare poco efficace rispetto a mercati caratterizzati da elevata velocità di innovazione e trasformazione.

Per cercare di rispondere a tali criticità, il legislatore unionale ha introdotto il Digital Markets Act, che introduce un modello di regolazione preventiva fondato sull'imposizione di obblighi e divieti specifici per i cosiddetti *gatekeeper*, con l'obiettivo di preservare la concorrenza nei mercati digitali.

La struttura dei mercati digitali si fonda su piattaforme multi-versante, nelle quali le dinamiche competitive si sviluppano a monte (*upstream*) nei rapporti con fornitori e utenti commerciali, o a valle (*downstream*) nei confronti degli utenti finali, con effetti strettamente interdipendenti tra i due livelli.

Sul versante *upstream* le imprese che utilizzano le piattaforme digitali per accedere al mercato possono trovarsi in situazioni di dipendenza economica, risultando esposte a rischi di pratiche escludenti, discriminatorie o caratterizzate da asimmetrie informative e contrattuali.

Sul versante *downstream* gli utenti finali beneficiano di servizi altamente personalizzati e spesso offerti senza un corrispettivo monetario diretto, a fronte della raccolta e dell'utilizzo dei propri dati, ma possono al contempo essere esposti a fenomeni di *lock-in*, limitata trasparenza e restrizioni alla libertà di scelta derivanti da meccanismi di fidelizzazione e dagli elevati costi di *switching*.

In tale contesto, l'applicazione degli strumenti tradizionali del diritto della concorrenza presenta complessità che emergono, tra l'altro, nella definizione del mercato rilevante con riferimento ad ecosistemi *multi-sided*, nell'individuazione del potere di mercato in presenza di servizi offerti a prezzo zero e nella valutazione degli effetti sull'innovazione.

Inoltre, la durata e la complessità dei procedimenti antitrust, unitamente agli elevati *standard* probatori richiesti, rischiano di ridurre l'efficacia degli interventi in mercati caratterizzati da rapida evoluzione tecnologica.

Per far fronte a tali criticità, il Digital Markets Act introduce un modello di regolazione *ex ante* che integra gli strumenti tradizionali del diritto antitrust. Attraverso l'imposizione di obblighi e divieti specifici nei confronti dei *gatekeeper*, il DMA mira a prevenire condotte suscettibili di compromettere la contendibilità dei mercati digitali, senza che sia necessario un accertamento caso per caso di illeciti.

Il DMA attribuisce alla Commissione europea un ruolo centrale nelle attività di vigilanza e di *enforcement*, perseguendo l'obiettivo di garantire un'applicazione uniforme della disciplina e di limitare il rischio di frammentazione normativa. Ciò non esclude, tuttavia, la necessità di un efficace coordinamento con le autorità nazionali competenti, al fine di assicurare coerenza applicativa ed un utilizzo efficiente delle risorse disponibili[7].

Sotto il profilo economico, il DMA è destinato ad incidere sulle dinamiche concorrenziali dei mercati digitali, favorendo condizioni potenzialmente più favorevoli all'ingresso di nuovi operatori ed una maggiore apertura degli ecosistemi digitali.

La sfida principale per il legislatore e per le autorità di *enforcement* consiste nel mantenere un equilibrio tra la tutela della concorrenza, da un lato, e la promozione dell'innovazione e dello sviluppo economico, dall'altro.

PROPOSTA

Si propone l'adozione di un protocollo di *best practices* ispirato ai principi del Digital Markets Act e del diritto della concorrenza, volto a promuovere maggiore trasparenza, equità e contendibilità nei mercati digitali.

Il Protocollo si configura come un *framework* operativo destinato ad orientare concretamente i comportamenti degli operatori e ad agevolare l'adozione di modelli organizzativi in linea con l'evoluzione del quadro normativo europeo.

7 In tale contesto, assume particolare rilievo l'indagine avviata nel giugno 2026 dall'Autorità Garante della Concorrenza e del Mercato, in cooperazione con la Commissione europea ai sensi dell'art. 38, par. 7, del DMA, nei confronti di Apple in relazione alla possibile non conformità all'obbligo di interoperabilità previsto dall'art. 6, par. 7, del DMA. L'indagine, relativa alle condizioni di accesso dei fornitori terzi di servizi *cloud consumer* alle funzionalità dei sistemi operativi iOS e iPadOS, rappresenta il primo esercizio da parte dell'AGCM dei poteri di indagine previsti dal DMA e costituisce un significativo esempio applicativo dei temi dell'interoperabilità, della contendibilità dei mercati digitali e della riduzione dei fenomeni di *lock-in* negli ecosistemi digitali controllati dai *gatekeeper*.

A tal fine, il Protocollo si articola nei seguenti ambiti prioritari di intervento, tra loro complementari.

(i) Accesso e condivisione dei dati

Nei mercati digitali, l'accesso ai dati assume un ruolo strategico ai fini della concorrenza e dell'innovazione. In tale prospettiva, appare opportuno promuovere criteri chiari per l'accesso e la condivisione delle informazioni strategiche, assicurando un adeguato equilibrio tra apertura del mercato, tutela dei diritti e protezione degli interessi economici degli operatori. Sotto questo profilo, la riduzione delle asimmetrie informative rappresenta un elemento essenziale per favorire la contendibilità dei mercati digitali.

(ii) Rapporti tra piattaforme, utenti commerciali e utenti finali

Nei rapporti con gli utenti commerciali (*upstream*), assume particolare rilievo il rispetto dei principi di correttezza, trasparenza e non discriminazione, con specifico riferimento alle condizioni contrattuali e ai criteri che incidono sull'accesso al mercato, sul posizionamento e sulla visibilità all'interno delle piattaforme. Tali presidi contribuiscono a ridurre le asimmetrie informative e a favorire condizioni di concorrenza più eque.

Nei confronti degli utenti finali (*downstream*), appare opportuno rafforzare la trasparenza dei sistemi algoritmici, assicurando una maggiore conoscibilità dei criteri che incidono sulla personalizzazione dei servizi e sulla profilazione. In tale prospettiva, si propone l'introduzione di *standard* minimi di *explainability* e di adeguati meccanismi di verifica, anche indipendenti, volti a mitigare possibili effetti distorsivi sui comportamenti degli utenti e sui processi decisionali.

(iii) Interoperabilità e portabilità dei dati

La promozione di *standard* di interoperabilità e strumenti efficaci di portabilità dei dati, è essenziale per ridurre il rischio di *lock-in* e favorire una maggiore apertura degli ecosistemi digitali. Tali misure possono contribuire a rafforzare la contendibilità dei mercati digitali ed a favorire una più agevole interazione tra servizi e piattaforme, in linea con gli obiettivi perseguiti dal legislatore unionale.

(iv) Integrazione nei sistemi di *governance* aziendale

Il Protocollo prevede l'integrazione dei principi di trasparenza, equità e contendibilità nei sistemi di *governance* delle organizzazioni, attraverso la chiara individuazione delle funzioni responsabili, l'adozione di procedure di monitoraggio e verifica e la predisposizione di strumenti di reporting periodico. Ciò consente di incorporare tali principi nei processi decisionali e nei sistemi di controllo aziendale, rafforzando l'efficacia delle misure adottate e favorendo una gestione responsabile delle attività digitali.

2. Algoritmi, determinazione dei prezzi, termini e condizioni d'uso per utenti e consumatori

STATUS QUO 2026

Il *pricing* algoritmico si è affermato come pratica strutturale nei mercati digitali e ad alta intensità di dati, abilitato da tecnologie ormai mature che consentono variazioni di prezzo in tempo reale, profilazione individuale degli utenti e ottimizzazione continua dei ricavi. Se sul piano teorico la discriminazione di prezzo può avvicinare il prezzo al valore soggettivo del consumatore, generando efficienza allocativa e, in alcuni contesti, una maggiore accessibilità a prodotti e servizi, nella pratica emergono criticità rilevanti sotto diversi profili.

Sul versante della tutela del consumatore, l'opacità delle pratiche di scomposizione del prezzo e la profilazione basata su caratteristiche individuali o *proxy* rendono più difficile una scelta informata e consapevole, accentuando le asimmetrie informative strutturali.

Sul versante concorrenziale, la disponibilità differenziata di dati e la capacità di monitoraggio reciproco tra operatori espongono i mercati a rischi di allineamento dei prezzi e di consolidamento delle posizioni dominanti.

Sul versante regolatorio, gli strumenti contrattuali esistenti, come termini e condizioni d'uso, si rivelano spesso insufficienti in assenza di adeguati presidi normativi. Il divario tra la velocità dell'innovazione tecnologica e la capacità di risposta degli strumenti di tutela rappresenta, allo stato attuale, una delle principali tensioni irrisolte del fenomeno.

L'evoluzione tecnologica consente variazioni dei prezzi sempre più frequenti e granulari, sia attraverso sistemi di *pricing* automatizzato nei servizi online sia mediante strumenti digitali utilizzati nei punti vendita fisici. Tali pratiche possono incidere significativamente sulla trasparenza e sulla comparabilità delle offerte, soprattutto in presenza di meccanismi di scomposizione del prezzo, di progressiva aggiunta di servizi accessori o di modalità di determinazione del prezzo non immediatamente comprensibili per il consumatore.

Se la dinamicità del prezzo costituisce un elemento fisiologico di molti mercati e può riflettere dinamiche di domanda e offerta o specifiche condizioni di mercato, maggiori criticità emergono laddove il prezzo venga determinato sulla base di processi di profilazione individuale non sufficientemente trasparenti.

Sotto il profilo concorrenziale, la diffusione dei sistemi di *pricing* algoritmico pone ulteriori questioni. In mercati caratterizzati da elevata trasparenza e capacità di monitoraggio reciproco tra operatori, tali strumenti possono agevolare dinamiche di allineamento dei prezzi. Al contempo, la disponibilità ed il controllo dei dati rappresentano un fattore competitivo centrale, con il rischio che operatori dotati di maggiori capacità informative possano rafforzare la propria posizione sul mercato.

In tale contesto, i termini e le condizioni d'uso assumono un ruolo sempre più rilevante nel disciplinare le modalità di raccolta e utilizzo dei dati, nonché i criteri di determinazione e variazione dei prezzi. Assume particolare rilievo la qualità delle informazioni rese agli utenti, al fine di garantire adeguati livelli di trasparenza ed effettiva comprensibilità delle modalità di funzionamento dei sistemi utilizzati, soprattutto in presenza di sistemi algoritmici particolarmente complessi.

Non mancano, tuttavia, profili positivi. I sistemi di *pricing* algoritmico possono contribuire a una più efficiente allocazione delle risorse, ad una migliore gestione della domanda e dell'offerta e, in alcuni casi, ad una maggiore accessibilità di beni e servizi. Essi possono inoltre contribuire ad una gestione più efficiente delle scorte e delle risorse produttive, con effetti positivi in termini di riduzione degli sprechi, dei costi operativi e dei consumi energetici. Alla luce di tali considerazioni,

appare necessario individuare un equilibrio tra innovazione, efficienza e tutela degli utenti, attraverso strumenti idonei a garantire trasparenza, correttezza ed adeguata verifica dei sistemi di *pricing* automatizzato.

PROPOSTA

In tale prospettiva, si formulano le seguenti proposte operative:

(i) Trasparenza dei prezzi

Rafforzare la trasparenza dei prezzi attraverso l'indicazione del prezzo complessivo sin dalle prime fasi del processo di acquisto, la limitazione di pratiche di scomposizione artificiale del prezzo ed una chiara evidenza delle eventuali variazioni dinamiche intervenute nel corso della transazione.

(ii) Utilizzo dei dati nei sistemi di *pricing*

Introdurre adeguati presidi in relazione all'utilizzo dei dati nei sistemi di *pricing*, promuovendo l'adozione di criteri oggettivi e verificabili e limitando il ricorso a elementi suscettibili di generare distorsioni, anche attraverso linee guida e *best practices* di settore.

(iii) Monitoraggio e *audit* dei sistemi algoritmici

Sviluppare strumenti di monitoraggio e *audit* dei sistemi algoritmici, anche al fine di individuare tempestivamente fenomeni anomali o potenzialmente dannosi per il consumatore e per il corretto funzionamento dei mercati.

(iv) Termini e condizioni d'uso

Rafforzare la chiarezza e l'accessibilità dei termini e delle condizioni d'uso, con particolare riferimento alle clausole relative alla determinazione e alla modifica dei prezzi, nonché all'utilizzo dei dati per finalità di profilazione e di *pricing*.

(v) Cooperazione istituzionale ed *enforcement*

Promuovere la cooperazione tra le autorità competenti ed il potenziamento delle capacità di intervento, anche in termini di tempestività, nei mercati caratterizzati da elevata dinamicità.

DEFINIZIONI, ABBREVIAZIONI E GLOSSARIO

Abbreviazioni

AI Act. Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio sull'Intelligenza Artificiale, entrato in vigore il 1° agosto 2024. Introduce un sistema di classificazione dei rischi dei sistemi di IA (inaccettabile, alto, limitato, minimo) e obblighi differenziati per *provider*, *deployer* e *importer*.

CdA (Consiglio di Amministrazione). Organo collegiale di governo societario responsabile dell'indirizzo strategico e della supervisione dell'impresa.

CISO (Chief Information Security Officer). Responsabile della sicurezza delle informazioni e dei sistemi informatici aziendali.

DMA (Digital Markets Act). Regolamento (UE) 2022/1925 sui mercati equi e contendibili nel settore digitale. Introduce obblighi e divieti specifici per i *gatekeeper* al fine di garantire contestabilità e fairness nei mercati digitali.

EAR/BIS (Export Administration Regulations / Bureau of Industry and Security - Dipartimento del Commercio USA). Normativa statunitense che disciplina le restrizioni all'esportazione di tecnologie *dual-use* e *hardware* AI verso determinati paesi.

ERM (Enterprise Risk Management). *Framework* integrato per l'identificazione, valutazione, gestione e monitoraggio dei rischi aziendali su base olistica. Riferimento principale: COSO ERM Framework.

ESG (Environmental, Social, Governance). Insieme di criteri non finanziari utilizzati per valutare la sostenibilità e l'impatto sociale di un'impresa. Incorpora fattori ambientali (E), sociali (S) e di *governance* (G) nelle strategie e nei processi decisionali aziendali.

GDPR (General Data Protection Regulation). Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati.

HR (Human Resources). Funzione aziendale responsabile della gestione del personale, delle relazioni di lavoro e dello sviluppo delle competenze.

IA / AI (Intelligenza Artificiale / Artificial Intelligence). Sistema basato su macchine che, per un insieme dato di obiettivi definiti dall'uomo, è in grado di effettuare previsioni, formulare raccomandazioni o prendere decisioni che influenzano ambienti reali o virtuali (definizione AI Act).

IT (Information Technology). Funzione aziendale o settore industriale relativo alle tecnologie dell'informazione, ivi incluse infrastrutture, sistemi e applicazioni digitali.

PMI (Piccole e Medie Imprese). Categoria di imprese definita dalla Raccomandazione della Commissione europea 2003/361/CE: meno di 250 dipendenti e fatturato annuo non superiore a 50 milioni di euro (o totale di bilancio non superiore a 43 milioni di euro).

Glossario

Accountability. Responsabilità documentabile e verificabile di un soggetto per le decisioni prese e i risultati prodotti. In ambito IA, implica la capacità di attribuire la responsabilità degli *output* algoritmici a specifici attori dell'organizzazione.

Agenti IA (AI Agents). Sistemi di intelligenza artificiale in grado di operare in modo autonomo per il raggiungimento di obiettivi complessi, pianificando e eseguendo sequenze di azioni e adattando il proprio comportamento in funzione del contesto.

AI Champion. Figura interna all'organizzazione incaricata di promuovere l'adozione consapevole e responsabile dell'intelligenza artificiale all'interno del proprio team o funzione, fungendo da punto di riferimento per la formazione e il cambiamento culturale.

AI Impact Assessment. Valutazione preventiva dell'impatto dei sistemi di intelligenza artificiale su diritti fondamentali, equità e sicurezza, condotta prima del *deployment* del sistema.

Audit Trail. Registro cronologico e immodificabile delle operazioni effettuate da un sistema, utilizzato a fini di controllo e verifica. In ambito IA, consente la tracciabilità delle decisioni automatizzate.

Bias (algoritmico). Distorsione sistematica nei risultati prodotti da un sistema di intelligenza artificiale, derivante da dati di addestramento non rappresentativi o da scelte progettuali del modello. Può generare discriminazioni nei confronti di individui o gruppi.

Cloud sovrano. Infrastruttura di *cloud computing* progettata per garantire che i dati e le elaborazioni rimangano sotto la giurisdizione e il controllo di uno Stato o di un'area geografica determinata, riducendo la dipendenza da operatori extracomunitari.

Data spaces. Ecosistemi digitali federati e interoperabili per la condivisione sicura e controllata dei dati tra organizzazioni di uno stesso settore o filiera, promossi dalla Strategia europea per i dati.

Deployer. Ai sensi dell'AI Act: soggetto, pubblico o privato, che utilizza un sistema di IA nell'ambito della propria attività professionale. Distinto dal *provider*, che sviluppa o immette il sistema sul mercato.

Essential facility doctrine. Principio del diritto della concorrenza secondo cui il titolare di un'infrastruttura o risorsa indispensabile per operare in un mercato, non replicabile da concorrenti a costi ragionevoli, può essere obbligato a consentirne l'accesso a terzi a condizioni eque.

Explainability (spiegabilità). Capacità di un sistema di intelligenza artificiale di rendere comprensibili le ragioni e la logica sottese alle proprie decisioni o raccomandazioni, sia agli utenti finali sia ai soggetti responsabili della supervisione.

Friend-shoring. Strategia di diversificazione delle *supply chain* che privilegia fornitori e partner localizzati in paesi alleati o con valori geopolitici allineati, al fine di ridurre i rischi connessi a dipendenze politicamente instabili.

Gatekeeper. Ai sensi del Digital Markets Act: grande piattaforma online che, per la propria posizione di mercato, è soggetta a obblighi specifici di correttezza e trasparenza nei confronti degli utenti commerciali e degli utenti finali.

Human-in-the-loop. Modalità di supervisione dei sistemi di intelligenza artificiale che prevede il coinvolgimento attivo di un essere umano nelle fasi decisionali critiche, garantendo un controllo effettivo sugli *output* prima che producano effetti giuridici o pratici significativi.

Hyperscaler. Fornitore di servizi *cloud* di grandissime dimensioni che gestisce infrastrutture computazionali su scala globale.

Lock-in tecnologico. Condizione in cui un'organizzazione è vincolata all'utilizzo di tecnologie o servizi di un singolo fornitore a causa di dipendenze architetturali o contrattuali che rendono costoso e complesso il passaggio a soluzioni alternative.

Modelli generativi (Generative AI). Classe di sistemi di intelligenza artificiale in grado di generare nuovi contenuti — testo, immagini, audio, codice — a partire da pattern appresi durante la fase di addestramento su grandi *dataset*.

Nearshoring. Strategia di riorganizzazione della catena di fornitura che prevede lo spostamento di attività produttive o di approvvigionamento verso paesi geograficamente vicini, al fine di ridurre rischi logistici e dipendenze da aree distanti.

Network effects (effetti di rete). Fenomeno per cui il valore di un prodotto o servizio aumenta all'aumentare del numero dei suoi utenti. Nei mercati digitali tendono a favorire la concentrazione del potere di mercato in capo ai grandi operatori.

Open Innovation. Paradigma di innovazione che valorizza la collaborazione con soggetti esterni — startup, università, centri di ricerca — per l'accesso ad *asset* tecnologici di frontiera, distribuendo costi e rischi della ricerca e sviluppo.

Pricing algoritmico. Pratica di determinazione automatizzata dei prezzi mediante algoritmi che elaborano in tempo reale dati di mercato e di profilazione individuale degli utenti. Può comportare discriminazione di prezzo e opacità informativa nei confronti del consumatore.

Provider. Ai sensi dell'AI Act: soggetto che sviluppa un sistema di IA a proprio nome al fine di immetterlo sul mercato o metterlo in servizio.

Reshoring. Strategia di riportare attività produttive o di approvvigionamento precedentemente delocalizzate nel paese di origine dell'impresa, al fine di aumentare il controllo sulla catena di fornitura e ridurre rischi geopolitici.

Reskilling. Processo di formazione finalizzato all'acquisizione di nuove competenze professionali da parte di lavoratori le cui mansioni sono state trasformate o rese obsolete dall'automazione o dall'introduzione di nuove tecnologie.

Switching costs. Costi economici, operativi e organizzativi che un'organizzazione sostiene per passare da un fornitore, tecnologia o piattaforma a un'altra. Alti *switching costs* costituiscono barriera all'ingresso nei mercati digitali e favoriscono il *lock-in*.

Upskilling. Processo di aggiornamento e potenziamento delle competenze professionali esistenti di un lavoratore, finalizzato ad adattare il proprio profilo alle evoluzioni tecnologiche e organizzative in atto.

APPENDICE
SINTESI GRAFICA DELLE PROPOSTE

INTELLIGENZA ARTIFICIALE ED ETICA AZIENDALE

1. *Governance* e regolamentazione, valutazione e gestione del rischio

PROPOSTA

(i) Integrazione sistemica nel *risk management* e mappatura dei rischi

Integrare i sistemi di IA nei modelli di Enterprise Risk Management (ERM) prevedendo specifici indicatori di rischio, quali rischio algoritmico, rischio *bias*, rischio reputazionale.

(ii) Centralità del CdA e dei comitati endoconsiliari

Assicurare il coinvolgimento del CdA e, ove presenti, dei comitati endoconsiliari (in particolare quelli competenti in materia di controllo interno, rischi e sostenibilità) attribuendo loro la definizione delle politiche aziendali in materia di IA e la supervisione della relativa attuazione.

(iii) *Accountability* diffusa

Promuovere una chiara attribuzione di responsabilità lungo tutta la struttura operativa.

(iv) *Framework* di classificazione dei sistemi di IA

Adottare modelli interni di classificazione coerenti con l'approccio *risk-based* dell'AI Act, garantendo l'aggiornamento continuo in funzione dell'evoluzione tecnologica e normativa.

(v) Sistemi di tracciabilità e documentazione

Implementare adeguati sistemi di tracciabilità delle decisioni e degli *output* generati dai sistemi di IA al fine di assicurare *audit trail* efficaci e verificabili.

(vi) Funzioni di controllo indipendenti

Prevedere verifiche periodiche attraverso *audit* interni o esterni, volti a valutare la conformità e l'affidabilità dei sistemi di IA adottati.

2. Strategia, sostenibilità e responsabilità sociale (Strategia aziendale e integrazione dei principi ESG)

PROPOSTA

Si propone di integrare l'IA nei *framework* esistenti di gestione del rischio, *compliance* e responsabilità degli organi societari.

A tal fine, si individuano le seguenti *best practices* operative:

(i) *Governance* e supervisione del CdA

L'attenzione del Consiglio di Amministrazione e dei comitati endoconsiliari competenti (quali ad esempio i comitati rischi e sostenibilità) dovrà concentrarsi su profili quali l'attribuzione della responsabilità per gli *output* generati dai sistemi di IA, la tracciabilità delle decisioni automatizzate, la prevenzione dei c.d. *bias* (intesi quali pregiudizi) e fenomeni discriminatori, nonché la gestione dei rischi reputazionali e di *compliance*.

In tal contesto, la supervisione da parte di figure dotate di adeguate competenze tecniche e giuridiche assume un ruolo fondamentale. Le attività di vigilanza e controllo devono essere reinterpretate alla luce delle nuove dinamiche introdotte dall'automazione decisionale, garantendo che i processi decisionali automatizzati siano comprensibili, verificabili e coerenti con gli obiettivi aziendali e con i requisiti normativi.

L'IA diventa quindi materia di governo societario, con rilevanti implicazioni in termini di doveri fiduciari degli amministratori, responsabilità nei confronti degli azionisti e aspettative degli investitori.

La supervisione degli esperti e di coloro che sono deputati a controllare tali *output* alla luce di una nuova declinazione dei concetti di vigilanza e controllo devono restare fondamentali. In questo senso, l'AI diventa materia di governo societario, con ricadute sui doveri fiduciari degli amministratori, sulla responsabilità verso gli *shareholders* e sulle aspettative degli investitori.

(ii) Ruolo dei *corporate leaders*

L'adozione di sistemi di IA richiede un approccio interdisciplinare che integri competenze giuridiche, tecnologiche, organizzative e di *risk management*, attraverso:

- la definizione di *policy* interne sull'utilizzo di sistemi di IA, secondo criteri etici e giuridici chiaramente individuati;
- la valutazione preventiva dei rischi mediante strumenti quali gli *AI impact assessments* e le *algorithmic risk reviews*;
- l'istituzione ed il coordinamento di comitati di supervisione interdisciplinari;
- la definizione di processi di responsabilità interna attraverso i modelli di *accountability* documentati e verificabili.

In questo modo, i *corporate leaders* assumono una funzione di garanzia nella *governance* dell'IA, assicurando coerenza tra innovazione tecnologica, strategie di investimento, obblighi normativi e valori aziendali. A tale funzione si affianca un ruolo di indirizzo culturale, volto a promuovere trasparenza, formazione, consapevolezza del rischio e procedure organizzative che preservino la centralità della persona anche nell'era dell'automazione.

2. Strategia, sostenibilità e responsabilità sociale (Strategia aziendale, sostenibilità e intelligenza artificiale)

PROPOSTA

Si propone di strutturare l'implementazione dei modelli AI-ESG attraverso un approccio integrato che coinvolga *governance*, pianificazione strategica e valutazione degli impatti.

(i) Coinvolgimento degli stakeholder

Il dialogo con investitori, dipendenti e fornitori rappresenta elemento essenziale per l'efficace integrazione dei principi ESG nei processi di adozione dell'intelligenza artificiale. A tal fine, è opportuno promuovere forme di comunicazione trasparente e continua, favorendo il coinvolgimento degli stakeholder nelle decisioni strategiche e nei processi di trasformazione organizzativa maggiormente rilevanti.

(ii) Definizione di una *roadmap* AI-ESG

L'implementazione di modelli AI-ESG richiede la predisposizione di una *roadmap* strutturata che individui obiettivi, priorità, tempistiche e responsabilità. La *roadmap* dovrebbe articolare il percorso di implementazione in fasi progressive, prevedendo obiettivi di breve, medio e lungo periodo, nonché meccanismi di monitoraggio e revisione periodica dei risultati conseguiti.

(iii) Integrazione della FRIA nei processi di *governance*

Si propone di strutturare la Fundamental Rights Impact Assessment (FRIA) non come un adempimento documentale isolato bensì come uno strumento integrato nel sistema di *governance* dell'IA. In tale prospettiva, la FRIA dovrebbe essere coordinata con i processi di *risk management* previsti dall'art. 9 AI Act e con la Data Protection Impact Assessment (DPIA) di cui all'art. 35 GDPR, attraverso un percorso articolato nelle fasi di mappatura del sistema, individuazione dei diritti coinvolti, analisi del rischio e valutazione di proporzionalità delle misure adottate. La valutazione dovrebbe concludersi con l'individuazione di misure di mitigazione verificabili e obblighi di revisione periodica, affinché la tutela dei diritti fondamentali divenga un elemento strutturale della *governance* dei sistemi di IA ad alto rischio.

2. Strategia, sostenibilità e responsabilità sociale (Responsabilità sociale)

PROPOSTA

Si propone un approccio equilibrato che preveda la formazione della forza lavoro, nonché politiche di supporto per la transizione verso un'economia automatizzata.

(i) Il divario nell'adozione dell'AI rischia di amplificare le disuguaglianze economiche esistenti tra grandi imprese, PMI e microimprese. Chi dispone di maggiori risorse economiche, infrastrutture tecnologiche avanzate e competenze specializzate può investire massicciamente nella tecnologia, creando un *gap* competitivo che rischia di marginalizzare ulteriormente alcune realtà di mercato, con un fenomeno di concentrazione del potere economico che riduce la competitività delle PMI e delle microimprese e aumenta le disuguaglianze nel tessuto produttivo.

(ii) È fondamentale promuovere politiche di incentivazione e supporto per l'adozione dell'IA nelle PMI e nelle microimprese, fornendo accessi agevolati a infrastrutture tecnologiche, formazione mirata e consulenza per la strutturazione dei dati. Solo attraverso un ecosistema inclusivo sarà possibile garantire che i benefici dell'intelligenza artificiale siano ampiamente accessibili.

3. Analisi della struttura aziendale, dei dati e del personale *accountable* per *step*

PROPOSTA

(i) Definizione dell'approccio di mappatura

La scelta dell'approccio alla mappatura dei sistemi di IA dovrebbe essere sviluppata secondo un approccio coerente con la cultura organizzativa dell'azienda e del livello di maturità dell'impresa. È possibile individuare due alternative principali.

Un primo approccio, di tipo processo-centrico, parte dall'analisi dei processi aziendali già esistenti e risulta particolarmente adatto alle organizzazioni che intendono integrare l'IA all'interno di modelli operativi già consolidati.

Un secondo approccio, basato sui casi d'uso (*use-cases*), muove invece dall'identificazione degli specifici impieghi dell'IA e dei relativi livelli di rischio. In tale prospettiva, si ritiene preferibile una lettura per livelli di rischio, che consenta di differenziare i presidi organizzativi in funzione dell'impatto che ciascun sistema può avere sui diritti della persona (ad esempio in ambito sanitario e di selezione del personale), sui processi decisionali e sulle attività aziendali.

(ii) Registro dei sistemi di IA

Si propone l'adozione di un registro dei sistemi di intelligenza artificiale volto a censire i sistemi già utilizzati o in fase di implementazione, documentando i profili descritti di seguito:

- il ruolo ricoperto dall'organizzazione ai sensi dell'AI Act (*provider*, *deployer*, *importer* o altro soggetto rilevante);
- la finalità del sistema;
- le categorie di dati trattati;
- il livello di rischio attribuito secondo la classificazione prevista dall'AI Act;
- le misure di sicurezza e di controllo adottate.

(iii) *Vendor* e *Internal risk assessment*

Particolare attenzione deve essere dedicata ai rapporti con i fornitori esterni di sistemi di IA. La valutazione effettuata dal *provider* ai sensi dell'AI Act non esaurisce infatti le responsabilità dell'impresa utilizzatrice (*deployer*).

Si propone pertanto che ogni sistema IA sia sottoposto ad una duplice valutazione:

- *vendor risk assessment*: a cura del fornitore;
- *internal risk assessment*: a cura dell'organizzazione utilizzatrice, tenendo conto delle specificità dei dati trattati, delle finalità perseguite e dell'impatto sui processi decisionali interni.

(iv) Matrice organizzativa

Si propone l'adozione di una matrice organizzativa che consenta di individuare chiaramente ruoli, responsabilità, funzioni di controllo e livelli di autorizzazione associati ai sistemi di IA, assicurando la tracciabilità delle decisioni e l'effettività dei meccanismi di *governance*.

(v) Sistemi ad alto rischio e adempimenti normativi

I sistemi classificati come ad alto rischio ai sensi dell'AI Act richiedono l'adozione di presidi specifici. In particolare, è opportuno:

- identificare i sistemi ad alto rischio presenti nel contesto operativo dell'organizzazione;
- verificare gli obblighi previsti dalla normativa applicabile e le relative tempistiche di adempimento;
- adottare tempestivamente le misure necessarie per garantire la conformità ai requisiti normativi.

4. Coordinamento con altri *framework* aziendali ed organizzativi

PROPOSTA

(i) Coordinamento e integrazione delle *policy* aziendali

Si propone di adottare un approccio unitario nella definizione delle *policy* aziendali, assicurando il coordinamento tra i diversi requisiti normativi e la loro integrazione con riferimento all'utilizzo dei sistemi di IA.

(ii) Coordinamento interfunzionale

Favorire il coordinamento tra le funzioni aziendali coinvolte, tra cui legal, IT, HR, *compliance*, *risk management* e *cybersecurity*, anche attraverso l'istituzione di comitati o gruppi di lavoro dedicati.

(iii) Monitoraggio del quadro normativo e delle prassi applicative

Istituire presidi dedicati al monitoraggio delle evoluzioni normative, regolatorie, giurisprudenziali e delle prassi di mercato, al fine di garantire un costante aggiornamento dei modelli organizzativi e delle *policy* aziendali.

5. *Training* e formazione interna

PROPOSTA

(i) Struttura della formazione e del *training*

Le organizzazioni dovrebbero definire una strategia formativa chiara e continuativa, articolata secondo le seguenti linee direttrici:

- mappatura delle competenze in materia di IA presenti nelle diverse funzioni aziendali, con individuazione delle conoscenze di base che l'intera popolazione aziendale dovrebbe possedere e tempestiva identificazione degli eventuali *gap* formativi;
- sviluppo di programmi di formazione ed aggiornamento continuo, personalizzati in funzione dei ruoli e periodicamente aggiornati alla luce dell'evoluzione tecnologica, normativa ed organizzativa (es. "*real time training*");
- diffusione della conoscenza delle *policy* aziendali in materia di IA, delle regole relative all'utilizzo dei dati, dei sistemi di IA generativa e dei relativi presidi organizzativi;
- preparazione agli scenari evolutivi dell'intelligenza artificiale, inclusi i modelli di IA agentica e le relative implicazioni organizzative e di *governance*;

- definizione e comunicazione di ruoli, responsabilità e presidi organizzativi connessi all'utilizzo dell'IA, anche attraverso l'individuazione di referenti interni o figure di supporto al cambiamento (ad es. "AI Champion");
- predisposizione di percorsi di reskilling e upskilling mirati in funzione delle specificità dell'azienda e dell'evoluzione delle competenze richieste.

(ii) Requisiti di qualità della formazione

È essenziale integrare i percorsi formativi con i processi aziendali e progettati in modo da favorire un apprendimento concreto, continuativo e misurabile. A tal fine, appare opportuno privilegiare metodologie innovative e ad elevato coinvolgimento, in grado di tradurre i principi generali in comportamenti operativi.

Esempi di frontiere formative innovative possono includere:

- soluzioni digitali di supporto (*chat box* interattivi) in grado di segnalare potenziali criticità operative, di *compliance* o di natura etica nello svolgimento delle attività lavorative;
- simulazioni, esercitazioni e modelli di apprendimento basati su casi pratici, finalizzati a favorire una maggiore consapevolezza dei rischi e delle responsabilità connesse all'utilizzo dell'IA.

(iii) Approccio metodologico consigliato

Si ritiene preferibile adottare un approccio ibrido, che combini una base comune di conoscenze e principi destinata all'intera popolazione aziendale con percorsi specialistici calibrati sulle esigenze delle diverse funzioni. Tale modello consente di:

- evitare sia il rischio di formazione eccessivamente generica sia la frammentazione derivante da approcci esclusivamente settoriali;
- promuovere la diffusione di un linguaggio e di principi comuni all'interno dell'organizzazione;
- garantire competenze specialistiche adeguate ai diversi ruoli e livelli di responsabilità;
- favorire la collaborazione interfunzionale e la coerenza dei processi decisionali;
- rafforzare i meccanismi di *accountability* individuale ed organizzativa.

CAMBIAMENTI GLOBALI: ESG, COMPLIANCE, POLITICHE ECONOMICHE E GEOPOLITICA – IL RUOLO DEI CORPORATE LEADERS

1. Scenari di innovazione e concorrenza: impatto sugli operatori economici

PROPOSTA

In un'ottica di competitività sistemica, le imprese, ed in particolare le microimprese, dovrebbero perseguire modelli di cooperazione tecnologica fondati su paradigmi di *open innovation*. L'attivazione di sinergie con associazioni di categoria, startup, poli universitari e centri di eccellenza consente l'internalizzazione di *asset* tecnologici di frontiera, mitigando l'onere finanziario connesso alle attività di ricerca e sviluppo.

2. Condizioni "eque" di accesso ai dati, all'infrastruttura digitale, alle capacità computazionali ed alle filiere strategiche critiche (*cloud* sovrano)

PROPOSTA

Al fine di rafforzare la propria resilienza digitale, le imprese dovrebbero adottare una serie di misure strutturate lungo le seguenti direttrici.

(i) Mitigazione del rischio di dipendenza tecnologica
Si dovrebbero progettare le proprie architetture digitali secondo logiche orientate all'interoperabilità ed alla portabilità fin dall'origine, limitando il rischio di dipendenza da un singolo fornitore e favorendo, ove possibile, l'adozione di modelli *multi-provider*. A tal fine, assume particolare rilievo la possibilità di migrazione tra piattaforme con costi ed impatti organizzativi contenuti, evitando la necessità di una sostanziale riprogettazione dell'architettura applicativa.

(ii) Valorizzazione e censimento del patrimonio informativo
Si propone di censire e classificare il patrimonio informativo aziendale attraverso una data strategy che identifichi gli *asset* informativi di maggiore valore strategico, le relative modalità di utilizzo ed i livelli di protezione necessari in funzione della loro rilevanza.

(iii) Protezione del patrimonio informativo

Le imprese dovrebbero sviluppare una maggiore consapevolezza in merito alla localizzazione, alla circolazione e all'utilizzo dei dati impiegati nei sistemi di IA, con particolare riferimento ai casi in cui tali informazioni possano essere trasferite al di fuori del perimetro aziendale (e potenzialmente dell'Unione europea). A tal fine, appare necessario adottare misure proporzionate alla sensibilità dei dati, quali tecniche di anonimizzazione o pseudonimizzazione, soluzioni di *cloud* privato e, ove opportuno, modelli IA implementati in ambienti *on-premise*.

3. Quale ruolo per i *corporate leaders* nelle scelte aziendali in un contesto geopolitico complesso?

PROPOSTA

Si propone l'adozione di un protocollo di *best practices* per integrare il rischio geopolitico nei processi di Enterprise Risk Management.

A tal fine, si individuano i seguenti ambiti prioritari di intervento.

(i) *Geopolitical risk assessment* e *scenario planning*

Le organizzazioni dovrebbero sviluppare processi strutturati di valutazione del rischio geopolitico, basati sull'analisi degli scenari e sull'identificazione delle principali vulnerabilità relative a fornitori strategici, infrastrutture critiche, mercati di riferimento e dipendenze tecnologiche.

(ii) Resilienza delle filiere e diversificazione delle dipendenze strategiche

Al fine di ridurre l'esposizione a rischi geopolitici e operativi, appare opportuno limitare la dipendenza da singole aree geografiche, fornitori o tecnologie critiche. In tale prospettiva, strategie di *reshoring*, *near-shoring*, *friend-shoring* e diversificazione delle *supply chain* possono contribuire a rafforzare la resilienza complessiva dell'organizzazione, pur comportando, in alcuni casi, maggiori costi nel breve periodo.

(iii) Dialogo istituzionale e monitoraggio regolatorio

Il dialogo con istituzioni pubbliche, autorità, organizzazioni internazionali e associazioni di categoria non dovrebbe essere considerato un mero adempimento di *compliance*, bensì uno strumento di presidio strategico finalizzato a comprendere tempestivamente l'evoluzione del contesto normativo e a ridurre l'incertezza operativa.

(iv) Formazione continua dei *corporate leaders*

La formazione continua dei vertici aziendali sui temi della geopolitica economica, della sicurezza tecnologica, del commercio internazionale e della *governance* dell'intelligenza artificiale costituisce un elemento essenziale per rafforzare la capacità dell'organizzazione di anticipare i cambiamenti e adattarsi a contesti caratterizzati da elevata complessità e volatilità.

CONSUMATORI DEL FUTURO, ANTITRUST E NUOVI MERCATI

1. Pressioni competitive nei mercati digitali, *upstream* e *downstream*: concorrenza, innovazione e ruolo del diritto antitrust

PROPOSTA

Si propone l'adozione di un protocollo di *best practices* ispirato ai principi del Digital Markets Act e del diritto della concorrenza, volto a promuovere maggiore trasparenza, equità e contendibilità nei mercati digitali.

Il Protocollo si configura come un *framework* operativo destinato ad orientare concretamente i comportamenti degli operatori e ad agevolare l'adozione di modelli organizzativi in linea con l'evoluzione del quadro normativo europeo.

A tal fine, il Protocollo si articola nei seguenti ambiti prioritari di intervento, tra loro complementari.

(i) Accesso e condivisione dei dati

Nei mercati digitali, l'accesso ai dati assume un ruolo strategico ai fini della concorrenza e dell'innovazione. In tale prospettiva, appare opportuno promuovere criteri chiari per l'accesso e la condivisione delle informazioni strategiche, assicurando un adeguato equilibrio tra apertura del mercato, tutela dei diritti e protezione degli interessi economici degli operatori. Sotto questo profilo, la riduzione delle asimmetrie informative rappresenta un elemento essenziale per favorire la contendibilità dei mercati digitali.

(ii) Rapporti tra piattaforme, utenti commerciali e utenti finali

Nei rapporti con gli utenti commerciali (upstream), assume particolare rilievo il rispetto dei principi di correttezza, trasparenza e non discriminazione, con specifico riferimento alle condizioni contrattuali e ai criteri che incidono sull'accesso al mercato, sul posizionamento e sulla visibilità all'interno delle piattaforme. Tali presidi contribuiscono a ridurre le asimmetrie informative e a favorire condizioni di concorrenza più eque.

Nei confronti degli utenti finali (*downstream*), appare opportuno rafforzare la trasparenza dei sistemi algoritmici, assicurando una maggiore conoscibilità dei criteri che incidono sulla personalizzazione dei servizi e sulla profilazione. In tale prospettiva, si propone l'introduzione di *standard* minimi di *explainability* e di adeguati meccanismi di verifica, anche indipendenti, volti a mitigare possibili effetti distorsivi sui comportamenti degli utenti e sui processi decisionali.

(iii) Interoperabilità e portabilità dei dati

La promozione di *standard* di interoperabilità e strumenti efficaci di portabilità dei dati è essenziale per ridurre il rischio di *lock-in* e favorire una maggiore apertura degli ecosistemi digitali. Tali misure possono contribuire a rafforzare la contendibilità dei mercati digitali ed a favorire una più agevole interazione tra servizi e piattaforme, in linea con gli obiettivi perseguiti dal legislatore unionale.

(iv) Integrazione nei sistemi di *governance* aziendale

Il Protocollo prevede l'integrazione dei principi di trasparenza, equità e contendibilità nei sistemi di *governance* delle organizzazioni, attraverso la chiara individuazione delle funzioni responsabili, l'adozione di procedure di monitoraggio e verifica e la predisposizione di strumenti di reporting periodico. Ciò consente di incorporare tali principi nei processi decisionali e nei sistemi di controllo aziendale, rafforzando l'efficacia delle misure adottate e favorendo una gestione responsabile delle attività digitali.

2. Algoritmi, determinazione dei prezzi, termini e condizioni d'uso per utenti e consumatori

PROPOSTA

In tale prospettiva, si formulano le seguenti proposte operative:

(i) Trasparenza dei prezzi

Rafforzare la trasparenza dei prezzi attraverso l'indicazione del prezzo complessivo sin dalle prime fasi del processo di acquisto, la limitazione di pratiche di scomposizione artificiale del prezzo ed una chiara evidenza delle eventuali variazioni dinamiche intervenute nel corso della transazione.

(ii) Utilizzo dei dati nei sistemi di *pricing*

Introdurre adeguati presidi in relazione all'utilizzo dei dati nei sistemi di *pricing*, promuovendo l'adozione di criteri oggettivi e verificabili e limitando il ricorso a elementi suscettibili di generare distorsioni, anche attraverso linee guida e *best practices* di settore.

(iii) Monitoraggio e *audit* dei sistemi algoritmici

Sviluppare strumenti di monitoraggio e *audit* dei sistemi algoritmici, anche al fine di individuare tempestivamente fenomeni anomali o potenzialmente dannosi per il consumatore e per il corretto funzionamento dei mercati.

(iv) Termini e condizioni d'uso

Rafforzare la chiarezza e l'accessibilità dei termini e delle condizioni d'uso, con particolare riferimento alle clausole relative alla determinazione e alla modifica dei prezzi, nonché all'utilizzo dei dati per finalità di profilazione e di *pricing*.

(v) Cooperazione istituzionale ed *enforcement*

Promuovere la cooperazione tra le autorità competenti ed il potenziamento delle capacità di intervento, anche in termini di tempestività, nei mercati caratterizzati da elevata dinamicità.

OSSERVATORIO
CORPORATE LEADERS

MILANO FINANZA · MADONNA DI CAMPIGLIO · TRENTINO

EXPERTS TALK®
CORPORATE LEADERS

MADONNA DI CAMPIGLIO
2-4 DICEMBRE 2026

Per maggiori informazioni e per partecipare:
www.the-experts-talk.com

OSSERVATORIO
CORPORATE LEADERS