ASSOLOMBARDA

L’integrazione dell’intelligenza artificiale in azienda per monitorare i rischi reato e efficientare il modello organizzativo 231

Avv. Elena Tiberio – Area Diritto d’Impresa

7 ottobre 2025 - Incontro in AODV

Sistema di IA

Regolamento (UE) 2024/1689
del Parlamento Europeo e del Consiglio (AI ACT - Art. 3, n.1)

Legge 132/2025, art. 2, comma 1, lett. a)

Sistema di IA : un sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

caratteristiche essenziali

- l'interazione tra uomo e macchina → l'uomo imposta gli obiettivi da raggiungere e inserisce i dati di ingresso;
- l'aspetto innovativo → l'IA ha la capacità di elaborare e di interpretare un ingente volume di dati in tempi estremamene ridotti, imparando (machine learning) e creando nuove correlazioni (autonomia e adattabilità) che consentono di andare oltre gli schemi preimpostati dall'intervento umano iniziale e di ottenere nuovi output;
- la componente umana → l'uomo rimane responsabile degli obiettivi impostati (input) e dei risultati ottenuti dall'IA (output) : principio antropocentrico (ben espresso anche nell'art. 3, comma 3, L. 132/2025)

AI ACT – Rischio

L'AI ACT

- regolamenta l'intelligenza artificiale tramite un approccio basato sul rischio

probabilità e gravità dell'impatto negativo che un sistema di IA potrebbe avere sui diritti individuali e sulla società

- prevede regole e obblighi diversi per fornitori e utenti, a seconda del livello di rischio derivante dal sistema IA:

più alto è il rischio, > le responsabilità per chi sviluppa e per chi usa i sistemi IA

Tale approccio basato sul rischio è lo stesso del GDPR: tendenzialmente si può fare tutto, bilanciando obiettivi e garanzie

AI ACT – Rischio

L'AI ACT definisce 4 livelli di rischio:

SISTEMI A RISCHIO INACCETTABILE

Vietati da febbraio 2025, costituiscono una minaccia inaccettabile per i diritti e libertà fondamentali degli individui o possono essere utilizzati in modo manipolativo o ingiusto.

- software di sorveglianza di massa
- social scoring (sistema di AI che valuta o classifica persone in base al comportamento sociale, caratteristiche personali o tratti della personalità)
- sfruttamento delle vulnerabilità delle persone
- utilizzo di tecniche manipolative subliminali
- identificazione biometrica remota in tempo reale in spazi accessibili
- riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione
- web scraping di immagini per la creazione o l'espansione di banche dati

SISTEMI A RISCHIO ELEVATO

Sistemi di IA utilizzati in ambiti critici quali sanità, sicurezza, trasporti, giustizia.
Essi devono soddisfare requisiti rigorosi in termini di trasparenza, sicurezza, supervisione
ES:

- Sistemi di Biometria;
- Sistemi di diagnosi medica;
- Sistemi applicati a infrastrutture critiche (traffico stradale, fornitura di acqua, gas, riscaldamento ed elettricità);
- Sistemi volti a favorire l'occupazione, gestione dei lavoratori e accesso al lavoro autonomo (anche in fase di recruiting);
- Sistemi per l'accesso a servizi e a prestazioni pubblici e privati essenziali (assistenza sanitaria, valutazione dell'affidabilità creditizia)

AI ACT – Rischio

SISTEMI A RISCHIO LIMITATO

(o A RISCHIO TRASPARENZA)

Ad essi si applicano specifiche attenzioni (es. definizione di misure di sicurezza informatica, mitigazione dei rischi potenziali, trasparenza a salvaguardia degli individui che si interfacciano con tale tecnologia)

ES:

- Sistemi destinati a interagire direttamente con le persone fisiche (i.e: Chatbot)
- Sistemi che generano contenuti *deep fake*
- Sistemi per finalità generali, che generano contenuti audio, immagini, video o testuali sintetici

SISTEMI A RISCHIO MINIMO O NULLO

Non causano alcun impatto sulla società e sui diritti individuali, dunque non sono soggetti ad alcuna restrizione particolare, ma solo alle norme generali sulla protezione dei dati e sulla sicurezza.

ES:

- Assistente virtuale per la pianificazione di attività quotidiane
- Videogame abilitati all'AI
- Filtri antispam

AI ACT – Rischio

L'AI ACT

- prevede, per le pratiche di IA più rischiose (ma ammesse) – un sistema di gestione del rischio articolato «*sul rispetto di particolari standard di sicurezza, nonché di procedure dirette tanto a far ottenere al sistema una validazione preventiva, quanto a garantire il rispetto costante dei requisiti richiesti nel momento in cui è immesso sul mercato*»

- definisce il sistema di gestione del rischio (art. 9, par. 2) come «*un processo iterativo continuo, eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un aggiornamento costante e sistematico*», nonché una serie di attività volte a identificare, valutare e gestire (anche con azioni di mitigazione) i rischi (noti e prevedibili) che possono derivare dall'utilizzo di un sistema di IA

Fundamental rights impact assessment – FRIA: valutazione di impatto introdotta dall'AI ACT cui sono tenuti gli operatori e sviluppatori di sistemi di IA considerati ad alto rischio per garantire che l'applicazione e l'uso dei sistemi di IA rispettino i diritti umani e le libertà fondamentali.
La sua funzione principale è di identificare preventivamente i potenziali rischi legali derivanti dall'utilizzo di sistemi IA, con l'obiettivo di mitigarli prima che possano manifestarsi

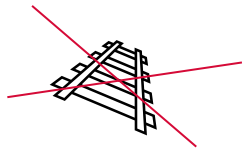
L’IA in azienda

Quando l’azienda (*deployer*) decide di introdurre uno o più sistemi di IA, deve sapere che ne deve fare

utilizzo corretto, trasparente e responsabile (art. 1 L.132/2025)

I dati sono il carburante con cui si alimentano i sistemi di IA, senza dati i sistemi di IA non funzionano

1. avere consapevolezza dell’importanza dei dati



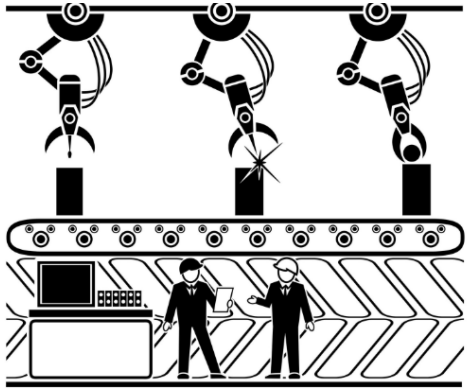
2. applicare tecniche appropriate di *data governance*

3. conoscere e valutare i rischi

- Violazione di principi etici
- Atti illeciti
- Reati
- Reati presupposto

L’IA in azienda: cosa monitorare

Spesso l’azienda non ha contezza dell’importanza, della quantità e della qualità dei dati generati al suo interno e nelle relazioni con l’esterno, ad esempio con fornitori e clienti (*know how*) …
anche se i dati contribuiscono a costituire l’identità stessa dell’azienda



I dati in azienda sono in continua evoluzione, si modificano, si trasformano, si aggiornano.
Pertanto vanno monitorati e controllati lungo tutto il loro percorso

Questo approccio è perfettamente applicabile ai sistemi di IA, che devono essere monitorati all’inizio, nel mentre e alla fine

L’IA in azienda: cosa monitorare

I dati in entrata

IA addestrata su dati distorti, crea risultati distorti

Per il momento, qualsiasi sistema di IA si basa su quello che «vede», dai dati di input.

Qualora i dati di input siano viziati o non aggiornati (ovvero soggetti a *bias* - distorsioni) il processo di elaborazione può essere condizionato da questa “falla” *ab origine* del sistema.

Bias di esclusione:

un addestramento eseguito dalla direzione commerciale / marketing, basato su dati storici, che non tiene conto dei cambiamenti del mercato o delle preferenze dei consumatori

→ rischio per l’ente: previsioni errate nel campo delle vendite e conseguente danno economico

Bias cognitivo:

un addestramento su un gruppo demografico ristretto per la selezione di CV, pur in assenza di pregiudizi, può portare a escludere alcune categorie di candidati, negando opportunità a determinati gruppi di persone

→ rischio per l’ente : danno reputazionale / violazione di principi etici

L’IA in azienda: cosa monitorare

I dati in entrata

L’attenzione ai dati in entrata non riguarda solo dati eventualmente viziati o errati: anche in casi di inserimento di dati corretti si potrebbe configurare un rischio per l’azienda.

Esempio:

l’addestramento di una IA con informazioni esatte, ma tutelate dalla legge sul diritto d’autore (a prescindere dal fatto che l’output sia identico e/o simile a lavori precedentemente esistenti di un artista, da cui il sistema di IA ha attinto per la creazione di un nuovo risultato)

L’ art. 25, comma 1, lett. b), Legge 132/2025 prevede l’inserimento nella Legge 633/1941 dell’art. 70 *septies*:

«*… la riproduzione e l’estrazione da opere o da altri materiali …attraverso modelli e sistemi di intelligenza artificiale anche generativa, sono consentite in conformità con gli articoli 70-ter e 70-quater.*»

e cioé

- da parte di istituti di ricerca o di istituti a tutela del patrimonio culturale per scopi di ricerca scientifica
- quando la riproduzione o estrazione non sia stata espressamente riservata da parte dei titolari del diritto d’autore.

L’IA in azienda: cosa monitorare

I dati «nel mentre»

Facciamo il caso di dipendenti che inseriscono dati personali e/o informazioni riservate su un sistema IA che però li condivide in rete

→ rischi per l’ente : violazione della normativa privacy, divulgazione di informazioni riservate e/o segreti

Per questo è importante

- integrare algoritmi di investigazione, utili per individuare anomalie all’interno dei dati raccolti;
- capire se, dove o con chi l’IA eventualmente condivide i dati;
- adottare ulteriori misure tecniche e organizzative per prevenire la perdita dei dati personali e delle informazioni aziendali;
- incrementare la sicurezza delle reti e dei sistemi informatici per prevenire il cyber crime ed evitando un attacco informatico all’IA

L’IA in azienda: cosa monitorare

I dati in uscita

I sistemi di IA possono produrre risposte non consone, anche se basati su dati rappresentativi e/o su di un addestramento efficace.
È per questo necessario adottare misure preventive nell’uso degli output, introducendo come prassi la verifica dei risultati ottenuti.

Azienda leader nel settore del fashion introduce piattaforma di IA per l’aiuto nello sviluppo di nuove collezioni
L’azienda utilizza la piattaforma di IA, crea una nuova collezione e la presenta al pubblico.
Immediatamente dopo la presentazione, riceve una diffida in quanto un abito indossato da una modella interferisce con la creazione di un altro designer → rischio per l’ente: interferenza con un diritto di proprietà intellettuale / danno reputazionale

Chat GPT: talvolta è percepita come più intelligente della persona che vi dialoga … tuttavia è ancora indietro rispetto a una persona davvero competente, attenta alla cura della lingua, al senso della frase, ben capace di individuare le fonti…

L'IA in azienda: cosa monitorare

Possibili nuovi rischi

Il rischio «sistemico»

Un errore o una condotta illecita di un uomo tendono a restare isolati, ma se il sistema di IA è mal addestrato o manipolato, l'errore che produce può propagarsi automaticamente in altri processi, sistemi, documenti o decisioni dell'azienda

↓

un errore negli automatismi contabili può riflettersi su migliaia di registrazioni.

Rischi per l'ente → reati societari di cui all'art. 25 *ter* D.Lgs. 231/2001 – per es: falso in bilancio, false comunicazioni sociali

frodi informatiche per applicazione massiva di operazioni illecite da parte dell'algoritmo

Il rischio «opaco»

Se un dipendente sbaglia, è probabile che si possa ricostruire il processo che ha portato a tale errore (con documenti, email, testimonianze).

Con i sistemi di IA complessi (es. deep learning) la logica è spesso una "*black box*", cioè non è chiaro perché una decisione sia stata presa.

↓

Sistema di IA che rifiuta un cliente ritenuto rischioso, senza spiegarne il motivo

Rischio per l'ente: impossibilità di spiegare il processo decisionale, mancanza di trasparenza

Possibili reati presupposto

Qualche esempio di reati presupposto ex D.Lgs. 231/2001 che possono essere commessi tramite l'uso dell'IA

- Reati in violazione delle norme sulla salute e sicurezza dei lavoratori

La presenza dell'IA nelle attrezzature, se non opportunamente governata, ne può determinare il malfunzionamento (o il funzionamento diverso) rispetto alle previsioni originarie, mettendo a rischio la sicurezza delle persone e la qualità e sicurezza dei prodotti oggetto di lavorazione.

- Reati Ambientali

L'IA può essere utilizzata per eludere controlli e comunicare dati ambientali falsi, ad esempio, attraverso la manipolazione di dati relativi alle emissioni

- Frode informatica / delitti informatici

L'IA può essere utilizzata per attacchi di phishing, per manipolare i dati, per accedere abusivamente a sistemi informatici (art. 24-bis D.Lgs. 231/01)

Possibili reati presupposto

- Manipolazione del mercato

L'IA può essere utilizzata:

- per creare un numero illimitato di account di posta elettronica e generare, tramite chatbot, altrettante recensioni non veritiere per promuovere scorrettamente la propria attività commerciale;
- per diffondere notizie false o fuorvianti al fine di gonfiare artificialmente il prezzo di un titolo in borsa, inducendo gli investitori ad acquistarlo e permettendo ai manipolatori di venderlo a prezzi elevati.

Art. 26, comma 4, L. 132/2025
Modifica l'art. 185 TUF – Manipolazione del mercato
Chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni.
La pena è della reclusione da due a sette anni e della multa da euro venticinquemila a euro sei milioni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale

Possibili reati presupposto

- Corruzione e concussione

L'IA potrebbe essere utilizzata per agevolare pratiche corruttive

- Riciclaggio e l'autoriciclaggio

Strumenti di IA possono rendere più difficile il tracciamento delle operazioni

- Reato di truffa

L'IA può essere utilizzata, per esempio, per

- generare contenuti falsi: l'IA può creare messaggi, email o annunci pubblicitari ingannevoli che sembrano autentici, inducendo le vittime a compiere azioni dannose;

- per simulare foto, video o audio di persone reali, creando situazioni in cui le vittime credono di interagire con persone vere in cui ripongono fiducia.

Art. 26, comma 1, lett. c) L. 132/2025
introduce l' art. 612 *quater* cod. pen. - Illecita diffusione di contenuti generati o alterati con sistemi di IA
Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni (...)

Entra in gioco la Governance

D.Lgs. 231/2001 – art. 6. comma 1, lett. a

ORGANO DIRIGENTE = è la guida strategica dell'organizzazione e a cui ne è affidata la gestione ordinaria e straordinaria, di regola con facoltà di delegare le proprie attribuzioni a uno o più dei suoi componenti

Il controllo è sopravvivenza

La compliance è la base per un'organizzazione di successo

L'integrazione in azienda dell'IA comporta una trasformazione.

Per ottenere valore dall'uso dell'IA non sono necessarie solo nuove tecnologie, ma anche investimenti rilevanti (in termini di organizzazione e formazione).

Per fare questo è necessaria una leadership consapevole ed efficace

Il sistema di controllo interno: 3 livelli (+ 1)

Letteratura e pratica aziendale individuano 3 livelli di controllo interno:

1° livello → quello dell'*owner*, il controllo operativo del responsabile del processo;

2° livello → quello delle funzioni competenti al monitoraggio dei controlli di 1° livello e degli elementi costitutivi del sistema di controllo interno;

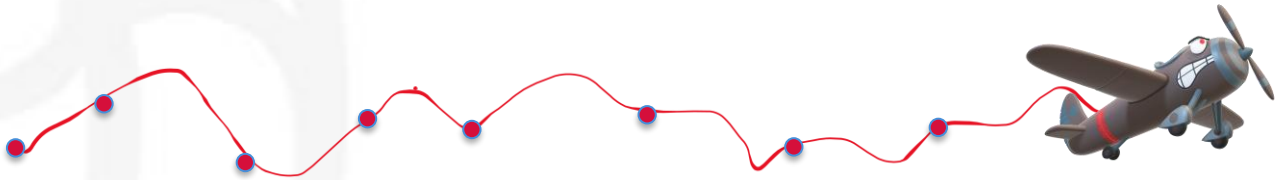
3° livello → quello dell'*internal auditor* / ODV / altri organi o funzioni indipendenti, deputati alla verifica dell'impostazione e del correlato funzionamento del sistema di controllo interno;

+ 1

A seconda delle organizzazioni, 1° livello e/o 2° livello di controllo ricomprenderanno il controllo dell'IA, ovvero di «CAIO»

Il percorso di integrazione dell'IA

L'integrazione dell'IA in azienda è un percorso e non può prescindere da una serie di attività fondamentali:



- Chiedersi quale sia l'uso che si vuole fare dei sistemi di IA
- Mappare i processi aziendali ove si vorrebbero inserire i sistemi di IA
- Eseguire un audit sui sistemi di IA che si vorrebbero acquistare per l'uso individuato
- Valutare i *terms and conditions* dei fornitori [es: riservatezza, tutela dei diritti IP, luogo dove sono trattati i dati (soprattutto se sistemi di IA sono usati in modalità cloud /SAAS), sistem card e model card cioè quelle schede che indicano gli usi consentiti e gli usi sconsigliati (es: software il cui uso è sconsigliato in ambito medico), etc.]
- Individuare - tramite una valutazione di impatto - i profili di rischio correlati all'uso dell'IA
- Gestire l'IA in modo coerente con le diverse normative (es: AI ACT, GDPR, NIS2, DATA ACT...) => soprattutto in una fase di «*over regulation*», la compliance è un vantaggio competitivo
- Stabilire il «*risk appetite*» ossia l'entità e il tipo di rischio che si è disposti ad affrontare

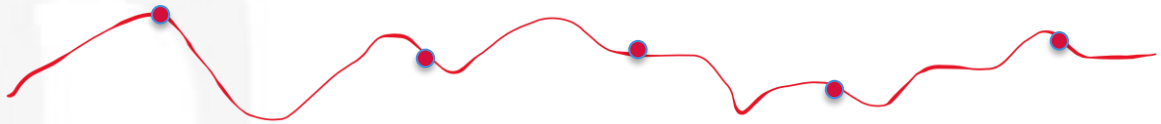
Il percorso di integrazione dell'IA

- Individuare «CAIO», il responsabile dell'IA – colui che «muove i fili» dell'IA e che può essere a capo di un team multidisciplinare per governare i diversi aspetti dell'IA (es: IT + cybersecurity + legal/compliance)
- Regolamentare l'uso dei sistemi di IA, tramite la redazione di policy specifiche, considerando l'impatto dell'IA su tutti gli *stakeholder*
- Formare il personale sull'uso sicuro e conforme dei sistemi di IA => art. 4 AI ACT «AI literacy»

  Commissione Europea => «*Living Repository of AI Literacy Practices"* = > raccolta dinamica di pratiche e iniziative concrete per promuovere la cultura dell'Intelligenza Artificiale tra chi sviluppa, adotta o utilizza sistemi IA

Open Sky Data System: dopo avere fatto formazione, ha sviluppato dei KPI per capire l'impatto di questa formazione => numero di progetti di IA dopo la formazione sono aumentati e il tempo di implementazione dei progetti di IA si è ridotto
formazione => un acceleratore di business

Il percorso di integrazione dell'IA



- Rivedere i contratti con i clienti: Art. 50 AI ACT => obblighi di trasparenza => i clienti devono sapere che l'azienda fa uso di sistemi di IA
- Implementare misure tecniche e organizzative per proteggere i dati personali, le informazioni , il know-how aziendali e i diritti di terzi
- Introdurre misure tecniche e organizzative per garantire di utilizzare i sistemi ad alto rischio conformemente alle istruzioni del fornitore
- Monitorare i comportamenti in modo costante e intervenire se si superano i limiti di guardia
- Eseguire assesment sui rischi legati alla robustezza (in materia cyber sicurezza)
- Revisionare il MOG 231, per intercettare e neutralizzare i nuovi rischi di reato, partendo dal Codice Etico

4.1 Schema riassuntivo degli adempimenti per i sistemi di alto rischio

Obblighi e responsabilità dei fornitori	
Valutazione del rischio	Prima dell'immissione sul mercato, i provider devono valutare la conformità dei sistemi IA, con l'identificazione della classe di rischio associata.
Documentazione e trasparenza	Mantenere una documentazione completa sulle caratteristiche e sulle procedure di sicurezza dei sistemi IA, per fornire ai deployer informazioni chiare agli utenti riguardo al funzionamento del sistema e alle logiche decisionali adottate.
Monitoraggio e segnalazione	I provider sono tenuti a monitorare costantemente i sistemi IA sul mercato, e correggere tempestivamente eventuali problemi di conformità e segnalando alle autorità competenti qualsiasi incidente grave.
Cooperazione nella catena di fornitura	I provider devono monitorare costantemente i sistemi IA sul mercato e correggere tempestivamente eventuali problemi di conformità e segnalando alle autorità competenti qualsiasi incidente grave.

Obblighi e responsabilità dei deployer
Uso conforme e misure di sicurezza
Monitoraggio
Formazione del personale
Valutazione di impatto

Fonte: Confindustria

L'IA per il Sistema Italia

Report 2025

I vantaggi dell'IA applicata ai controlli

- ❑ L'IA può aumentare l'efficacia preventiva dell'azione di compliance. Essa è in grado di
- rilevare in modo tempestivo le carenze organizzative sulla base dei rischi rilevati;
- elaborare dati rilevanti in «tempo reale» (sino ad oggi i modelli di compliance si sono basati solo su dati non previsionali);
- seguire le strutture comportamentali nel loro sviluppo e distinguere se e quando le regole saranno probabilmente ignorate o rispettate;
- simulare scenari di rischio emergente, attraverso «stress testing» del MOG 231

Ne consegue una maggiore "tenuta" del MOG 231 in ipotesi sottoposto al vaglio del Giudice Penale.

Esempio: con riferimento alle fattispecie di reato corruttive, sono in grado di controllare i comportamenti umani corrispondenti a fattispecie di reato, attraverso l'attivazione di red flags in caso di rilevamento automatizzato di movimenti anomali di risorse finanziare, anomalie nella fissazione dei prezzi, acquisiti da fonti esterne.

- ❑ L'IA può combinare molteplici dati provenienti da input diversi (i.e. provenienti dalle diverse funzioni interne) e restituire un risultato unitario.

- ❑ L'IA, reperendo velocemente e monitorando in modo costante i dati scambiati, può essere strumento di ausilio nel sistema dei flussi informativi: i programmi di raccolta e studio dei dati permettono di inviare un'informativa in tempo reale a tutti gli interessati e di garantire un aggiornamento costante dei dati forniti, instaurando un flusso di informazioni continuo.

I vantaggi dell'IA nel sistema 231

- In un'ottica di compliance integrata, le diverse funzioni di controllo possono partire da un *data set* comune e operare su un registro unico, migliorando il livello di coordinamento, evitando sovrapposizioni, riducendo le tempistiche di scambio dei documenti ed evitando errori di reporting, con una conseguente diminuzione dei costi complessivi del controllo.

- In un'ottica 231, in caso di modifiche normative che introducono nuovi reati presupposto, l'utilizzo dell' IA potrebbe aggiornare automaticamente il Modello Organizzativo, ricalcolando il rischio in relazione al nuovo reato.

- Grazie a piattaforme di e-learning intelligenti, l'IA può personalizzare la formazione del personale sul MOG 231, offrendo corsi su misura in base ai rischi aziendali e al ruolo di ciascun dipendente

- … … …

AI WON’T REPLACE HUMANS,

BUT HUMANS WITH AI

WILL REPLACE

HUMANS WITHOUT AI

Karim R. Lakhani
Professor of Business Administration,
Harvard Business School

ASSOLOMBARDA

www.assolombarda.it
www.genioeimpresa.it