

Indice

Introduzione

Capitolo 1 - Resilienza Organizzativa e Trasformazione Digitale

1.1 Concetto di resilienza aziendale

1.2 Trasformazione digitale come fonte di opportunità e rischio

1.3 Ruolo della progettazione organizzativa e della cultura aziendale

Capitolo 2 - L'Intelligenza Artificiale come leva strategica

2.1 Definizione e principali applicazioni dell'IA in ambito aziendale

2.2 Automazione dei processi decisionali e adattabilità organizzativa

2.3 Analisi predittiva e anticipazione delle crisi di mercato

2.4 IA e gestione del rischio operativo e strategico

Capitolo 3- Casi Studio: Le Big Tech

3.1 Amazon – IA per supply chain, logistica e resilienza operativa

3.2 IBM – Watson e l'IA applicata alla gestione dei rischi e al decision-making

3.3 Google - Data analytics, IA e adattabilità dei modelli di business

3.4 Confronto comparativo tra le tre aziende

Capitolo 4- Rischi e Sfide Etiche dell'IA

4.1 Bias algoritmico e rischi reputazionali

4.2 Trasparenza e accountability delle decisioni automatizzate

4.3 Impatto su lavoro, competenze e organizzazione interna

4.4 Normative e governance etica dell'IA

Conclusioni

Bibliografia

Introduzione

La trasformazione digitale e i progressi tecnologici degli ultimi anni hanno profondamente cambiato i modelli di business e il modo in cui le organizzazioni lavorano. Vale la pena considerare che le aziende si trovano a dover affrontare un ambiente sempre più complesso e incerto, dove la capacità di adattarsi velocemente e rispondere agli shock esterni è diventata essenziale non solo per la sopravvivenza, ma anche per mantenere viva la competitività (Bennett & Lemoine, 2014).

Il concetto di resilienza organizzativa ha acquistato un'importanza cruciale nel divario accademico e manageriale, poiché la resilienza consente non solo di superare le crisi, ma anche di imparare dall'esperienza e di prepararsi alle sfide future (Duchek, 2020).

La resilienza consta in un insieme di pratiche e capacità che permettono alle aziende di garantire la continuità operativa, adattarsi a cambiamenti imprevedibili e creare un vantaggio competitivo duraturo (Lengnick-Hall, Beck & Lengnick-Hall, 2011).

Allo stesso tempo, l'Intelligenza Artificiale (IA) si è confermata come una delle tecnologie più rivoluzionarie dei nostri tempi, capace di influenzare significativamente i processi decisionali, le strategie aziendali e le strutture organizzative, infatti rappresenta uno strumento strategico per le imprese che vogliono stimolare l'innovazione e potenziare la resilienza (Brynjolfsson & McAfee, 2017).

Il legame tra IA e resilienza è quindi un ambito di crescente interesse: da un lato, l'IA fornisce strumenti per prevedere, prevenire e gestire le crisi, attraverso analisi predittive, automazione e gestione del rischio; dall'altro, porta con sé nuove problematiche relative alla governance, all'etica e ai bias algoritmici (Floridi & Cowls, 2021).

Muovendo da queste premesse, l'obiettivo principale di questa ricerca è capire come le imprese possano sfruttare le potenzialità dell'IA per rafforzare la propria resilienza senza rinunciare a valori fondamentali come responsabilità, equità e trasparenza; si intende analizzare l'impatto della progettazione organizzativa sulla resilienza aziendale in un contesto di continua trasformazione digitale, ponendo particolare attenzione al ruolo dell'IA. La ricerca esplorerà inizialmente i concetti di resilienza organizzativa e di progettazione strutturale e culturale, per poi approfondire come l'IA possa migliorare la capacità delle aziende di reagire, adattarsi e trasformarsi (Russell & Norvig, 2021).

Capitolo 1

Resilienza Organizzativa e Trasformazione Digitale

1.1 Concetto di resilienza aziendale

Quando si parla di resilienza organizzativa ci si riferisce alla forza di un'azienda nel fronteggiare eventi imprevisti. Non significa soltanto resistere all'urto di una crisi, ma anche adattarsi, riprendersi e continuare a operare in condizioni accettabili. In altre parole, è la capacità di trasformare un ostacolo in un momento di stabilità e, a volte, persino di crescita. (Duchek, 2020). Studi basati sulle dynamic capabilities sottolineano anche un aspetto proattivo e trasformativo, ovvero la capacità dell'impresa di reagire alle interruzioni evolvendosi e sfruttando opportunità emergenti (Garrido-Moreno, García-Morales & Martín-Rojas, 2024).

Ulteriori studi integrano ulteriormente il concetto includendo la previsione e preparazione a potenziali minacce future, sostenendo che la resilienza oscilla tra la capacità reattiva (superare un imprevisto) e quella anticipatoria (prevenire ed evitare effetti negativi) (Duchek, 2020). Definizioni più recenti sottolineano che le organizzazioni resilienti non solo riducano le perdite- ma possano anche prosperare e crescere grazie alle crisi- attraverso: l'apprendimento continuo, l'innovazione e la riorganizzazione delle risorse (Georgescu et al., 2024; Chen, Zhang & Xu, 2021).

La capacità di adattamento abbraccia la business continuity ovvero la continuità operativa durante e dopo un evento critico e la capacità di adattamento evolutivo a lungo termine (Corrales-Estrada, et al., 2025) inoltre si manifesta attraverso la capacità di resistere e riprendersi velocemente da una crisi e dalla facoltà di apprendere dall'esperienza e trasformarsi per affrontare con successo le sfide future (Lengnick-Hall, Beck & Lengnick-Hall, 2011).

L'IA può supportare entrambe queste dimensioni, fornendo strumenti sia per la reazione rapida agli imprevisti sia per individuare precocemente i trend emergenti (Benhamou, 2020). In letteratura si parla a questo proposito di capacità dinamiche: alcuni autori distinguono tra capacità di primo ordine, focalizzate sulla risposta e il recupero nel breve termine, e capacità di secondo ordine, che influenzano l'adattamento strategico di lungo periodo (Eisenhardt & Martin, 2017).

Quando facciamo riferimento alla resilienza organizzativa non parliamo solo di prevenzione ma anche di continuità operativa (Böhme et al., 2019; Ye, 2025).

Ricerche empiriche indicano che, sebbene numerosi dirigenti vedano la resilienza organizzativa come una priorità, meno della metà afferma di possedere una definizione chiara e condivisa di cosa la resilienza significhi concretamente nella loro organizzazione (Kraus et al., 2020). Nonostante sia una strategia, la resilienza è un concetto che le aziende faticano a mettere in pratica. Ad oggi, comunque, si è affermata come una proprietà che abbraccia processi, persone e tecnologia in modo olistico (Georgescu, Dospinescu & Dospinescu, 2024; Chen, Zhang & Xu, 2021).

Un'organizzazione resiliente è in grado di anticipare, assorbire e trasformarsi di fronte alle difficoltà. I vantaggi di una solida resilienza aziendale si evidenziano in diversi aspetti: dall'adattabilità strategica, che permette di trovare soluzioni in ogni situazione per garantire la continuità del business anche in periodi di crisi (Roberts et al., 2022), al miglioramento della governance, supportato da una cultura interna basata su fiducia, trasparenza e innovazione, che aiuta a gestire le sfide attuali e future senza compromettere i valori fondamentali dell'organizzazione (Lengnick-Hall et al., 2011). Altri vantaggi riscontrati includono un aumento della produttività (grazie a personale più motivato e fiducioso nell'azienda) e un miglioramento del benessere organizzativo generale, poiché la resilienza sposta l'attenzione dalla sola gestione del rischio a una visione più ampia di successo sostenibile e qualità della vita lavorativa.

1.2 Trasformazione digitale come fonte di opportunità e rischio

La trasformazione digitale – vista come l'adozione pervasiva di tecnologie digitali (cloud computing, big data, Internet of Things, Intelligenza Artificiale, ecc.) nei processi di business – ha modificato il contesto in cui operano le imprese, generando al contempo nuove opportunità e nuove sfide per la resilienza organizzativa (Bharadwaj et al., 2013; Vial, 2019). Da una parte, le tecnologie digitali offrono strumenti forti per fare crescere l'efficienza, l'agilità e la capacità decisionale: per fare un caso concreto, piattaforme di data analytics consentono di ottenere insight in tempo reale, i servizi cloud aumentano la scalabilità e disponibilità delle infrastrutture, le soluzioni di collaborazione digitale permettono al lavoro di proseguire anche da remoto durante eventi avversi (si pensi alla continuità operativa garantita dallo smart working durante la pandemia Covid-19) (Kraus et al., 2020). Tutto ciò può incrementare la resilienza operativa, diminuendo i tempi di reazione e aumentando la flessibilità con cui l'organizzazione fa fronte ai cambiamenti dell'ambiente.

Ma la digitalizzazione porta con sé anche diversi rischi. Ad esempio, l'affidamento crescente su sistemi informativi complessi e interconnessi espone le aziende a minacce cyber senza precedenti (data breach, attacchi ransomware, ecc.), a guasti sistemici del software e a interruzioni infrastrutturali (down di servizi cloud, blackout delle telecomunicazioni). Negli ultimi due decenni le strategie di resilienza si sono dovute adattare ad un mondo centrato sull'hardware a uno centrato sul software e sulle reti digitali (Bada & Nurse, 2019; Linkov et al., 2018).

Inizialmente si è tentato di applicare approcci tradizionali (es. ridondanza fisica) alle nuove tecnologie, ma in ambienti cloud ibridi ciò non basta. Serve un approccio completo che mappi tutte le potenziali minacce digitali e le gestisca con un "approccio a tutti i rischi" (Kure et al., 2018). Questa tendenza si riflette anche sul piano regolamentare: ad esempio, l'Unione Europea ha introdotto normative come il Digital Operational Resilience Act (DORA) per il settore finanziario e la direttiva NIS2 per le infrastrutture critiche, proprio per assicurare che le organizzazioni adottino misure di resilienza ICT adeguate nell'era digitale (Regulation (EU) 2022/2554; Directive (EU) 2022/2555).

La trasformazione digitale è un'arma a doppio taglio per la resilienza aziendale. Da un lato le aziende che sanno valorizzare il digitale possono accrescere la propria resilienza: ad esempio, l'automazione intelligente dei processi riduce la dipendenza da singoli individui e limita gli errori umani; la connettività e l'analisi dei dati permettono di identificare segnali deboli di crisi imminenti; le tecnologie cloud e le architetture distribuite eliminano i punti singoli di guasto grazie a ridondanze geografiche e sistemi di failover automatici (Weill & Woerner, 2018). Un esempio significativo è l'implementazione di piattaforme di business continuity management basate su cloud, che durante eventi come disastri naturali permettono di trasferire rapidamente le operazioni a siti secondari senza perdere dati o interrompere servizi critici (Alhawari et al., 2021).

D'altro canto, la digitalizzazione crea una maggiore dipendenza dell'azienda dal funzionamento corretto delle tecnologie. Problemi tecnici come errori software, attacchi informatici o interruzioni di corrente possono propagarsi su vasta scala, paralizzando un'organizzazione digitalizzata più facilmente rispetto a quanto accadeva in passato con sistemi manuali o analogici (Linkov et al., 2018).

Inoltre, il ritmo incalzante dell'innovazione digitale implica che le competenze possono diventare obsolete rapidamente e che emergano nuovi rischi ignoti. Basti pensare all'Intelligenza Artificiale: se da un lato è un potente abilitatore, dall'altro crea superfici d'attacco inedite e vettori di minaccia più sofisticati, richiedendo approcci di sicurezza e

resilienza del tutto nuovi (Brundage et al., 2018; Galaz et al., 2021). Ciò ci fa capire che per sfruttare appieno l'opportunità dell'IA occorre anche preoccuparsi di rendere robusti e sicuri gli stessi sistemi di IA, altrimenti si rischia di introdurre nella catena del valore un anello debole capace di compromettere l'intera resilienza organizzativa (Cummings, 2021).

La trasformazione digitale amplifica sia le capacità sia i rischi delle imprese. La resilienza nell'era digitale dipende dalla capacità di neutralizzare le rigidità e potenziare la flessibilità organizzativa (Teece et al., 2016), così da non restare intrappolati in schemi monolitici incapaci di adattarsi.

1.3 Ruolo della progettazione organizzativa e della cultura aziendale

La resilienza dipende anche da come l'organizzazione è progettata e da quale cultura aziendale caratterizza l'ambiente interno. Strutture organizzative flessibili, decentralizzate e con adeguati canali di comunicazione favoriscono risposte più rapide ed efficaci in caso di crisi rispetto a strutture gerarchiche rigide e silos funzionali isolati (Lengnick-Hall, Beck & Lengnick-Hall, 2011). Allo stesso modo, una cultura organizzativa che promuove l'innovazione, l'adattabilità e l'apprendimento costante rende i dipendenti più tempestivi a fronteggiare gli imprevisti al posto di una cultura non propensa al cambiamento o centrata sul timore dell'errore visto come ostacolo alle crisi (Denyer, 2017; Daft, 2004).

Nella progettazione organizzativa, uno dei principi chiave per incrementare la resilienza è incrementare la flessibilità ed evitare le rigidità. Ciò può voler dire, ad esempio, adottare un modello meno burocratico, con meno livelli gerarchici, in modo da accelerare il flusso decisionale nelle situazioni d'emergenza. Significa anche creare ridondanza funzionale: avere team cross-funzionali o dipendenti polivalenti capaci di coprire ruoli critici all'occorrenza, così che l'assenza o il sovraccarico di una singola unità non blocchi l'intera organizzazione (Vogus & Sutcliffe, 2007). Gli esperti sottolineano l'importanza di "neutralizzare le rigidità e potenziare la flessibilità organizzativa, per non restare intrappolati in schemi monolitici che non consentono di accogliere il cambiamento" (Teece, Peteraf & Leih, 2016). In pratica, le organizzazioni resilienti investono nella riprogettazione dei processi di lavoro, migliorando la comunicazione interna, abbattendo i silos, favorendo la cooperazione e il supporto reciproco tra reparti (Somers, 2009).

Parallelamente alla struttura, la cultura aziendale costituisce il "terreno" su cui attecchisce (o meno) la resilienza. Una cultura che valorizza la fiducia, la trasparenza e la capacità di innovare è alla base di una governance resiliente (Boin & van Eeten, 2013). Quando i dipendenti sentono di poter comunicare in modo libero problemi ed errori senza timore di

ripercussioni, l'azienda riesce a capire prima le criticità e in seguito correggerle, sviluppando una specie di "sistema immunitario" organizzativo (Carmeli & Markman, 2011). Inoltre, culture orientate all'empowerment dei collaboratori – dove le persone - a tutti i livelli- sono incoraggiate a prendere iniziative per risolvere i problemi, facilitano risposte rapide quando una crisi richiede decisioni immediate sul campo (Mallak, 1998). La resilienza si nutre anche dei comportamenti e atteggiamenti individuali: dipendenti resilienti (capaci di fronteggiare stress e apprendere dalle avversità) contribuiscono alla costruzione di un'organizzazione resiliente. Non a caso, in fase di selezione del personale molte aziende iniziano a considerare la resilienza una soft skill desiderabile, da coltivare e inserire tra i valori aziendali (Lengnick-Hall et al., 2011).

Uno studio significativo in materia di cultura della resilienza è quello del professor Ranjay Gulati (Harvard Business School), che ha individuato cinque leve culturali per promuovere la resilienza organizzativa:

1. Coordinazione tra le diverse parti dell'azienda, tramite scambio continuo di informazioni e collaborazione interfunzionale;
2. Cooperazione autentica tra management e dipendenti nel perseguire fini condivisi;
3. Condivisione di una direzione orientata al cliente (customer-centric, anziché company-centric), così che anche nelle crisi tutti mantengano il focus sugli obiettivi di valore per il cliente;
4. Competenza non solo tecnica ma anche nelle soft skill, con una mentalità di apprendimento continuo e apertura allo scambio di idee;
5. Connessione con l'esterno, ovvero lo sviluppo di una rete di relazioni con clienti, partner e altri stakeholder, in modo da poter gestire gli imprevisti in sinergia con l'ecosistema anziché in isolamento (Gulati, 2022).

Spetta infatti ai leader, con il proprio esempio, modellare i comportamenti desiderati, favorendo un ambiente che stimoli la flessibilità, l'adattabilità e il miglioramento continuo. (Sutcliffe, 2003).

Capitolo 2

L'Intelligenza Artificiale come leva strategica

2.1 Definizione e principali applicazioni dell'IA in ambito aziendale

Nonostante il crescente clamore mediatico attorno all'Intelligenza Artificiale (IA), il concetto di IA non è monolitico e merita di essere definito con precisione.

Per Intelligenza Artificiale si intende la capacità di un sistema informatico di svolgere compiti tipicamente associati all'intelligenza umana come: l'apprendimento da esempi, il ragionamento, la risoluzione di problemi, la comprensione del linguaggio naturale, la percezione visiva e così via (Russell & Norvig, 2021). La potremmo vedere come “la capacità di un sistema di interpretare correttamente dati esterni, apprendere da tali dati e utilizzare queste conoscenze per raggiungere obiettivi specifici tramite un adattamento flessibile” (Haenlein & Kaplan, 2019). Nel settore aziendale, l'IA assume in genere forme settoriali e mirate (Artificial Narrow Intelligence), ovvero algoritmi o sistemi progettati per migliorare compiti specifici – ad esempio, un modello di machine learning che prevede la domanda di mercato, un chatbot che risponde alle domande dei clienti, o un algoritmo di visione artificiale che ispeziona la qualità dei prodotti in fabbrica.

Le principali applicazioni dell'IA in ambito aziendale sono:

- Automazione intelligente dei processi: l'IA viene utilizzata per automatizzare attività ripetitive o complesse che dapprima richiedevano l'intervento umano. Ciò include sistemi di Robotic Process Automation (RPA) arricchiti con AI per gestire flussi di lavoro amministrativi, ma anche robotica avanzata nelle linee produttive e magazzini. Un esempio è l'uso di robot dotati di algoritmi AI nei magazzini Amazon, i quali movimentano e smistano prodotti ottimizzando percorsi e tempi di prelievo senza intervento umano (Wurman, D'Andrea & Mountz, 2008).
- Analisi dei dati e predictive analytics: Algoritmi di IA sono impiegati per previsioni (ad es. previsione delle vendite, della domanda o di trend di mercato), per sistemi di raccomandazione (ad es. suggerire prodotti a clienti online in base ai loro comportamenti) e per individuare pattern nascosti nei dati che possano indicare rischi o opportunità. Aiuta le aziende ad anticipare gli eventi invece di reagire a posteriori. Tra le applicazioni più comuni vi è: l'analisi testuale (es. analisi di sentiment su social media, estrazione di informazioni da documenti), i sistemi di raccomandazione e i

sistemi di ottimizzazione (Chui, Manyika & Miremadi, 2018; Davenport & Ronanki, 2018).

- Sistemi conversazionali e customer service: grazie ai progressi nel Natural Language Processing (NLP), molte imprese hanno adottato chatbot e assistenti virtuali basati su IA per gestire le interazioni con i clienti 24\7 garantendo supporto costante (Huang & Rust, 2021). Questi sistemi sono in grado di comprendere domande in linguaggio naturale e fornire risposte o eseguire azioni (prenotazioni, risoluzione problemi comuni).
- Supporto alle decisioni e sistemi adattivi: l'IA viene anche integrata nei processi decisionali per fornire raccomandazioni ai manager o addirittura decisioni automatizzate in tempo reale. Ad esempio, algoritmi di trading algoritmico nel settore finanziario prendono decisioni di acquisto/vendita in frazioni di secondo seguendo strategie apprese da dati storici. L'adozione di sistemi AI adattivi può rendere l'azienda più veloce: ad esempio Netflix ha sviluppato un motore AI chiamato Stryer che regola dinamicamente la capacità dei server in base al traffico previsto, allocando risorse prima che avvengano picchi e garantendo così continuità del servizio durante improvvisi aumenti di domanda (Alipour, 2019).
- Gestione del rischio e sicurezza: l'uso di IA per identificare e gestire rischi sia operativi sia strategici. Questo include algoritmi di fraud detection nel settore finanziario, che scansano transazioni in tempo reale segnalando quelle anomale, oppure sistemi di cybersecurity basati su AI in grado di rilevare intrusioni o malware mai visti prima tramite anomaly detection (Buczak & Guven, 2016). Nel risk management aziendale complessivo, l'IA viene usata per modellare scenari di stress test, valutare probabilità di default clienti, ottimizzare portafogli di rischio, ecc. Studi recenti confermano che una quota crescente di istituzioni finanziarie assegna priorità agli investimenti in IA per la conformità normativa e la gestione del rischio (Naim, 2022).

Queste categorie delineano come l'IA accontenti praticamente ogni funzione aziendale: produzione (manutenzione predittiva degli impianti), logistica (ottimizzazione percorsi, gestione scorte), marketing (segmentazione clienti automatizzata, campagne pubblicitarie ottimizzate in tempo reale), finanza (previsione flussi di cassa, rilevazione anomalie contabili), risorse umane (screening di CV con algoritmi, analisi del sentiment interno), e così via. Si parla sempre più di azienda AI-driven per indicare un'organizzazione in cui i dati e

l'intelligenza artificiale guidano i processi decisionali ad ogni livello.

Come osservano alcuni studiosi, “l'IA non è un fattore produttivo come gli altri: le sue abilità di percepire, comprendere, decidere, agire e imparare vanno oltre ciò che tradizionalmente consideriamo possibile”, almeno in domini ristretti (Brynjolfsson & McAfee, 2017). Questa potenza trasformativa dell'IA spiega perché oggi sia considerata una leva strategica di prim'ordine per le aziende che vogliono rafforzare la propria innovazione e resilienza.

2.2 Automazione dei processi decisionali e adattabilità organizzativa

Uno dei contributi più tangibili che l'IA offre alle imprese è la capacità di automatizzare decisioni e processi che in precedenza richiedevano tempo e intervento umano, aumentando così la velocità e l'adattabilità dell'organizzazione. Quindi significa che alcune scelte operative possono essere prese da algoritmi in tempo reale, sulla base di regole apprese dai dati, spesso più rapidamente e accuratamente di quanto farebbe un umano. Ciò ha implicazioni dirette sulla resilienza: decisioni più veloci e consistenti permettono all'azienda di far fronte quasi immediatamente a mutamenti nelle condizioni operative, riducendo i ritardi (Davenport & Ronanki, 2018; Brynjolfsson & McAfee, 2017).

Nel dynamic routing a proposito della logistica possiamo notare i suoi effetti: in una rete di consegne, un sistema AI può ricalcolare continuamente i percorsi dei corrieri in base al traffico, alle urgenze delle consegne e ad altri vincoli, adattandosi al volo a incidenti stradali o a richieste sopraggiunte. Amazon, ad esempio, ha implementato algoritmi di ottimizzazione logistica che riorganizzano dinamicamente il piano di consegne giornaliero; questo ha contribuito a ridurre i tempi medi di spedizione, specialmente dopo il 2020, quando innovazioni AI nel routing e nella gestione dei magazzini hanno accelerato la delivery (Wurman, D'Andrea & Mountz, 2008). Un beneficio analogo si riscontra nell'automazione della gestione dell'inventario: Amazon impiega robotica e machine learning nei propri fulfillment center per gestire lo stoccaggio e il prelievo merci con minima supervisione umana, riducendo drasticamente i tempi di evasione ordini e gli errori di picking. Quindi, l'automazione intelligente rende i processi più veloci e affidabili, qualità che rafforzano la resilienza operativa.

Nell'automazione via IA è anche la maggiore coerenza metodologica e la riduzione della soggettività rispetto alle decisioni umane poiché i sistemi di IA possono garantire valutazioni standardizzate e ripetibili su diversi set di dati, diminuendo l'errore umano e l'inconsistenza legata a valutazioni manuali (Makridakis, 2017). Nella valutazione dei rischi creditizi, un

modello di machine learning applica gli stessi criteri a tutti i clienti eliminando possibili bias inconsci di un analista; questo porta a decisioni più uniformi e scalabili, un vantaggio in termini di equità e conformità normativa oltre che di efficienza. Tuttavia, ciò introduce anche il problema dei bias algoritmici insiti nei dati, quindi la coerenza dell'IA va monitorata attentamente (Barocas, Hardt & Narayanan, 2019).

Sul fronte della adattabilità organizzativa, l'automazione AI ha un ruolo chiave nel fornire all'azienda capacità di risposta quasi "in tempo reale" e nell'abilitare modelli operativi adattivi.

L'IA contribuisce all'adattabilità nel lungo periodo fornendo alle organizzazioni strumenti per imparare e riconfigurarsi velocemente. Un'azienda che registra in maniera automatizzata dati dettagliati su ogni operazione (grazie a sistemi AI che monitorano e analizzano continuamente i processi) avrà una base informativa ricca per capire cosa è andato storto durante una crisi e come migliorare. Inoltre, alcune applicazioni di IA rientrano nel cosiddetto continuous improvement: per esempio, algoritmi di apprendimento per rinforzo possono sperimentare continuamente piccole modifiche a un processo, identificando gradualmente le soluzioni ottimali (Silver et al., 2017).

Ma ci sono anche dei limiti e delle sfide nell'automazione decisionale via IA perché per quanto efficienti, possono commettere errori diversi da quelli umani; automatizzare e velocizzare un processo senza una corretta governance può significare "accelerare nella direzione sbagliata" se l'algoritmo non è allineato agli obiettivi strategici. I sistemi di IA hanno anch'essi bias e punti deboli, che vanno gestiti attentamente (Barocas et al., 2019). Un esempio limite è il caso di Flash Crash borsistici innescati da trading algoritmico automatizzato: la mancanza di supervisione umana immediata ha portato algoritmi a entrare in loop auto-distruttivi amplificando la volatilità (Johnson et al., 2013). Pertanto, le aziende devono implementare l'automazione in modo responsabile: stabilire confini e criteri per l'intervento umano (human-in-the-loop), fare test rigorosi (es. simulazioni di crisi) e predisporre "freni d'emergenza" in caso i processi automatizzati escano dai parametri attesi. L'automazione dei processi decisionali tramite IA è una potente leva per aumentare l'agilità e la resilienza operativa di un'organizzazione: se implementata con criterio, consente di reagire più rapidamente e con azioni più mirate agli eventi avversi, nonché di adattare progressivamente l'azienda ai mutamenti di contesto. Tuttavia, richiede solidi framework di governance, audit regolari e policy interne adeguate (Floridi & Cowls, 2021), oltre a investimenti nelle competenze del personale per gestire e convivere con queste tecnologie. In organizzazioni che riescono in questo bilanciamento, l'IA e le pratiche di business continuity

finiscono per integrarsi come pilastri interconnessi a sostegno della resilienza complessiva, piuttosto che come ambiti separati.

2.3 Analisi predittiva e anticipazione delle crisi di mercato

Rilevante è nel campo dell'Intelligenza Artificiale che si mostra particolarmente utile per la resilienza aziendale è l'analisi predittiva. Grazie ad algoritmi di machine learning, le imprese possono identificare schemi ricorrenti nei dati e utilizzarli per anticipare eventi futuri, anziché limitarsi a reagire a posteriori.

L'analisi predittiva consente alle organizzazioni di “giocare d'anticipo” rispetto a una vasta gamma di rischi e opportunità, non si tratta di eliminare l'incertezza, ma di ridurla al minimo, fornendo ai manager informazioni tempestive e affidabili per prendere decisioni più consapevoli e rafforzare così la resilienza complessiva (Shmueli & Koppius, 2011; Lee et al., 2015).

Un'applicazione classica è la manutenzione predittiva: sensori IoT installati su macchinari e linee produttive raccolgono dati in tempo reale (temperature, vibrazioni, consumi), che vengono analizzati da algoritmi AI capaci di segnalare in anticipo l'insorgere di anomalie. Ciò permette di sostituire un componente prima che causi un guasto, evitando interruzioni della produzione e costi maggiori di riparazione (Lee et al., 2015). Oltre alla produzione, la manutenzione predittiva trova ampio impiego nei trasporti, nelle utility e in altri settori infrastrutturali.

Vale la pena considerare anche la previsione della domanda: catene di distribuzione e aziende di e-commerce utilizzano sistemi di predictive analytics per stimare i volumi futuri delle vendite sulla base di dati storici, stagionalità e variabili esterne come meteo o eventi sociali. Questo ci dà la possibilità di pianificare meglio gli approvvigionamenti, diminuendo sprechi e stock-out (Bose, 2009).

L'analisi predittiva è centrale nel risk management: algoritmi di AI consentono di costruire modelli di early warning in grado di segnalare situazioni di rischio emergenti. In questo senso, l'analisi predittiva potenzia le capacità di resilienza delle imprese, perché permette di anticipare crisi e ridurre la loro intensità di impatto.

Come ultimo aspetto l'analisi predittiva trova crescente applicazione nella cybersecurity. Sistemi basati su anomaly detection e deep learning possono individuare pattern sospetti nel traffico di rete prima che si concretizzi un attacco informatico, dando tempo

all'organizzazione di predisporre difese efficaci (Buczak & Guven, 2016). La combinazione di grandi volumi di dati, capacità computazionale e algoritmi avanzati rende oggi possibile un approccio predittivo alla sicurezza, che sposta il baricentro dalla mera reazione all'attacco alla sua prevenzione.

2.4 IA e gestione del rischio operativo e strategico

L'IA viene impiegata per monitorare in tempo reale variabili critiche, analizzare enormi volumi di dati e individuare anomalie che potrebbero indicare la presenza di minacce o vulnerabilità. A differenza degli approcci tradizionali, che si basano su analisi retrospettive e modelli statici, i sistemi AI sono in grado di aggiornare dinamicamente le proprie valutazioni sulla base di flussi di dati, adattandosi a scenari in continuo cambiamento (Naim, 2022).

Nel settore finanziario, l'IA è ormai diffusa nei sistemi di fraud detection, che analizzano milioni di transazioni e ne segnalano in tempo reale di sospette, riducendo drasticamente i tempi di reazione rispetto a controlli manuali (Ngai et al., 2011). Oltre alle frodi, l'IA viene utilizzata per il credit risk management, con modelli predittivi che stimano la probabilità di insolvenza di clienti e fornitori, permettendo alle banche e alle imprese di ridurre le esposizioni e migliorare la stabilità complessiva (Lessmann et al., 2015).

In ambito cybersecurity, gli algoritmi di machine learning sono utilizzati per individuare minacce informatiche sconosciute (zero-day attacks) tramite tecniche di anomaly detection.

L'IA consente di rilevare comportamenti sospetti che non corrispondono a pattern noti, anticipando così potenziali attacchi prima che provochino danni (Buczak & Guven, 2016).

La gestione del rischio tramite AI non si limita al breve termine, ma può supportare anche strategie di risk forecasting ad esempio, sistemi basati su deep learning possono simulare scenari complessi – come shock macroeconomici o disastri naturali – e stimare le conseguenze sull'organizzazione, aiutando i manager a predisporre piani di emergenza più accurati (Makridakis, 2017).

Importante è l'integrazione dell'IA nei processi di enterprise risk management (ERM). Alcuni studi evidenziano come l'IA permetta non solo di ridurre i rischi esistenti, ma anche di identificare nuove opportunità, trasformando il risk management in una leva strategica per l'innovazione e la resilienza.

L'Intelligenza Artificiale rende la gestione del rischio più proattiva, tempestiva e adattiva. Le imprese che investono in queste tecnologie non solo reagiscono più velocemente alle

minacce, ma sviluppano anche la capacità di anticipare scenari futuri e costruire una resilienza strutturale più solida. Tuttavia, ciò richiede una governance attenta: algoritmi non trasparenti o mal gestiti possono introdurre nuovi rischi, come bias nei modelli o vulnerabilità sistemiche. È quindi fondamentale accompagnare l'adozione dell'IA con pratiche di audit, supervisione e allineamento agli obiettivi strategici (Floridi & Cowls, 2021).

Capitolo 3

Casi Studio: Le Big Tech

Per concretizzare i concetti fin qui discussi, analizziamo ora come tre grandi aziende tecnologiche – **Amazon, IBM e Google** – hanno integrato l’Intelligenza Artificiale nei loro modelli operativi e strategici al fine di potenziare la propria resilienza. Queste “Big Tech” sono casi emblematici poiché, disponendo di risorse e dati notevoli, sono spesso all’avanguardia nell’utilizzo dell’IA.

Ognuna opera in ambiti differenti (e-commerce/logistica, servizi tecnologici e consulenza, servizi digitali e pubblicità) e offre quindi prospettive complementari su come l’IA possa rafforzare la resilienza nei vari contesti. Si esamineranno per ciascuna gli utilizzi principali dell’IA correlati alla resilienza operativa e strategica, evidenziando i punti di forza e traendo indicazioni generali.

3.1 Amazon – IA per supply chain, logistica e resilienza operativa

Amazon, colosso mondiale dell’e-commerce e del cloud, è oggi considerata un modello di riferimento per aver costruito una delle supply chain più resilienti al mondo. Alla base di questo successo c’è l’uso esteso e sistematico dell’Intelligenza Artificiale e dell’automazione, che permeano logistica, gestione dell’inventario e distribuzione.

Uno degli obiettivi di Amazon è quello di garantire consegne sempre più affidabili e rapidi ai clienti di tutto il mondo, riducendo al minimo costi in un contesto caratterizzato da una complessità operativa straordinaria – centinaia di magazzini, milioni di prodotti e una domanda in continua evoluzione (D’Andrea, Wurman & Mountz, 2012).

Tra gli obiettivi di Amazon:

1. Investire nei dati è cruciale, perché senza dati accurati non c’è resilienza predittiva (Agrawal et al., 2018);
2. Automatizzare dove possibile i compiti ripetitivi, permettendo alle persone di concentrarsi su innovazione e gestione delle eccezioni;
3. Dare priorità alla flessibilità è fondamentale per sopravvivere in un mondo imprevedibile (Ivanov & Dolgui, 2020);

4. Adottare una visione di lungo termine, come ha fatto Amazon, investendo per anni in robotica e algoritmi prima che se ne vedessero i risultati, è ciò che distingue le aziende capaci di assorbire le crisi da quelle che le subiscono (Sheffi, 2021).

Uno dei pilastri di questo modello è l'AI-powered Demand Forecasting, ovvero la previsione della domanda basata su algoritmi di machine learning. Amazon riesce a combinare in tempo reale una quantità impressionante di dati – cronologia ordini, ricerche online, trend social, dati macroeconomici e persino previsioni meteo – per anticipare con grande precisione le variazioni della domanda in ogni singola area geografica (Agrawal, Gans & Goldfarb, 2018; Chui, Manyika & Miremadi, 2018).

Questo tipo di previsione granulare non solo evita rotture di stock nei momenti più critici, ma rappresenta un chiaro esempio di resilienza proattiva: adattare scorte e rete logistica anticipando l'impatto degli eventi esterni, invece di subirlo.

Ad esempio, se i modelli climatici indicano l'arrivo di una tempesta, i sistemi AI possono prevedere un aumento improvviso della richiesta di generatori elettrici o scorte alimentari e suggerire di reindirizzare questi articoli verso i centri logistici più vicini alla zona interessata. Un altro tassello importante è l'Automated Inventory Management nei magazzini. Amazon ha automatizzato gran parte delle operazioni di stoccaggio, prelievo e imballaggio grazie a una combinazione di robotica avanzata (come i robot Kiva, oggi Amazon Robotics) e algoritmi di ottimizzazione. I robot mobili trasportano scaffali interi fino alle postazioni degli operatori, oppure gestiscono direttamente il movimento delle merci. Sistemi di visione artificiale e di Robotic Process Automation (RPA) organizzano gli spazi di stoccaggio per ridurre tempi e sprechi, mentre modelli di machine learning aggiornano costantemente soglie di riordino e distribuzione delle scorte. Il risultato è duplice: da un lato si riducono gli errori di picking, dall'altro si aumenta la velocità di evasione degli ordini, riuscendo a gestire senza intoppi anche picchi importanti come quelli del Prime Day o del Black Friday (Sheffi, 2021).

L'IA gioca un ruolo centrale anche nell'ottimizzazione logistica. Gli algoritmi di routing calcolano i percorsi dei corrieri considerando condizioni di traffico, finestre di consegna preferite dai clienti e sequenze di consegna più efficienti apprese dai dati storici. In prospettiva, Amazon sta sperimentando anche il reinforcement learning, così che i sistemi possano “imparare” continuamente i pattern migliori per l'allocazione dei pacchi e i tempi ottimali di partenza. L'impatto di queste innovazioni è evidente: dal 2019 al 2023 i tempi medi di consegna si sono progressivamente ridotti, con un'accelerazione particolare dopo il 2020, segno dell'efficacia delle ottimizzazioni basate sull'IA (Sheffi, 2021).

La prova più dura per la resilienza di Amazon è stata la pandemia da Covid-19. Durante i lockdown, la domanda di beni essenziali online esplose, mentre le restrizioni sanitarie limitavano le operazioni. Nonostante ciò, Amazon riuscì a mantenere un livello di servizio elevato grazie alla flessibilità offerta dai sistemi AI. L'azienda fu in grado di ricollocare inventario e risorse logistiche in tempi rapidissimi, spostare spedizioni dai magazzini congestionati a quelli meno colpiti e focalizzare le risorse sui prodotti essenziali (Ivanov & Dolgui, 2020). Mentre molti concorrenti faticavano a tenere il passo, Amazon consolidò la propria posizione, dimostrando che la resilienza non è solo capacità di resistere, ma anche di trarre vantaggio dai cambiamenti.

Gli effetti di questa trasformazione AI-driven si riflettono chiaramente negli indicatori di performance. Amazon ha ridotto i costi di inventario ottimizzando i livelli di stock, ha migliorato la velocità di consegna – con conseguente aumento della soddisfazione dei clienti – e ha reso le proprie operazioni più sostenibili, grazie alla riduzione degli sprechi e a un uso più efficiente delle risorse) (Sheffi, 2021).

3.2 IBM – Watson e l'IA applicata alla gestione dei rischi e al decision-making

IBM (International Business Machines) è una delle aziende tecnologiche più longeve al mondo, con oltre un secolo di storia. Negli ultimi anni IBM ha attraversato una profonda trasformazione strategica, spostando il focus dai prodotti hardware tradizionali verso servizi ad alto valore aggiunto come il cloud, la consulenza e soprattutto le soluzioni di Intelligenza Artificiale per le imprese. (Sheffi, 2021; Agrawal, Gans & Goldfarb, 2018). In questo cammino, l'IA – incarnata nella piattaforma IBM Watson e nelle sue evoluzioni recenti – ha giocato un duplice ruolo: da un lato come offerta che IBM propone ai clienti per aiutarli a essere più resilienti, dall'altro come strumento interno per migliorare i propri processi decisionali e la propria resilienza organizzativa, mantenendo IBM stessa competitiva in un settore in rapido cambiamento. (Ferrucci et al., 2013; Kalyanpur et al., 2012; Agrawal et al., 2018).

Il prodotto di punta è stato per anni IBM Watson, un sistema di intelligenza artificiale inizialmente noto per aver vinto il quiz televisivo “Jeopardy!” nel 2011, poi sviluppatosi in una serie di servizi AI aziendali (comprendenti machine learning, knowledge management). (Ferrucci et al., 2013; Kalyanpur et al., 2012). IBM ha applicato Watson in molteplici campi, ma uno dei più rilevanti ai fini della resilienza aziendale è la gestione dei rischi finanziari e operativi. Ad esempio, Watson viene utilizzato da banche e istituzioni finanziarie per potenziare le analisi di rischio di credito, di mercato e di conformità normativa. Un caso

spesso citato è l'uso di Watson da parte di un grande istituto per l'analisi del rischio di controparte: alimentando Watson con milioni di documenti (bilanci, notizie di mercato, storici di prezzo) e addestrandolo a individuare segnali di deterioramento finanziario, la banca è riuscita ad anticipare situazioni di default o crisi di partner con maggiore anticipo rispetto ai metodi tradizionali (Lessmann et al., 2015; Ngai et al., 2011). Secondo dati riportati, gli algoritmi di Watson hanno migliorato l'accuratezza dei modelli di rischio fino al 30%, riducendo il margine d'errore nelle stime e quindi migliorando le decisioni di investimento e allocazione del capitale. (Lessmann et al., 2015; Ngai et al., 2011). Questo è cruciale perché un errore di valutazione in ambito rischi può portare a perdite ingenti (pensiamo a portafogli di prestiti mal calibrati che generano insoluti in serie). Dunque, dotando le istituzioni finanziarie di "occhiali intelligenti", IBM Watson contribuisce a una maggiore robustezza finanziaria del sistema, limitando l'esposizione a shock imprevisti.

IBM stessa, essendo un attore globale, utilizza internamente strumenti di analytics e AI per il risk management. Un esempio è l'implementazione di IBM OpenPages with Watson, un software GRC (Governance, Risk & Compliance) che integra funzioni AI per aiutare le aziende (inclusa IBM) a gestire i vari domini di rischio (operativo, strategico, terze parti, IT, compliance) in modo unificato. OpenPages con Watson sfrutta il NLP per analizzare normative e documenti, e machine learning per segnalare aree di possibile non-conformità o rischio emergente. Arena, Arnaboldi & Azzone, 2010; Floridi & Cowls, 2021).

Un altro settore in cui IBM ha applicato l'IA al proprio interno è la gestione delle operazioni IT, con l'introduzione di IBM Watson AIOps. Le operazioni IT (monitoraggio infrastrutture, ticketing, risoluzione incidenti) sono critiche per la continuità operativa di un'azienda come IBM (che gestisce data center, servizi cloud per clienti, ecc.). Watson AIOps utilizza algoritmi per analizzare log, metriche e allarmi, individuando automaticamente correlazioni tra eventi e possibili cause radice di un problema, spesso prima che quest'ultimo impatti il servizio. (Dang et al., 2019; Lin et al., 2022). Ad esempio, analizzando pattern di log, il sistema può capire che un certo warning su un server seguito da un certo comportamento del database prelude a un blocco del servizio, e allertare i tecnici con un insight preciso (es. "possibile memory leak in applicazione X su server Y"). Ciò permette di prevenire molti outage o comunque di risolverli più velocemente. Per IBM, offrire ai propri clienti servizi con uptime altissimo è fondamentale per la reputazione, quindi Watson AIOps migliora la resilienza infrastrutturale dei servizi IBM e al contempo funge da vetrina commerciale (IBM può dimostrare coi fatti l'efficacia delle sue soluzioni AI-driven per la resilienza IT) (Lin et al., 2022).

IBM ha anche sfruttato l'IA per il decision-making strategico e il supporto ai propri manager. Un esempio notevole è l'iniziativa interna chiamata IBM Corporate Service Corps, in cui IBM inviava team multidisciplinari in paesi emergenti per risolvere problemi di business/sociali complessi, e faceva uso di strumenti di AI per mappare competenze e progetti adatti alle persone. Inoltre, IBM ha sviluppato assistenti virtuali interni per i propri dipendenti (ad esempio "AskHR" per le risorse umane) basati su Watson, che rispondono a domande e forniscono policy in modo istantaneo. Questo tipo di adozione migliora l'efficienza interna e libera tempo ai dipendenti per concentrarsi su attività di maggior valore (es: i professionisti HR dedicano meno tempo a rispondere a FAQ amministrative e più a iniziative strategiche per le persone). (Davenport & Ronanki, 2018; Huang & Rust, 2021). Un'organizzazione che scorre meglio internamente è più resiliente perché riduce attriti e colli di bottiglia operativi che in situazioni di crisi possono aggravare i problemi.

In ambito decisionale, IBM è nota anche per aver elaborato un quadro etico per l'IA e una pratica di "augmented intelligence": riconosce che l'AI deve aumentare le capacità umane, non sostituirle. (Floridi & Cowls, 2021). Ad esempio, nel caso di sistemi di raccomandazione per i manager, IBM adotta il principio per cui "le raccomandazioni dell'IA danno elementi ai manager, ma la decisione e la responsabilità restano umane". Ciò riflette una scelta strategica che a sua volta influenza la resilienza reputazionale e operativa: mantenendo l'uomo nel circuito decisionale, IBM evita rischi di over-reliance sulla macchina e può rispondere meglio di fronte a errori algoritmici (c'è sempre un livello di controllo umano). Questa filosofia è diventata in un certo senso un selling point di IBM rispetto ad altre Big Tech: la narrativa di IBM insiste sul concetto di "Trusted AI", l'IA affidabile e spiegabile per il business, un approccio prudente ma che riduce i rischi di rigetto o scandali e rende l'integrazione dell'IA più sostenibile nel lungo periodo. (Floridi & Cowls, 2021).

Un settore dove IBM ha incontrato difficoltà, da menzionare come lezione, è l'applicazione di Watson in domini altamente complessi come la sanità. Il celebre caso di Watson for Oncology (un progetto per supportare i medici nell'individuare terapie per il cancro) non ha raggiunto i risultati sperati ed è stato in parte dismesso. (Su performance e limiti: studi di concordanza e valutazioni cliniche, es. Somashekhar et al., 2018; Kim et al., 2019). Le ragioni sono varie (dati medici scarsi e sporchi, difficoltà di integrazione nei flussi ospedalieri, eccessive aspettative di marketing), ma l'insegnamento sul piano della resilienza è che l'IA non è una bacchetta magica: va implementata dove c'è contesto adatto e insieme a competenze specialistiche. L'International Business Machines ha imparato la lezione e ha rifocalizzato Watson su aree più remunerative e con dataset meglio strutturati (es. finanza, supply chain,

customer service). Questo adattamento strategico è esso stesso un atto di resilienza aziendale: riconoscere un progetto fallimentare, trarne insegnamento e ridirezionare risorse altrove. (Per il principio generale su adozione selettiva e contesto: Makridakis, 2017; Rajkomar, Dean & Kohane, 2019).

In termini di benefici misurati, IBM riferisce (anche in collaborazione con terze parti) vari successi quantitativi legati alle sue soluzioni AI per il rischio e le decisioni: ad esempio, una riduzione del 25% del tempo impiegato dagli analisti di rischio nelle attività di reporting grazie all'automazione Watson; oppure un miglioramento di alcune metriche di compliance (es. tempo di aggiornamento alle nuove normative) del 50% con strumenti AI. Dal lato clienti, banche come JPMorgan hanno usato l'AI (non solo di IBM) per fare stress test più completi, riportando un miglioramento del 20% dei loro indici di adeguatezza patrimoniale dopo aver integrato queste pratiche (Lessmann et al., 2015). Tutto ciò indica che l'AI può rendere più robusti sia i singoli processi sia la posizione generale di un'azienda di fronte ai requisiti di solidità.

L'International Business Machines offre un case study di una grande azienda matura che utilizza l'IA sia come strumento interno di trasformazione e resilienza (adeguando le proprie operazioni, dal risk management all'IT, per essere più efficiente e preparata ai rischi), sia come proposta di valore verso i clienti, aiutando altre aziende a diventare più resilienti (fornendo soluzioni AI per risk management, automazione, etc.) (Sheffi, 2021; Davenport & Ronanki, 2018).

Uno dei punti cardine dell'IBM è ha puntato sulla fiducia e sull'eticità dell'IA come elemento distintivo, cercando di mitigare i rischi intrinseci (bias, black box) e di diventare un partner affidabile nella trasformazione digitale dei suoi clienti. Questo approccio, insieme alla capacità di pilotare il proprio modello di business attorno a nuovi pilastri tecnologici, ha permesso a IBM di resistere e adattarsi nel tempo, rimanendo rilevante nonostante le rivoluzioni informatiche succedutesi (dal mainframe, al PC, a Internet, all'AI).

3.3 Google - Data analytics, IA e adattabilità dei modelli di business

Google (oggi parte di Alphabet Inc.) è un esempio paradigmatico di Big Tech che ha fatto dell'Intelligenza Artificiale un elemento centrale della propria strategia e della propria resilienza nel tempo. Nata come motore di ricerca alla fine degli anni '90, Google ha saputo evolvere e diversificare ampiamente il proprio modello di business negli ultimi due decenni,

passando dalla pubblicità online al cloud computing, dai sistemi operativi mobili alla ricerca avanzata in AI (Google Brain, DeepMind) e fino a “scommesse” futuristiche come Waymo e Verily. Questa straordinaria adattabilità strategica poggia sull’uso intensivo di dati e algoritmi per guidare le decisioni e sulla scelta di un approccio “AI-first”, dichiarato dal CEO Sundar Pichai nel 2017, che ha reso l’IA un motore di innovazione interna e resilienza competitiva (Pichai, 2017; Brin & Page, 1998).

Fin dal core business (il motore di ricerca), Google ha costruito il proprio vantaggio competitivo su algoritmi intelligenti, a partire da PageRank (Brin & Page, 1998), fino all’uso di modelli di machine learning avanzati come RankBrain e BERT per comprendere meglio il linguaggio naturale (Devlin et al., 2019). Questi progressi hanno protetto la rilevanza di Google Search di fronte all’evoluzione delle abitudini di ricerca, come il crescente uso del linguaggio colloquiale o delle query vocali. Anche altri prodotti consumer come Gmail hanno beneficiato di modelli di deep learning: Smart Compose, ad esempio, assiste milioni di utenti nella scrittura quotidiana con suggerimenti predittivi in tempo reale (Chen et al., 2019).

Uno dei settori dove Google applica massicciamente l’IA è l’advertising e la personalizzazione, l’algoritmo di ad selection valuta in millisecondi la probabilità di clic e conversione di miliardi di combinazioni utente-annuncio, adattando dinamicamente i budget pubblicitari. Un modello rappresentativo di questo approccio è il Wide & Deep Learning, sviluppato per i sistemi di raccomandazione di Google Play, che combina la capacità di memorizzare pattern frequenti con quella di generalizzare verso nuovi comportamenti (Cheng et al., 2016), l’uso di tali algoritmi ha garantito resilienza finanziaria anche durante la pandemia: quando Google Ads ha ricalibrato rapidamente spesa e target, proteggendo i ricavi nonostante la crisi (Hao et al., 2018).

Sul fronte dei prodotti, Google ha utilizzato l’IA per migliorare costantemente l’esperienza utente: Google Translate, grazie al sistema GNMT, ha ridotto drasticamente gli errori di traduzione (Wu et al., 2016); Google Maps impiega modelli predittivi per stimare traffico e tempi di percorrenza (Neubig, 2017); Gmail usa AI per filtrare automaticamente le e-mail importanti. Queste innovazioni hanno reso Google sempre più indispensabile per gli utenti, aumentando la sua resilienza a eventuali cambiamenti competitivi.

Un aspetto chiave della resilienza operativa è l’uso dell’IA per ottimizzare i data center: l’azienda gestisce strutture colossali in tutto il mondo e ha adottato sistemi di reinforcement learning sviluppati con DeepMind per regolare dinamicamente il raffreddamento. I primi risultati hanno mostrato risparmi energetici fino al 30% (DeepMind, 2016), mentre studi successivi hanno confermato riduzioni tra il 9% e il 13% in scenari industriali reali (Luo et al.,

2022). Questi progressi riducono i costi e aumentano l'affidabilità dei data center, diminuendo i rischi di downtime.

Google investe in IA anche per l'innovazione interna e la cultura organizzativa. I dipendenti hanno accesso a strumenti di ricerca intelligente basati su NLP per reperire informazioni in repository aziendali e possono sviluppare rapidamente nuovi progetti grazie a framework open source come TensorFlow (Abadi et al., 2016). Questo ha permesso all'azienda di reagire tempestivamente a sfide emergenti, come l'arrivo dei modelli generativi nel 2022: l'ampia base di ricerca e il know-how accumulato hanno consentito a Google di lanciare rapidamente soluzioni alternative come Bard, mostrando resilienza strategica nel riconfigurare risorse e priorità (Bommasani et al., 2021).

La forza organizzativa di Google è rafforzata anche dalla struttura di Alphabet. La holding consente di diversificare attraverso le "Other Bets", molte delle quali ruotano attorno all'AI (Waymo per la guida autonoma, Verily per la salute digitale, Wing per i droni logistici). Questa diversificazione rappresenta una forma di resilienza imprenditoriale: esplorare settori emergenti riduce la dipendenza da un'unica fonte di ricavi e mitiga i rischi legati a regolamentazioni sulla privacy o sull'advertising (Brynjolfsson & McAfee, 2017).

Google mostra livelli eccezionali di continuità di servizio: i downtime globali sono rarissimi, e l'efficienza operativa AI-driven ha consentito di mantenere margini elevati e continui investimenti in R&D (oltre 30 miliardi l'anno dal 2020 in poi). L'ottimizzazione interna e i modelli data-driven hanno migliorato la sostenibilità delle operazioni, riducendo sprechi e consumi energetici (Sheffi, 2021).

Oltre ai risparmi energetici nei data center, Google mostra continuità di servizio elevata e un profilo finanziario in grado di assorbire shock, grazie a efficienza AI-driven e ottimizzazione dei costi; sul piano prodotto, studi e paper pubblici indicano miglioramenti sostanziali nelle performance dei sistemi (es. GNMT con drastica riduzione degli errori rispetto ai sistemi precedenti; Smart Compose operativo su larga scala).

Google illustra come l'IA possa fungere da nervo vitale organizzativo: abilita l'adattamento continuo del modello di business e la gestione affidabile di operazioni globali. La combinazione di cultura aperta al cambiamento, dati su scala e competenza tecnica colloca Google in buona posizione per rispondere a crisi operative e sfide strategiche.

3.4 Confronto comparativo tra le tre aziende

I casi di Amazon, IBM e Google mostrano prospettive diverse sull'applicazione dell'IA alla resilienza aziendale, riflettendo le differenti nature di queste imprese, ma anche alcuni temi comuni.

Somiglianze e temi comuni: in primo luogo, tutte e tre le aziende hanno investito pesantemente nella raccolta e utilizzo di dati su larga scala e nello sviluppo/adozione di algoritmi AI avanzati come parte integrante delle loro operazioni. La data-driven culture è un denominatore comune: che si tratti dei dati di acquisto e logistica di Amazon, dei dati finanziari e di processo di IBM o dei dati utente di Google, ciascuna impresa ha costruito capacità analitiche tali da informare meglio le decisioni e automatizzare processi chiave. Un secondo tema è l'automazione intelligente: Amazon con i magazzini robotizzati e i flussi logistici dinamici, IBM con l'AI Ops e i processi di risk management automatizzati, Google con i data center autogestiti dall'AI e i flussi di advertising ottimizzati automaticamente. Tutte hanno ridotto la dipendenza dall'intervento manuale in settori critici, ottenendo velocità e coerenza impossibili da raggiungere altrimenti. Ciò porta al terzo tema comune: la ricerca di agilità e adattabilità. Ciascuna azienda ha usato l'IA non solo per essere più efficiente, ma soprattutto per essere più flessibile di fronte ai cambiamenti: Amazon rialloca risorse in tempo reale per seguire la domanda, IBM adegua rapidamente valutazioni e compliance grazie a insight AI, Google personalizza servizi e sposta investimenti su nuovi orizzonti guidata da analisi predittive. L'IA è dunque strumentale nel mantenere un assetto agile e nel coltivare capacità dinamiche. Inoltre, tutte e tre riconoscono – almeno nei principi – l'importanza del fattore umano in termini di supervisione e competenze: ad esempio, mantengono ruoli per interpretare e controllare l'operato dell'IA (umani nel loop di Amazon per le eccezioni, risk manager in IBM che convalidano i modelli, ingegneri in Google che curano continuamente gli algoritmi di ranking). Hanno in comune l'aver sviluppato strategie etiche e normative attorno all'uso dell'IA (Google ha un codice etico per l'AI dal 2018; IBM spinge su AI affidabile; Amazon ha un focus pratico su evitare bias nei suoi sistemi interni dopo casi come quello del recruiting).

Differenze specifiche: Sul fronte delle differenze, è utile notare come l'IA sia stata declinata per obiettivi di resilienza differenti a seconda del modello di business:

- Amazon mette l'accento sulla resilienza operativa e di supply chain: qui l'IA è un mezzo per garantire continuità del servizio al cliente (consegne puntuali nonostante

tutto) e robustezza logistica. È molto focalizzata sugli aspetti fisici (merci, magazzini, consegne).

- IBM punta soprattutto alla resilienza nei processi di gestione e IT – che è coerente col fatto che IBM stessa vende resilienza (in forma di soluzioni) ad altre aziende. L’IA in IBM è quasi “dietro le quinte”, orchestrando rischi, compliance, infrastrutture, più che toccare il cliente finale.
- Google sfrutta l’IA per una resilienza strategico-innovativa: mantenere rilevanza sul mercato, creare nuovi prodotti e migliorare quelli esistenti, con un occhio alla continuità dei servizi digitali. Il cliente finale sperimenta direttamente molte innovazioni AI di Google (ricerca migliore, funzioni intelligenti), a differenza di Amazon dove l’utente vede solo il risultato (consegna veloce) ma non l’IA in sé, e di IBM dove l’utente finale è spesso un’altra impresa.

In termini organizzativi, le strutture differiscono: Amazon integra l’IA nelle divisioni esistenti (logistica, retail, AWS), IBM ha divisioni specifiche (es. Data & AI) che sviluppano tech da applicare orizzontalmente e consulenti che la portano dai clienti, Google ha un team di ricerca come Brain/DeepMind e poi “AI features” diffuse in tutti i prodotti. Questo può influire: Amazon e Google tendono a produrre soluzioni AI proprietarie per sé, IBM crea soluzioni per sé ma anche prodotto vendibile.

Una dissimilarità di contesto è anche nei rischi affrontati: Amazon affronta rischi operativi (guasti supply, ritardi); IBM rischi di competenza (rimanere tecnologicamente indietro rispetto a concorrenti cloud e AI, oltre ai rischi gestionali tipici); Google rischi tecnologici/regolatori (disruption tecnologica, privacy). Ognuna ha calibrato l’uso dell’IA per mitigare i rischi più critici per il proprio business.

In definitiva, Amazon, IBM e Google mostrano che l’IA può aumentare la resilienza aziendale sotto molteplici aspetti (operativo, finanziario, strategico), ma va implementata con visione strategica, investimenti costanti e consapevolezza delle nuove sfide che essa comporta. Queste aziende fungono da laboratori viventi: i loro successi e inciampi forniscono preziose indicazioni per tutte le altre organizzazioni che, in misura diversa, si incamminano sulla strada della trasformazione digitale e dell’adozione dell’AI per rafforzare la propria capacità di prosperare in un mondo incerto.

Capitolo 4

Rischi e Sfide Etiche dell'IA

4.1 Bias algoritmico e rischi reputazionali

Uno dei primi problemi riguarda la parzialità o distorsione nei risultati prodotti dall'IA, il cosiddetto bias algoritmico. Un sistema di IA è tanto buono quanto i dati e le assunzioni con cui è stato costruito: se nei dati di addestramento esistono pregiudizi o distribuzioni non rappresentative, l'algoritmo tenderà a riprodurli, spesso amplificandoli. Ciò può portare a decisioni inique o discriminatorie in vari ambiti – dall'assunzione del personale, alla concessione di prestiti, fino al targeting pubblicitario – con conseguenze deleterie per individui e gruppi sociali (Barocas, Hardt & Narayanan, 2019). Per le aziende, l'emergere di bias nei propri sistemi di IA costituisce un serio rischio reputazionale e legale: può danneggiare l'immagine pubblica dell'organizzazione, far perdere la fiducia di clienti e stakeholder, ed esporre a possibili cause legali o sanzioni per violazione di leggi antidiscriminatorie (Mehrabi et al., 2021).

Un caso emblematico è quello di Amazon e il tool di recruiting AI sviluppato a metà degli anni 2010. L'azienda aveva addestrato un algoritmo di valutazione CV basato sui dati storici delle proprie assunzioni, sbilanciati verso candidati maschi, riflettendo la demografia del settore tech. Il risultato fu che l'IA penalizzava sistematicamente i CV che contenevano riferimenti al genere femminile (Crawford, 2021). Quando Amazon si accorse del problema, provò a correggerlo, ma senza garanzia che non ricomparisse su altre variabili. Alla fine decise di dismettere il progetto entro il 2017, come documentato da indagini giornalistiche e da successive analisi accademiche (Dastin, 2018; Raghavan et al., 2020). La vicenda è un monito chiarissimo: anche aziende leader possono inciampare nei bias algoritmici e, quando ciò avviene, la reazione deve essere rapida e trasparente.

Altri esempi noti includono: software di riconoscimento facciale che funzionano male su individui con pelle scura perché addestrati prevalentemente su volti caucasici – Joy Buolamwini (2018) ha dimostrato errori clamorosi nei sistemi commerciali di big tech (Buolamwini & Gebru, 2018); algoritmi di content moderation accusati di censurare in modo sproporzionato certi gruppi (Gillespie, 2018); o modelli di credito che penalizzano minoranze etniche perché i dati storici riflettono disuguaglianze pregresse, perpetuando fenomeni simili al redlining (Hurley & Adebayo, 2016). Come previsto tutti questi incidenti generano

indignazione pubblica, proteste e interventi regolatori, le imprese devono investire in IA responsabile, così che i benefici di efficienza e velocità non vengano annullati da decisioni ingiuste che minano la coesione e la legittimità dell'organizzazione.

Per le aziende, affrontare il problema dei bias è sia un imperativo etico sia un'esigenza di gestione del rischio reputazionale. Come notano Mittelstadt et al. (2016), i bias negli algoritmi non sono solo errori tecnici, ma distorsioni sistematiche che possono compromettere l'equità e la legittimità delle decisioni. Un'azienda percepita come scorretta rischia boicottaggi, perdita di partner o un calo di fiducia generale. Uno scandalo su bias può contagiare anche altri servizi: se i clienti credono che l'algoritmo di un social network discrimini, potrebbero abbandonare la piattaforma, colpendo i ricavi pubblicitari.

Inoltre vi è anche il rischio legale/regolatorio: normative sulla parità di trattamento e contro la discriminazione (come le direttive Equality in UE o le leggi EEOC negli USA) possono essere applicate anche ai sistemi di IA. Già il GDPR sancisce il diritto a non essere soggetti a decisioni automatizzate discriminatorie o non spiegabili. Nel futuro AI Act europeo, i sistemi ad alto rischio dovranno rispettare requisiti stringenti di equità e trasparenza, pena sanzioni elevate (Mesarčík et al., 2021).

Come affrontarlo in pratica? Le strategie includono: Curare i dataset di addestramento, rendendoli sia rappresentativi che bilanciati; applicare tecniche di fairness-aware; sottoporre i modelli ad audit indipendenti attraverso valutazioni esterne e team disciplinari; coinvolgere stakeholder diversi nello sviluppo per poter diminuire i bias che un team omogeneo ignorerebbe e mantenere una supervisione umana.

4.2 Trasparenza e accountability delle decisioni automatizzate

Un secondo grande tema etico con impatto sulla resilienza organizzativa è quello della trasparenza degli algoritmi di IA e della connessa accountability (responsabilizzazione) nelle decisioni automatizzate. Molti sistemi di IA, in particolare quelli basati su tecniche di deep learning, sono delle “scatole nere” difficili da interpretare anche per i loro creatori: forniscono un output (una decisione, una raccomandazione) senza che sia immediatamente chiaro come o perché siano giunti a tale risultato (Burrell, 2016; Lipton, 2018). Questo pone problemi quando tali output hanno effetti significativi su persone o processi di business: come fidarsi di una decisione presa da un modello incomprensibile? E in caso di errore o danno, chi ne risponde?

Dal punto di vista aziendale, la mancanza di trasparenza può indebolire la fiducia degli stakeholder e complicare la governance interna. Immaginiamo un dirigente che deve spiegare

al consiglio di amministrazione perché l'IA ha rifiutato un prestito e l'unica risposta è “perché il modello l'ha calcolato così”: è evidente che ciò è insoddisfacente. Allo stesso modo, verso l'esterno, un cliente o un regolatore potrebbero chiedere chiarimenti: se l'azienda non sa fornirli, rischia cause legali o sanzioni (Goodman & Flaxman, 2017). Inoltre, la mancanza di trasparenza ostacola l'accountability: in caso di outcome negativo (un algoritmo di guida autonoma causa un incidente, un software diagnostico sbaglia una diagnosi), di chi è la colpa? Del produttore, dell'utente, di nessuno? Questa zona grigia alimenta sfiducia e rigetto sociale (Wachter, Mittelstadt & Floridi, 2017).

Per questi motivi, si sta affermando a livello normativo e di best practice il principio della trasparenza e spiegabilità (explainability). L'Unione Europea, con la proposta di AI Act, introduce obblighi espliciti: i fornitori di sistemi ad alto rischio dovranno documentare funzionamento e limiti del modello e fornire spiegazioni comprensibili sulle decisioni (Mesarčík et al., 2021). Ciò implica, ad esempio, che se una banca usa un algoritmo per concedere mutui, deve spiegare al richiedente su quali fattori si basa la decisione (reddito, età, storico credito, ecc.), con modalità intelligibili. L'idea di “obblighi di spiegabilità” si lega al diritto già sancito dal GDPR a non essere soggetti unicamente a decisioni automatizzate (Selbst & Powles, 2017).

Questa spinta normativa è cruciale anche per la resilienza aziendale: aumenta l'accountability e quindi la fiducia nel sistema. Se le persone sanno che dietro l'IA vi è responsabilità umana e possibilità di verifica, saranno più propense ad accettarla. Al contrario, sistemi opachi rischiano di generare resistenze o rigetto (Doshi-Velez & Kim, 2017).

Dal punto di vista pratico, per garantire trasparenza e accountability si devono utilizzare modelli interpretabili quando possibile, o tecniche di Explainable AI (XAI) come LIME o SHAP, che mostrano quali variabili hanno influenzato la decisione (Ribeiro, Singh & Guestrin, 2016; Lundberg & Lee, 2017); documentare accuratamente i sistemi di IA: scopi, dati, logiche, performance, limitazioni, creando un “registro dei modelli”; istituire human oversight: la normativa UE prevede l'intervento umano (human-in-the-loop) per molte decisioni ad alto impatto (Mesarčík et al., 2021); attribuire responsabilità organizzative chiare: molte aziende hanno creato ruoli dedicati come AI Ethics Officer o comitati etici interni (Floridi & Cowls, 2019) e predisporre meccanismi di ricorso: il GDPR riconosce il diritto a revisione umana in caso di decisioni automatizzate significative (Wachter et al., 2017).

Quindi, trasparenza e accountability sono essenziali per mantenere l'accettazione sociale dell'IA e quindi la sostenibilità del suo impiego.

4.3 Impatto su lavoro, competenze e organizzazione interna

L'introduzione massiccia dell'Intelligenza Artificiale nelle imprese non è neutrale rispetto al lavoro umano: al contrario, modifica profondamente le modalità operative, le competenze richieste e la struttura stessa delle organizzazioni. Questo porta con sé opportunità (nuovi ruoli qualificati, aumento produttività, liberazione da compiti gravosi) ma anche rischi (esuberi, divario di competenze, resistenze al cambiamento, effetti sulla motivazione). La resilienza aziendale dipende fortemente dal capitale umano: persone preparate, adattabili e motivate rendono l'azienda capace di affrontare le crisi; viceversa, una workforce demoralizzata o priva delle skill necessarie può diventare un punto di rottura nei momenti di stress. Pertanto, le imprese devono gestire con attenzione la transizione verso l'AI dal punto di vista organizzativo, per massimizzare i benefici e minimizzare gli impatti negativi su lavoratori e clima aziendale.

Un primo aspetto da considerare è l'effetto sull'occupazione e sui ruoli. L'IA e l'automazione tendono a ridurre il fabbisogno di lavoro manuale o ripetitivo, mentre creano domanda di profili più tecnici e creativi. Secondo il Future of Jobs Report 2023 del World Economic Forum, entro il 2027 si prevede la creazione di circa 69 milioni di nuovi posti di lavoro legati all'AI e alla digitalizzazione, ma anche la perdita di 83 milioni di ruoli tradizionali, specialmente in mansioni amministrative routinarie (Di Battista et al., 2023). In altre parole, la trasformazione digitale ridistribuirà l'occupazione: alcuni ruoli diventeranno obsoleti (es. centralinisti, data entry), mentre nasceranno ruoli prima inesistenti (data scientist, ingegneri del prompt, specialisti di manutenzione robotica). Questo genera ansia nei lavoratori: il WEF parla di FOBO – Fear Of Becoming Obsolete, la paura di diventare obsoleti, che diversi studi confermano come crescente. Tale preoccupazione può minare il morale e la fiducia in azienda, se non affrontata.

La resilienza organizzativa impone quindi di accompagnare l'adozione dell'AI con forti politiche di upskilling e reskilling del personale. Più di due terzi dei dirigenti concordano che integrare analytics e AI richiede un aggiornamento costante delle competenze dei dipendenti (Daugherty & Wilson, 2018). Occorre uno sforzo sia formativo sia culturale: formativo nel fornire training sulle nuove tecnologie (come usare strumenti di AI, come interpretarne i risultati), culturale nel trasmettere l'idea che l'AI completi le skill umane anziché minarle (Brynjolfsson & McAfee, 2017). Ad esempio, un'azienda manifatturiera che introduce robot collaborativi deve riqualificare gli operai in operatori di macchina e tecnici di supervisione, mostrando che il contributo umano resta centrale. Anche competenze trasversali come

pensiero critico, creatività e apprendimento continuo diventano cruciali: l'OCSE nota che entro il 2030 circa il 63% dei lavoratori dovrà aggiornare le proprie competenze almeno ogni cinque anni (OECD, 2019). Ciò implica che le aziende devono farsi carico di offrire opportunità di formazione e i lavoratori devono essere disposti a rimettersi in gioco più volte nella carriera.

Dal punto di vista organizzativo, l'AI impone cambiamenti strutturali. Introdurre soluzioni di AI può significare creare nuove funzioni o reparti (es. un centro di eccellenza AI, un comitato etico, la figura del Chief Data Scientist). Secondo Gartner (2020), entro il 2025 il 30% delle organizzazioni avrà istituito nuovi ruoli dedicati alla resilienza digitale/AI. In parallelo, alcune funzioni tradizionali potrebbero ridursi o accorparsi. La struttura tende anche a diventare più ibrida: team composto da umani e AI che collaborano. Ad esempio, nei call center operatori umani lavorano affiancati da sistemi AI che suggeriscono risposte o trascrivono automaticamente le chiamate. La sfida del management è orchestrare questa convivenza ridefinendo processi e workflow.

Va considerato anche il clima interno e la motivazione. Se l'introduzione dell'AI non è gestita con sensibilità, i dipendenti possono percepirla come una minaccia, generando resistenze o calo di impegno. È compito della leadership comunicare chiaramente lo scopo (perché adottiamo l'AI), i benefici per tutti e rassicurare che il contributo umano resta essenziale. In alcuni casi è utile coinvolgere i lavoratori stessi nel design delle soluzioni AI. Una cultura aziendale solida e inclusiva è la risorsa più efficace per affrontare queste sfide (Schein, 2010). Se i dipendenti condividono la visione e si fidano dell'azienda, saranno più propensi a vedere l'AI come un'opportunità e ad adattarsi.

Un altro impatto riguarda la distribuzione geografica del lavoro: l'AI e la digitalizzazione spingono verso il lavoro da remoto e una forza lavoro globalizzata. La pandemia ha accelerato l'adozione dello smart working, e l'AI fornisce strumenti (meeting transcript automatici, traduzioni simultanee) che lo rendono sempre più efficiente (Carillo et al., 2021). Per la resilienza, avere team distribuiti può essere un vantaggio (più resistenza a crisi locali), ma serve mantenere coesione e comunicazione. Tecnologie di AI possono aiutare anche qui, ad esempio con sistemi che monitorano il morale dei dipendenti o favoriscono lo scambio di conoscenze.

Da non dimenticare la questione dei costi sociali. Se non gestite bene, le transizioni tecnologiche possono aumentare le disuguaglianze: lavoratori altamente qualificati vedono

crescere la domanda e i salari, mentre chi ha skill obsolete rischia disoccupazione o precarietà. Ciò ha riflessi anche sulla stabilità sociale e quindi sulla resilienza economica complessiva (Acemoglu & Restrepo, 2019). Alcune grandi aziende tech hanno riconosciuto questa responsabilità e creato programmi di riqualificazione: Amazon, ad esempio, ha avviato Upskilling 2025 per riqualificare 100.000 dipendenti in ruoli tecnici.

L'adozione dell'IA ridefinisce il rapporto tra persone e tecnologia. Le imprese più resilienti saranno quelle che sapranno integrare l'AI come amplificatore delle capacità umane, mantenendo alta la motivazione e aggiornando continuamente le competenze. Ciò richiede investimenti in formazione, comunicazione chiara, leadership partecipativa e talvolta scelte difficili di riorganizzazione. Ma se gestita con visione, la trasformazione può portare a un'organizzazione più efficiente e anche più appagante, liberando le persone dalle mansioni monotone per concentrarsi su quelle creative e di valore aggiunto. Come sintetizza il World Economic Forum (2023), l'obiettivo dev'essere che "l'AI completi le competenze umane anziché sostituirle" (Di Battista et al., 2023).

4.4 Normative e governance etica dell'IA

Di fronte alla rapida diffusione dell'Intelligenza Artificiale nei settori più disparati, istituzioni e società civile stanno elaborando risposte normative ed etiche per garantire che questa tecnologia venga utilizzata in modo sicuro, responsabile e al servizio del bene comune. Per le aziende, ciò significa muoversi in un panorama regolatorio in evoluzione e adottare forme di governance interna dell'AI per assicurare conformità e allineamento ai propri valori.

Un'efficace governance etica dell'IA non è solo un onere burocratico, ma può diventare un vantaggio competitivo: un'azienda che dimostra di usare l'IA in modo affidabile e trasparente guadagna fiducia da parte di clienti e regolatori, rafforzando la propria resilienza reputazionale e riducendo il rischio di contenziosi o sanzioni (Floridi et al., 2018).

Il quadro normativo più imminente e rilevante (almeno per chi opera in Europa) è l'Artificial Intelligence Act (AI Act) dell'Unione Europea. Questo regolamento (ancora in fase finale di approvazione nel 2025) intende essere la prima legislazione organica sull'IA, adottando un approccio basato sul rischio: obblighi più stringenti per le applicazioni AI considerate "ad alto rischio" (es. quelle in ambito sanitario, trasporti, istruzione, occupazione, credito, forze dell'ordine, infrastrutture critiche, ecc.) (Mesarčik et al., 2021).

Tra i requisiti previsti vi sono:

- Gestione del rischio e robustezza tecnica: i sistemi AI ad alto rischio dovranno soddisfare standard di sicurezza ed essere progettati per evitare malfunzionamenti, con piani di continuità operativa e recovery (Skiadioti, 2025).
- Trasparenza e documentazione: i fornitori dovranno documentare a fondo il modello e renderlo spiegabile agli utenti finali; per alcune AI (come quelle generative) vi sarà obbligo di segnalare esplicitamente che il contenuto è generato, e i deepfake dovranno essere identificati (Wachter, Mittelstadt & Floridi, 2017).
- Dati di training di qualità: i dataset dovranno essere rappresentativi ed equi, per ridurre bias e distorsioni (Barocas, Hardt & Narayanan, 2019).
- Supervisione umana: i sistemi dovranno permettere human-in-the-loop o human-on-the-loop (Mesarčik et al., 2021).
- Vigilanza e conformità: gli Stati membri designeranno autorità competenti e i fornitori dovranno registrare i loro sistemi in un database UE. Sono previste sanzioni severe (fino al 6% del fatturato annuo globale).

L'AI Act dovrebbe iniziare ad applicarsi pienamente dal 2026, con alcuni obblighi già dal 2025 (Skiadioti, 2025). Dal punto di vista della resilienza organizzativa, prepararsi è cruciale: chi investe ora in AI governance sarà in una posizione di vantaggio competitivo. Già oggi alcune imprese adottano framework come il NIST AI Risk Management Framework (NIST, 2023) o lo standard ISO/IEC 23894:2023 sulla gestione del rischio AI, che forniscono linee guida per valutare bias, resilienza operativa e cybersecurity.

Oltre all'AI Act, altre normative specifiche toccano l'IA: il Digital Operational Resilience Act (DORA) per il settore finanziario (Skiadioti, 2025), il Cyber Resilience Act per i prodotti digitali, e linee guida etiche come quelle dell'OMS sull'AI in sanità (Guidance, 2021) o della EEOC negli USA sull'uso etico dell'AI nel recruiting. La regolamentazione dell'IA non va vista come un ostacolo, ma come parte integrante della costruzione della fiducia a lungo termine.

Dal lato governance interna, molte grandi imprese hanno istituito AI Ethics Board o comitati dedicati (Mökander et al., 2021). Microsoft, Google e IBM hanno elaborato principi etici interni per l'AI e creato processi di revisione dei progetti. Alcune aziende hanno scelto di auto-regolamentarsi, rinunciando a vendere AI troppo rischiose: nel 2020, ad esempio,

Microsoft, IBM e Amazon hanno sospeso la vendita di sistemi avanzati di riconoscimento facciale alle forze dell'ordine, in attesa di regole più chiare, per evitare rischi reputazionali e legali (Hill, 2022).

La collaborazione internazionale è altrettanto rilevante: i Principi OCSE sull'AI (OECD, 2019) e le linee guida UNESCO sull'etica dell'IA (UNESCO, 2021) fissano valori comuni (trasparenza, equità, benessere umano, privacy) cui molte aziende si ispirano. Aderire a questi consorzi aiuta a rimanere aggiornati e a contribuire alla definizione di standard globali.

Le aziende capaci di adattamento saranno quelle capaci di anticipare le norme, integrarle nei propri standard e trasformarle in vantaggio competitivo. Nell'era dell'AI, etica e resilienza aziendale sono due facce della stessa medaglia: governare l'IA in modo responsabile è un investimento nella sostenibilità futura del business.

Conclusioni

La domanda di ricerca posta all'inizio di questo lavoro era: l'Intelligenza Artificiale può rendere le aziende più resilienti alle crisi? Alla luce dell'analisi condotta, la risposta appare complessivamente affermativa, seppur con importanti condizioni e cautele.

L'esame dei casi di Amazon, IBM e Google ha dimostrato che l'IA può fungere da autentico abilitatore di resilienza organizzativa, ma solo quando viene introdotta con una chiara strategia e un'adeguata governance. Amazon ha costruito una supply chain adattiva, capace di riallocare inventari e risorse in base a eventi esterni imprevedibili. Durante la pandemia questa agilità si è tradotta in un vantaggio competitivo notevole, permettendo all'azienda di mantenere operatività e servizio mentre molti concorrenti faticavano a soddisfare la domanda (Ivanov & Dolgui, 2020; Sarkar et al., 2022). IBM, con Watson e OpenPages, ha migliorato la gestione del rischio e il processo decisionale, ottenendo modelli predittivi più accurati e una governance più solida in termini di compliance e robustezza interna (Davenport & Ronanki, 2018). Google, invece, ha reso l'IA parte integrante del proprio DNA aziendale: da un lato ha potenziato i servizi digitali con strumenti di deep learning e NLP, dall'altro ha incrementato l'efficienza interna, ad esempio riducendo del 30% i consumi energetici nei data center grazie agli algoritmi di DeepMind (DeepMind, 2018).

Da queste esperienze emergono alcune lezioni trasversali. In primo luogo, l'IA permette una reattività e un adattamento senza precedenti, grazie all'analisi predittiva e all'automazione intelligente, che riducono ritardi e rendono più agili le organizzazioni (Teece, Peteraf & Leih, 2016). In secondo luogo, l'efficienza operativa migliora sensibilmente: l'automazione riduce errori e colli di bottiglia, garantendo continuità anche in condizioni critiche. Inoltre, l'IA consente decisioni più informate, basate su grandi quantità di dati, rafforzando la capacità dei manager di navigare l'incertezza (Brynjolfsson & McElheran, 2016). Può stimolare l'innovazione e la diversificazione, aprendo nuovi mercati e riducendo la dipendenza da singoli settori, come dimostra Google con le sue "Other Bets" in ambito guida autonoma, bioscienze e cloud.

Tuttavia, i benefici non vanno sopravvalutati. L'IA porta con sé nuove vulnerabilità che possono compromettere la resilienza stessa delle imprese; I bias algoritmici, come mostrato dal caso Amazon nel recruiting, rivelano i rischi reputazionali ed etici di modelli addestrati su dati distorti (Dastin, 2018; Barocas, Hardt & Narayanan, 2019). La mancanza di trasparenza dei modelli di deep learning pone problemi di accountability e fiducia, tanto che le nuove normative, come l'AI Act europeo, introducono obblighi stringenti di spiegabilità e

supervisione umana (Burrell, 2016; Mesarčik et al., 2021). La dipendenza tecnologica, inoltre, espone a rischi sistemici: cyber attacchi, blackout digitali o malfunzionamenti dei sistemi possono avere effetti paralizzanti, come evidenziato anche dalle linee guida del Digital Operational Resilience Act (Zetsche et al., 2021). Ma senza adeguate politiche di upskilling e reskilling, le imprese rischiano di non colmare il divario di competenze, generando resistenze interne e disuguaglianze crescenti (OECD, 2019).

Il quadro che emerge ha implicazioni anche per imprese non tecnologiche. Oggi l'IA è accessibile grazie a soluzioni cloud e applicazioni verticali, e può essere adottata in settori tradizionali per finalità come la manutenzione predittiva, l'ottimizzazione degli inventari o il contrasto alle frodi (Lee et al., 2015). Tuttavia, permane un divario di adozione tra grandi imprese e PMI, che rischia di tradursi in un gap di resilienza se non colmato da politiche mirate, partnership tecnologiche e programmi di formazione (OECD, 2019).

Guardando al futuro, è verosimile che l'IA diventi parte naturale delle organizzazioni, fino a scomparire come tecnologia distinta. Le nuove generazioni di IA generativa aprono ulteriori possibilità, ad esempio nel supporto creativo e nello sviluppo software, ma introducono anche nuove sfide di veridicità e di proprietà intellettuale (Bommasani et al., 2021). Allo stesso tempo, emerge il concetto di "AI resilience", ossia la resilienza dei sistemi di IA stessi: modelli robusti, sicuri e in grado di resistere a stress, guasti e attacchi avversari (Goodfellow, Shlens & Szegedy, 2014). L'IA non rafforzerà solo le singole aziende, ma l'intero tessuto economico e le filiere globali, contribuendo alla resilienza di società e istituzioni (Hobbs, 2020).

L'intelligenza Artificiale si configura come un driver di resilienza potente, ma non privo di rischi. Perché i suoi benefici si traducano in un vantaggio sostenibile, occorre accompagnarne l'adozione con solide politiche di governance, trasparenza e valorizzazione del capitale umano. L'azienda veramente resiliente nell'era digitale sarà quella capace di coniugare intelligenza artificiale e intelligenza umana: sfruttando l'agilità e la potenza dei dati senza rinunciare alla creatività, alla responsabilità e alla capacità di adattamento delle persone. Le Big Tech offrono esempi preziosi, ma la vera sfida sarà estendere questi modelli anche al tessuto economico più tradizionale, affinché i benefici dell'IA per la resilienza diventino condivisi e sostenibili nel lungo periodo.

Bibliografia

Roberts, D., Choudhury, I., Kovala, S., Roberts, S., & Tanvir, J. (2022). *Business Resilience: A Practical Guide to Sustained Progress Delivered at Pace*. Kogan Page Publishers.

Daft, R. L. (2004). *Organizzazione aziendale*. Apogeo Editore.

Chen, R., Xie, Y., & Liu, Y. (2021). Defining, conceptualizing, and measuring organizational resilience: A multiple case study. *Sustainability*, 13(5), 2517.

Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. *Business research*, 13(1), 215-246.

Garrido-Moreno, A., Martín-Rojas, R., & García-Morales, V. J. (2024). The key role of innovation and organizational resilience in improving business performance: A mixed-methods approach. *International Journal of Information Management*, 77, 102777.

Georgescu, I., Bocean, C. G., Vărzaru, A. A., Rotea, C. C., Mangra, M. G., & Mangra, G. I. (2024). Enhancing organizational resilience: The transformative influence of strategic human resource management practices and organizational culture. *Sustainability*, 16(10), 4315.

Kraus, S., Clauss, T., Breier, M., Gast, J., Zardini, A., & Tiberius, V. (2020). The economics of COVID-19: initial empirical evidence on how family firms in five European countries cope with the corona crisis. *International Journal of Entrepreneurial Behavior & Research*, 26(5), 1067–1092. <https://doi.org/10.1108/IJEBr-04-2020-0214>

Böhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. *Variance*, 12(2), 161-185.

Brynjolfsson, E., & McElheran, K. (2016). The rapid adoption of data-driven decision-making. *American Economic Review*, 106(5), 133-139.

Inguglia, C. (2020). Resilienza. *Risk elaboration*, 1, 50-51. (da aggiungere citazione psicologica)

Choudhury, P., Foroughi, C., & Larson, B. (2021). Work-from-anywhere: The productivity effects of geographic flexibility. *Strategic Management Journal*, 42(4), 655-683.

Benhamou, S. (2020). Artificial intelligence and the future of work. *Revue d'économie industrielle*, (169), 57-88.

Corrales-Estrada, A. M., Gómez-Santos, L. L., Bernal-Torres, C. A., Rodríguez-López, J. E., & Sandoval-Reyes, J. (2025). Dynamic capabilities contribution to organizational performance: the mediator role of business continuity ordinary capabilities. *Cogent Business & Management*, 12(1), 2493315.

Eisenhardt, K. M., & Martin, J. A. (2017). Dynamic capabilities: what are they?. *The SMS Blackwell handbook of organizational capabilities*, 341-363.

Ye, Q. (2025). Digital leadership enhances organizational resilience by fostering job crafting: the moderating role of organizational culture. *Scientific Reports*, 15(1), 24640.

Barocas, S., Hardt, M., & Narayanan, A. (2020). Fairness and machine learning. *Recommender systems handbook*, 1, 453-459.

Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77-91). PMLR.

Dastin, J. (2022). Amazon scraps secret AI recruiting tool that showed bias against women. In *Ethics of data and analytics* (pp. 296-299). Auerbach Publications.

Act, A. I. (2021). Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. *EUR-Lex-52021PC0206*.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Hurley, M., & Adebayo, J. (2016). Credit scoring in the era of big data. *Yale JL & Tech.*, 18, 148.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM computing surveys (CSUR)*, 54(6), 1-35.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 2053951716679679.

Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big data & society*, 3(1), 2053951715622512.

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608*.

Floridi, L., & Cowls, J. (2022). A unified framework of five principles for AI in society. *Machine learning and the city: Applications in architecture and urban design*, 535-545.

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation”. *AI magazine*, 38(3), 50-57.

Lipton, Z. C. (2018). The mythos of model interpretability: In machine learning, the concept of interpretability is both important and slippery. *Queue*, 16(3), 31-57.

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016, August). "Why should I trust you?" Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining* (pp. 1135-1144).

- Selbst, A., & Powles, J. (2018, January). "Meaningful information" and the right to explanation. In *conference on fairness, accountability and transparency* (pp. 48-48). PMLR.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International data privacy law*, 7(2), 76-99.
- Bennett, N., & Lemoine, J. (2014). What VUCA really means for you. *Harvard business review*, 92(1/2).
- McAfee, A., & Brynjolfsson, E. (2017). *Machine, platform, crowd: Harnessing our digital future*. WW Norton & Company.
- Russell, S. J., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*, Global Edition 4e.
- Agrawal, A., Gans, J., & Goldfarb, A. (2018). Prediction, judgment, and complexity: a theory of decision-making and artificial intelligence. In *The economics of artificial intelligence: An agenda* (pp. 89-110). University of Chicago Press.
- Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International journal of production research*, 58(10), 2904-2915.
- Sheffi, Y. (2020). *The new (ab) normal: Reshaping business and supply chain strategy beyond Covid-19*. Mit Ctl Media.
- Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, 35(7), 659-675.
- Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard business review*, 96(1), 108-116.
- Ferrucci, D., Brown, E., Chu-Carroll, J., Fan, J., Gondek, D., Kalyanpur, A. A., ... & Welty, C. (2010). Building Watson: An overview of the DeepQA project. *AI magazine*, 31(3), 59-79.
- Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. *Journal of the academy of marketing science*, 49(1), 30-50.
- Lessmann, S., Baesens, B., Seow, H. V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European journal of operational research*, 247(1), 124-136.
- Dang, Y., Lin, Q., & Huang, P. (2019, May). Aiops: real-world challenges and research innovations. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)* (pp. 4-5). IEEE.
- Makridakis, S. (2017). The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. *Futures*, 90, 46-60.

- Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems*, 50(3), 559-569.
- Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. *New England Journal of Medicine*, 380(14), 1347-1358.
- Jie, Z., Zhiying, Z., & Li, L. (2021). A meta-analysis of Watson for Oncology in clinical application. *Scientific reports*, 11(1), 5792.
- Brin, S. (1998). The PageRank citation ranking: bringing order to the web. *Proceedings of ASIS*, 1998, 98, 161-172.
- Cheng, H. T., Koc, L., Harmsen, J., Shaked, T., Chandra, T., Aradhye, H., ... & Shah, H. (2016, September). Wide & deep learning for recommender systems. In *Proceedings of the 1st workshop on deep learning for recommender systems* (pp. 7-10).
- Chen, M. X., Lee, B. N., Bansal, G., Cao, Y., Zhang, S., Lu, J., ... & Wu, Y. (2019, July). Gmail smart compose: Real-time assisted writing. In *Proceedings of the 25th ACM SIGKDD international conference on knowledge discovery & data mining* (pp. 2287-2295).
- Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019, June). Bert: Pre-training of deep bidirectional transformers for language understanding. In *Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers)* (pp. 4171-4186).
- Luo, J., Paduraru, C., Voicu, O., Chervonyi, Y., Munns, S., Li, J., ... & Mankowitz, D. J. (2022). Controlling commercial cooling systems using reinforcement learning. *arXiv preprint arXiv:2211.07357*.
- Wu, Y., Schuster, M., Chen, Z., Le, Q. V., Norouzi, M., Macherey, W., ... & Dean, J. (2016). Google's neural machine translation system: Bridging the gap between human and machine translation. *arXiv preprint arXiv:1609.08144*.
- Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Zheng, X. (2016). {TensorFlow}: a system for {Large-Scale} machine learning. In *12th USENIX symposium on operating systems design and implementation (OSDI 16)* (pp. 265-283).
- Bommasani, R. (2021). On the opportunities and risks of foundation models. *arXiv preprint arXiv:2108.07258*.
- DeepMind, A. I. (2016). reduces Google data centre cooling bill by 40%. *Deepmind.com/blog/article/deepmind-ai-reduces-google-data-centre-cooling-bill-40*.
- Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. *McKinsey Global Institute*, 4(1), 2-61.
- Neubig, G. (2017). Neural machine translation and sequence-to-sequence models: A tutorial. *arXiv preprint arXiv:1703.01619*.

- Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, 32(1), 50-65.
- Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393-410.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. (2013). Digital business strategy: toward a next generation of insights. *MIS quarterly*, 471-482.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.
- Cummings, M. (2021). Rethinking the maturity of artificial intelligence in safety-critical settings. *Ai Magazine*, 42(1), 6-15.
- Galaz, V., Centeno, M. A., Callahan, P. W., Causevic, A., Patterson, T., Brass, I., ... & Levy, K. (2021). Artificial intelligence, systemic risks, and sustainability. *Technology in society*, 67, 101741.
- Regulation, D. O. R. A. (2022). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU.) 2016/1011 (Text with EEA relevance)*. Retrieved March 15, 2024.
- Vial, G. (2021). Understanding digital transformation: A review and a research agenda. *Managing digital transformation*, 13-66
- Weill, P., & Woerner, S. L. (2018). Is your company ready for a digital future?. *MIT Sloan Management Review*, 59(2), 21-25.
- Denyer, D. (2017). Organizational Resilience: A summary of academic evidence, business insights and new thinking. *BSI and Cranfield School of Management*, 5, 8-25.
- Gulati, R. (2022). *Deep purpose: The heart and soul of high-performance companies*. Penguin UK.
- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human resource management review*, 21(3), 243-255.
- Mallak, L. A. (1998). Measuring resilience in health care provider organizations. *Health manpower management*, 24(4), 148-152.
- Rigby, D. K., Sutherland, J., & Noble, A. (2018). Agile at scale. *Harvard business review*, 96(3), 88-96

- Somers, S. (2009). Measuring resilience potential: An adaptive strategy for organizational crisis planning. *Journal of contingencies and crisis management*, 17(1), 12-23.
- Sutcliffe, K. M. (2003). Organizing for resilience. *Positive organizational scholarship: Foundations of a new discipline*.
- Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *California management review*, 58(4), 13-35.
- Vogus, T. J., & Sutcliffe, K. M. (2007, October). Organizational resilience: Towards a theory and research agenda. In *2007 IEEE international conference on systems, man and cybernetics* (pp. 3418-3422). IEEE.
- Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2), 1153-1176.
- Chui, M., Manyika, J., & Miremadi, M. (2018). What AI can and can't do (yet) for your business. *McKinsey Quarterly*, 1(97-108), 1.
- Chen, L., Mislove, A., & Wilson, C. (2016, April). An empirical analysis of algorithmic pricing on amazon marketplace. In *Proceedings of the 25th international conference on World Wide Web* (pp. 1339-1349).
- Nathan, S., Ghosh, R., Mukherjee, T., & Narayanan, K. (2017, April). Comicon: A co-operative management system for docker container images. In *2017 IEEE international conference on cloud engineering (IC2E)* (pp. 116-126). IEEE.
- Naim, A. (2022). Role of artificial intelligence in business risk management. *American Journal of Business Management, Economics, and Banking*, 1, 55-66.
- Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California management review*, 61(4), 5-14.
- Huang, M. H., & Rust, R. T. (2021). A strategic framework for artificial intelligence in marketing. *Journal of the academy of marketing science*, 49(1), 30-50.
- Wurman, P. R., D'Andrea, R., & Mountz, M. (2008). Coordinating hundreds of cooperative, autonomous vehicles in warehouses. *AI magazine*, 29(1), 9-9. <https://doi.org/10.1609/aimag.v29i1.2082>
- Alipour, H. (2019). *Model-Driven Machine Learning for Predictive Cloud Auto-scaling* (Doctoral dissertation, Concordia University).
- Johnson, N., Zhao, G., Hunsader, E., Qi, H., Johnson, N., Meng, J., & Tivnan, B. (2013). Abrupt rise of new machine ecology beyond human response time. *Scientific reports*, 3(1), 2627.

- Silver, D., Schrittwieser, J., Simonyan, K., Antonoglou, I., Huang, A., Guez, A., ... & Hassabis, D. (2017). Mastering the game of go without human knowledge. *nature*, 550(7676), 354-359.
- Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *California management review*, 58(4), 13-35.
- Bose, R. (2009). Advanced analytics: opportunities and challenges. *Industrial Management & Data Systems*, 109(2), 155-172.
- Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, 3, 18-23.
- Shmueli, G., & Koppius, O. R. (2011). Predictive analytics in information systems research. *MIS quarterly*, 553-572.
- Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. *Journal of economic perspectives*, 33(2), 3-30.
- Carillo, K., Cachat-Rosset, G., Marsan, J., Saba, T., & Klarsfeld, A. (2021). Adjusting to epidemic-induced telework: Empirical insights from teleworkers in France. *European Journal of Information Systems*, 30(1), 69-88.
- Wilson, H. J., & Daugherty, P. R. (2018). Collaborative intelligence: Humans and AI are joining forces. *Harvard business review*, 96(4), 114-123.
- Top, G. (10). Strategic Technology Trends for 2020. URL: <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020>.
- OCDE. (2019). Employment Outlook 2019: The future of work.
- Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2). John Wiley & Sons.
- Di Battista, A., Grayling, S., Hasselaar, E., Leopold, T., Li, R., Rayner, M., & Zahidi, S. (2023, November). Future of jobs report 2023. In *World Economic Forum* (pp. 978-2).
- Skiadioti, M. F. (2025). *Examining compliance requirements under the EU's Digital Operational Resilience Act (DORA) for the financial sector* (Master's thesis, Πανεπιστήμιο Πειραιώς).
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and machines*, 28(4), 689-707.
- Hill, K. (2022). Wrongfully accused by an algorithm. In *Ethics of Data and Analytics* (pp. 138-142). Auerbach Publications.

Mökander, J., Morley, J., Taddeo, M., & Floridi, L. (2021). Ethics-based auditing of automated decision-making systems: Nature, scope, and limitations. *Science and Engineering Ethics*, 27(4), 44.

AI, N. (2023). Artificial intelligence risk management framework (AI RMF 1.0). URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai>, 100-1.

United Nations Educational, Scientific and Cultural Organization. (2021). Recommendation on the ethics of artificial intelligence.

Guidance, W. H. O. (2021). Ethics and governance of artificial intelligence for health. *World Health Organization*.

Sarkar, P., Mohamed Ismail, M. W., & Tkachev, T. (2022). Bridging the supply chain resilience research and practice gaps: pre and post COVID-19 perspectives. *Journal of Global Operations and Strategic Sourcing*, 15(4), 599-627.

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard business review*, 96(1), 108-116.

Mesarčík, M., Solárová, S., Podroužek, J., & Bielikova, M. (2021). Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence—Artificial Intelligence Act. *Kempelen Institute of Intelligent Technologies*.

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*.