



Dipartimento di Impresa e Management

Cattedra di Diritto Pubblico dell'Economia

Artificial Intelligence Act: regolamentazione dell'intelligenza artificiale in Europa e confronto con il panorama internazionale.
Analisi dell'impatto su IBM e Amazon.

Relatore

Prof. Pellegrini Mirella

Candidato

D'Ermo Francesca

matr. 285481

Anno Accademico 2024/2025

Con immensa gratitudine dedico questa tesi ai miei genitori, pilastri della mia vita, per l'amore incondizionato e il sostegno che non mi hanno mai fatto mancare. Grazie per avermi accompagnata in ogni passo di questo percorso.

Indice

Indice	1
Introduzione	2
1 Artificial Intelligence Act: principi e finalità	4
1.1 La necessità di regolamentazione	4
1.1.1 Definizione, funzionamento e applicazioni dell'IA	4
1.1.2 Rischi e opportunità.....	6
1.1.3 Evoluzione normativa a livello europeo	9
1.2 AI Act: struttura e obiettivi	14
1.2.1 Classificazione dei sistemi IA e livelli di rischio	15
1.2.2 Impatto sulle imprese e sulle tecnologie emergenti	22
1.3 Confronto tra regolazione europea e strategie internazionali	26
1.3.1 AI Act vs GDPR, <i>Digital Services Act</i> e <i>Digital Markets Act</i>	26
1.3.2 Confronto con approcci regolatori extraeuropei (USA, Cina, Regno Unito).....	31
2 Applicazione dell'AI Act nei Paesi europei: armonizzazione e criticità	39
2.1 L'implementazione dell'AI Act nei principali Stati membri	39
2.1.1 Francia: approccio regolatorio, primi risultati e parentesi sulle PMI.....	39
2.1.2 Germania: impatto sulle imprese tecnologiche	44
2.1.3 Italia: recepimento e criticità	49
2.2 Divergenze tra Stati membri e conseguenze competitive sui mercati globali.....	52
2.3 Il ruolo dell'AI Act nel contesto globale	61
3 Case study: aziende e conformità all'AI Act	64
3.1 Impatto del regolamento sulle imprese: compliance e difficoltà	64
3.2 Conformità e best practice: il ruolo di IBM	68
3.3 Sfide e criticità nella governance dell'intelligenza artificiale: il caso Amazon	70
Conclusioni	76
Bibliografia	79
Sitografia	86

Introduzione

L'avvento dell'intelligenza artificiale (AI) sta trasformando profondamente il panorama economico, sociale e giuridico a livello globale. Le sue applicazioni spaziano da ambiti altamente specializzati, come la diagnostica medica e l'analisi predittiva, fino a settori di uso quotidiano, come l'e-commerce e i servizi digitali. Tuttavia, questa rapida evoluzione tecnologica solleva questioni cruciali in materia di regolamentazione, trasparenza e tutela dei diritti fondamentali. Per rispondere a queste sfide, l'Unione Europea ha introdotto l'*Artificial Intelligence Act* (AI Act), il primo quadro normativo organico volto a regolamentare l'uso dell'intelligenza artificiale nel mercato europeo, con un approccio basato sulla classificazione del rischio.

L'obiettivo di questa tesi è analizzare l'impatto della regolamentazione sulle aziende e le sfide connesse alla sua implementazione nei diversi Stati membri, per comprendere se e in che modo questa normativa possa fungere da modello per altri ordinamenti internazionali.

L'AI Act rappresenta un passaggio cruciale nel tentativo dell'Unione Europea di garantire un utilizzo responsabile e sicuro dell'intelligenza artificiale, bilanciando innovazione e tutela dei diritti fondamentali.

Dal punto di vista metodologico, la ricerca si baserà su un'analisi delle normative vigenti, dei documenti ufficiali della Commissione Europea, delle linee guida fornite dalle autorità regolatorie e delle *best practices* adottate dalle imprese. Verranno inoltre esaminati studi accademici, report istituzionali e fonti aziendali per offrire una prospettiva critica sul tema. L'approccio sarà sia normativo che empirico, includendo un confronto tra diverse regolamentazioni a livello internazionale, con un focus sulle strategie di *compliance* adottate dalle aziende.

La tesi si articolerà in tre macro-sezioni principali: il quadro normativo dell'AI Act, con un'analisi dei principi fondamentali del regolamento, della classificazione dei sistemi AI in base al livello di rischio e degli obblighi imposti alle imprese; l'implementazione nei Paesi europei e le criticità, esaminando il recepimento dell'AI Act nei principali Stati membri e le difficoltà di armonizzazione; e infine un'analisi di due *case study*, *IBM* e *Amazon*, per valutare le strategie di adeguamento e le problematiche incontrate

nell'applicazione del regolamento. Questa tesi si propone, dunque, di valutare l'impatto concreto dell'AI Act sulle aziende operanti in Europa, fornendo una chiave di lettura che non solo evidenzia le opportunità derivanti da una regolamentazione chiara e strutturata, ma anche i potenziali ostacoli e le sfide connesse all'adeguamento normativo in un contesto tecnologico in continua evoluzione.

CAPITOLO PRIMO

L'Artificial Intelligence Act: principi e finalità

1.1 La necessità di regolamentazione

1.1.1. Definizione, funzionamento e applicazioni dell'IA

Negli ultimi anni, l'intelligenza artificiale è stata sicuramente una delle innovazioni più significative, rendendosi protagonista nello sviluppo di settori strategici come la sanità, l'amministrazione pubblica, la finanza e l'industria¹. L'elaborazione dei dati, la capacità di apprendere da essi e la produzione automatica di sintesi per il supporto alle decisioni sono le caratteristiche principali dell'intelligenza artificiale². Questa tecnologia, definita per la prima volta nel 1956 dall'informatico *John McCarthy* come "la scienza e l'ingegneria di costruire macchine intelligenti"³, nel tempo è divenuta sempre più importante, fino a rendere necessaria una regolazione. A livello normativo internazionale, lo standard ISO/IEC 42001:2023⁴ definisce l'IA come "la capacità di acquisire, elaborare, creare e applicare conoscenza, conservata sotto forma di modello, per svolgere uno o più compiti determinati". In altre parole, l'IA riguarda la capacità di un sistema di imparare, ragionare e prendere decisioni in modo autonomo, come un essere umano.

¹ European Commission, *Artificial Intelligence for Europe, Publications Office of the European Union*, 2018, p. 5.

² *Kaplan, J., Artificial Intelligence: What Everyone Needs to Know, Oxford University Press*, 2016, p. 25. Disponibile su: https://www.researchgate.net/publication/347667829_Artificial_Intelligence_What_Everyone_Needs_to_Know

³ *McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, AI Magazine*, 2006, vol. 27 n. 4, 12. Disponibile su: [1904-Article Text-1900-1 file:///C:/Users/utente/Downloads/1904-Article%20Text-1900-1-10-20080129%20\(1\).pdf-10-20080129 \(1\).pdf](file:///C:/Users/utente/Downloads/1904-Article%20Text-1900-1-10-20080129%20(1).pdf-10-20080129%20(1).pdf)

⁴ Nel 2023, l'Organizzazione internazionale per la standardizzazione ha introdotto la norma ISO/IEC 42001:2023 che affronta i problemi legati alla qualità, fornendo un quadro di riferimento che consente alle organizzazioni aziendali di stabilire un sistema di gestione della qualità ("Artificial Intelligence Management system - AIMS") che aiuta le organizzazioni stesse a prepararsi e a mantenere la compliance alle normative sull'AI esistenti e future. L'AIMS contribuisce a garantire un uso etico, la trasparenza, la responsabilità e il miglioramento continuo delle applicazioni di IA affrontando i rischi e le opportunità associati all'IA, promuovendo pratiche di IA standardizzate e regolamentate.

⁵ *The European House – Ambrosetti, AI 4 Italy: Impatti e prospettive dell'Intelligenza Artificiale Generativa per l'Italia e il Made in Italy*, settembre 2023, p.24. Disponibile su: <https://www.astrid-online.it/static/upload/ai-4/ai-4-italy-microsoft-report-2023-2023090109.pdf>fti-2023-Microsoft-Agosto.indb

L'intelligenza artificiale può essere classificata in base ai compiti che sa svolgere e al grado di replicazione della conoscenza umana. Per ognuna di queste due macro-categorie, l'analisi individua tre tipologie di AI⁵:

In base alla capacità di replicare l'intelligenza umana:

- *Narrow AI* (Intelligenza Artificiale ristretta) → Sistemi specializzati nell'esecuzione di un singolo compito (come gli assistenti vocali).
- *General AI* (Intelligenza Artificiale Generale) → Sistemi che si servono di abilità tipiche di quelle umane, in grado di apprendere e applicare conoscenze in realtà diverse.
- *Super AI* (Superintelligenza Artificiale) → Sistemi con capacità nettamente al di sopra di quelle dell'uomo, attualmente ipotetici e oggetto di ricerca.

In base ai compiti che sa svolgere:

- *Natural Language Processing* (NLP) → Tecnologie che comprendono e generano testo o audio (come i *chatbot* avanzati).
- *Computer Vision* → Algoritmi in grado di riconoscere e analizzare immagini e oggetti (es. sistemi di riconoscimento facciale).
- *Predictive Analytics* → Strumenti in grado di elaborare grandi quantità di dati per formulare previsioni (es. modelli di *credit scoring* bancario).

Sebbene il contributo dell'IA allo sviluppo economico sia evidente, il suo utilizzo ha sollevato problematiche di natura giuridica ed etica, rendendo necessaria l'adozione di una regolamentazione uniforme a livello europeo, al fine di garantire sicurezza, affidabilità e rispetto dei diritti fondamentali. In risposta a queste sfide, il 13 Marzo del 2024, l'Unione Europea ha approvato *l'Artificial Intelligence Act*, ovvero la prima normativa globale volta a disciplinare in maniera specifica l'intelligenza artificiale, con

l'obiettivo di affrontare problematiche quali l'autonomia crescente degli algoritmi, la scarsa trasparenza nei processi decisionali e le conseguenze socio-economiche di questa innovazione tanto promettente quanto complessa.

1.1.2 Rischi e opportunità

L'innovazione tecnologica recente, con l'utilizzo di sistemi di intelligenza artificiale e algoritmi studiati, costituisce un motore di crescita e sviluppo, favorendo l'ottimizzazione delle risorse, l'efficienza operativa e lo sviluppo economico. Tuttavia, il progresso attraverso tali strumenti, non è esente da rischi, in quanto solleva questioni di natura giuridica, etica ed economica. Considerando le opportunità insite nell'IA, vi è sicuramente l'integrazione di quest'ultima nei processi produttivi: le applicazioni dell'intelligenza artificiale possono contribuire ad una crescita della produttività lavorativa allo 0,1%-0,6% annuo fino al 2040, in base al tempo di adozione della tecnologia e redistribuzione del tempo dei lavoratori in altre attività⁶. Inoltre, in un'ottica di valorizzazione delle opportunità economiche e produttive, tali sistemi innovativi favoriscono l'emergere di servizi avanzati in settori quali *fintech* e *healthcare*. In riferimento a quest'ultimo, ad esempio, l'AI⁷ può essere utilizzata per realizzare immagini mediche, supportando i medici nella diagnosi precoce di patologie e personalizzazione delle cure⁸, mentre per la finanza digitale, le tecnologie digitali saranno applicate sempre di più alle attività finanziarie, come il *mobile banking* e pagamenti senza contatto⁹. Affinché tali opportunità risultino vantaggiose anche per il mercato del lavoro, è essenziale un adattamento delle competenze professionali e regolamentazione delle

⁶ Chui, M., Hazan, E., Roberts, R., Singla, A., Smaje, K., Sukharevsky, A., Yee, L., Zimmel, R., *The Economic Potential of Generative AI: The Next Productivity Frontier*, McKinsey Global Institute, giugno 2023, p. 15. Disponibile su: <https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontier.pdf>

⁷Artificial Intelligence, termine inglese per indicare l'Intelligenza Artificiale.

⁸Petricca R., Agenda Digitale, IA al servizio della salute: come cambiano diagnosi e cure, Network360, 11 luglio 2024. Disponibile su: IA al servizio della salute: come cam <https://www.agendadigitale.eu/sanita/ia-al-servizio-della-salute-limpatto-su-diagnosi-e-cure/biano-diagnosi-e-cure-Agenda-Digitale>

⁹Niketani S., *Artificial Intelligence in Digital Payments | The Future of Digital Wallets*, Nimble AppGenie, 11 febbraio 2025. Disponibile su: Artificial Intelligence in Digital Payments | The <https://www.nimbleappgenie.com/blogs/artificial-intelligence-in-digital-payments/e-Future-of-eWallets>

¹⁰ *World Economic Forum, Future of Jobs Report*, maggio 2023. Disponibile su: WEF_Future_of_Jobs_2023 https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf

nuove forme di impiego. Infatti, il 23% delle aziende globali prevede un aumento delle assunzioni in ruoli legati all'IA e non solo compiti ripetitivi verranno automatizzati ma saranno creati 69 milioni di nuovi posti lavorativi entro il 2027, con la crescente richiesta di nuove specializzazioni¹⁰. L'automazione intelligente, la riduzione del carico manuale e il miglioramento dell'efficienza operativa insieme a quello della qualità del lavoro, permettono una riallocazione delle risorse verso attività con maggior valore aggiunto. L'uso ottimale e regolato dell'intelligenza artificiale può condurre a benefici importanti anche nella pubblica amministrazione e nel campo della ricerca. Nell'ambito della pubblica amministrazione, l'IA è efficace nel migliorare i servizi pubblici, promuovere l'interazione con gli utenti e personalizzare i servizi, aumentando così la soddisfazione e la partecipazione dei cittadini¹¹. Per quanto riguarda la ricerca, i sistemi avanzati possono simulare processi scientifici complessi, riducendo la necessità di esperimenti fisici dispendiosi e lunghi¹². Nonostante le opportunità, l'adozione dei sistemi, deve essere accompagnata da norme che garantiscano un equilibrio tra innovazione e tutela dei diritti fondamentali dell'uomo¹³. In questo contesto emergono rischi quali mancanza di trasparenza, il cosiddetto “*black box problem*”¹⁴, *bias* algoritmici, *privacy* e sicurezza dei dati ed infine rischi legati all'impatto sul mercato del lavoro e sostituzione dei lavoratori. Per quanto riguarda la mancanza di trasparenza, occorre soffermarsi sul cosiddetto “*black box problem*”, ovvero “problema della scatola nera”. Ciò è collegato all'opacità degli algoritmi di intelligenza artificiale, attraverso i quali non è chiaro come le informazioni ed i dati vengano elaborati e dunque si arrivi ad un risultato/decisione, senza che l'utente

¹¹ Agenzia per l'Italia Digitale (AgID), Piano Triennale per l'Informatica nella Pubblica Amministrazione 2024–2026 – Strumento 5: Intelligenza Artificiale nella Pubblica Amministrazione, dicembre 2023, p. 5. Disponibile su: Piano triennale per l'info https://www.agid.gov.it/sites/agid/files/2024-06/piano_triennale_per_linformatica_nella_pa_2024-2026.pdf Informatica nella PA 2024-2026

¹² European Commission, *White Paper on Artificial Intelligence: A European approach to excellence and trust*, Publications Office of the European Union, 19 febbraio 2020, p. 5.

¹³ Floridi, L., *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford University Press, 2023.

¹⁴ Tale espressione nasce nell'ambito dell'ingegneria nel XX secolo ed indica sistemi complessi il cui il funzionamento intero non è direttamente osservabile, ma da cui si possono analizzare solo gli input e output.

¹⁵ Capacità di attribuire la responsabilità ai soggetti coinvolti nel ciclo di vita dell'IA dalla progettazione all'uso per gli esiti negativi del suo impiego.

¹⁶ Gibraltar Solutions, *Navigating the AI Black Box Problem*, 11 giugno 2024. Disponibile su: Navigating the AI Black Box Pro <https://gibraltarsolutions.com/blog/navigating-the-ai-black-box-problem/blem>

¹⁷ Gos M., Spridon S., *AI Bias in Credit & Loan Processing: Is AI Biased When Assessing Credit Worthiness?*, ITIMAGINATION, 2023. Disponibile su: AI Bias in Credit & Loan Processing: Is AI Biased When Assessing Credit Worthiness? <https://www.itmagination.com/blog/credit-loan-processing-ai-biased-when-assessing-credit-worthiness>

abbia la capacità di verificare i processi utilizzati. Tale problematica introduce il problema dell'*accountability*¹⁵, legato a sua volta ad un rischio legale ed etico, dal momento che le decisioni dei sistemi IA possono essere errate, discriminatorie o non contestabili¹⁶. L'*AI Act* tenta di garantire la trasparenza dei sistemi scontrandosi però con la loro complessità tecnica, rendendo la sicurezza delle informazioni un obiettivo non ancora del tutto realizzabile. Esempio pratico di questo problema si può riscontrare nel settore bancario, dove algoritmi di *credit scoring*, sono in grado di individuare con metodo statistico la probabilità di solvibilità di una persona, ovvero negare prestiti a particolari categorie di clienti senza un valido motivo¹⁷. A livello giuridico, è cruciale comprendere che ciò comporta la violazione dei diritti dell'uomo. Un altro profilo di rischio che l'*AI Act* cerca di mitigare è rappresentato dalla duplicazione e/o amplificazione degli algoritmi esistenti, attraverso il controllo dei dati relativi all'addestramento dei sistemi IA e la valutazione dei rischi associati. Tale criticità, nota come "*bias algoritmico*"¹⁸ può causare gravi incongruenze nell'erogazione dei servizi pubblici, processi usati dalle risorse umane ed in ambito giudiziario, penalizzando determinati gruppi sociali, a discapito di altri. Nel dibattito sui rischi legati all'intelligenza artificiale, una delle tematiche che assume primaria importanza riguarda la gestione dei dati da parte di governi e di grandi imprese, dove vengono raccolte ed elaborate quantità enormi di informazioni personali. Tali attività fanno emergere interrogativi sul rispetto della *privacy*, sulla sicurezza delle informazioni in particolare di quelle più sensibili attinenti alla sfera privata degli utenti¹⁹. In merito, studi della sociologa statunitense *Shoshana Zuboff*, evidenziano come l'IA consolidi un modello economico di sorveglianza pervasiva, dove il crescente utilizzo di algoritmi predittivi, rischia di compromettere le libertà fondamentali dei cittadini, trasformando questi ultimi in meri fornitori di dati per scopi a loro non chiari o noti²⁰. In questo scenario, l'*AI Act* interviene limitando, ad esempio, l'uso di sistemi di

¹⁸ Distorsione sistematica nei risultati prodotti da un algoritmo, causata da pregiudizi presenti nei dati utilizzati per addestrarlo, nelle modalità di progettazione o nelle scelte effettuate durante la sua implementazione. *Barocas, S., Hardt, M., & Narayanan, A., Fairness and Machine Learning: Limitations and Opportunities, Fairness and Machine Learning LLC, 2019.*

¹⁹ Garante per la Protezione dei Dati Personali, *Web scraping ed intelligenza artificiale generativa: nota informativa e possibili azioni di contrasto*, 20 maggio 2024. Disponibile su: <https://www.gpdp.it/documents/10160/0/Web+scraping+ed+intelligenza+artificiale+generativa+-+nota+informativa+e+possibili+azioni+di+contrasto.pdf/40b4600c-80f5-a3ce-a74e-604a8e88e601?version=4.0c-80f5-a3ce-a74e-604a8e88e601>

²⁰ *Zuboff S., "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", Public Affairs, 2018.*

riconoscimento facciale negli spazi comuni e imponendo requisiti di trasparenza specifici. L'evoluzione di tecnologie così complesse non incide solo sulla *privacy* ma anche nel mercato del lavoro. Se da un lato, entro il 2027 si prevede la creazione di circa 69 milioni di nuovi posti di lavoro legati all'IA, dall'altro si stima che 83 milioni di posti potrebbero essere eliminati a causa dell'automazione, rendendo necessario un intervento tempestivo per evitare squilibri occupazionali²¹. La sostituzione dei lavoratori non riguarda solo l'industria, ma anche settori professionali ampiamente specializzati come quello finanziario, legale e sanitario. Questo fenomeno rischia di accrescere le disuguaglianze sociali, creando un divario tra chi possiede competenze precise legate all'IA e chi invece rischia di rimanere escluso poiché non formato sull'argomento. I rischi sopra delineati evidenziano le difficoltà di interazione tra le dimensioni della realtà quotidiana e la prospettiva di cambiamento che si verrà a creare con un sempre maggiore impiego dell'IA in tutti gli ambiti. A riguardo, il filosofo italiano Luciano Floridi, professore di etica dell'informazione presso l'Università di *Oxford*, definisce la realtà odierna "Infosfera", uno spazio digitale in cui gli esseri umani, le tecnologie e i sistemi di informazione cooperano continuamente, fino ad arrivare ad un punto in cui il confine tra mondo fisico e digitale è sempre più sfumato, e conseguentemente più complicato da gestire e da regolare²².

1.1.3 Evoluzione normativa a livello europeo

Alla luce delle opportunità e dei rischi precedentemente esaminati, risulta ormai imprescindibile un intervento regolatorio strutturato, che al contempo garantisca la tutela dei diritti fondamentali dell'individuo e l'innovazione tecnologica. Di conseguenza, per l'impiego responsabile dell'intelligenza artificiale, l'Unione Europea si è distinta come la prima realtà giuridica al mondo a intervenire con una disciplina organica e vincolante, armonizzata. Diverse fasi hanno caratterizzato l'evoluzione di tale disciplina normativa,

²¹ *World Economic Forum, "Future of Jobs Report", op.cit.*

²² Floridi L., *"The Fourth Revolution: How the Infosphere is Reshaping Human Reality"*, Oxford University Press, 2014. Disponibile su: https://issc.al.uw.edu.pl/wp-content/uploads/sites/2/2022/05/Luciano-Floridi-The-Fourth-Revolution_-How-the-infosphere-is-reshaping-human-reality-Oxford-University-Press-2014.pdf Fourth Revolution: How the Infosphere Is Reshaping Human Reality

²² Insieme di norme, principi, linee guida, raccomandazioni o codici di condotta che, pur non essendo giuridicamente vincolanti, esercitano un'influenza rilevante sul comportamento degli attori pubblici e privati. Della Cananea G., *Diritto amministrativo europeo, Il Mulino, Bologna, 2020, p. 134.*

inizialmente caratterizzata da raccomandazioni etiche ed emendamenti di *soft law*²³ fino ad arrivare all'*Artificial Intelligence Act*.

Il presente paragrafo si pone l'obiettivo di ripercorrere, servendosi di un approccio cronologico e sistematico, le tappe fondamentali che hanno condotto l'Unione Europea alla formulazione dell'AI Act.

Il primo passo concreto verso una regolazione autonoma dell'intelligenza artificiale è avvenuto nel 2018. Nell'aprile di questo anno, l'Unione Europea, attraverso la Comunicazione della Commissione "*Artificial Intelligence for Europe*"²⁴, ha segnato l'avvio di un percorso normativo incentrato su IA etica, sicura e conforme ai diritti dell'uomo, inizialmente attraverso la *soft law*. L'atto individua le seguenti tre priorità:

- Stimolare gli investimenti pubblici e privati;
- Preparare il mercato del lavoro alle trasformazioni digitali;
- Garantire un quadro giuridico affidabile.

Nel 2018 è stato pubblicato il Piano Coordinato sull'IA²⁵ per massimizzare il potenziale dell'Europa di competere a livello mondiale, definire azioni e strumenti di finanziamento per l'adozione dell'IA in tutti i settori, incoraggiare gli Stati membri a sviluppare le proprie strategie nazionali.

Su queste basi, il processo di regolazione è continuato nel 2019 sotto la supervisione di un gruppo di esperti indipendenti sull'IA *High-Level Expert Group on Artificial Intelligence* (HLEG), che tenendo conto di un orientamento più strutturato e caratterizzato da un taglio operativo, politico, etico e morale ha prodotto le linee guida per l'etica e l'affidabilità dei sistemi²⁶. L'obiettivo delle linee guida rimaneva quello di garantire che l'adozione dell'intelligenza artificiale fosse compatibile con i valori dell'Unione, delineando così diversi requisiti, che ancora oggi si trovano al centro del dibattito sociale

²⁴ Commissione Europea, Comunicazione *Artificial Intelligence for Europe*, COM(2018) 237 final, Bruxelles, 25 aprile 2018.

²⁵ Commissione Europea, Comunicazione *Piano Coordinato per l'IA* COM(2018) 795 final, Bruxelles, 7 dicembre 2018.

²⁶ *High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, A DEFINITION OF AI: MAIN CAPABILITIES AND DISCIPLINES Definition developed for the purpose of the AI HLEG's deliverables*, Commissione Europea, Aprile 2019. Disponibile su: [a_definition_of_ai_-_en_37CE316A-F727-A512-2B30CA76D7484_file:///C:/Users/utente/Downloads/a_definition_of_ai_-_en_37CE316A-F727-A512-2B30CA76D7484D66_60651.pdf](file:///C:/Users/utente/Downloads/a_definition_of_ai_-_en_37CE316A-F727-A512-2B30CA76D7484_file:///C:/Users/utente/Downloads/a_definition_of_ai_-_en_37CE316A-F727-A512-2B30CA76D7484D66_60651.pdf)

in materia di tecnologie intelligenti e predittive, come il controllo umano delle decisioni, la sicurezza dei sistemi, la *privacy*, la trasparenza nei processi decisionali e le responsabilità degli autori. Tali requisiti rispettano la Carta Fondamentale dei Diritti dell'uomo²⁷, perfettamente coerenti con i 3 requisiti dell'IA, ovvero:

- 1) Legalità (conformità alle direttive europee e nazionali);
- 2) Eticità (rispetto dei principi etici);
- 3) Robustezza tecnica e sociale (affidabilità sia in senso ingegneristico che sociale).

Le linee guida sottolineano inoltre che la fiducia dei cittadini è cruciale per l'accettazione dell'Intelligenza Artificiale ed il suo uso consapevole.

Conclusa la fase etico-programmatica del 2019, la Commissione Europea ha avviato nel 2020 una riflessione più completa sul ruolo dell'Intelligenza Artificiale, chiaramente rappresentata dalla promulgazione del Libro Bianco²⁸, documento che segna la transizione dalla *soft law* verso una disciplina giuridica vincolante (*hard law*). Attraverso tale atto, l'Unione Europea, ha iniziato a riconoscere il potenziale delle tecnologie intelligenti in settori quali sanità, istruzione, sicurezza e giustizia con lo scopo di rafforzare la sovranità tecnologica in tutti i contesti economici e sociali. Tra gli obiettivi primari, vi è quello di evitare la frammentazione normativa tra gli Stati Membri e la creazione di sistemi intelligenti antropocentrici, rispettando l'etica ma anche garantendo l'innovazione, soprattutto in un mondo dominato da potenze come Stati Uniti e Cina. Come si legge nel Libro Bianco del 2020: "L'Europa possiede tutto il necessario per diventare un *leader* mondiale nel campo dell'intelligenza artificiale, dal talento alle istituzioni di ricerca, fino a un mercato unico forte e a un apparato normativo consolidato".

La Commissione nel 2021 ha aggiornato il Piano coordinato sull'IA²⁹ che si propone principalmente di accelerare gli investimenti pubblici e privati, nelle tecnologie IA per stimolare la ripresa economica (*post-covid*), allineare la politica in materia di IA per

²⁷ Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza il 7 dicembre 2000 e adattata a Strasburgo il 12 dicembre 2007, GUUE C 326 del 26 ottobre 2012.

²⁸ Commissione Europea, Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, COM(2020) 65 final, Bruxelles, 19 febbraio 2020.

²⁹ Commissione Europea, Comunicazione *Promuovere un approccio europeo all'intelligenza artificiale*, COM(2021) 205 final, Bruxelles, 22 aprile 2021.

evitare la frammentazione all'interno dell'UE e sviluppare competenze digitali per permettere ai cittadini o alle imprese di acquisire sempre più consapevolezza sul tema, e attuare tempestivamente strategie per garantire che l'UE massimizzi i vantaggi derivanti dall'adozione precoce.

La fase legislativa vincolante, la vera e propria *hard law*, è iniziata il 21 Aprile 2021, quando la Commissione Europea, propone il regolamento sull'IA³⁰ e da avvio quindi all'iter legislativo verso *l'Artificial Intelligence Act*, caratterizzato da negoziati continui tra il Parlamento Europeo e il Consiglio. La scelta dello strumento di regolamento è data dalla volontà dell'Unione Europea di creare un mercato unico digitale, evitando frammentazioni giuridiche che ne possono ostacolare la creazione. L'architettura proposta, è stata concepita come orizzontale, ovvero che si può adattare a tutti gli scenari economici e sociali in cui è presente l'intelligenza artificiale, a prescindere dal contesto d'uso specifico. Una riduzione della settorialità e l'anticipazione dell'evoluzione di tecnologie digitali sono i risultati di tale proposta di regolamento. Quest'ultima inoltre nasce come partecipativa, ovvero è frutto di un processo lungo di consultazione pubblica, con il coinvolgimento di attori istituzionali, privati ed enti di ricerca. Non proviene sicuramente da una tecnica-legislativa *top-down*, in cui le norme vengono decise "dall'alto" senza un coinvolgimento preliminare. La modalità partecipativa ha reso possibile l'integrazione di vari punti di vista e modifiche successive in maniera flessibile. Infine, oltre all'armonizzazione della legge, il criterio fondante dell'intervento legislativo europeo, è quello del *risk based approach*, ovvero un approccio regolatorio che designa obblighi e tutele in base al grado di rischio di una particolare attività o questione e permette di adattare misure di sicurezza a problemi specifici³¹.

Dopo oltre due anni di intense trattative, il 9 Dicembre 2023 le istituzioni europee hanno raggiunto un accordo sul contenuto definitivo *dell'Artificial Intelligence Act*. L'intesa è stata un passaggio fondamentale verso il regolamento ufficiale dell'IA. Questo accordo politico è noto come "intesa in fase di trilogia", ovvero un negoziato tra Parlamento Europeo, Consiglio e Commissione che ha l'obiettivo di trovare un compromesso sul

³⁰ Commissione Europea, Proposta di regolamento che stabilisce regole armonizzate in materia di intelligenza artificiale (*Artificial Intelligence Act*), COM(2021) 206 final, Bruxelles, 21 aprile 2021.

³¹ EU AI Act: *Key issues Risk Based Approach, holistic AI*. Disponibile su: <https://www.euaiact.com/key-issue/3>

testo legislativo proposto³². Tale intesa non ha efficacia giuridica ma serve solo a consolidare l'accordo che soltanto in seguito verrà approvato da Parlamento e Consiglio nei loro iter decisionali. In particolare, quello del Parlamento terminò il 13 marzo del 2024, data in cui quest'ultimo approvò il contenuto definitivo dell'AI Act, tramite un regolamento che confermò l'orientamento dell'Unione Europea verso l'adozione dell'Intelligenza Artificiale in maniera responsabile, evidenziando la classificazione dei sistemi di IA in base al livello di rischio e imponendo obblighi per garantire la sicurezza e i diritti fondamentali. L'iter normativo verrà completato in seguito, il 21 maggio 2024, grazie all'approvazione dell'adozione definitiva del regolamento anche del Consiglio. Infatti, questa è l'ultima fase della procedura di codecisione, come sancito anche dall'articolo 294 del Trattato sul funzionamento dell'Unione Europea (TFUE)³³, e ne sancisce il carattere di norma vincolante immediatamente applicabile negli ordinamenti degli Stati membri. L'*Artificial Intelligence Act* è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 12 luglio del 2024 ed entrato ufficialmente in vigore, seppur con applicazione graduale, il 1 agosto del 2024³⁴. Dal 1° febbraio 2025 saranno vietati alcuni sistemi ad alto rischio, come quelli basati sulla manipolazione comportamentale o sul *social scoring*, mentre a partire dal 1 agosto 2026 entreranno in vigore gli obblighi più stringenti per i fornitori e gli utilizzatori di sistemi di intelligenza artificiale ad alto rischio, come previsto dal titolo III del regolamento. In sintesi, l'evoluzione normativa dell'AI Act ha seguito un percorso graduale ma determinato, passando dalla *soft law* arrivando ad un impianto giuridico vincolante (Regolamento) con efficacia per tutti gli Stati europei. Tale regolamento non si limita solo a stabilire regole tecniche, ma riflette i principi e i valori etici dell'Unione Europea. La proposta riflette tre grandi pilastri³⁵:

- Etica: centralità della persona e diritti fondamentali umani;
- Sostenibilità sociale e ambientale: servizi dell'AI a disposizione della collettività;

³² Parlamento europeo, Il processo legislativo ordinario: triloghi e negoziati interistituzionali, scheda sintetica sul funzionamento dei triloghi. Disponibile su: Procedura legislativa ordinaria | Parlamento europeo https://www.europarl.europa.eu/infographic/legislative-procedure/index_it.html

³³ Art. 294 TFUE, Trattato sul funzionamento dell'Unione europea, GUUE C 202 del 7 giugno 2016.

³⁴ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale, 13 giugno 2024.

³⁵ Floridi L., *Artificial Intelligence and the European Union's Artificial Intelligence Act — A Brief Ethical Evaluation*, in *Philosophy & Technology*, vol. 35, n. 3, 3 giugno 2021, pp. 411–417. Disponibile su: s13347-021-004 file:///C:/Users/utente/Downloads/s13347-021-00460-9.pdf60-9.pdf

- Sovranità digitale europea: L'Europa è la prima ad adottare una tale legge e ciò rappresenta una forma di *leadership* normativa. Questo concetto viene descritto in dottrina come "*Brussels Effect*"³⁶, espressione coniata dalla professoressa *Anu Bradford* della *Columbia Law School*, e indica la capacità dell'Unione Europea di influenzare la normativa globale attraverso l'imposizione di *standard* nel proprio mercato interno. In questo modo, il diritto europeo diviene riferimento anche per operatori economici extraeuropei, seppur in assenza di un accordo internazionale standardizzato e specifico. Così tutte le aziende extraeuropee si trovano a dover rispettare regole precise per poter accedere al mercato unico europeo, anche se geograficamente non sono presenti all'interno di esso.

1.2 AI Act: struttura e obiettivi

Il regolamento (UE) 2024/1689, rappresenta un quadro normativo vincolato, pensato per garantire una regolazione efficace dell'intelligenza artificiale in Europa. L'approccio utilizzato è definito come orizzontale e tecnologicamente neutrale. Per quanto riguarda il primo termine, il regolamento non è settoriale, quindi non si applica solo ad un ambito specifico come la finanza, la sanità o il commercio ma è pensato per applicarsi trasversalmente a tutti i contesti in cui è usata l'IA. D'altro canto, è considerato tecnologicamente neutrale perché non fa distinzione tra le tecnologie utilizzate (*machine learning*³⁷, *deep learning*³⁸, logiche simboliche ecc...) ma si concentra sulla funzionalità e sui rischi del sistema, a prescindere dalla tecnologia utilizzata per svilupparlo. Il testo normativo dell'AI Act si compone di 113 articoli, suddivisi in 12 titoli e accompagnato da 13 allegati tecnici, che specificano dettagli operativi. Ciascun titolo, affronta una dimensione distinta della regolamentazione: viene definito in apertura l'ambito di applicazione e le nozioni fondamentali, per poi introdurre un elenco di pratiche vietate, e

³⁶ *Bradford A., The Brussels Effect: How the European Union Rules the World, Oxford University Press, 5 ottobre 2021. Disponibile su: The Brussels Effect - Paperback <https://global.oup.com/academic/product/the-brussels-effect-9780190088651?cc=it&lang=en&k> - Anu Bradford - Oxford University Press*

³⁷ E' chiamato anche apprendimento automatico, ed è un ramo dell'intelligenza artificiale che si focalizza sull'insegnare ai computer ad imparare dai dati senza essere esplicitamente programmati. In pratica, il Machine Learning consente ai sistemi informatici di migliorare le proprie prestazioni nel tempo, adattandosi a nuovi dati ed esperienze.

³⁸ E' un metodo di intelligenza artificiale che insegna ai computer ad elaborare i dati seguendo una modalità ispirata al cervello umano. I modelli di deep learning possono riconoscere immagini, testi, suoni e altri schemi di dati complessi per produrre approfondimenti e previsioni accurati.

regolare in maniera differenziata i sistemi in base al livello di rischio. Le disposizioni contenute nei titoli finali, disciplinano obblighi per gli operatori economici, i criteri di trasparenza, la sorveglianza del mercato, le autorità di controllo e le sanzioni, delineando un quadro giuridico uniforme e valido per tutti gli Stati Membri. In coerenza con l'approccio neutro adottato, l'AI Act, introduce una definizione unica di "sistema di intelligenza artificiale", senza concentrarsi su singole metodologie. Ai sensi dell'articolo 3 del Regolamento (UE) 2024/1689, il sistema di IA è definito come:

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

L'articolo 1 del Regolamento AI Act, definisce lo scopo del regolamento stesso che intende migliorare il funzionamento del mercato interno, promuovendo un utilizzo sicuro e affidabile dell'intelligenza artificiale. Il regolamento mira inoltre a tutelare i diritti fondamentali sanciti dalla Carta dei diritti, tra cui la democrazia, lo Stato di diritto, e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e promuovendo l'innovazione.

1.2.1. Classificazione dei sistemi AI e livelli di rischio

Il rischio rappresenta uno degli elementi che distingue l'AI Act rispetto ad altre discipline settoriali. Di conseguenza, gli articoli 5, 6 e 52 del Regolamento riguardano la classificazione dei sistemi di IA. In particolare, l'articolo 5 fa riferimento ai sistemi di IA vietati, l'articolo 6 classifica i sistemi ad alto rischio mentre il 52 sottolinea gli obblighi di trasparenza per sistemi con finalità generali, in particolare quelli a rischio limitato, che presentano obblighi minimi, come informare l'utente che si sta relazionando con un'IA. Il Regolamento definisce quattro livelli di rischio principali, disposti secondo una gerarchia crescente in termini di impatto potenziale. Tale classificazione, descritta dagli articoli sopra citati, è strutturata come segue:

- Sistemi a rischio inaccettabile

I sistemi di intelligenza artificiale considerati con un livello di rischio inaccettabile, come sottolineato dall'articolo 5, sono completamente vietati. Essi non possono essere

commercializzati né impiegati in Europa, poiché sono ritenuti in contrasto con i diritti fondamentali dell'Unione. Un esempio sono i sistemi che usano tecniche manipolative in maniera dolosa per distorcere il comportamento degli individui, quelli che utilizzano il *social scoring*³⁹ per attribuire punteggi sociali alle persone fisiche con effetti pregiudizievoli, i sistemi che caratterizzano a livello biometrico le persone al fine di dedurre caratteristiche sensibili come l'opinione politica o le origini. Inoltre, sono presenti in tale categoria anche le tecnologie *web scraping*⁴⁰, ovvero quelle che creano banche dati biometriche attraverso la raccolta di immagini da internet o videosorveglianza in modo indiscriminato. E' vietata anche qualsiasi intelligenza che sfrutta la vulnerabilità legata all'età, alla condizione sociale o a situazioni di disabilità della persona fisica. L'uso di sistemi che consentono il riconoscimento biometrico a distanza in tempo reale ed in luoghi pubblici, è permesso soltanto in casi eccezionali alle forze dell'ordine. La profilazione discriminatoria, sorveglianza invasiva e classificazione biometrica illegittima ledono fortemente i diritti base dell'umanità come la sicurezza, la libertà e la dignità.

- Sistemi ad alto rischio

La lista dei settori nei quali un sistema di intelligenza artificiale è classificato come ad alto rischio è contenuta nell'Allegato III del Regolamento (UE) 2024/1689, il quale rappresenta una parte integrante e vincolante dell'impianto normativo, soggetta a eventuali aggiornamenti tramite atti delegati della Commissione. I settori ritenuti ad alto rischio, poiché coinvolgono ambiti ad elevata sensibilità sociale o giuridica, sono elencati nell'Allegato III e includono:

- Biometria e identificazione (es. riconoscimento facciale)
- Infrastrutture critiche (trasporti, energia, reti digitali)
- Istruzione e formazione professionale
- Occupazione, gestione delle risorse umane
- Accesso a servizi essenziali e benefici pubblici
- Forze dell'ordine e prevenzione dei reati

³⁹ Sistema che valuta le persone sulla base del loro comportamento sociale o personale, assegnando punteggi che possono incidere sull'accesso ai servizi.

⁴⁰ Tecnica automatizzata che consente di estrarre dati da siti web, spesso senza il consenso degli utenti o dei titolari del sito, sollevando rilevanti questioni di privacy e protezione dei dati personali.

- Gestione della migrazione, asilo e controllo delle frontiere
- Amministrazione della giustizia e processi democratici

Esempi concreti di sistemi ad alto rischio sono quelli che profilano persone fisiche. Possono essere i sistemi di concessione di prestiti bancari, come software di *credit scoring* che possono escludere in maniera ingiustificata il soggetto dall'accesso al credito, oppure algoritmi che analizzano i *curriculum* per determinare chi selezionare. Entrambe, potrebbero riscontrare il rischio di discriminazione di genere, etnia o età⁴¹. Inoltre anche i sistemi utilizzati nella giustizia predittiva possono rappresentare un alto rischio, in quanto usano algoritmi misure cautelari o pene, il che può ledere il diritto ad un processo equo oppure presentare pregiudizi nella valutazione⁴².

Per tali motivi, negli articoli 16-29 del Regolamento AI Act vengono elencati i requisiti di sicurezza e conformità per i fornitori e gli utenti di sistemi considerati ad alto rischio. Tra questi risultano di particolare importanza i seguenti:

1) Qualità dei dati e governance dei dati (Art. 10)

I set di dati tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico ambito geografico, contestuale, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

2) Sistema di gestione dei rischi (Art. 9)

Il sistema di gestione dei rischi è inteso come un processo iterativo continuo pianificato per analizzare, documentare e mitigare i rischi associati alle tecnologie lungo l'intero ciclo di vita, che richiede un riesame e un aggiornamento costante e sistematico.

3) Documentazione tecnica (Art. 11)

⁴¹ Dal Lago D., *Bias e Discriminazione negli Algoritmi: Come Riconoscerli e Prevenirli*, LinkedIn Plus, 13 febbraio 2025. Disponibile su: (18) Bias e Dis [https://www.linkedin.com/pulse/bias-e-discriminazione-negli-algoritmi-come-diego-dal-lago-zl4ff/criminazione negli Algoritmi: Come Riconoscerli e Prevenirli | LinkedIn](https://www.linkedin.com/pulse/bias-e-discriminazione-negli-algoritmi-come-diego-dal-lago-zl4ff/criminazione%20negli%20Algoritmi:%20Come%20Riconoscerli%20e%20Prevenirli%20|%20LinkedIn)

⁴² Sorrentino C., *Giurimetria e Giustizia predittiva: intelligenza artificiale e Legal tech*, *Diritto.it*, 26 luglio 2023. Disponibile su: *Giurimetria e Giustizia predittiva: inte* [https://www.diritto.it/giurimetria-giustizia-predittiva-i-a-legaltech/lligenza artificiale e Legal tech](https://www.diritto.it/giurimetria-giustizia-predittiva-i-a-legaltech/lligenza%20artificiale%20e%20Legal%20tech)

Ha il compito principale di dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti fornendo le informazioni necessarie per valutarne la conformità ai requisiti stessi.

4) Registrazione presso il database europeo (Art. 71)

Obbligo di notificare il sistema AI agli organi preposti prima della commercializzazione.

5) Marcatura CE (Art. 71)

Prima di immettere sul mercato un sistema di IA ad alto rischio, gli importatori e/o i distributori verificano che esso rechi la necessaria marcatura CE del produttore, che sia accompagnato da una copia della dichiarazione di conformità UE e dalle istruzioni per l'uso.

6) Trasparenza e fornitura di informazioni agli utenti (Art. 13)

I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire a vari *users*⁴³ di interpretare l'output del sistema e utilizzarlo adeguatamente.

7) Sorveglianza umana (Art. 14)

I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina per essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali.

8) Robustezza, accuratezza e cybersicurezza (Art. 15)

⁴³ Una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.

L'articolo 15 dell'AI Act impone obblighi stringenti per garantire l'accuratezza, robustezza e cibersecurity dei sistemi di IA classificati come ad alto rischio. Tali sistemi devono essere progettati per mantenere prestazioni affidabili durante l'intero ciclo di vita. La normativa richiede la dichiarazione esplicita dei livelli di accuratezza nelle istruzioni d'uso, l'adozione di misure per prevenire guasti e feedback distorti e l'implementazione di soluzioni di ridondanza tecnica. Inoltre, devono essere previste misure di difesa contro attacchi informatici, come il *data poisoning*⁴⁴ e gli esempi antagonisti. La Commissione promuove lo sviluppo di metodologie comuni per valutare queste prestazioni, coinvolgendo varie autorità.

Tale struttura normativa, risultato non solo di tecnicità ma anche di una classificazione settoriale, riflette la volontà dell'Unione di assicurare un equilibrio tra innovazione e protezione dei diritti fondamentali.

Oltre alla definizione normativa e agli obblighi tecnici, l'AI Act introduce una definizione rilevante per le diverse figure coinvolte nell'uso di questi sistemi. In particolare, l'articolo 3 distingue tra fornitori (*providers*), che sviluppano e inseriscono nel mercato il sistema e gli utilizzatori (*deployers*) che utilizzano i sistemi. Tale distinzione è fondamentale nella responsabilità operativa. Le disposizioni presenti negli articoli 16-29 si applicano principalmente ai fornitori, ma alcuni come la supervisione umana o gestione dei *log* di sistema⁴⁵, anche agli utilizzatori. Il fornitore è colui che, come disposto dall'articolo 61 dell'AI Act, deve monitorare il comportamento del sistema, correggere preventivamente eventuali rischi o problematiche e aggiornare la documentazione tecnica periodicamente. La costanza nel monitoraggio è fondamentale per garantire un uso sicuro dell'intelligenza artificiale, dal momento che gli algoritmi presentano natura evolutiva, che possono modificare il loro comportamento nel tempo e causare effetti imprevisti e non

⁴⁴Tipo di attacco informatico in cui gli aggressori manipolano o corrompono i dati di training utilizzati per sviluppare modelli di machine learning o intelligenza artificiale.

⁴⁵ Un log di sistema è una registrazione cronologica degli eventi che accadono in un sistema operativo, come avvisi, arresti, errori, avvisi e modifiche al sistema. I log sono essenziali per il monitoraggio della salute e del funzionamento del sistema, permettendo agli amministratori di sistema di identificare e risolvere problemi rapidamente.

recuperabili se gestiti male. Inoltre, in una realtà di innovazione continua, è importante analizzare cosa può essere adattato e cosa deve essere rivalutato.

Essendo i sistemi intelligenti ad alto rischio molto sensibili, il Regolamento in materia prevede anche una clausola di salvaguardia volta a evitare che l'impiego di modelli pre-addestrati comporta una implementazione parziale dei requisiti per i sistemi più rischiosi. Quindi se un modello di intelligenza artificiale generale (*General AI*) viene introdotto in un sistema ad alto rischio, quest'ultimo comunque dovrà attenersi a tutti gli obblighi previsti dall'allegato III del Regolamento, e più approfonditamente a quelli previsti dalle Autorità di notifica di cui all'articolo 28 del testo.

- Sistemi a rischio limitato

Al di sotto della soglia ad alto rischio, la Commissione Europea ha individuato dei sistemi con rischio limitato. Secondo l'AI Act sono sistemi che interagiscono direttamente con le persone, influenzandone le scelte o generando contenuti che potrebbero essere scambiati come umani. Il diritto principale dell'utente in queste situazioni è quello di sapere che si sta relazionando con l'intelligenza artificiale. A disciplinare l'uso di sistemi a rischio limitato è l'articolo 52 del Regolamento. Esso dispone che l'utente venga chiaramente avvisato che il contenuto in questione è:

- generato da IA;
- manipolato con *deepfake*⁴⁶;
- chiaro, tempestivo ed affidabile.

Tali obblighi non si configurano come tecnici o stringenti ma comunque rappresentano tutele minime di trasparenza, quindi sono soltanto informativi, perché in questa categoria il livello di rischio è basso, ma persiste. Infatti, assumono sempre più rilevanza, soprattutto in un contesto in cui i contenuti realizzati attraverso l'uso di sistemi di IA proliferano con maggior frequenza. È fondamentale salvaguardare la fiducia degli utenti e prevenire inganni, anche involontari. Esempi di sistemi di intelligenza artificiale a rischio limitato sono assistenti virtuali nei servizi pubblici o

⁴⁶ Contenuti multimediali (video, audio o immagini) manipolati mediante tecniche avanzate di intelligenza artificiale, in particolare tramite algoritmi di deep learning, con l'obiettivo di far apparire persone che dicono o fanno cose che in realtà non hanno mai detto o fatto.

bancari, *chatbot* commerciali che simulano conversazioni umane, *software* generativi in ambito educativo e sistemi di raccomandazioni che influenzano le scelte del consumatore senza considerare i diritti individuali. Al contrario dei sistemi ad alto rischio, in cui è fondamentale la marcatura CE, questi non richiedono valutazione di conformità. Tuttavia, in alcuni casi, il rischio limitato può essere transitorio, ed un sistema apparentemente innocuo può diventare ad alto rischio in base al contesto d'impiego. Anche se non pericolosi, i sistemi che simulano l'umano devono dichiararsi come IA. La trasparenza nelle interazioni uomo-macchina rappresenta una condizione essenziale per assicurare che l'utente sia informato e in grado di esercitare consapevolmente i propri diritti digitali. Per supportare ciò, l'approccio europeo si fonda sul principio di proporzionalità, che consente di rendere flessibile la regolazione in base al livello di rischio presente e di ridurre i costi amministrativi per le imprese.

Infine, nonostante gli obblighi siano solo informativi, i soggetti restano giuridicamente responsabili in caso di violazioni della trasparenza o della concorrenza.

- Sistemi a rischio minimo o nullo

Per questa ultima categoria di sistemi a rischio minimo o nullo che non incidono sulla sicurezza degli individui né minacciano i diritti fondamentali dell'uomo, l'AI Act non prevede nessun obbligo informativo né tecnico né procedurale. In ottica di proporzionalità e promozione dell'innovazione, tenuto conto che tali sistemi si applicano a tante tecnologie molto diffuse, il legislatore europeo ha deciso di non inserire vincoli ulteriori per questa categoria. Esempi di sistemi a rischio minimo sono riconducibili a:

- Sistemi di ottimizzazione del traffico;
- Filtri *antispam*⁴⁷ nelle caselle di posta elettronica;
- Motori di ricerca interni nei siti *web*;
- Algoritmi per il suggerimento di video o *playlist* musicali.

Nonostante tali sistemi non compromettono la trasparenza e non sono né pericolosi né sensibili, l'AI Act comunque incoraggia a rispettare i codici di condotta relativi,

⁴⁷ Un filtro antispam è un meccanismo di sicurezza che aiuta a proteggere dalla posta indesiderata (spam) e potenzialmente pericolosa, spesso integrato in servizi di posta elettronica o in software di sicurezza.

autoregolamentazione, i certificati etici degli operatori e a garantire comunque l'affidabilità⁴⁸, oltre gli obblighi formali dell'Unione Europea.

Infine, un sistema di IA può essere aggiornato nel tempo dal momento che l'evoluzione tecnologica è in continua crescita e quindi anche i rischi, che non possono essere statici o rigidi, possono modificarsi comportando potenzialmente un salto del sistema nella classificazione in base al rischio (vedi grafico⁴⁹ di seguito).



1.2.2. Impatto sulle imprese e sulle tecnologie emergenti

Gli operatori economici coinvolti nello sviluppo sono sottoposti ad una serie di obblighi specifici presenti accuratamente nell'AI Act. Oltre a quelli già citati in precedenza, soprattutto per i sistemi ad alto rischio, il Regolamento si inserisce in un contesto molto più ampio che considera anche implicazioni etiche e reputazionali, oltre che giuridiche, nei processi aziendali. Considerando ciò, la Commissione Europea ha raccomandato alle imprese di adottare una *policy* interna aziendale in merito all'Intelligenza artificiale ben precisa soprattutto per la formazione del personale o le varie linee di controllo⁵⁰. Dopo l'entrata in vigore dell'AI Act, in Germania, la società di tecnologia medica *Siemens Healthineers*, ha integrato un sistema di controllo di qualità IA conforme ai requisiti di

⁴⁸I fornitori di sistemi ad alto rischio devono garantire un monitoraggio continuo del comportamento dei sistemi anche dopo la loro immissione sul mercato o messa in servizio, per individuare e affrontare tempestivamente eventuali rischi che emergano nel tempo. Tale previsione è cruciale per evitare effetti imprevisti derivanti dalla natura evolutiva degli algoritmi.

⁴⁹ Christakis T. e Karathanasis T., "Tools for Navigating the EU AI Act: (2) Visualisation Pyramid", MIAI, 7 marzo 2024. Disponibile su: Tools for Navigating the EU AI Act: (2) Visualisation Pyramid - MIAI

⁵⁰ Commissione Europea, "Domande e risposte: la legge sull'intelligenza artificiale dell'UE", 21 aprile 2021. Disponibile su: https://ec.europa.eu/commission/presscorner/detail/it/qanda_21_1683 Intelligenza artificiale — Domande e risposte

risk assessment, tracciabilità e supervisione umana (*white papers* aziendali⁵¹). I sistemi della Siemens sono classificati come aventi alto rischio, e nel rispetto della normativa, la società ha implementato un sistema di *compliance* su tre livelli: prevenzione, rilevamento e risposta. L'obiettivo è garantire informazioni chiare per tutti i dipendenti e gli utenti. Inoltre, trattandosi di impiego di sistema IA nel settore sanitario identificato ad alto rischio, è stato sviluppato un portafoglio di oltre 80 soluzioni basate sull'IA per risolvere diagnosi complesse e migliorare l'accuratezza nelle cure dei pazienti. Altri esempi di imprese sono Bosch nel settore automobilistico, H&M nella moda e Intesa San Paolo nel settore bancario. La Bosch, nel 2023 ha pubblicato un *AI Code of Ethics*⁵² e strumenti per *audit* interni in preparazione dell'entrata in vigore del Regolamento, mentre H&M ha modificato le interfacce *chatbot*⁵³ e i sistemi predittivi, introducendo avvisi automatici di interazione AI, rispettando l'articolo 52 del Regolamento che prevede, come citato in precedenza, l'obbligo informativo per chi utilizza i sistemi di IA. Inoltre, l'azienda ha dichiarato che userà un'iniziativa per creare gemelli digitali⁵⁴ di IA e applicarli nelle campagne di *marketing*⁵⁵. Un'altra grande realtà, Intesa San Paolo, già nel 2022 aveva preparato un progetto di *internal governance* sull'uso dell'IA nel *credit scoring* e *risk assessment*, che nel 2024, ha allineato al *framework* dell'AI Act⁵⁶. La banca ha adottato un approccio basato su quattro principi fondamentali:

- Comprensione (capacità di comprensione della decisione prodotta)
- Equità

⁵¹ Siemens Healthineers, *Medical Imaging in the Age of Artificial Intelligence*, 2021. Disponibile su: White-Paper_Artificial-Intelligence-in-Medical https://marketing.webassets.siemens-healthineers.com/1800000004384573/b4d5c4186b3f/White-Paper_Artificial-Intelligence-in-Medical-Imaging_1800000004384573.pdf - Imaging_1800000004384573.pdf

⁵² Bosch, *Code of Ethics for AI*, 19 febbraio 2020. Disponibile su: Cod <https://www.bosch-ai.com/industrial-ai/code-of-ethics-for-ai/e> of Ethics for AI | Bosch Center for Artificial Intelligence

⁵³ Innova, *Intelligenza artificiale e chatbot nel retail e digital marketing: migliorare l'engagement e il servizio clienti*. Disponibile su: Intelligenza artificiale <https://innova.ms/intelligenza-artificiale-e-chatbot-nel-retail-digital-marketing-migliorare-l-engagement-e-il-servizio-clienti/> e chatbot nel retail digital marketing: migliorare l'engagement e il servizio clienti - INNOVA

⁵⁴ Un gemello digitale è una rappresentazione virtuale di un oggetto, nel caso di specie un fotomodello/a, un sistema o un processo fisico, che viene aggiornata continuamente con dati in tempo reale provenienti da sensori e altre fonti.

⁵⁵ Casciabanca F., *"H and M lancia i cloni digitali dei suoi modelli per i social, Ninja Marketing*, 1 Aprile 2025. Disponibile su: H&M lancia i <https://www.ninja.it/modelli-digitali-di-hm-ai/>loni digitali dei suoi modelli - Ninja Business School

⁵⁶ Intesa San Paolo, *TCFD Report*, 2022. Disponibile su: TCFD <https://group.intesasanpaolo.com/content/dam/portalgroup/repository-documenti/sostenibilit%C3%A0/tcfd/tcfd-report-2022/TCFD%20Report%202022.pdf>port 2022.pdf

- Qualità dei dati
- Supervisione Umana (*Human in the Loop*)

Inoltre, recentemente Intesa San Paolo ha avviato una *partnership* con *Google Cloud* per migliorare la gestione del rischio dei sistemi IA e affrontarne lo sviluppo integrando in modo strutturale fin dalla fase progettuale del prodotto o servizio i requisiti della Regolamento. La banca ha anche aderito all'*AI Pact*⁵⁷, iniziativa della Commissione Europea che incoraggia le imprese o organizzazioni a pianificare strategie in anticipo per adattarsi alle misure del Regolamento, promuovendo nel miglior modo un'intelligenza artificiale affidabile.

La *policy* la dovrebbero adottare anche le imprese che non usano sistemi ad alto rischio, dal momento che consente di prevenire le violazioni e sviluppare una cultura di *compliance* dalle prime fasi di progettazione, tenendo conto anche delle raccomandazioni dell'*AI Act* in merito ai sistemi con rischio minimo e il carattere evolutivo e imprevedibile dell'innovazione tecnologica. Conseguentemente, se le imprese non procedono in questo modo, rischiano di trovarsi con tecnologie difficilmente aggiornabili tra pochi anni o non più utilizzabili. Tale rischio è definito come rischio di obsolescenza normativa, ed è fondamentale limitarlo tramite l'adozione di un principio "*compliance by design*", per il quale ogni soluzione deve tener conto sin dalla fase di progettazione dei requisiti normativi e quindi mantenere la validità nel tempo, nonostante i cambiamenti. Tale sfida è considerata una tra le più difficili da affrontare in merito alla regolazione dell'intelligenza artificiale, poiché fa riferimento alla capacità di prevedere l'evoluzione dell'innovazione tecnologica.

L'*AI Act*, disciplina l'impegno dell'Unione a garantire che l'innovazione non sia solo accessibile alle grandi imprese ma dedica una particolare attenzione alle piccole e medie imprese (PMI). Il 58% delle PMI è interessato al tema, grazie all'attenzione mediatica e allo sviluppo di un mercato di strumenti pronti all'uso e *low-cost*, ma solo il 7% delle piccole e il 15% delle medie imprese ha avviato progetti afferenti l'IA, tramite sviluppo interno o rivolgendosi a fornitori esterni⁵⁸. Per raggiungere un maggiore coinvolgimento

⁵⁷ Commissione Europea *AI Pact*. Disponibile su: <https://digital-strategy.ec.europa.eu/it/policies/ai-pact>

⁵⁸ La Repubblica, *Osservatorio Artificial Intelligence* Polimi: boom del mercato italiano, +58%, 1,2 miliardi di euro, 6 febbraio 2025. Disponibile su: *Osservatorio Artificial Intelligence* Polimi: boom del mercato italiano, +58%, 1,2 miliardi di euro - Economia e Finanza -

delle PMI, il Regolamento prevede l'utilizzo di *sandbox* normativi, ovvero ambienti controllati dove intermediari vigilati e operatori possono testare per un periodo di tempo limitato prodotti e servizi tecnologicamente innovativi. Vengono applicati principalmente nel settore *Fintech*⁵⁹, dove gli operatori finanziari, assicurativi o bancari operano in costante dialogo con le autorità di vigilanza, che in Italia, sono rispettivamente CONSOB, IVASS e Banca D'Italia, le quali possono attuare eventuali deroghe normative nella fase di sperimentazione. Oltre all'applicazione nel *Fintech*, un altro esempio è stato promosso in Francia dall'Inria (Istituto nazionale di ricerca per il digitale) che coordina il progetto "*PARTAGES*", selezionato nell'ambito del programma France 2030, con l'obiettivo di rendere l'intelligenza artificiale generativa disponibile per i professionisti della salute generando analisi automatiche di testi clinici⁶⁰. Questi progetti si stanno diffondendo anche in altri paesi dell'Unione dimostrando la flessibilità dell'AI Act.

In questa direzione, si inserisce anche il Capo VI del Regolamento, che prevede specifici strumenti per la sperimentazione. In particolare, oltre ai *sandbox* normativi, sono previsti canali di consulenza dedicati, linee guida pratiche e iniziative varie, non solo per garantire l'equità ma anche per evitare che la complessità normativa diventi una barriera troppo difficile da affrontare per soggetti emergenti (PMI e *start-up*). Per esempio, le *start up* potrebbero adottare *policy* interne di *governance* per l'utilizzo di strumenti di IA di terze parti.

Un altro articolo del Regolamento fondamentale da menzionare è l'articolo 56, il quale fa riferimento ai codici di condotta volontari. Oltre alle *policy* interne, obbligatorie per determinate categorie di rischio, le imprese con livelli di sensibilità inferiori sono comunque fortemente incoraggiate a seguire buone pratiche. In tale contesto, l'ufficio europeo per l'IA⁶¹ si occupa di coordinare la creazione delle linee guida, coinvolgendo fornitori di modelli, autorità e società civili. Inoltre, definisce obiettivi chiari e indicatori

https://finanza.repubblica.it/News/2025/02/06/osservatorio_artificial_intelligence_polimi_boom_del_mercato_italiano_+58percento_1_2_miliardi_di_euro-89/ Repubblica.it

⁵⁹ Insieme di innovazioni tecnologiche applicate ai servizi e prodotti finanziari.

⁶⁰ CNRS, *Démocratiser l'IA générative en santé : l'Etat, à travers France 2030, sélectionne le projet PARTAGES*, 27 novembre 2024. Disponibile su: <https://www.cnrs.fr/fr/presse/democratiser-lia-generative-en-sante-letat-travers-france-2030-selectionne-le-projet> CNRS

⁶¹ Commissione Europea, *European AI Office*. Disponibile su: <https://digital-strategy.ec.europa.eu/en/policies/ai-office>

di prestazione per garantire trasparenza e inclusione, ricevendo rapporti periodici sull'attuazione degli impegni e il rispetto delle regole.

1.3 Confronto tra regolazione europea e strategie internazionali

1.2.1 AI Act vs GDPR, Digital Services Act e Digital Markets Act

Nell'ambito del diritto digitale europeo, oltre il Regolamento sull'Intelligenza Artificiale sono presenti altre regolamentazioni. Il processo evolutivo è iniziato con la promulgazione del GDPR (*General Data Protection Regulation*), Regolamento (UE) 2016/679, che ha come tematica principale la protezione dei dati personali ed è entrato in vigore il 24 maggio del 2016, ma è divenuto pienamente applicabile il 25 maggio 2018. Ha sancito l'importanza della *privacy* e la tutela dei dati personali. Sempre nell'ottica di creare e continuare ad operare in un Mercato Unico Digitale, ovvero un mercato in cui vengono eliminati gli ostacoli alle transazioni *online* e le barriere commerciali tra Stati membri, al GDPR sono stati aggiunti due strumenti complementari: il *Digital Services Act* (DSA)⁶², Regolamento (UE) 2022/2065 e il *Digital Markets Act* (DMA)⁶³, Regolamento (UE) 2022/1925, entrambi pubblicati nella Gazzetta Ufficiale il 27 ottobre 2022 e pienamente operativi a partire dal 16 novembre del 2022. La necessità dei citati Regolamenti nasce principalmente per rispondere alle nuove dinamiche dell'economia digitale e regolamentare le grandi piattaforme *online*. Il presente paragrafo si propone di analizzare i punti di intersezione e divergenza tra i quattro strumenti normativi citati per avere una visione chiara della regolazione europea in materia di tecnologie digitali e intelligenza artificiale.

Come già sottolineato, i soggetti destinatari dell'AI Act sono i fornitori e gli utenti, operatori economici, ma anche enti pubblici, privati e principalmente i sistemi di IA ad alto rischio. I destinatari invece del GDPR sono diversi. La normativa si rivolge a:

- Titolari del trattamento: coloro che stabiliscono le finalità e i mezzi del trattamento come le aziende, enti pubblici o piattaforme principali;

⁶²Commissione Europea, Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali). Disponibile su: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065>

⁶³ Commissione Europea, Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), 14 settembre 2022.

- Responsabili del trattamento: soggetti terzi quali fornitori dei servizi informatici e delle tecnologie;
- Autorità di controllo: come il Garante della *privacy*⁶⁴.

Gli ambiti di applicazione dell'AI Act sono quello territoriale e oggettivo. L'ambito territoriale riguarda qualsiasi sistema IA che riesca a produrre effetti nel mercato interno, indipendentemente dal luogo in cui si è sviluppato (extra-territorialità) e l'ambito oggettivo riguarda l'immissione sul mercato di sistemi di IA, come precisato dall'articolo 2 del Regolamento. A differenza, di questo il GDPR disciplina come già citato in precedenza il trattamento dei dati personali, ovvero qualsiasi operazione effettuata su dati che identificano una persona fisica, da parte di soggetti pubblici o privati, stabiliti nell'UE o che trattano di cittadini, anche provenienti da paesi terzi. L'ambito di applicazione è settoriale ma di fatto si estende a qualsiasi area poiché i dati personali sono sempre necessari per identificare i soggetti giuridici nei diversi contesti.

Il *Digital Markets Act*, è un regolamento di natura concorrenziale, che ha l'obiettivo di limitare il potere delle grandi aziende nell'ecosistema digitale. Si applica ai seguenti soggetti:

- Coloro che hanno una forte posizione economica nel mercato europeo;
- Fungono da intermediari tra un gran numero di utenti commerciali e utenti finali.

La designazione di *gatekeepers*, ovvero quelle imprese, che per dimensione, potere di mercato e impatto sull'economia digitale possono esercitare una posizione di controllo strutturale sui mercati strategici influenzando la concorrenza in maniera significativa, avviene da parte della Commissione Europea, con rispetto degli articoli 3 e 4 del DMA. Secondo il Regolamento, un'impresa viene qualificata come *gatekeeper* se:

- Fornisce uno o più servizi di piattaforma di base quindi oltre ai *social networks* anche motori di ricerca o *market place online*;
- Ha un fatturato annuo significativo all'interno dell'Unione europea (superiore a 7,5 miliardi di euro negli ultimi 3 esercizi oppure una capitalizzazione di almeno 75 miliardi di euro);

⁶⁴ Regolamento (UE) 2016/679, GDPR, art. 4, parr. 7-8 e art. 51 ss.

- Ha come clienti più di 45 milioni di utenti finali mensili e 10.000 utenti aziendali attivi ogni anno nell'Unione Europea.
- Ha mantenuto i precedenti criteri quantitativi negli ultimi tre anni.

Dopo la designazione i *gatekeepers* sono tenuti a rispettare una serie di obblighi fondamentali, volti a evitare una serie di pratiche anticoncorrenziali. Tra questi vi sono:

- Divieto di pratiche di auto-preferenza (*self-preferencing*), che riguarda l'auto preferenza dei propri prodotti nei risultati di ricerca;
- Obbligo di garantire interoperabilità tra i propri servizi e quelli di terze parti, come ad esempio con sistemi di software e/o messaggistica;
- Condivisione dei propri dati non personali alle imprese concorrenti che ne fanno richiesta;
- Limitazione nella combinazione di dati raccolti per fornire il consenso all'utente;
- Facilitazione della portabilità dei dati e possibilità degli utenti di poter disinstallare le applicazioni.

Nel settembre 2023 i soggetti che la Commissione ha designato come *gatekeepers* sono: *Alphabet (Google), Amazon, Apple, Meta (Facebook e Instagram), Microsoft e ByteDance (TikTok)*. Tali aziende sono vincolate a rispettare le prescrizioni entro 6 mesi dalla designazione⁶⁵.

Il *Digital Services Act*, si applica a chiunque fornisca servizi digitali agli utenti, indipendentemente dalle sedi legali⁶⁶. L'applicazione viene definita più funzionale. Il regolamento distingue diversi destinatari:

- Motori di ricerca online;
- Servizi di *hosting (Cloud, archiviazione)*;
- Piattaforme *online*;
- Servizi di intermediazione di base (*mere conduit*⁶⁷, *caching*⁶⁸)

⁶⁵Commissione Europea, “*Digital Markets Act: Commission designates six gatekeepers*”, 6 settembre 2023.

⁶⁶ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali (Digital Services Act), articolo 3, GUUE L 277, 27.10.2022, p. 1–102.

⁶⁷ Trattasi di trasporto di segnali come il provider di internet o rete di telecomunicazione

⁶⁸ Memorizzazione temporanea per velocizzare l'accesso

- *Very Large Online Platforms* (VLOPs): piattaforme con almeno 45 milioni di utenti attivi mensilmente nell'Unione Europea.

Come si può notare, tra i quattro regolamenti vi è una sovrapposizione funzionale che comporta l'obbligo di rispettare tra i vari soggetti, come cittadini, imprese o enti, una conformità incrociata, valutata e adottata in base ai dati, alla tecnologia e all'ambito di applicazione. Ne deriva l'urgenza di adottare tecnologie intelligenti per poi elaborare una *compliance* sistemica.

Nel confronto emerge che i regolamenti in argomento hanno ambiti, obiettivi e finalità diversi. Le finalità del GDPR⁶⁹ sono quelle di tutelare i dati personali, minimizzare i rischi dei dati soprattutto in merito alla *privacy* e diritto alla spiegazione dei casi di decisioni automatizzate. Sicuramente le tematiche relative alla trasparenza e alla responsabilità dei processi sono in comune con le finalità dell'AI Act. Le finalità del *Digital Services Act* (DSA) e *Digital Markets Act* (DMA) riguardano: nel primo caso⁷⁰, assicurare il contrasto alla disinformazione *online*, rafforzare la trasparenza dei contenuti digitali e definire le responsabilità delle piattaforme per gestire il rischio e moderare i contenuti; mentre nel secondo caso prevenire gli abusi e la posizione dominante nei mercati digitali⁷¹.

Relativamente al requisito di trasparenza, entrambe i regolamenti sono parzialmente sovrapponibile con l'AI Act poiché nel primo caso si impone la trasparenza algoritmica dei sistemi predittivi e per la diffusione dei contenuti, mentre nel secondo caso per evitare che le società consolidino il vantaggio competitivo.

Si può notare come il legislatore europeo intende costruire una governance multi-livello, non solo per disciplinare le tecnologie ma garantire veri principi. Tale complementarità normativa, genera la cosiddetta *cross-regulatory compliance*: l'obbligo delle aziende, di operatori, di enti pubblici, di rispettare simultaneamente più regolamenti, spesso appartenenti a settori giuridici diversi, ma interconnessi tra loro⁷².

⁶⁹ Regolamento (UE) 2016/679, art. 1, GDPR.

⁷⁰ Regolamento (UE) 2022/2065, art. 1, Digital Services Act.

⁷¹ Regolamento (UE) 2022/1925, art. 1, Digital Markets Act.

⁷² Allio L., Delia R., Andres Amo P., *Multi-Level Regulatory Governance: Policies, Institutions and Tools for Regulatory Quality and Policy Coherence*, OECD Working Papers on Public Governance No. 13, OECD, 2009. Disponibile su: Multi-Level Regulatory Governance https://www.oecd.org/content/dam/oecd/en/publications/reports/2009/06/multi-level-regulatory-governance_g17a1cdc/224074617147.pdf (EN)

Gli approcci regolatori tra i vari regolamenti sono diversi. Se da un lato l'AI Act classifica i sistemi in base al rischio (*risk based approach*) consentendo una proporzionalità normativa, dall'altro il GDPR adotta un modello *principle-based* fondato su principi generali quali: la correttezza, trasparenza, liceità, e la limitazione per la conservazione dei dati⁷³. L'approccio regolatorio del DSA si basa su una combinazione di responsabilità:

- *Ex ante*: volte a prevenire determinati comportamenti, e quindi obblighi di valutazione del rischio, *audit*, trasparenza algoritmica;
- *Ex post*: volte a monitorare, correggere o sanzionare violazioni per contenuti illegali, oltre che intervenire per mancata moderazione.

Tale dualismo è dato dal fatto che il modello è di regolazione simmetrica e si applica a diversi tipi di piattaforme come VLOSEs⁷⁴, VLOPs, hosting e motori di ricerca.

Nell'approccio regolatorio del DMA, invece, sono presenti solo obblighi *ex ante* rigidi e precisi per i cosiddetti *gatekeepers*, volti a prevenire comportamenti anticoncorrenziali⁷⁵.

Da notare che la regolamentazione dell'AI Act, del GDPR e del DSA è orizzontale ovvero disciplina tutti i settori trasversalmente senza tener conto del tipo di operatore coinvolto mentre quella del DMA è verticale, perché si focalizza esclusivamente sulla categoria di soggetti economici particolarmente influenti.

L'efficacia di un quadro normativo dipende anche dai meccanismi di attuazione e controllo dello stesso. In particolare, la governance digitale utilizza un approccio decentralizzato nel caso del GDPR e un approccio centralizzato nel caso dell'AI Act, del DMA e del DSA. L'*enforcement* è cruciale nel diritto pubblico, dal momento che rappresenta il complesso delle attività delle quali si servono le autorità pubbliche per garantire il rispetto delle norme giuridiche. La decentralizzazione affida il compito dell'*enforcement* alle autorità nazionali competenti che applicano le norme in base al loro ordinamento, seppur in linea con l'Europa. Invece nella centralizzazione, l'attuazione e il

⁷³ Regolamento (UE) 2016/679, art. 5, General Data Protection Regulation (GDPR).

⁷⁴ *Very Large Online Search Engines*. Motori di ricerca online di grandissime dimensioni.

⁷⁵ Regolamento (UE) 2022/1925, art. 5–7, Digital Markets Act (DMA).

controllo delle norme è affidato ad un'unica unità sovranazionale, che è appunto la Commissione Europea⁷⁶.

L'AI Act è caratterizzato da una rete multilivello di *enforcement*. Ogni Stato membro ha il compito di designare un'autorità competente nazionale, coordinata a livello europeo dallo *European AI Office*, che svolge principalmente 3 funzioni: sorveglianza, competenza tecnica e armonizzazione applicativa. Le sanzioni previste arrivano fino a 35 milioni di euro o al 7% del fatturato annuo, come approfondiremo meglio in seguito⁷⁷.

Nel GDPR, l'*enforcement* è affidato alle autorità nazionali per la protezione dei dati, nel caso italiano è il *Garante della Privacy* e alla cooperazione tramite lo *European Data Protection Board* (EDPB), ovvero il Comitato europeo per la protezione dei dati. Tale modello garantisce un'interpretazione uniforme, nonostante sia decentralizzato⁷⁸. Infine, sia nel DMA che nel DSA, la Commissione Europea è l'organo che si occupa dell'*enforcement* dei *gatekeepers* o VLOPs. Per complementarità, il DSA prevede anche un *Board* dei Servizi Digitali, mentre il DMA solo ispezioni, *audit*, rimedi strutturali o comportamentali.

In conclusione, come sintetizzato nell'analisi esposta, la sovrapposizione tra AI Act, GDPR, DSA e DMA impone alle imprese un'elevata complessità gestionale per rispettare le norme. Questo scenario richiede un approccio "*compliance by design*" trasversale affinché la progettazione di soluzioni di IA sia allineata sin dall'origine ai diversi obblighi regolatori.

1.2.2 Confronto con approcci regolatori extraeuropei (USA, Cina, Regno Unito)

Sebbene a livello europeo si parli di AI Act quale *hard law*, nei Paesi extraeuropei, come la Cina, Usa e Regno Unito, l'approccio regolatorio è ancora basato su strategie politiche e strumenti di *soft law*, con eccezioni limitate a pochi settori. In questo contesto, è utile considerare anche i riferimenti, le linee guida, i principi e i rapporti elaborati da istituzioni internazionali, come l'OCSE, che offrono una prospettiva comparata e multilivello sullo

⁷⁶ Söderlund, K., & Larsson, S., *Enforcement Design Patterns in EU Law: An Analysis of the AI Act*. *Digital Society*, 3, Articolo 41, 25 luglio 2024. Disponibile su: s44206-02 file:///C:/Users/utente/Downloads/s44206-024-00129-8.pdf4-00129-8.pdf

⁷⁷ Regolamento (UE) 2024/1689, articolo 71, AI Act.

⁷⁸ Regolamento (UE) 2016/679, art. 51–70, *General Data Protection Regulation* (GDPR).

sviluppo e la governance dell'IA a livello globale. L'approccio europeo si distingue da quello degli altri Paesi per ragioni politiche, economiche e sociali. Analizzare queste differenze è il primo passo da compiere per comprendere a pieno la governance globale dell'intelligenza artificiale e per valutare le sfide connesse all'armonizzazione dei sistemi giuridici. A differenza dell'Unione Europea, gli Stati Uniti non hanno una legislazione federale (centrale) completa che regoli lo sviluppo dell'intelligenza artificiale. Infatti, il modello statunitense è caratterizzato dalla decentralizzazione: le competenze regolatorie si spartiscono tra Stati federati, agenzie federali e privati⁷⁹. Secondo un report internazionale dell'OCSE, tale scelta proviene dal fatto che gli USA preferiscono concentrarsi quasi completamente sull'innovazione o la competitività, dando meno importanza all'intervento pubblico diretto⁸⁰. Vi sono comunque diversi quadri regolatori, seppur alcuni con applicazioni limitate, che cercano di diffondere un uso etico e corretto delle tecnologie.

La prima legge americana in materia di AI è il *National AI Initiative Act*⁸¹ del 2020, che ha l'obiettivo principale di ampliare la ricerca e lo sviluppo nel campo tecnologico. Il documento è stato approvato dal Congresso degli Stati Uniti nel dicembre 2020 ed è stato pubblicato sotto la guida della *White House Office of Science and Technology Policy* (OSTP). Il *National AI Initiative Act* istituisce anche il *National Artificial Intelligence Initiative Office*, responsabile della supervisione e implementazione della strategia statunitense sull'IA. Promulgato come parte del *National Defense Authorization Act* (NDAA)⁸² per l'anno fiscale 2021 ed è stato approvato dal Congresso degli Stati Uniti nel dicembre 2020. Il documento non impone obblighi normativi vincolanti ma stabilisce una strategia per l'utilizzo dell'IA. In particolare, le disposizioni più rilevanti riguardano la promozione di standard e dell'educazione e formazione in materia, finanziamento di

⁷⁹ Gasser, Urs, and Virgilio A.F. Almeida. "A Layered Model for AI Governance." *IEEE Internet Computing*, 21, 6 novembre 2017 : 58–62. Disponibile su: [w6gov-18-LATEX.pdf](#)

⁸⁰ OCSE, *State of Implementation of the OECD AI Principles: Insights from National AI Policies*, OECD Publishing, 2021. Disponibile su: https://www.oecd.org/en/publications/state-of-implementation-of-the-oecd-ai-principles_1cd40c44-en.html implementation of the OECD AI Principles | OECD

⁸¹ Congresso, *National Artificial Intelligence Initiative*, 12 Marzo 2020. Disponibile su: <https://www.congress.gov/bill/116th-congress/house-bill/6216/text>

⁸² Legge federale statunitense approvata annualmente dal Congresso per stabilire il bilancio e le priorità di spesa per il Dipartimento della Difesa degli Stati Uniti.

¹⁰⁹ Ufficio della Casa Bianca istituito nel 1976 con l'obiettivo di fornire consulenza al Presidente degli Stati Uniti sulle implicazioni scientifiche, tecnologiche e ingegneristiche delle politiche pubbliche.

programmi di ricerca e sviluppo di partnership pubblico-private. Rappresenta la base su cui si fondano i regolamenti degli anni a venire.

L'OSTP della Casa Bianca, il 4 ottobre 2022, pubblica il *Blueprint for an AI Bill of Rights*⁸³. Quest'ultimo rappresenta un primo passo verso la definizione di standard etici, pur non avendo forza di legge. I punti trattati sono:

- Efficacia e sicurezza dei sistemi;
- Protezione contro discriminazione algoritmica;
- Privacy dei dati;
- Notifica e spiegazione ai cittadini sui funzionamenti e le decisioni dei sistemi;
- Intervento umano quando si verificano problematiche con sistemi automatizzati.

Successivamente, il 30 ottobre del 2023, il presidente in carica in quel periodo, *Joe Biden*, firma l'*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*⁸⁴. Quest'ultimo si differenzia dal precedente per un carattere più prescrittivo. Infatti tra i contenuti principali sono presenti linee guida sulla sicurezza e test di affidabilità dei sistemi, formazione del personale federale in materia, misure per proteggere la privacy e obblighi per i fornitori di comunicare al governo federale sistemi particolarmente potenti, come quelli che potrebbero compromettere la sicurezza nazionale. Inoltre sono inserite richieste esplicite di *auditing* di *bias* e pratiche discriminatorie per tutelare i lavoratori.

A completamento dell'*Executive Order*, il 1 marzo del 2024, la Casa Bianca, tramite l'*Office of Management and Budget (OMB)*, ha pubblicato il *Memorandum M-24-10, National Security Memorandum* sull'Intelligenza Artificiale⁸⁵, documento strategico che anticipa l'attuazione normativa dell'ordine esecutivo. Non rappresenta un atto cogente, ma fornisce alle imprese e alle agenzie federali linee guida su come gestire sistemi di IA in modo etico. Entro il 24 ottobre 2024 vi era l'obbligo per le imprese USA di conformarsi

⁸³ *The White House, Blueprint for an AI bill of rights*, ottobre 2022. Disponibile su: <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>

⁸⁴ *The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 October 2023. Disponibile su: <https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf>

⁸⁵ *The White House, Office of Management and Budget (OMB), Memorandum M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, 28 Marzo 2024. Disponibile su: <https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf>

a tale *Memorandum*. Il testo distingue sistemi di IA ad alto rischio, per cui è raccomandata la valutazione del rischio periodica, e sistemi a basso rischio per i quali vi si devono adottare misure di trasparenza. Inoltre, il Memorandum sottolinea come è sconsigliato l'utilizzo di IA per settori ad alta sensibilità come l'immigrazione, la giustizia penale o l'accesso ai servizi pubblici. Infatti, per questi ultimi, viene suggerito di consultare *stakeholders* prima di adottare soluzioni prodotte da intelligenza artificiale. Il Memorandum, ha anche introdotto un sistema di allocazione delle responsabilità, secondo il quale ogni agenzia federale ha l'obbligo di pubblicare annualmente un report sull'utilizzo dell'IA. L'*Executive Order* nel 2024 ha istituito l'interagenzia denominata *AI Executive Council*. Tale inter-agenzia ha funzioni di coordinamento strategico per le politiche di IA e affianca i lavori dell'*Office of Science and Technology Policy* (OSTP) ed è composto da membri del *Department of Commerce*, *Department of Defense*, *Office of Science and Technology Policy*. Nel 2024, il *National Institute of Standards and Technology*⁸⁶ (NIST), ha aggiornato il *AI Risk Management Framework*⁸⁷, divenuto punto di riferimento per molte aziende, seppur non vincolante. A seguito dell'emissione di tale documento molti stati americani si sono avvicinati all'*hard law* federale, e sono state avviate diverse iniziative per proporre nuove leggi federali, quali l'*Algorithmic Accountability Act* e l'*AI Foundation Model Transparency Act*.

A differenza dell'approccio statunitense, che si può descrivere come decentrato e frammentato, l'approccio europeo si serve di un ordinamento direttamente applicabile. Infatti analizzando le differenze normative, mentre l'AI Act europeo è direttamente applicabile, con strutture vincolanti e obblighi giuridici da rispettare da parte di tutti gli Stati membri, gli Stati Uniti mancano di una legge federale unitaria. Prevalgono linee guida etiche, framework tecnici e i pochi tentativi di normazione di carattere generale. Mentre in Europa l'AI Act riferisce chiaramente ai requisiti della Carta dei Diritti fondamentali dell'Uomo, nei testi USA sono presenti gli stessi riferimenti ma sono trattati con meno enfasi e non inseriti tra quelli vincolanti. Il controllo dei sistemi di IA in UE è principalmente *ex-ante*, ed avviene tramite registro pubblico europeo e verifica della

⁸⁶ Agenzia del Dipartimento del Commercio degli Stati Uniti, fondata nel 1901, che si occupa di sviluppare standard, linee guida e buone pratiche per garantire qualità, sicurezza e interoperabilità in settori scientifici e tecnologici.

⁸⁷ *National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, Gennaio 2023. Disponibile su: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

conformità prima dell'immissione del regolamento, mentre negli Stati Uniti, il controllo avviene *ex-post*, e non vi è nessun obbligo di certificazione. Una ulteriore differenza tra UE e USA riguarda gli obiettivi. Per le istituzioni europee è fondamentale che l'AI Act garantisca il doppio obiettivo di tutela dei diritti dell'uomo ed allo stesso tempo venga perseguita l'innovazione. Per il congresso statunitense, l'accento principale viene posto in modo principale sull'innovazione e sulla competitività globale, tralasciando l'importanza dei diritti dell'uomo.

Lo *State Council of China*, nel 2017, ha emanato *New Generation Artificial Intelligence Development Plan*⁸⁸, il primo documento strategico ufficiale con cui la Cina delinea l'obiettivo di diventare *leader* mondiale dell'IA entro il 2030. I contenuti principali riguardano gli investimenti nella ricerca e nello sviluppo, l'emissione di standard industriali e tecnici, la messa in sicurezza dei sistemi di IA per usi militari e civili. Sempre in linea con la tecnicità delle operazioni di intelligenza artificiale, il *China Electronics Standardization Institute*, nel 2018, ha rilasciato l'*Artificial Intelligence Standardization White Paper*⁸⁹ con l'obiettivo di preparare standard tecnici per la governance e l'implementazione dell'IA, sia collaborando con enti industriali per ottenere certificazioni valide in materia, sia creando linee guida su affidabilità e trasparenza. Un esempio di collaborazione tra il governo cinese e le società cinesi è quella avviata con la società Alibaba Group, coinvolta nello sviluppo di strumenti per *cloud computing* e commercio elettronico. Anche con *Huawei Technologies*, vi è stata una *partnership* per implementare meglio l'IA per le reti di telecomunicazione 5G, per l'*edge computing*⁹⁰ e per l'IA nei dispositivi mobili. La *Cyberspace Administration of China* (CAC), nel 2022, ha promulgato il documento *Internet Information Service Algorithmic Recommendation*

⁸⁸ Creemers R., Kania E., Triolo P., Webster G., *Full Translation: China's 'New Generation Artificial Intelligence Development Plan'*, *DigiChina*, 1 agosto 2017. Disponibile su: [Full Trahttps://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/nslation: China's 'New Generation Artificial Intelligence Development Plan' \(2017\)](https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/nslation: China's 'New Generation Artificial Intelligence Development Plan' (2017))

⁸⁹ CESI, SAC, *Artificial Intelligence Standardization White Paper, translated on 12 ay 2020 by Etcetera Language Group, Inc., Ben Murphy, CSET Translation Lead*, Pechino 21 Ottobre 2021. Disponibile su: <https://cset.georgetown.edu/publication/artificial-intelligence-standardization-white-paper-2021-edition/>

⁹⁰ Architettura di elaborazione distribuita che avvicina il calcolo e l'analisi dei dati al luogo in cui i dati stessi vengono generati (ossia ai margini della rete), riducendo la latenza, migliorando la velocità di risposta e ottimizzando l'uso delle risorse di rete rispetto ai modelli centralizzati basati solo su *cloud computing*.

*Management Provisions*⁹¹, per regolare l'uso di algoritmi di raccomandazione su social network come TikTok oppure nell'e-commerce. I punti chiave sono:

- Obbligo di trasparenza nei criteri di raccomandazione;
- Obblighi specifici per la tutela di lavoratori, anziani e minori;
- Obbligo di registrazione degli algoritmi e sottoporli a valutazioni di sicurezza.

Tutti i citati obblighi sono validi anche per le aziende straniere che offrono servizi *online* in Cina.

Nel 2023, per regolare i contenuti dell'IA Generativa, viene pubblicato "*Provisions on Management of Deep Synthesis Internet Information Services*⁹². Deepfake, testi, audio e immagini generati artificialmente devono essere certificati, limitato l'uso di sintesi vocale o video e non devono essere diffuse notizie false o offensive. Ma la prima regolazione ufficiale specifica sull'AI Generativa, in questo caso, come ChatGPT, avviene solo nel 2023 tramite *Interim Measures for the Management of Generative Artificial Intelligence Services*⁹³, per il quale:

- I fornitori devono registrare il servizio presso le autorità;
- I contenuti devono riflettere "i valori fondamentali del socialismo";
- Controllo preventivo dei dati di addestramento, di sicurezza, ideologici e culturali;
- Obbligo di protezione contro *bias*, disinformazione e contenuti illegali.

Tali strumenti normativi sono tutti appartenenti alla *soft law*, ad esclusione del *Internet Information Service Algorithmic Recommendation Management Provisions* e del *Interim Measures for the Management of Generative Artificial Intelligence Services*, che sono

⁹¹ Creemers R., Toner H., Webster G., *Translation: Internet Information Service Algorithmic Recommendation Management Provisions*, *DigiChina*, 10 gennaio 2022. Disponibile su: <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/> *Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022*

⁹² *China Law Translate, Provisions on the Administration of Deep Synthesis Internet Information Services*, 11 dicembre 2022. Disponibile su: <https://www.chinalawtranslate.com/en/deep-synthesis/Internet-Information-Services>

⁹³ *China Law Translate, Interim Measures for the Management of Generative Artificial Intelligence Services*, 13 luglio 2023. Disponibile su: <https://www.chinalawtranslate.com/en/generative-ai-interim/Interim-Measures-for-the-Management-of-Generative-Artificial-Intelligence-Services>

invece vincolanti. Nonostante ciò, il sistema cinese permette alla *soft law* di avere effetti molto incisivi, poiché è caratterizzato da un coordinamento verticale tra società statali o società che operano in settori strategici e lo Stato. Inoltre, in Cina il controllo politico è centralizzato⁹⁴, quindi l'adeguamento ai regolamenti è incentivato da ragioni legate alla lealtà o al consenso, sebbene non vi siano obblighi giuridici espliciti.

Il modello cinese è notevolmente diverso da quello europeo per varie ragioni. In primo luogo, l'AI Act appartiene *all'hard law* mentre in Cina, il quadro normativo sull'IA è articolato in maniera diversa. Infatti, oltre alle leggi formali, esistono numerosi atti amministrativi che, pur non avendo sempre, lo status gerarchico di una legge formale, risultano vincolanti nella pratica per gli operatori economici. In secondo luogo, l'AI act si fonda sul rispetto dei diritti fondamentali e la protezione del mercato interno, mentre in Cina, vengono combinati obiettivi di innovazione tecnologica con esigenze di sicurezza nazionale e controllo sociale. Questo porta a normative che non solo disciplinano gli aspetti tecnici dell'intelligenza artificiale ma intervengono anche sui contenuti, imponendo vincoli sul piano politico e valoriale.

Oltre ai modelli normativi statunitensi e cinesi, merita attenzione il caso del Regno Unito, il quale si è distinto dall'Unione Europea, per la regolazione dell'IA⁹⁵. Nel 2021, il governo britannico ha pubblicato la *National AI Strategy*⁹⁶, definendo le priorità del paese in merito all'IA. La strategia decennale si articola su 3 piani: promuovere il Regno Unito come leader etico nel settore, sviluppare ecosistemi di ricerca e garantire un'adozione sicura in tutti i sistemi. Nel 2023 è stato pubblicato il *white paper A pro-innovation*

⁹⁴ U.S.-China Economic and Security Review Commission, *CCP DECISION-MAKING AND XI JINPING'S CENTRALIZATION OF AUTHORITY*, Chapter 1, in 2022 Annual Report to Congress, novembre 2022. Disponibile su: https://www.uscc.gov/sites/default/files/2022-11/Chapter_1--CCP_Decision-Making_and_Xi_Jinpings_Centralization_of_Authority.pdf

⁹⁵ European Parliamentary Research Service (EPRS), *The United Kingdom and artificial intelligence*, 2024. Disponibile su: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762285/EPRS_ATA\(2024\)762285_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762285/EPRS_ATA(2024)762285_EN.pdf)

⁹⁶ UK Government, *National AI Strategy, Presented to Parliament by the Secretary of State for Digital, Culture, Media and Sport by Command of Her Majesty*, Settembre 2021. Disponibile su: https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf

*approach to AI regulation*⁹⁷ e, in occasione dell'*AI Safety Summit*⁹⁸, è stata proposta su ed approvata la Bletchley Declaration⁹⁹. Il primo documento è stato rilasciato dal *Department of Science, Innovation and Technology* (DSIT), e identifica i seguenti cinque principi:

- Sicurezza e robustezza dei sistemi AI;
- Trasparenza;
- Equità;
- Responsabilità;
- Sorveglianza umana.

Questi principi possono essere adattati ai vari contesti in cui sono utilizzati ma sono tuttavia focalizzati sull'innovazione.

In occasione dell'*AI Safety Summit*, il governo britannico ha anche annunciato la creazione dell'*AI Safety Institute*, che oltre alla valutazione del funzionamento dei modelli avanzati di IA, propone la coordinazione internazionale. La decisione del governo britannico di non utilizzare l'*hard law* ma di lasciare spazio all'evoluzione tecnica e al dialogo tra innovatori e autorità costituisce la differenza principale tra il Regno Unito e l'Unione Europea in materia di IA.

⁹⁷ UK Government, *Department for Science, Innovation and Technology and Office for Artificial Intelligence, AI regulation: a pro-innovation approach*, 29 marzo 2023. Disponibile su: <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach> - GOV.UK

⁹⁸ Il summit si è tenuto il 1 e il 2 Novembre 2023 presso Bletchley Park, Buckinghamshire.

⁹⁹ Con la Dichiarazione 28 paesi, tra cui USA, Cina e Unione europea, hanno delineato l'impegno per uno sviluppo sicuro, etico e responsabile dell'intelligenza artificiale sottolineando la necessità di cooperazione internazionale per gestire i rischi e sfruttare i benefici dell'IA per la comunità globale. Disponibile su: <https://www.astrid-online.it/static/upload/the-the-bletchley-declaration-ai-safety-summit.pdf>

CAPITOLO SECONDO

Applicazione dell'AI Act nei Paesi europei: armonizzazione e criticità

2.1 L'implementazione dell'AI Act nei principali Stati membri

2.1.1 Francia: approccio regolatorio, primi risultati e parentesi sulle PMI

L'Artificial Intelligence Act si inserisce in un contesto normativo e internazionale ben preciso. Questo capitolo si pone l'obiettivo di approfondire l'implementazione del Regolamento nei principali Stati Membri dell'Unione Europea, dopo averne attentamente esaminato le caratteristiche. In particolare, è fondamentale evidenziare i punti di forza e di debolezza, considerando che uno degli scopi fondamentali è l'armonizzazione della regolazione. Con il termine armonizzazione si intende il processo attraverso il quale l'Unione Europea interviene per ridurre le differenze legislative tra gli Stati membri per garantire l'efficace funzionamento del mercato interno, assicurando sia i diritti fondamentali che la prevenzione di disparità competitive tra gli ordinamenti. Fattori politici, istituzionali ed economici possono rendere l'attuazione pratica dell'AI Act difficile in ciascun ordinamento nazionale. La realtà in cui si inserisce l'AI Act, è già normativamente stratificata, come analizzato nel confronto con GDPR, DSA e DMA, e di conseguenza sono coinvolti una pluralità di attori, tra cui autorità nazionali, imprese e centri di ricerca con livelli di preparazione ed esigenze differenziate. Questo scenario rende particolarmente complessa la piena uniformità dell'applicazione, sollevando questioni sia interpretative che operative. Di conseguenza, gli obiettivi principali di questo capitolo sono due: da un lato, esaminare lo stato di implementazione del regolamento in tre Paesi chiave – Francia, Germania e Italia – selezionati per la loro rilevanza economica, tecnologica e giuridica; dall'altro, evidenziare le principali difficoltà di armonizzazione e le implicazioni che esse possono generare per le imprese e per la competitività dell'Unione nel contesto globale. Al fine di individuare come avviene il recepimento del regolamento e quali sono gli effetti concreti sulle aziende, il presente capitolo si serve di dati aggiornati, fonti accademiche e report istituzionali. A supporto di ciò, sono introdotti anche grafici e strumenti comparativi per facilitare la comprensione dei divari applicativi tra i diversi ordinamenti, e riflettere sull'impatto dell'AI Act sulle strategie aziendali e sull'equilibrio tra innovazione e regolazione.

La Francia è uno dei Paesi europei che ha assunto un atteggiamento più reattivo all'attuazione dell'*Artificial Intelligence Act*. Già nel 2018, il deputato *Cédric Villani* venne incaricato dal governo di redigere una strategia nazionale sull'intelligenza artificiale: tale documento è chiamato Rapporto Villani¹⁰⁰ e ha rappresentato una base importante per la regolazione dell'IA in Francia. I quattro settori considerati prioritari sono: sanità, difesa, ambiente e trasporti, con un' enfasi particolare posta sulla regolazione etica e la sovranità tecnologica. La strategia è stata aggiornata nel 2021, anno in cui il governo francese ha deciso di investire complessivamente 2 miliardi di euro, di cui 1,5 miliardi proveniente direttamente da fondi pubblici¹⁰¹. Tale operazione è stata annunciata come parte del piano *France 2030*, iniziativa lanciata da Emmanuel Macron nel 2021, per rafforzare la competitività industriale e tecnologica francese nel decennio a seguire. Altri obiettivi del piano includono l'investimento di 500 milioni di euro da parte di investimenti privati e partnership privato-pubbliche. I fondi in questione sono principalmente destinati a finanziare *start-up AI* e *scale-up deeptech*¹⁰², creare poli di ricerca di eccellenza come PRAIRIE¹⁰³, che sta per "*PaRis Artificial Intelligence Research InstitutE*", ovvero uno dei quattro istituti interdisciplinari di IA creati in Francia, insieme a MIAI (*Multidisciplinary Institute in Artificial Intelligence*) con sede a Grenoble, ANITI¹⁰⁴, situato a Tolosa. A questi, noto per il focus sull'intelligenza artificiale ibrida, combinando metodi simbolici e di apprendimento automatico, si aggiunge il *3IA Côte d'Azur*, con sede a Nizza, il quale si concentra sull'applicazione dell'IA in settori come la medicina, le smart cities e l'energia sostenibile¹⁰⁵. Un altro obiettivo della strategia "*France 2030*" è quello di formare almeno 20000 nuovi talenti IA tra tecnici e dottorandi entro il 2025 e rafforzare la sovranità tecnologica, anche per ciò che riguarda cloud e semiconduttori.

¹⁰⁰ Villani C., *Donner un sens à l'intelligence artificielle, – Pour une stratégie nationale et européenne, Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation*, marzo 2018. Disponibile su : Donner un sens à l'int https://fichiers.acteurspublics.com/redac/pdf/2018/2018-03-28_Rapport-Villani.pdf intelligence artificielle

¹⁰¹ *Gouvernement français, France 2030: Un plan d'investissement pour la France de demain*, 2021. Disponibile su : France 2030 | info.g <https://www.info.gouv.fr/grand-dossier/france-2030ouv.fr>

¹⁰² Aziende tecnologiche ad alto potenziale di crescita che hanno superato la fase iniziale di start-up e operano in settori avanzati.

¹⁰³ PRAIRIE Institut, *Official Site*. Disponibile su : PRAIRIE Institut <https://prairie-institute.fr/e> - Prairie

¹⁰⁴ ANITI, *Artificial and Natural Intelligence Toulouse Institute*. Disponibile su: AN <https://aniti.univ-toulouse.fr/ITI>

¹⁰⁵ *3IA Côte d'Azur, About Us*. Disponibile su: 3IA Côte d'Azur - Interdisciplinary Inst <https://3ia.univ-cotedazur.eu/itute> for Artificial Intelligence

Dopo che l'AI Act è stato approvato, la Francia ha affidato le funzioni di implementazione e sorveglianza all'*Autorité de la Concurrence e al CNIL*, l'ente garante per la protezione dei dati. Quest'ultimo, nel 2024, ha lanciato un programma per le imprese normative "AI Sandbox" secondo quanto previsto dall'Articolo 53 del Regolamento, per appunto testare le applicazioni della tecnologia in un ambiente regolamentato, con l'obiettivo di consentire a tutti gli ecosistemi coinvolti di beneficiare di queste raccomandazioni sostenendo l'innovazione¹⁰⁶. Per citare un esempio, la startup *Hugging Face* ha collaborato con il governo per sviluppare framework di audit etico nei modelli generativi, ed è stata infatti selezionata dal CNIL per il programma "*Enhanced Support*" nel 2023, che offre supporto legale e tecnico a imprese innovative per aiutarle a conformarsi al GDPR, soprattutto per la protezione di dati nel campo dell'intelligenza artificiale¹⁰⁷. La start up ha avanzato critiche in materia di compliance sottolineando come solo le grandi aziende possano permettersi ottime regolamentazioni interne, danneggiando le start up francesi. Soprattutto per tale motivo, *Hugging Face* ha anticipato pratiche di trasparenza e creato una guida per gli sviluppatori *open source* dell'intelligenza artificiale¹⁰⁸. Tutto ciò è stato reso possibile soprattutto grazie alla CNIL, che oltre ad essere stata creata da un dipartimento IA interno nel gennaio 2023, ha stabilito delle linee guida pratiche per la valutazione degli algoritmi e, nello specifico, è stata indicata come autorità nazionale principale per l'attuazione dell'AI Act. D'altro canto, l'Antitrust francese, dal 28 giugno del 2024 possiede solo capacità di fornire pareri formali con consultazione pubblica

¹⁰⁶ *CNIL, Artificial intelligence and public services: the CNIL publishes the results of its "sandbox"*, 18 aprile 2025. Disponibile su: Artificial intelligence and public services: <https://www.cnil.fr/en/artificial-intelligence-and-public-services-cnil-publishes-results-its-sandbox>the CNIL publishes the results of its "sandbox" | CNIL

¹⁰⁷ *CNIL, Enhanced support: the CNIL selects 3 digital companies with strong potential*, 11 maggio 2023. Disponibile su: Enhanced support: the CNIL selects 3 digital companies <https://www.cnil.fr/en/enhanced-support-cnil-selects-3-digital-companies-strong-potential> with strong potential | CNIL

¹⁰⁸ *Govil A., Hugging Face Advocates Open-Source AI in Regulatory Framework*, LinkedIn, 20 marzo 2025. Disponibile su: (17) Hugging Face A <https://www.linkedin.com/pulse/hugging-face-advocates-open-source-ai-regulatory-framework-amit-govil-gsraf/dvocates-Open-Source-AI-in-Regulatory-Framework-LinkedIn>

sull'IA generativa¹⁰⁹ e ha raccomandato l'estensione delle tutele del DMA anche all'AI Act, preoccupandosi dei vantaggi competitivi che le Big Tech come *Google, Microsoft, Amazon e Meta* possono assumere nel mondo odierno.

Tuttavia, nonostante il grado di partecipazione e anticipazione strategica dimostrata, emergono criticità sia in ambito interpretativo che applicativo. Infatti, le PMI francesi hanno ancora difficoltà ad applicare gli obblighi legati ai sistemi ad alto rischio, come previsto dagli articoli 16-29 dell'AI Act. Nel 2023, solo il 4,7% delle imprese francesi con 10-49 dipendenti ha adottato soluzioni di IA, mentre tra le imprese con 50-249 dipendenti la percentuale sale al 10,2%. Questi dati indicano una bassa adozione dell'IA tra le PMI francesi, soprattutto se confrontati con paesi come la Germania, dove le percentuali sono rispettivamente del 9,7% e del 16,2% per le stesse categorie di imprese¹¹⁰. Le PMI, ed in particolare quelle francesi, affrontano diverse sfide nell'adozione dell'IA,¹¹¹ tra cui:

- Costi elevati: l'implementazione di soluzioni di IA richiede investimenti significativi in *hardware, software* e formazione del personale.
- Competenze limitate: molte PMI non dispongono internamente delle competenze necessarie per sviluppare e gestire soluzioni di IA, rendendo necessario il ricorso a consulenti esterni o a programmi di formazione specifici.
- Gestione dei dati: La mancanza di dati di qualità e di sistemi informativi adeguati rappresenta un ostacolo significativo per l'adozione efficace dell'IA.

Nonostante le criticità sopra menzionate che continuano a caratterizzare il tessuto delle PMI francesi, è comunque possibile osservare una dinamica di crescita in alcuni ambiti specifici, come ad esempio il settore del marketing, che si sta affermando come un elemento trainante per la competitività e l'innovazione aziendale. Secondo il report

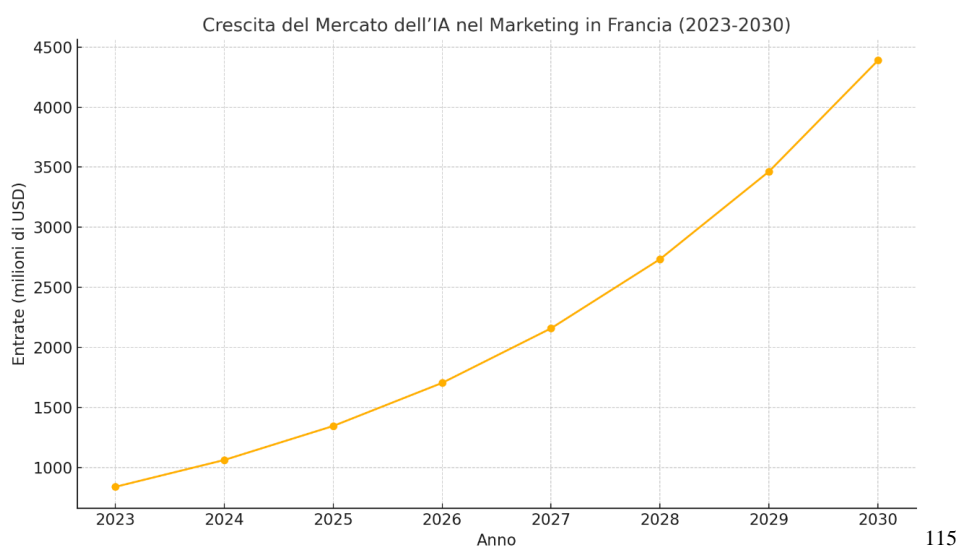
¹⁰⁹ *Autorité de la Concurrence, Intelligence artificielle générative : l'Autorité rend son avis sur le fonctionnement concurrentiel du secteur de l'intelligence artificielle générative*, 28 Giugno 2024. Disponibile su : [Intelligence artificielle générative : l'Autorité rend son avis sur le fonctionnement concurrentiel du secteur de l'intelligence artificielle générative | Autorité de la concurrence](#)

¹¹⁰ *IUS Letter Informazione e aggiornamento giuridico, Il G7: Pmi frenate sull'intelligenza artificiale*, Il Sole 24 Ore, 15 ottobre 2024. Disponibile su:

[Il G7: Pmi frenate sull'intelligenza artificiale - Iusletter](#)

¹¹¹ *OECD, BCG, Insead Business School, The Adoption of Artificial Intelligence in Firms, New Evidence for Policy Making*, 2 maggio 2025. Disponibile su: [f9ef33c3-en.pdf](#)
file:///C:/Users/utente/Downloads/f9ef33c3-en.pdf df

*France Artificial Intelligence (AI) in Marketing Market Forecast 2024–2030*¹¹² il valore del mercato francese dell'IA applicata al marketing ha raggiunto 837,4 milioni di dollari nel 2023, con una previsione di crescita fino a 4,39 miliardi entro il 2030, a un CAGR¹¹³ pari al 26,7%. La componente dei servizi è la più rilevante ed anche quella che si sta espandendo di più. Nonostante gli oneri di compliance, l'ecosistema francese, è in grado di promuovere l'IA soprattutto per l'adozione commerciale. L'inserimento di strumenti generativi, chatbot avanzati, sistemi di *targeting* predittivo¹¹⁴, nonché l'automazione di campagne pubblicitarie, costituisce una delle applicazioni più diffuse dell'IA tra le PMI digitali francesi. Tale andamento è coerente con la traiettoria delineata dal piano *France 2030* e dagli investimenti pubblici in ricerca e sviluppo.



A completamento di questo scenario, nel febbraio 2025, in occasione del vertice sull'intelligenza artificiale tenutosi a Parigi, il presidente *Emmanuel Macron* ha annunciato un nuovo e ambizioso piano di investimenti pubblici e privati, per un totale di

¹¹² Grand View Research, *France Artificial Intelligence (AI) in Marketing Market Size & Outlook*, 2030. Disponibile su: <https://www.grandviewresearch.com/horizon/outlook/artificial-intelligence-ai-in-marketing-market/france>

¹¹³ *Compound Annual Growth Rate*

¹¹⁴ Utilizzano algoritmi di intelligenza artificiale e machine learning per analizzare grandi quantità di dati comportamentali, demografici e contestuali, al fine di anticipare le preferenze e i comportamenti futuri dei consumatori.

¹¹⁵ Grafico rielaborato con dati provenienti da Grand View Research, *France Artificial Intelligence (AI) in Marketing Market Size & Outlook*, 2030. Disponibile su: <https://www.grandviewresearch.com/horizon/outlook/artificial-intelligence-ai-in-marketing-market/france>

Germania ha cercato di prepararsi già a partire dal 2018 ad una futura armonizzazione europea normativa ed in merito la strategia ha influenzato la decisione della Commissione Europea di adottare un approccio *risk-based* per l'AI Act. Nel 2020, il piano nazionale è stato aggiornato con la collaborazione tra il Ministero Federale per l'Economia e la Protezione Climatica (BMWK) e il Ministero Federale dell'Istruzione e della Ricerca (BMBF), stabilendo uno stanziamento complessivo di 5 miliardi di euro entro il 2025, integrati nel pacchetto "*Zukunftspaket*" finanziato anche attraverso fondi del *Next Generation EU* post-pandemia¹²¹. Sempre nello stesso anno, è stata attivata l'Agenzia Federale per l'Innovazione dirompente, avente il compito di finanziare tecnologie ad alto potenziale in settori critici, tra cui la sanità, la cybersicurezza e l'energia¹²². L'obiettivo, negli anni, è rimasto quello di rendere l'intelligenza artificiale una tecnologia di uso quotidiano per cittadini e aziende tedesche. Nel 2023 sono stati potenziati programmi come *l'AI Made in Germany 2030*, per creare un ecosistema conforme all'UE e il *Sprunginnovationen* (SPRIND). Quest'ultimo agisce come uno strumento agile ed indipendente dalla burocrazia ministeriale. Oltre alla SPRIND, l'infrastruttura tedesca di governance per l'IA include:

- il *Bundesministerium für Digitales und Verkehr (BMDV)*, che coordina progetti per la mobilità autonoma¹²³;
- il *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, coinvolto nella definizione di standard di cybersicurezza per sistemi AI¹²⁴;

¹²¹ Bundesregierung, *Strategie Künstliche Intelligenz der Bundesregierung, Fortschreibung 2020*, Dicembre 2020. Disponibile su: https://www.ki-strategie-deutschland.de/files/downloads/201201_Fortschreibung_KI-Strategie.pdf

¹²² SPRIND – D, *Zwei Jahre Bundesagentur für Sprunginnovationen*. Disponibile su: <https://www.sprind.org/worte/magazin/zwei-jahre-sprind>

¹²³ Federal Ministry of Transport, *Federal Government publishes strategy for autonomous driving in road transport, Autonomous driving is the future, says Federal Minister Wissing*, Press Release, 4 dicembre 2024. Disponibile su: <https://www.bmv.de/SharedDocs/EN/PressRelease/2024/106-wissing-autonomous-driving.html>

¹²⁴ Federal Office for Information Security, *Artificial Intelligence Bringing you close to technology*. Disponibile su: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html

¹²⁵ Steiner F., *AI regulation: German government reveals supervisory regime plan*, Heise Online, 26 settembre 2024. Disponibile su: <https://www.heise.de/en/news/AI-regulation-German-government-reveals-supervisory-regime-plan-9954191.html>

- il *Bundesnetzagentur*, potenziale autorità preposta alla vigilanza nell'ambito dell'AI Act¹²⁵;
- il *BfDI* (Garante federale per la protezione dei dati), già operativo sul fronte privacy¹²⁶.

Alcuni rapporti, come quello della *Stiftung Neue Verantwortung*, sottolineano che nonostante l'eccellenza scientifica tedesca in ambito AI, il Paese ha sofferto per una certa lentezza nell'implementazione pratica della strategia, burocrazia complessa e mancanza di strumenti vincolanti fino all'intervento europeo con l'AI Act¹²⁷.

Per assicurare il recepimento dell'AI Act la Germania ha designato due autorità:

- *Bundesnetzagentur (BNetzA)*: nominata come autorità nazionale di sorveglianza del mercato per i sistemi di intelligenza artificiale, avente il compito di monitorare la conformità dei sistemi AI alle disposizioni del regolamento, effettuare controlli e, se necessario, imporre sanzioni.
- *Deutsche Akkreditierungsstelle (DAkkS)*: designata come organismo notificato responsabile delle valutazioni di conformità dei sistemi AI ad alto rischio, con lo scopo di accreditare enti terzi che effettueranno le valutazioni richieste per l'immissione sul mercato di tali sistemi.

Inoltre, le autorità tedesche per la protezione dei dati (*Data Protection Authorities, DPAs*) hanno pubblicato linee guida per l'implementazione e l'uso dell'IA in conformità con il GDPR, fornendo indicazioni pratiche su come mitigare e prevenire i rischi associati all'uso dell'IA. Tra questi si possono riscontrare il trattamento illecito dei dati personali e la discriminazione attraverso dati distorti. Oltre alla designazione delle autorità competenti, nel 2024, la Germania ha introdotto un disegno di legge nazionale, noto come

¹²⁶ Federal Office for International Security, *Artificial Intelligence*. Disponibile su: BSI - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html Artificial Intelligence

¹²⁷ Stiftung Neue Verantwortung, *AI Talent Flows in Germany*, 14 dicembre 2022. Disponibile su: AI Talent Flows in Germa <https://www.interface-eu.org/publications/ai-talent-flows-germany>

KI-Marktüberwachungsgesetz (KIMÜG), il quale prevede l'istituzione di due entità chiave all'interno della *Bundesnetzagentur*:

- *UKIM (Unabhängige KI-Marktüberwachungskammer)*: un'unità indipendente responsabile della sorveglianza dei sistemi AI ad alto rischio, che garantisce un controllo imparziale e conforme alle normative europee¹²⁸.
- *KoKIVO (Koordinierungs- und Kompetenzzentrum für KI-Marktüberwachung)*: un centro di coordinamento e competenza che fornisce supporto tecnico e facilita la collaborazione tra le diverse autorità coinvolte nella supervisione dell'IA¹²⁹.

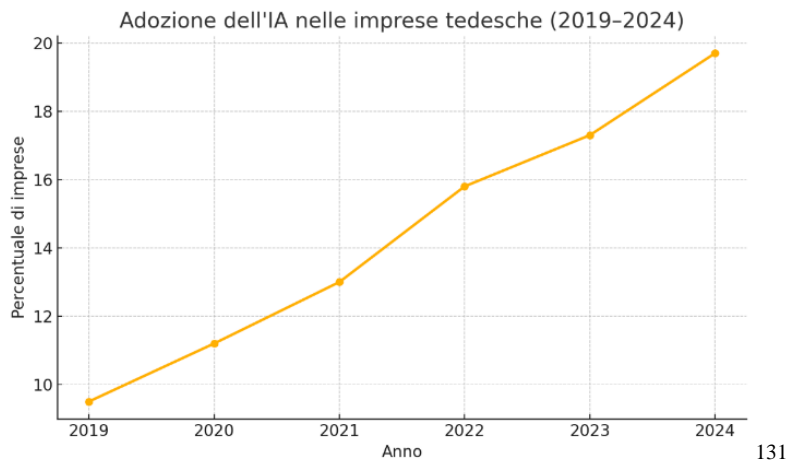
Inoltre, per promuovere l'innovazione e facilitare l'adozione dell'IA, la Germania ha introdotto sandbox regolamentati. Questi ambienti controllati permettono alle imprese, in particolare alle PMI, di sviluppare e testare sistemi AI in condizioni reali, beneficiando di un supporto normativo e tecnico durante il processo. Tale approccio mira a ridurre le barriere all'ingresso e a garantire la conformità ai requisiti dell'AI Act.

Negli ultimi anni, sempre più imprese tedesche hanno adottato sistemi di intelligenza artificiale, segnando una crescita costante e significativa. Secondo un'indagine del 2024, quasi il 19,7 % delle aziende ha già integrato soluzioni di IA nei loro processi, dato superiore alla media UE (13,5%) e Italia (8,2 %) ¹³⁰. L'AI Act ha accelerato questo trend, molto apprezzato dalle grandi imprese per accesso più facilitato a mercato regolamentato e maggior innovazione. Il grafico sottostante mostra l'andamento dell'adozione dell'IA nelle aziende tedesche dal 2019 al 2024:

¹²⁸ Rödl & Partner, *The draft bill for the AI Market Surveillance Act: German Implementation of the AI Act*, 26 febbraio 2025. Disponibile su: <https://www.roedl.it/it/temi/data-protection-bites/2-2025/draft-bill-ai-market-surveillance-act-german-implementation-ia-act#:~:text=Recent-,The%20draft%20bill%20for%20the%20AI%20Market%20Surveillance%20Act,Implementation%20of%20the%20AI%20Act&text=The%20EU%20Artificial%20Intelligence%20Regulation,for%20high%20Risk%20AI%20systems.eillance%20Act:German%20Implementation%20of%20the%20AI%20Act|Rödl%20&Partner>

¹²⁹ *Bundesministerium für Wirtschaft und Klimaschutz (BMWK) und Bundesministerium der Justiz (BMJ), Referentenentwurf zum KI-Marktüberwachungsgesetz (KIMÜG)*, 2024. Disponibile su: [1736937860406 file:///C:/Users/utente/Desktop/1736937860406.pdf](file:///C:/Users/utente/Desktop/1736937860406.pdf)

¹³⁰ Eurostat, *Use of artificial intelligence in enterprises*, 23 gennaio 2025. Disponibile su: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises - Statistics Explained - Eurostat



Uno degli esempi più emblematici dell'applicazione avanzata di intelligenza artificiale è rappresentato dalla multinazionale tedesca SAP, leader nel settore dei software gestionali. Nel 2023, l'azienda ha integrato nei suoi sistemi Joule, l'assistente intelligente in grado di generare codici, tesi e insight aziendali personalizzati¹³². Nel secondo trimestre del 2024, l'IA ha avuto un impatto positivo sulle performance aziendali: il 20% delle trattative commerciali ha incluso funzionalità AI avanzate, contribuendo a una crescita del 33% delle vendite ERP in cloud¹³³. Il fatturato complessivo ha raggiunto 8,29 miliardi di euro, in aumento del 10% rispetto all'anno precedente¹³⁴. SAP ha anche avviato una

¹³¹ Rielaborazione propria su dati Eurostat, Use of artificial intelligence in enterprises, 23 gennaio 2025.

¹³² SAP, Joule: *New Generative AI Assistant*, 26 settembre 2023. Disponibile su: SAP <https://news.sap.com/2023/09/joule-new-generative-ai-assistant/> Announces Joule, a New Generative AI Assistant | SAP News Center

¹³³ Vendite di soluzioni di Enterprise Resource Planning (ERP) erogate in modalità cloud, ovvero software gestionali accessibili via internet, ospitati su server remoti, che permettono alle imprese di gestire attività integrate come contabilità, supply chain, risorse umane e vendite, spesso con modello di abbonamento (Software as a Service, SaaS), senza necessità di installazione locale.

¹³⁴ PR Newswire, *SAP Announces Q2 2024 Results*, 22 luglio 2024. Disponibile su: SAP <https://www.prnewswire.com/news-releases/sap-announces-q2-2024-results-302203021.html#:~:text=Second%20Quarter%202024,-In%20the%20second&text=Cloud%20revenue%20was%20up%205,down%207%25%20at%20constant%20currencies.> nounces Q2 2024 Results

¹³⁵ CRN, *SAP Restructuring Now Expected To Impact Up To 10,000 Jobs*, 23 luglio 2024. Disponibile su: SAP Restructuring No <https://www.crn.com/news/software/2024/sap-restructuring-now-expected-to-impact-up-to-10-000-jobs> Expected To Impact Up To 10,000 Jobs

¹³⁶ Ifo Institute, *Press Release, Many companies are hesitant about artificial intelligence – Germany nevertheless performs well in a European comparison*, 6 settembre 2024. Disponibile su: Many companies are hesitant about artificial intelligence – Germany nevertheless performs well in a European comparison | Press release | ifo Institute

¹³⁷ ZEW Mannheim, *AI Adoption Stagnates in German Companies*, 28 agosto 2024. Disponibile su: Press Release: AI Adoption Stagnates in German Compa <https://www.zew.de/en/press/latest-press-releases/ai-adoption-stagnates-in-german-companies> nies | ZEW

profonda riorganizzazione interna, coinvolgendo 10.000 dipendenti per allineare le competenze alla transizione tecnologica¹³⁵.

Nonostante alcune stime indichino che quasi un'impresa su cinque in Germania utilizza soluzioni IA, secondo fonti autorevoli come *Ifo Institut*¹³⁶ e ZEW, l'adozione avanzata dell'IA è ancora limitata a circa l'11-12% delle aziende, e mostra segnali di stagnazione¹³⁷. Questa discrepanza riflette una polarizzazione interna al tessuto imprenditoriale: le grandi imprese e le startup ad alta intensità tecnologica trainano l'innovazione, mentre una larga parte delle PMI fatica a introdurre strumenti realmente trasformativi. Un'ulteriore difficoltà riscontrata in Germania riguarda l'approccio ancora incerto delle imprese verso l'intelligenza artificiale generativa. Molte aziende, pur consapevoli del suo potenziale trasformativo, dichiarano di non essere pronte ad adottarla in modo sistemico, temendo di restare indietro rispetto ai concorrenti internazionali. A ciò si aggiunge il ritardo del comparto manifatturiero, tradizionalmente centrale per l'economia tedesca, dove l'adozione di strumenti AI è ancora marginale. Questo ritardo si spiega sia con la scarsità di risorse tecniche e umane, sia con dubbi persistenti sull'effettiva affidabilità delle tecnologie disponibili e sul ritorno dell'investimento nel medio termine.

2.1.3 Italia: recepimento e criticità

L'Italia, non ha reagito con la stessa tempestività della Germania o della Francia, ma comunque ha accelerato i propri sforzi negli ultimi anni per adattarsi alle politiche dell'EU in materia di IA. Nel 2021 è stata pubblicata una proposta per adottare una strategia da parte del Ministero dello Sviluppo Economico (MIMIT), in collaborazione con il Ministero dell'Università e della Ricerca (MUR) e il Dipartimento per la trasformazione digitale¹³⁸. La versione definitiva del 2022 ha come obiettivi principali lo sviluppo di una realtà innovativa ma etica, rafforzare la ricerca e sostegno al trasferimento tecnologico, in linea con l'AI Act. Per quest'ultimo, l'Italia ha già avviato un sistema di

¹³⁸ Gruppo di Esperti MISE IA, Ministero dello Sviluppo Economico (MIMIT), Ministero dell'Università e della Ricerca (MUR), Dipartimento per la Trasformazione Digitale, Proposte per una Strategia Italiana per l'Intelligenza Artificiale, 2021. Disponibile su: 25-0 https://www.mimit.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf7-20

recepimento¹³⁹, che coinvolge diversi attori, anche se la designazione delle autorità competenti è ancora in corso, da quanto è emerso nei lavori parlamentari¹⁴⁰. Si prevede comunque un quadro composto da diversi attori:

- Il Garante per la protezione dei dati personali che supervisiona le questioni relative alla *privacy*;
- Il Ministero delle Imprese e del Made in *Italy*, per valutare la conformità delle tecnologie a livello industriale;
- L'AGID (Agenzia per l'Italia Digitale), che definisce le linee guida tecniche e l'interoperabilità;
- L'INAIL, per regolare l'IA in materia di lavoro e sicurezza pubblica.

Nonostante l'Italia ha aderito a livello formale all'*AI Pact*, proposto dalla Commissione Europea, per il momento non risultano attivi sandbox normativi, come quelli già presenti in Germania, nei Paesi Bassi o in Francia. Infatti per quanto riguarda le criticità normative, emergono diverse sfide che l'Italia sta affrontando e dovrà affrontare nei prossimi anni. Tra queste è importante sottolineare la mancanza di una governance centralizzata, con conseguente rischio di frammentare le responsabilità tra enti diversi, rendendo molto difficile una supervisione corretta. Inoltre, vi è un ritardo normativo tra l'AI Act e alcuni settori italiani quali la giustizia o la sanità che ancora non hanno stabilito obblighi in materia di trasparenza algoritmica o *auditing ex ante*¹⁴¹. Uno dei maggiori problemi, però, è rappresentato dalla mancanza di competenze tecniche nella pubblica amministrazione, sia locale che centrale. Di conseguenza, diviene difficile adattarsi all'AI Act, soprattutto per la comprensione e applicazione della valutazione e documentazione tecnica. Inoltre, l'Italia è molto dipendente da fornitori esterni, spesso neanche europei,

¹³⁹ Dipartimento per la trasformazione digitale, Agenzia per l'Italia Digitale, *STRATEGIA ITALIANA PER L'INTELLIGENZA ARTIFICIALE 2024-2026*, 2024. Disponibile su: https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf

¹⁴⁰ Camera dei Deputati, Senato della Repubblica, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, Dossier XIX Legislatura, 14 aprile 2025.

¹⁴¹ Francario S., *AI Act e pubblica amministrazione*, Giustizia Insieme, 31 ottobre 2024. Disponibile su: [www.giustiziainsieme.it](https://www.giustiziainsieme.it/it/diritto-e-processo-amministrativo/3286-ai-act-e-pubblica-amministrazione-simone-francarionsieme.it) <https://www.giustiziainsieme.it/it/diritto-e-processo-amministrativo/3286-ai-act-e-pubblica-amministrazione-simone-francarionsieme.it>

¹⁴² POLIMI School of Management, *Nel PNRR 48 miliardi per l'Agenda Digitale, "chiamata" senza precedenti all'Italia*, Osservatori.net digital innovation, 2023. Disponibile su: <https://www.osservatori.net/comunicato/agenda-digitale/agenda-digitale-pnrr/#:~:text=Il%20PNRR%20dedica%20al%20digitale,48%20miliardi%20di%20risorse%20complessive,one 48 mld>

per l'implementazione di AI nei settori strategici, rendendo necessarie misure più costose e adeguate a garantire comunque la sovranità digitale. Nonostante ciò, il Paese ha destinato 48 miliardi di euro per la transizione digitale, usando fondi provenienti dal PNRR (Piano Nazionale di Ripresa e Resilienza), la quota più alta tra i Paesi dell'Unione, che ha permesso all'Italia di posizionarsi prima in classifica nell'Unione, per quanto riguarda il numero di progetti di IA implementati nella PA¹⁴². Tuttavia, gli italiani si collocano al 23° posto in Europa per competenze digitali, con solo il 46% degli adulti che possiede competenze informatiche di base e il tasso di laureati in discipline ICT è tra i più bassi dell'Unione, attestandosi all'1,5¹⁴³. È proprio questa discrepanza tra investimenti effettuati e capacità del capitale umano di usufruire correttamente dell'IA una delle più grandi sfide tecnologiche per l'Italia. La Strategia Italiana per l'Intelligenza Artificiale 2024-2026 riconosce queste sfide e pone l'accento sulla necessità di rafforzare le competenze digitali nella PA, promuovendo la formazione e l'aggiornamento del personale. In tale contesto, a partire da maggio 2024, è stato istituito l'Istituto Italiano per l'Intelligenza Artificiale per l'Industria (AI4I), con sede a Torino, pensato come centro di eccellenza per la promozione della ricerca applicata in ambito industriale¹⁴⁴. È un punto strategico per il trasferimento tecnologico tra mondo accademico e imprese offrendo anche un punto di accesso per le PMI italiane alle risorse computazionali e infrastrutturali connesse alle *future gigafactory*¹⁴⁵ europee dell'IA. Risulta fondamentale non solo che l'innovazione tecnologica venga seguita da riforme istituzionali ma anche che ci sia un coordinamento efficace tra i vari livelli istituzionali e un adeguamento delle competenze, soprattutto in materia di conoscenze, applicazioni e ricerca.

¹⁴³ Network360, Digitalizzazione: *Italia al 23° posto in EU, ma in cima per progetti AI nel pubblico*, Innovation Post, 29 novembre 2024. Disponibile su: Digitalizzazione: Italia al 2° posto in EU, ma in cima per progetti AI nel pubblico - Innovation Post [https://www.innovationpost.it/attualita/digitalizzazione-italia-al-23-posto-in-eu-ma-in-cima-per-progetti-ai-nel-pubblico/3° posto in EU, ma in cima per progetti AI nel pubblico - Innovation Post](https://www.innovationpost.it/attualita/digitalizzazione-italia-al-23-posto-in-eu-ma-in-cima-per-progetti-ai-nel-pubblico/3°%20posto%20in%20EU,%20ma%20in%20cima%20per%20progetti%20AI%20nel%20pubblico)

¹⁴⁴ Ministero dell'Economia e delle Finanze, *Nasce Fondazione Ai4Industry. Giorgetti: presidiare intelligenza artificiale per sviluppo industriale*, 3 maggio 2024. Disponibile su: Nasce Fondazione [https://www.mef.gov.it/inevidenza/Nasce-Fondazione-Ai4Industry.-Giorgetti-presidiare-intelligenza-artificiale-per-sviluppo-industriale/ Ai4Industry. Giorgetti: presidiare intelligenza artificiale per sviluppo industriale - MEF](https://www.mef.gov.it/inevidenza/Nasce-Fondazione-Ai4Industry.-Giorgetti-presidiare-intelligenza-artificiale-per-sviluppo-industriale/Ai4Industry.Giorgetti:presidiareintelligenzaartificialeperlosviluppoindustriale-MEF)

¹⁴⁵ Grandi impianti industriali dedicati alla produzione di hardware avanzato necessario per l'IA.

2.2 Divergenze tra Stati membri e conseguenze competitive sui mercati globali

Il problema della coerenza interpretativa tra gli Stati Membri rappresenta una sfida importante per l'Unione Europea, nonostante l'adozione del Regolamento (UE) 2024/1689. Il principale obiettivo di quest'ultimo è quello di garantire un quadro uniforme, volto a tutelare i diritti fondamentali e il corretto funzionamento del mercato interno. Nonostante ciò, i contesti amministrativi nazionali sono molto diversi tra di loro e ciò lascia molto spazio sia all'interpretazione che all'applicazione delle regole. La parità concorrenziale tra operatori economici, la libera circolazione dei servizi e la certezza del diritto rischiano di essere minati. La funzione regolativa dell'AI Act rischia di essere compromessa seriamente con effetti rilevanti sul mercato unico digitale europeo. Come già è stato citato, l'articolo 3 del Regolamento definisce l'intelligenza artificiale come “un sistema basato su tecniche di apprendimento automatico, logiche o basate sulla conoscenza”, quindi progettato per influenzare le decisioni. Tale definizione è molto ampia e lascia margini di discrezionalità¹⁴⁶ alle amministrazioni nazionali infatti, si rende necessario definire in via preliminare cos'è un sistema automatico, un'analisi automatizzata oppure un algoritmo predittivo. Inoltre, un numero eccessivo di applicazioni può essere incluso nella definizione di cui all'Articolo 3 e ciò può rappresentare un ostacolo per i fornitori e i destinatari dei sistemi¹⁴⁷. Sussiste anche una problematica di natura geografica, poiché in realtà transfrontaliere può divenire molto difficile far convivere sistemi di intelligenza artificiale trattati in modo diverso dagli Stati confinanti. Come conseguenza, ciò può condurre a frizioni regolatorie e qualificazioni giuridiche non chiare.

Un altro articolo di difficile applicazione è l'articolo 6 dell'AI Act, il quale identifica i “sistemi ad alto rischio” sulla base dei settori di applicazione e dei criteri qualitativi. Anche in tal caso sussistono diverse interpretazioni. Un esempio di diversa interpretazione è quello della definizione degli “impieghi in ambiti sensibili”, laddove il grado di sensibilità è determinato dagli Stati Membri. È evidente pertanto la problematica nella classificazione dei sistemi di IA in base al loro rischio. Per risolvere tale

¹⁴⁶ Corte dei Conti Europea, *Applicazione del diritto dell'UE: le responsabilità della Commissione europea in materia di vigilanza ai sensi dell'articolo 17, paragrafo 1, del trattato sull'Unione europea*, 2018.

¹⁴⁷ Veale, M., & Zuiderveen Borgesius, F. *Demystifying the Draft EU Artificial Intelligence Act*. *Computer Law Review International*, 2021, 22(4), 97–112. Disponibile su: file:///C:/Users/utente/Downloads/VealeBorgesius2021_typeset.pdf

problematica sono state proposte metriche oggettive come matrici di costi-benefici oppure standard settoriali per evitare l'eccessiva soggettività nel processo di classificazione¹⁴⁸. Tali ambiguità distorcono il mercato creando incertezza e frizione normativa nell'uso dell'AI, soprattutto per le imprese attive in più Paesi. Ogni Stato, infatti, teoricamente potrebbe sviluppare una sua linea normativa vanificando l'obiettivo di armonizzazione perseguito dal Regolamento e aumentando il rischio di frammentazione normativa.

Un'altra divergenza nell'Unione Europea è data dalle differenze istituzionali adottate dagli Stati per attuare il Regolamento. Il testo normativo, determinando che sono gli Stati a designare le autorità competenti per sorvegliare il mercato, ha originato modelli organizzativi eterogenei, che non sono compatibili tra loro poiché utilizzano prassi diverse ed hanno capacità tecnica diverse oltre ad indirizzare in modo distribuito le competenze tra varie agenzie governative.

Ad esempio, in Germania è stata istituita l'autorità nazionale di vigilanza sui sistemi di IA (BNetzA) e l'Agenzia *Deutsche Akkreditierungsstelle (DAkkS)* per valutare la conformità delle decisioni. Inoltre, al fine di rafforzare il coordinamento tra le unità operative soprattutto in materia di *machine learning* sono state aggiunte ulteriori due strutture: l'UKIM (*Unabhängige KI-Marktüberwachungskammer*) e il KoKIVO. Tale approccio si differenzia da quello francese o, ancora di più, da quello italiano. Infatti, in Francia è presente la *Commission Nationale de l'Informatique et des Libertés (CNIL)* per la protezione dati e l'*Autorité de la Concurrence* per monitorare la concorrenza che trattano anche i sistemi di IA. Mentre, nel contesto italiano i compiti sono praticamente distribuiti tra il Garante per la protezione dei dati personali, il Ministero delle imprese e del Made in Italy e l'Agenzia per l'Italia Digitale. Le istituzioni / agenzie citate hanno dotazioni organiche (personale) ed amministrative (laboratori di prova e validazione) diverse e con diversa specializzazione, pertanto la probabilità di creare difformità organizzative è sempre maggiore. In alcuni Paesi, le agenzie tecniche sono permanenti e interagiscono in tempo reale con le imprese, gli enti notificati oppure AI *Office* europeo,

¹⁴⁸ Fraser, H. L., & Bello y Villarino, J.-M.. *Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough*. European Journal of Risk Regulation, 27 luglio 2023. Disponibile su: <ssr://C:/Users/utente/Downloads/ssrn-4516917.pdf>

mentre in altri è quasi impossibile sorvegliare realmente i sistemi di IA immessi nel mercato. La mancata armonizzazione delle strutture di controllo compromette non solo l'effettività del diritto dell'Unione ma genera anche asimmetrie concorrenziali rispetto al mercato unico¹⁴⁹. Su tali presupposti è facile dedurre che nel caso dell'AI Act la governance multilivello, può diventare una sovrapposizione di ruoli, competenze e decisioni. Il rischio principale è quello di ottenere una regolazione solo formale dell'intelligenza artificiale attraverso l'impiego di modelli ibridi, centralizzati o decentrati senza che ci sia un modello di base comune europeo, valido per tutti gli Stati Membri e soprattutto dotato di attività specifiche comuni. Un'ulteriore causa di divergenza tra gli Stati Membri riguarda gli approcci regolatori adottati che sono molto diversi tra di loro. Le priorità politiche e le strategie di innovazione digitale sono argomenti fondamentali supportati dai vari Paesi ma con metodi differenti, nonostante essi condividano lo stesso testo normativo. Nell'applicazione quotidiana delle norme europee, questo produce effetti disomogenei. È confermato che alcuni Paesi, come la Spagna, la Francia o i Paesi Bassi, avevano già strategie nazionali preesistenti in materia di IA¹⁵⁰, con obiettivi pro-innovazione, fondi dedicati e sistemi di supporto tecnico per le imprese¹⁵¹, invece altri ordinamenti hanno un approccio più frammentario e prudenziale, caratterizzato da reattività e non proattività. Per quanto riguarda gli strumenti adottati, Stati come la Germania o la Spagna hanno introdotto *sandbox* normativi per testare l'AI Act ma in

¹⁴⁹ Novelli, C., Hacker, P., Morley, J., Trondal, J., Floridi, L., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, *European Liberal Forum*, 2023. Disponibile su: <https://arxiv.org/pdf/2407.10369> for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities

¹⁵⁰ European Commission, *AI Watch National strategies on Artificial Intelligence A European perspective in 2019*, JRC TECHNICAL REPORT, 2020. Disponibile su: [file:///C:/Users/utente/Downloads/national_strategies_on_artificial_intelligence_final_1%20\(1\).pdf](file:///C:/Users/utente/Downloads/national_strategies_on_artificial_intelligence_final_1%20(1).pdf)

¹⁵¹ OECD, *An overview of national AI strategies and policies*, OCSE, 3 agosto 2021. Disponibile su: <file:///C:/Users/utente/Downloads/c05140d9-en.pdf>

BMWK: "*Regulatory Sandboxes – Testing Environments for Innovation and Regulation*", BMWK, Federal Ministry of Economic Affairs and Energy, novembre 2024.

¹⁵³ BOLETÍN OFICIAL DEL ESTADO, MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL, Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial, 10 novembre 2023.

¹⁵⁴ Uuk, K., Madiaga, T. & Vigano, E., *Operationalising the Definition of General-Purpose AI Systems*, Stanford University, Future of Life Institute, 2023. Disponibile su: <https://arxiv.org/pdf/2306.02889>

settori strategici come la sanità o l'*automotive*¹⁵²: rispettivamente il programma *Reallabore* oppure il *sandbox* spagnolo AESIA¹⁵³. Ci sono, al contrario, altri Paesi che invece si limitano a rispettare la regolamentazione o gli obiettivi dell'Unione in maniera formale. Lo sviluppo di uno spazio giuridico digitale può essere ostacolato da una distorsione nell'applicazione sostanziale del diritto, creata dalla frammentazione degli approcci regolatori¹⁵⁴. Inoltre, le imprese in questo modo possono alimentare fenomeni di *regulatory arbitrage*¹⁵⁵, dal momento che possono essere incentivate ad allocare le attività di sviluppo in Stati che presentano un orientamento molto più permissivo.

A conferma di tale eterogeneità applicativa, è utile esaminare alcuni casi emblematici che mostrano come, pur condividendo il medesimo quadro normativo europeo, gli Stati Membri interpretino e implementino l'AI Act secondo priorità, strumenti e sensibilità molto diverse.

La Spagna

Il Paese ha istituito la prima autorità di vigilanza nazionale dedicata solo all'intelligenza artificiale: la *Agencia Española de Supervisión de la Inteligencia Artificial (AESIA)*. Non solo quest'ultima ha poteri di supervisione, autorizzazione e sanzione, ma ha avviato un programma di *sandbox* regolatori per affiancare le imprese nell'implementazione dell'AI Act. Nonostante ciò, il sistema spagnolo applica criteri più flessibili nella classificazione dei modelli di intelligenza artificiale, senza alimentare un'impostazione restrittiva, come la Germania o la Francia¹⁵⁶.

I Paesi Bassi

Nei Paesi Bassi invece è presente l'Autorità olandese della Protezione Dati (AP). Principalmente quest'ultima si pone l'obiettivo di dialogare al meglio con le imprese, alimentare la co-regolazione e adottare linee guida non vincolanti. Questo, per i Paesi Bassi, permette di integrare più facilmente i requisiti ma solleva interrogativi sulla reale

¹⁵⁵ Pratica con cui imprese o operatori economici sfruttano le differenze normative tra giurisdizioni per ridurre i costi di conformità o aggirare vincoli regolatori.

¹⁵⁶ Holistic AI, *Spain's Approach to AI Regulation: A Flexible Model for Innovation*, 23 marzo 2023. Disponibile su: AI Regulation Around the World <https://www.holisticai.com/blog/spain-ai-regulation>: Spain

forza cogente delle misure soprattutto in settori che necessitano di particolare sensibilità come l'istruzione o la sanità¹⁵⁷.

L'Estonia

L'Estonia ha invece adottato un approccio sperimentale, che ha sollevato alcune critiche. Il Ministero della Giustizia estone ha avviato l'uso di sistemi per risolvere controversie civili minori, affidando a software il compito di emettere decisioni vincolanti nei procedimenti inferiori a 7000 euro¹⁵⁸. Tale dinamica non è compatibile con gli articoli 6 e 14 dell'AI Act, i quali impongono trasparenza, diritto al ricordo e supervisione umana. La dottrina ha utilizzato il termine "automazione opaca", dal momento che è stato violato il principio di proporzionalità europeo. La coesistenza di pratiche divergenti rappresenta già una realtà con effetti che si riversano sulla certezza del diritto e sulla competitività nei vari mercati nazionali. L'intervento dell'AI Office è reso urgente dall'assenza di un quadro interpretativo vincolante condiviso.

Le divergenze tra gli Stati membri possono portare conseguenze negative per le imprese, se non gestite con una linea di coordinamento europeo gestita in maniera efficace. La duplicazione degli oneri di conformità rappresenta il primo effetto evidente: le aziende applicano diversamente le regole sui sistemi di intelligenza artificiale, anche se la norma sostanziale rimane la stessa. Ciò comporta costi maggiori in consulenze, adeguamento comportamentale e valutazione di conformità. Un esempio rilevante riguarda l'azienda tedesca *Siemens Healthineers*, che sviluppa software diagnostici ad alto rischio basati sull'IA per analizzare immagini mediche. Il problema principale riguarda il fatto che, operando in Paesi diversi con applicazioni divergenti sull'applicabilità del Regolamento, l'azienda ha attivato procedure parallele di valutazione della conformità, ha dovuto adattare i diversi requisiti o interagire con autorità multiple (BNetzA in Germania, AESIA in Spagna, AGID/Garante in Italia). La conseguenza è stata l'aumento dei costi di compliance e conformità. Questi per un singolo modello ad alto rischio si possono aggirare anche intorno ai 29.277 euro, considerando 23.000 euro da spendere per la

¹⁵⁷ Autoriteit Persoonsgegevens (AP) – *Rapporto su IA e Rischi Algoritmici nei Paesi Bassi (Inverno 2023–2024)*.

¹⁵⁸ Niiler E., "Can AI Be a Fair Judge in Court? Estonia Thinks So", WIRED, 25 marzo 2019. Disponibile su: [Can AI Be a Fair Judge in Court? Estoni https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/a](https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/a) Thinks So | WIRED

certificazione e altri costi di compliance, arrivando anche a circa 50.000 euro l'anno¹⁵⁹. Con la mancanza di standard armonizzati, tali costi possono solo aumentare. Inoltre, si è verificato un ritardo per quanto concerne l'introduzione di nuovi sistemi di IA in almeno tre mercati europei, a causa di mancanza di chiarezza sulle procedure normative. L'assenza di definizioni uniformi in materia di intelligenza artificiale rende difficile, per le imprese, prevedere l'impatto dell'introduzione di sistemi intelligenti nei mercati esteri. Questa incertezza normativa rischia di ostacolare seriamente l'attività economica transfrontaliera, compromettendo il principio di certezza del diritto, tutelato tanto dalla giurisprudenza della Corte di Giustizia dell'Unione Europea quanto dall'articolo 41 della Carta dei diritti fondamentali dell'UE.

Un esempio emblematico di *forum shopping* regolatorio è rappresentato dalla startup tedesca *Jina AI*, fondata da *Han Xiao* e specializzata nello sviluppo di framework open source per l'intelligenza artificiale. Per forum shopping regolatorio, si intende un fenomeno per cui imprese o soggetti economici scelgono di operare in uno Stato o in un ordinamento giuridico piuttosto che in un altro, non per motivi economici o logistici, ma per sfruttare un contesto normativo più favorevole. Di fronte alle difficoltà normative e alla frammentazione del quadro regolatorio europeo, *Jina AI* ha deciso di spostare parte delle sue operazioni negli Stati Uniti, attratta da un contesto più favorevole all'innovazione e meno focalizzato su vincoli regolatori stringenti. *Xiao* ha spiegato che in Germania e più in generale in Europa il discorso sull'IA ruota attorno a etica e regolamentazione, mentre negli Stati Uniti e in Cina gli investitori sono principalmente orientati alla crescita e allo sviluppo tecnologico¹⁶⁰. Questa scelta evidenzia come le startup europee, pur avendo radici solide nei loro paesi d'origine, possano cercare ambienti esteri più flessibili per evitare rallentamenti competitivi derivanti da normative complesse. Se l'AI Office non vincola fortemente gli Stati, il rischio è quello di generare

¹⁵⁹ 2021.AI, *Understanding the EU AI Act penalties and achieving regulatory compliance*, January 2024. Disponibile su: <https://2021.ai/news/understanding-the-eu-ai-act-penalties-and-achieving-regulatory-compliance#:~:text=To%20incentivize%20adherence%2C%20the%20EU,meet%20ethical%20and%20safety%20standards.alties and achieving regulatory compliance>

¹⁶⁰ The Wall Street Journal, *The Tech Industry Is Huge—and Europe's Share of It Is Very Small*, 19 maggio 2025. Disponibile su: <https://www.wsj.com/tech/europe-big-tech-ai-1f3f862cy Is Huge—and Europe's Share of It Is Very Small - WSJ>

una convergenza normativa che però è solo apparente¹⁶¹. Tale situazione non combacerebbe con l'Articolo 4, par. 3 del TUE, il quale impone agli Stati membri una cooperazione leale per attuare il diritto e la creazione di un mercato unico europeo, che sia però effettivamente integrato e competitivo, proprio per permettere lo sviluppo aziendale in Europa ed evitare che portino le loro sedi all'estero.

Oltre alla presenza di divergenze normative, le imprese che operano in più Stati Membri si trovano ad affrontare ostacoli pratici e strutturali che condizionano l'espansione, l'innovazione e la conformità aziendale. Le imprese, in particolare quelle tecnologiche, che operano in più Stati membri, devono affrontare una serie di operatività strategiche e organizzative legate al fatto che le pratiche sono eterogenee. La conformità giuridica e le modalità con cui le aziende integrano i propri processi decisionali e possono essere un problema. Le multinazionali tecnologiche o le grandi imprese *AI Native*¹⁶², gestiscono operazioni parallele in vari ordinamenti e quindi spesso è necessario duplicare unità regolatorie interne per ciascun mercato. Ciò conduce a inefficienze organizzative, che si manifestano soprattutto nei reparti di compliance, *deployment* tecnico e *product management*. Come conseguenza, la formulazione della documentazione dei rischi e l'adozione dell'algoritmo a livello europeo ha subito ritardi e discrepanze. Le imprese sono costrette a suddividere le strategie in base al mercato, dal momento che, almeno per adesso, è impossibile adottare un modello unico operativo valido per tutti gli Stati Membri, perché la sua attuazione cambierebbe da Paese a Paese: questo non vale solo per le grandi imprese ma anche per le *scale up europee* con focus nel *cloud*, *natural language processing* o sanità digitale. I sistemi basati sull'intelligenza artificiale, pur essendo progettati per operare in modo flessibile, risultano difficilmente scalabili a livello transnazionale. Le imprese sono quindi costrette a personalizzare i propri prodotti in funzione delle normative dei singoli Stati Membri, anche se queste derivano dallo stesso Regolamento europeo. Questo processo di adattamento coinvolge diversi aspetti, tra cui le procedure di *audit*, le informative agli utenti e i requisiti normativi, che vengono

¹⁶¹ Novelli C., Hacker P., Morley J., Trondal J., Floridi L., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, *European Journal of Risk Regulation*, vol. 4, pp. 1–25, 8 maggio 2024. Disponibile su: [a-robust-g file:///C:/Users/utente/Downloads/a-robust-governance-for-the-ai-act-ai-office-ai-board-scientific-panel-and-national-authorities.pdf](file:///C:/Users/utente/Downloads/a-robust-governance-for-the-ai-act-ai-office-ai-board-scientific-panel-and-national-authorities.pdf)

¹⁶² Aziende che hanno incorporato l'intelligenza artificiale come elemento fondativo del loro modello di business, processo produttivo o offerta di prodotti/servizi, fin dalla loro nascita.

interpretati e attuati in modo diverso. Il fenomeno è particolarmente rilevante in settori sensibili come la cybersicurezza, la sanità digitale (*health-tech*) e l'elaborazione del linguaggio naturale (NLP), dove anche piccole differenze nella classificazione del rischio possono costringere le aziende a dividere i percorsi di sviluppo del prodotto e a trattare mercati distinti come se fossero separati. Le conseguenze sono evidenti: frammentazione del ciclo di vita del prodotto, maggiore complessità nei sistemi di certificazione e rallentamenti nel rilascio degli aggiornamenti. Inoltre, le piattaforme virtuali di assistenza tecnica, utilizzate ad esempio nella pubblica amministrazione o nel settore bancario, e basate su algoritmi generativi, subiscono trattamenti diversi a seconda del contesto nazionale: in alcuni Paesi sono semi-automatizzate, mentre in altri è obbligatorio prevedere forme più rigorose di supervisione umana, soprattutto a causa di differenze interpretative tra GDPR e AI Act. L'efficienza e l'effettiva interoperabilità dei mercati vengono ostacolate dai fornitori che devono mantenere versioni separate dello stesso sistema. Questa complessità normativa e operativa, unita alla mancanza di uniformità nell'attuazione pratica del quadro europeo, sta spingendo sempre più imprese tecnologiche a rivedere le proprie strategie di localizzazione e sviluppo. Un caso emblematico, oltre a quello dei sistemi di assistenza virtuale, è rappresentato da *Bird*, una startup olandese specializzata in comunicazioni cloud, che nel febbraio 2025 ha annunciato l'intenzione di trasferire la maggior parte delle sue operazioni fuori dall'Europa. Il CEO, *Robert Vis*, ha motivato la scelta sottolineando che l'ambiente normativo europeo risulta troppo restrittivo per sostenere l'innovazione nell'ambito dell'intelligenza artificiale, aggravato anche dalla difficoltà nel reperire talenti altamente specializzati. Per questo motivo, l'azienda ha deciso di delocalizzare le sue attività principali a *New York, Singapore e Dubai*, mantenendo in Europa solo un ufficio in Lituania e la sede fiscale nei Paesi Bassi¹⁶³.

Le piccole e medie imprese sono quelle che si trovano in una posizione non avvantaggiata per l'adozione transnazionale dell'IA, dal momento che non hanno strutture di compliance e team legali dedicati per affrontare la questione. L'AI Act prevede misure

¹⁶³ Reuters, *Dutch software firm Bird to leave Europe due to onerous regulations in AI era, says CEO*, 24 febbraio 2025. Disponibile su: Dutch sof [https://www.reuters.com/technology/dutch-software-firm-bird-leave-europe-due-onerous-regulations-ai-era-says-ceo-2025-02-24/#:~:text=AMSTERDAM%2C%20Feb%2024%20\(Reuters\),difficulties%20hiring%20skilled%20technology%20workers.tware firm Bird to leave Europe due to onerous regulations in AI era, says CEO | Reuters](https://www.reuters.com/technology/dutch-software-firm-bird-leave-europe-due-onerous-regulations-ai-era-says-ceo-2025-02-24/#:~:text=AMSTERDAM%2C%20Feb%2024%20(Reuters),difficulties%20hiring%20skilled%20technology%20workers.tware firm Bird to leave Europe due to onerous regulations in AI era, says CEO | Reuters)

per le PMI ma, nonostante linee guida e sandbox normativi, ancora non è accompagnato da strumenti normativi sufficientemente armonizzati tra i Paesi, quindi l'adozione dell'IA resta un obiettivo difficile da raggiungere per la maggioranza delle realtà di impresa, piccole o medie. Infatti, meno del 20% delle PMI sono a conoscenza dei programmi governativi di supporto per l'adozione di strumenti digitali, e tra coloro che ne sono a conoscenza, molti segnalano difficoltà nell'accesso a tali programmi a causa di burocrazia e mancanza di risorse¹⁶⁴. Questo si applica particolarmente all'*healthtech*, la finanza o risorse umane, dove ogni Stato membro può richiedere adattamenti documentali e valutazioni che una PMI non riuscirebbe senza un grande supporto esterno. L'adeguamento all'AI Act può comportare per una PMI produttrice di soluzioni di IA un costo stimato di circa 300.000 euro, pari all'1,3% del fatturato annuo. Questo importo copre attività come *auditing* esterno, gestione della qualità dei dati e valutazioni di conformità. Sebbene inferiore alle stime iniziali, tale cifra rappresenta comunque un onere rilevante per molte PMI¹⁶⁵.

È evidente come è presente il rischio di ampliare il divario competitivo tra grandi gruppi multinazionali e imprese minori e rischia di creare, al posto di un'innovazione distribuita, un effetto sistemico in cui il mercato unico globale è accessibile solo alle grandi aziende.

L'AI Act mira a definire obblighi tecnici, informativi e procedurali, ma lascia agli Stati membri il compito di istituire registri, sportelli digitali, sistemi di notifica con il risultato che spesso questi sistemi sono disomogenei o addirittura anche assenti. Quindi le imprese devono interfacciarsi con strumenti e modalità diverse da paese a paese. Mentre in Germania è già attivo un sistema di centralizzazione o tracciamento per i fornitori di sistemi ad alto rischio, in Italia o in alcuni Paesi dell'Est Europa, le imprese sono costrette a ricorrere a modalità quali via PEC oppure manuali. Un portale unico europeo per la notifica, assistenza tecnica o certificazione di sistemi IA manca e tale mancanza rappresenta un limite per la creazione di un mercato unico europeo. La *Digital Europe* e

¹⁶⁴ OECD SME and Entrepreneurship Papers, *SME Digitalisation to manage shocks and transitions 2024* OECD D4SME survey, 16 settembre 2024. Disponibile su: FINAL-D <https://www.oecd.org/content/dam/oecd/en/networks/oecd-digital-for-smes-global-initiative/FINAL-D4SME-2024-Survey-Policy-Highlights.pdf>

¹⁶⁵ Intellera Consulting, *AI Act, Intellera: 300mila euro per la conformità di una PMI*, in Innovation Post, aprile 2024. Disponibile su: AI Act <https://www.innovationpost.it/tecnologie/industrial-security/ai-act-intellera-rivela-300mila-euro-per-la-conformita-di-una-pmi/>, Intellera rivela: 300mila euro per la conformità di una PMI

'European Digital SME Alliance hanno richiesto uno sportello unico internazionale coordinato a livello europeo, simile a l'OSS (*One Stop Shop*) per fiscalità digitale e GDPR. Questa infrastruttura può aiutare le PMI o in generale le imprese che ne sentono la necessità ad adeguare efficacemente il Regolamento internamente e prevenire la duplicazione procedurale¹⁶⁶. Nel 2025, *Aiman Ezzat*, CEO di Capgemini, ha dichiarato che l'UE ha esagerato nel regolare l'IA, rendendo più difficile l'adozione del sistema dell'azienda globale all'interno della propria regione. *Ezzat* ha sottolineato come ciò rappresenti un "incubo" per le aziende, che sono costrette a regolarsi in base a norme diverse in ogni Paese in cui operano, dovendo dimostrare ogni volta cosa possono o non possono fare e le responsabilità come fornitori¹⁶⁷.

In sintesi, le sfide principali per le imprese transnazionali sono l'efficacia operativa, la scalabilità e l'espansione, date dall'assenza di un'attuazione realmente uniforme dell'AI Act. Differenze istituzionali e infrastrutturali limitano l'efficacia del Regolamento come strumento di integrazione economica. L'Unione Europea, oltre a stabilire norme le deve affiancare anche con una governance applicativa e coordinata che effettivamente aiuta le imprese. Solo in questo modo, l'AI Act potrà ottenere veramente successo.

2.3 Il ruolo dell'AI Act nel contesto globale

Per rafforzare la propria posizione globale in materia di Intelligenza Artificiale, l'Unione Europea ha intensificato le sue attività in materia recentemente. Nel febbraio 2025, durante l'*AI Action Summit* di Parigi, la presidente della Commissione Europea *Ursula von der Leyen*, ha annunciato l'iniziativa *InvestAI*, un piano da 200 miliardi di euro volto a potenziare l'ecosistema europeo dell'IA e colmare il divario tra Stati Uniti e Cina. Nel finanziamento di 200 miliardi, 50 provengono da fondi pubblici dell'UE, tra cui il programma *Digital Europe*, *Horizon Europe* e *InvestEU* e gli altri 150 da oltre 60 aziende

¹⁶⁶ European DIGITAL SME Alliance, *Artificial Intelligence Policy*. Disponibile su: <https://www.digitalsme.eu/artificial-intelligence/Intelligence> - European DIGITAL SME Alliance

¹⁶⁷ Reuters, *Capgemini CEO says EU went 'too far' with AI rules*, 10 febbraio 2025. Disponibile su: <https://www.reuters.com/technology/artificial-intelligence/capgemini-ceo-says-eu-went-too-far-with-ai-rules-2025-02-10/uters>

europee¹⁶⁸, creando il più grande partenariato pubblico-privato al mondo nel settore dell'IA. Oltre a questo, gli altri obiettivi di *InvestAI* fanno riferimento alla costruzione di 4 o 5 *gigafactories* dedicate all'intelligenza artificiale. Per garantire questo, si prevede di investire 20 miliardi di euro per realizzare grandi centri di calcolo per addestrare modelli di IA avanzati. Le *gigafactories* saranno accessibili a ricercatori, start up per creare innovazione collaborativa. Ognuna sarà equipaggiata da 100.000 chip di ultima generazione, andando ad aumentare notevolmente la capacità attuale delle *AI factories*. L'*InvestAI* si inserisce all'interno di una pianificazione maggiore, nominata "AI Continent", la quale prevede lo sviluppo di 4 *Gigafactories* e 13 *AI Factories*, l'implementazione di *AI Data Labs*, e il lancio dell'iniziativa *GenAI4EU*, che riguarda l'applicazione dell'IA generativa in settori strategici e la creazione di un *AI Service Desk* per supportare le aziende nella conformità normativa. Nonostante tali sforzi, l'Europa continua a mostrare un ritardo competitivo rispetto ad altri blocchi economici, soprattutto in termini di sviluppo autonomo di modelli di IA avanzati e di consolidamento di un ecosistema tecnologico realmente integrato. L'AI Act impone alle aziende la costruzione di un assetto significativo per quanto riguarda la *compliance*, con effetti significativi sul piano organizzativo, operativo e commerciale. Il paragrafo 1 dell'Articolo 2 del Regolamento, stabilisce che anche soggetti stabiliti al di fuori dell'Unione, sono obbligati a conformarsi all'AI Act se i loro sistemi di IA vengono immessi nel mercato europeo o utilizzati all'interno dell'Unione Europea. Molte *big tech* statunitensi o asiatiche, in vista di questa situazione, si trovano a gestire requisiti normativi più stringenti rispetto ai loro ordinamenti interni: ci sono metodi di tracciabilità dei dati, sicurezza e non discriminazione diversi. In assenza di conformità, le multinazionali hanno adottato *policy* specifiche per il mercato europeo con la conseguente duplicazione dei processi aziendali. I costi di conformità e *compliance* per i sistemi di intelligenza artificiale ad alto rischio possono rappresentare circa il 17% dell'investimento totale in AI¹⁶⁹. Per le grandi aziende, questo può tradursi in costi che variano da 250.000 a quasi 2 milioni di euro, a seconda della complessità e dell'ambito di applicazione dei sistemi AI. Si stima anche che l'AI Act

¹⁶⁸ Foo Yun Chee, *EU's AI push to get 50 billion euro boost, says von der Leyen*, Reuters, 11 febbraio 2025. Disponibile su: <https://www.reuters.com/technology/artificial-intelligence/eus-ai-push-get-50-bln-euro-boost-eus-von-der-leyen-says-2025-02-11/s> von der Leyen | Reuters

¹⁶⁹ CEPS, *Clarifying the costs for the EU's AI Act*, 24 settembre 2021. Disponibile su: <https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/g> the costs for the EU's AI Act - CEPS

potrebbe comportare costi annuali di conformità per le imprese europee pari a 10,9 miliardi di euro entro il 2025, con un impatto cumulativo sull'economia di oltre 30 miliardi di euro¹⁷⁰. È importante monitorare continuamente i sistemi IA e non limitarsi solo alla fase di progettazione di quest'ultimi, ma valutare anche le altre fasi di vita del prodotto. Alcune multinazionali stanno cercando di introdurre versioni "ridotte" dei loro prodotti in Europa per evitare costi troppo onerosi. A questo si aggiunge il fatto che, per i sistemi di IA generativa, il Regolamento prevede una disciplina autonoma (GDPAI), ovvero *General - Purpose AI Model*, che impone obblighi ancora maggiori di trasparenza e sicurezza. Se ci si adatta per tempo, i costi complessi possono trasformarsi in un vantaggio per le multinazionali. Infatti, come già evidenziato nel primo capitolo, aziende come *Bosch* o *Siemens* implementarono sistemi di monitoraggio ex ante, trasformando l'adeguamento dell'AI Act in un'opportunità strategica.

In tale scenario, il terzo capitolo approfondirà i casi di IBM e Amazon, descrivendo un'interessante dicotomia tra strategie di compliance avanzata e difficoltà di adattamento. IBM ha scelto di agire proattivamente, investendo nella costruzione di una governance per AI interna mentre Amazon ha subito ostacoli importanti per quanto riguarda la trasparenza algoritmica e la gestione dei dati biometrici, come in *Rekognition*. Il quadro normativo è molto complesso e ciò spinge le multinazionali a ridefinire non solo l'assetto interno ma anche la propria presenza strategica sul mercato europeo. L'AI Act rappresenta, non solo uno strumento regolatorio, ma anche una modalità per testare le imprese resilienti, che riescono attraverso i giusti strumenti, a coniugare l'innovazione con la legalità.

¹⁷⁰ Mueller B., Center for Data Innovation, *How Much Will the Artificial Intelligence Act Cost Europe?*, 26 Luglio 2021. Disponibile su: <https://datainnovation.org/2021/07/how-much-will-the-artificial-intelligence-act-cost-europe/> *Intelligence Act Cost Europe? – Center for Data Innovation*

CAPITOLO TERZO

Case study: aziende e conformità all'AI Act

3.1 Impatto del regolamento sulle imprese: compliance e difficoltà

L'obiettivo della creazione di un mercato unico è stato reso sempre più possibile grazie all'introduzione dell'AI Act, con sistemi di intelligenza artificiale impiegati secondo criteri di sicurezza, trasparenza e protezione dei diritti fondamentali. Nonostante ciò, l'ambizione regolatoria porta a costi di adeguamento che non sono per niente trascurabili per le imprese, ma anzi molto rilevanti: variano a seconda della natura e della dimensione dell'impresa e del settore in cui è inserita. Una delle sfide più grandi riguarda il bilanciamento tra gli oneri e i benefici per la competitività dell'industria europea nel contesto globale.

I costi relativi all'implementazione degli obblighi imposti dall'AI Act possono essere anche l'1,3 % del fatturato¹⁷¹. Se per le grandi imprese questo può essere gestibile, per le PMI, di dimensione minore e con meno risorse disponibili, i costi possono rappresentare un serio problema da affrontare e arrivare anche ad essere pari a 300.000 in totale, soprattutto per quelli relativi alla documentazione tecnica, verifiche di conformità, aggiornamento delle policy aziendali, registrazione presso le autorità competenti con un conseguente impatto sulla capacità di innovazione e internazionalizzazione. Oltre a tali costi diretti, si aggiungono anche costi indiretti, quali:

- Fabbisogno crescente di personale specializzato in data governance o audit tecnici;
- Rallentamento del *time-to-market* basato su prodotti IA;
- Duplicazione delle procedure per l'immissione in mercati con normative divergenti.

Per citare un esempio, la PMI danese Corti, specializzata in IA per il settore sanitario, ha dichiarato che sebbene la regolamentazione sia importante, i costi di conformità possono arrivare a raggiungere anche cifre a sei zeri per un'azienda con 50 dipendenti equiparando

¹⁷¹ Aliperto D., *Artificial Intelligence Act, la compliance costerà alle PMI 300mila euro*, Network360, CorCom, 16 novembre 2022. Disponibile su: <https://www.corrierecomunicazioni.it/digital-economy/ai-act-la-compliance-costerà-alle-pmi-300mila-euro/ce-costerà-alle-pmi-dieci-volte-meno-del-previsto>

¹⁹⁷ OODALOOP, *Europe's rushed attempt to set the rules for AI*, 16 luglio 2024. Disponibile su: [Europe's rushed attempt to set the rules for AI — OODALoop](https://oodaloop.com/briefs/news-briefs/europes-rushed-attempt-to-set-the-rules-for-ai/oop)

a tali costi una tassa aggiuntiva per le piccole imprese, e quindi la legislazione diventerebbe anche difficile da sostenere per le aziende che non se lo possono permettere. Di conseguenza, l'adeguamento può segnare mesi di ritardo per quanto riguarda l'immissione di un nuovo prodotto sul mercato, portando ad una perdita temporanea di competitività, rispetto per esempio ad operatori non soggetti agli stessi vincoli¹⁷². In primo luogo, se le imprese, invece, riescono ad adeguarsi bene, l'adeguamento all'AI Act può condurre anche a diversi benefici. Sicuramente tra questi vi è un aumento della certezza del diritto, una riduzione dei rischi legati a interpretazioni divergenti oppure a contenziosi legati ad un uso improprio dell'intelligenza artificiale. In secondo luogo, il rispetto dell'AI Act porta anche a far sì che investitori o clienti acquisiscono più fiducia nell'impresa, che quindi riesce ad aderire a standard internazionali, si presenta come attore responsabile e attenta alla protezione dei diritti fondamentali. In merito, la start up estone *Veriff*, attiva nel settore dell'identificazione digitale basata su IA, ha sviluppato un sistema conforme al Regolamento sin da subito, rispettando i principi di trasparenza e prevenzione di *bias*¹⁷³. È proprio grazie a questo che l'azienda, nel 2024, è riuscita a conquistare il mercato francese e tedesco, accedendo in maniera agevolata a programmi di *procurement* pubblico o partecipando a partnership istituzionali. Infatti, il CEO di *Veriff*, *Kaarel Kotkas*, ha dichiarato che “essere pienamente compliant al framework europeo ci ha permesso di differenziarci rispetto a competitor extra-UE ancora poco regolamentati”.

Diverse imprese hanno già implementato strumenti di governance proattivi previsti dal Regolamento, come l'integrazione di funzioni IT, *legal* o *compliance* nella gestione dei processi algoritmici. Questo può diventare un'opportunità per migliorare i processi interni, sviluppare nuove competenze o rendere più efficiente l'intelligenza artificiale. Analogamente al GDPR, il fatto che l'AI Act possa divenire un riferimento a livello globale, andrebbe a favorire le imprese sul piano competitivo, permettendo ad esse di agire come imprese *first-mover* nel mercato¹⁷⁴ e quindi ottenere un vantaggio competitivo

¹⁷³ Veriff, *The European Union AI Act: First Regulation on Artificial Intelligence*, 14 agosto 2024. Disponibile su: <https://www.veriff.com/fraud/learn> [https://www.veriff.com/fraud/learn/the-european-union-ai-act-first-regulation-on-artificial-intelligence](https://www.veriff.com/fraud/learn/the-european-union-ai-act-first-regulation-on-artificial-intelligence/the-european-union-ai-act-first-regulation-on-artificial-intelligence)

¹⁷⁴ Aziende che entrano per prime in un nuovo mercato o introducono per prime un nuovo prodotto o tecnologia, prima dei concorrenti.

non indifferente. Di conseguenza, se questo meccanismo funziona, gli standard potrebbero essere replicati con molta probabilità anche negli altri Paesi. In sintesi, la regolamentazione non deve rappresentare un vincolo, ma uno strumento che permette di attrarre investimenti qualificati per le imprese, attuare una leva strategica o rafforzare la normativa europea in un contesto globale in cui i modelli regolativi sono principalmente eterogenei.

Per le aziende è fondamentale adattarsi all'AI Act non solo per il piano tecnico-operativo ma anche per quello organizzativo. La conformità formale può rappresentare un primo obiettivo, ma oltre questo l'AI Act permette anche di rischi reputazionali, di aumentare la fiducia dei consumatori e migliorare in generale il posizionamento competitivo nel mercato interno europeo.

Una delle prime misure implementata dalle aziende è stata la creazione di *AI Ethics Boards*, ovvero comitati interdisciplinari che si pongono l'obiettivo di supervisionare l'impatto sociale, giuridico e anche tecnico dei modelli algoritmici. Infatti, una delle figure che è sempre più emergente nelle aziende è l'*AI Compliance Officer*, oppure *Head of AI Ethics*, le quali sono responsabili costantemente della gestione del rischio e della verifica della normativa. Oltre queste, le imprese dovrebbero adottare una governance ben precisa sull'implementazione dell'intelligenza artificiale¹⁷⁵. Tali iniziative combaciano perfettamente con quanto richiesto dal Titolo III del Regolamento (UE) 2024/1689, ed in particolari con gli articoli 9, 14 e 29 sull'adozione di misure correttive *ex ante* e identificazione di rischi.

Un'altra strategia fondamentale per adattarsi alle tecnologie IA è rappresentata dalla formazione interna. Grandi aziende come ING oppure *Carrefour*, hanno implementato percorsi di aggiornamento molto specifici rivolti a manager, sviluppatori o *compliance officer*. Gli obiettivi sono proprio quelli di sensibilizzare sul tema della trasparenza algoritmica, sulla protezione dei dati e la supervisione umana. In particolare, *Carrefour*, leader della grande distribuzione, ha avviato un programma di trasformazione digitale denominato "*Digital Retail Strategy 2026*". Tra le iniziative principali vi è una

¹⁷⁵ Horton International, *The EU AI Act And Beyond: A Leadership Guide To Ethical AI Governance*, 7 maggio 2025. Disponibile su: [The EU AI Act and Beyond: A Leadership Guide to E](https://hortoninternational.com/the-eu-ai-act-leadership-guide-to-ethical-ai-governance/)
[https://hortoninternational.com/the-eu-ai-act-leadership-guide-to-ethical-ai-governance/thical AI](https://hortoninternational.com/the-eu-ai-act-leadership-guide-to-ethical-ai-governance/)

formazione sull'intelligenza artificiale per tutti i collaboratori, da attuare entro il 2025. Inoltre, il gruppo si concentrerà sull'integrazione di assistenti virtuali basati sull'IA per supportare processi interni, aumentare la fidelizzazione e l'esperienza del cliente e promuovere l'innovazione digitale. L'accelerazione, per adottare soluzioni intelligenti e avanzate, verrà resa possibile anche grazie alle partnership con aziende tecnologiche come *Google* o *Meta*. Quest'ultima è un'altra ambiziosa strategia per consentire alle imprese di adattarsi meglio all'IA¹⁷⁶.

Dal punto di vista operativo, molte imprese, tra cui anche *IBM*, pioniera in questo, ricorrono anche a strumenti e *toolkit* fondamentali per la documentazione tecnica automatizzata, la spiegabilità dei modelli e l'auditing ex post. Esempi di questi strumenti sono *l'AI Fairness 360*¹⁷⁷ e *l'Adversarial Robustness Toolbox*¹⁷⁸. Il primo, è una piattaforma *open – source* per aiutare gli sviluppatori a mitigare i *bias* nei dati e nei modelli di apprendimento automatico. È caratterizzato da oltre 70 metriche per valutare la presenza di *bias* e da più di 10 algoritmi per ridurli, applicati anche in diverse fasi del ciclo di vita del prodotto. Il secondo, è sempre una libreria open-source sviluppata però per migliorare la robustezza dei modelli di apprendimento contro attacchi avversari. Viene utilizzata per migliorare la sicurezza dei modelli in settori critici, quali finanza, sanità e sicurezza informatica.

Altre strategie utilizzate dalle imprese riguardano la collaborazione pubblico-privato e i sandbox regolatori. In Francia, il CNIL e il *Cluster AI Paris*¹⁷⁹, hanno promosso ambienti

¹⁷⁶ Carrefour Group, *Digital Strategy 2026*. Disponibile su: Digital <https://www.carrefour.com/en/digital-retail-strategy-2026> Retail Strategy 2026 | Carrefour Group

¹⁷⁷ Irving M., Blog Post Series: *AI Fairness 360- Mitigating Bias in Machine Learning Models*, Medium, 30 luglio 2024. Disponibile su: Blog Post Ser <https://medium.com/@james.irving.phd/blog-post-series-ai-fairness-360-mitigating-bias-in-machine-learning-models-clc744c91c4ies>: AI Fairness 360- Mitigating Bias in Machine Learning Models | by James M. Irving, Ph.D. | Medium

¹⁷⁸ Nicolae, M.-I., Sinn, M., Tran, M. N., Buesser, B., Rawat, A., Wistuba, M., Zantedeschi, V., Baracaldo, N., Chen, B., Ludwig, H., Molloy, I. M., & Edwards, B., *Adversarial Robustness Toolbox v1.0.0*, *IBM Research– Ireland 2Univ Lyon, UJM-Saint-Etienne, CNRS, Institut d'Optique Graduate School*, 3 luglio 2018. Disponibile su: [1807.01069] Adver <https://arxiv.org/abs/1807.01069>sarial Robustness Toolbox v1.0.0

¹⁷⁹ Centro interdisciplinare di eccellenza dedicato all'intelligenza artificiale (IA) e all'analisi dei dati, situato nel campus di Palaiseau, all'interno del polo scientifico di Paris-Saclay.

di sperimentazione. Aziende come *Orange*¹⁸⁰ e *Renault*¹⁸¹ hanno testato i propri algoritmi di raccomandazione o ottimizzazione dei flussi logistici, adattandoli e combinando alle loro strategie il cosiddetto *clustering*¹⁸². Se da un lato, società come IBM hanno implementato strumenti di governance dell'IA¹⁸³, ci sono anche grandi aziende tech che, pur firmando *l'AI Pact*, non sono riuscite pienamente a conformarsi ad esso. Un esempio è, in questo ultimo caso, Amazon, la quale nonostante sia stata tra le prime 100 aziende a firmare, è stata coinvolta nel 2023, in problemi di reclutamento automatizzato, e sorveglianza dei lavoratori e dei cittadini. Infatti, risulta evidente come l'azienda ancora non ha chiarito come intenda gestire la conformità per questi sistemi ad alto rischio e potrebbe essere soggetta ad ulteriori sanzioni una volta che l'AI Act entrerà pienamente in vigore, se non adatterà le sue pratiche.

3.2 Conformità e *best practice*: il ruolo di IBM

IBM, leader globale nel settore dell'intelligenza artificiale, ha affrontato in maniera molto positiva e proattiva le sfide conseguenti all'entrata in vigore dell'AI Act. Azienda statunitense nel settore informatico, commercializza *hardware*, *software* per computer, *middleware*¹⁸⁴ e servizi informatici, offrendo infrastrutture, servizi di hosting e *cloud computing*. La struttura di governance adottata da IBM per le proprie iniziative legate all'IA riflette un modello articolato molto bene¹⁸⁵. Come illustrato nella figura seguente, l'architettura si basa su responsabilità crescenti. Vi è il *network di advocacy interna*

¹⁸⁰ Orange, *Combining Clustering and AI for Congestion-Free Mobile Networks*, 12 giugno 2024. Disponibile su: [Combining Clustering and AI for Congestion-Free Mobile Networks – Hello Future](https://hellofuture.orange.com/en/combining-clustering-and-ai-for-congestion-free-mobile-networks/ee-Mobile-Networks)

¹⁸¹ Renault Group, *AI at Renault Group: Empowering People, Enhancing Creativity*, FutuRgen, LinkedIn, 11 febbraio 2025. Disponibile su: (20) AI at Renault Group: Em [https://www.linkedin.com/pulse/ai-renault-group-empowering-people-enhancing-creativity-aygle/powering People, Enhancing Creativity | LinkedIn](https://www.linkedin.com/pulse/ai-renault-group-empowering-people-enhancing-creativity-aygle/powering-People, Enhancing Creativity | LinkedIn)

¹⁸² Tecnica usata nell'analisi dei dati e nel machine learning per raggruppare oggetti simili tra loro. Serve per scoprire strutture nascoste nei dati quando non hai etichette predefinite.

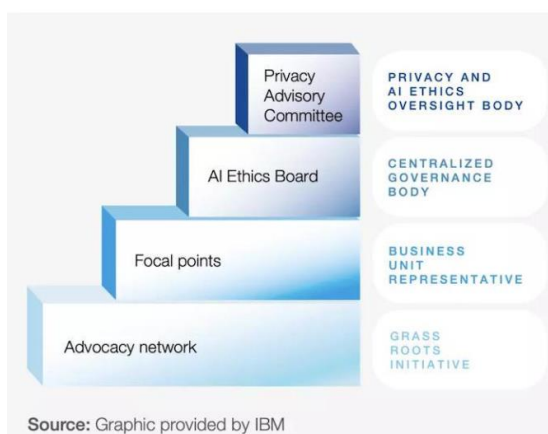
¹⁸³ TopLegal, Bini (Ibm): «Vi racconto la nostra governance dell'AI», 23 aprile 2024. Disponibile su: Bini (Ib <https://www.toplegal.it/art/bini-ibm-vi-racconto-la-nostra-governance-dell-ai/m>): «Vi racconto la nostra governance dell'AI» - TopLegal

¹⁸⁴ Software intermedio che fa da “ponte” tra due o più applicazioni, sistemi o componenti, permettendo loro di comunicare e scambiarsi dati anche se sono diversi tra loro.

¹⁸⁵ Green B., Lim D., World Economic Forum, *3 lessons from IBM on designing responsible, ethical AI*, 28 settembre 2021. Disponibile su: 3 lessons from I [https://www.weforum.org/stories/2021/09/case-study-on-ibm-ethical-use-of-artificial-intelligence-technology/BM on designing ethical AI technology | World Economic Forum](https://www.weforum.org/stories/2021/09/case-study-on-ibm-ethical-use-of-artificial-intelligence-technology/BM-on-designing-ethical-AI-technology)

(*Grassroots Initiative*), ovvero una rete di dipendenti volontari e stakeholder interni, i quali mirano a sensibilizzare e coinvolgere tutti i livelli di organizzazione per costruire un'IA responsabile. Il sistema è formato anche dalla creazione di referenti per le unità operative (*Focal Points*) e dell'*AI Ethics Board*, il quale è un organo centrale di supervisione. A questi si aggiunge il *Privacy Advisory Committee*, altro supervisore etico e di equità algoritmica. In coerenza con le finalità di AI Act, un tale modello consente un'integrazione trasversale di principi etici e normativi in tutte le fasi di sviluppo, deployment e auditing dei modelli di intelligenza artificiale. Questo approccio è in linea con gli articoli 9, 14 e 29 del Regolamento (UE) 2024/1689, i quali impongono ai fornitori di sistemi AI ad alto rischio obblighi di trasparenza, gestione del rischio e supervisione umana.

FIGURE 2 | Governance structure for IBM's AI efforts



Per l'azienda è fondamentale conformarsi alle nuove normative per garantire la fiducia dei clienti e mantenere la propria posizione competitiva. Di conseguenza, IBM ha implementato "*watsonx.governance*", reso disponibile a partire dal 2023, una piattaforma creata proprio per gestire per intero l'intero ciclo di vita dei modelli di intelligenza artificiale. I benefici della piattaforma riguardano:

- Automazione della documentazione
- Monitoraggio continuo dei modelli
- Gestione dei rischi associati

La piattaforma permette di valutare il rischio, tracciare delle decisioni algoritmiche e generazione di report conformi alle normative vigenti. L'adozione di queste misure, per

IBM, ha condotto a notevoli vantaggi sia per quanto riguarda la trasparenza decisionale e l'aumento di fiducia da parte dei consumatori e degli investitori. Inoltre, l'efficienza operativa complessiva, ha migliorato di molto i processi di audit e ridotto i tempi necessari per le verifiche di conformità. L'adozione della piattaforma ha inoltre favorito l'allineamento ai meccanismi di governance algoritmica previsti dal Titolo III dell'AI Act, che disciplina la gestione responsabile dei sistemi ad alto rischio e la loro tracciabilità.

Utilizzando i dati e i numeri, l'introduzione di *watsonx.governance* ha portato ad aumento del 40 % di produttività nel dipartimento risorse umane, IBM ha automatizzato più del 90 % delle interazioni nei contact center, migliorando sia l'efficienza che la soddisfazione del cliente. L'aumento della produttività è stato reso possibile anche per la modernizzazione delle applicazioni, di una misura almeno pari al 60 %¹⁸⁶.

In conclusione, l'approccio adottato da IBM, rappresenta un modello che le imprese tecnologiche che si confrontano con l'AI Act possono prendere come punto di riferimento. La solida governance interna adottata unita con la combinazione di strumenti tecnologici, rappresentano come gli obblighi normativi possono essere trasformati in opportunità strategiche e come la posizione dell'azienda nel mercato può essere trasformata, promuovendo un'intelligenza artificiale responsabile. L'integrazione di strumenti conformi all'*AI Act* ha consentito a IBM non solo di anticiparne l'applicazione, ma anche di posizionarsi come *first mover* tra le big tech nella regolazione europea, con un impatto positivo anche sulla reputazione aziendale e sulle relazioni istituzionali con i *policy maker* UE.

3.3 Sfide e criticità nella governance dell'intelligenza artificiale: il caso Amazon

Amazon, uno dei principali attori globali nel settore della tecnologia e nell'e-commerce, utilizza da diverso tempo tecnologie di intelligenza artificiale per ottimizzare la logistica, i processi decisionali e l'interazione con i clienti. Nonostante ciò, l'entrata in vigore dell'AI Act si scontra con i requisiti di conformità previsti, soprattutto in termini di diritti fondamentali, quali la protezione dei dati personali, la trasparenza e la discriminazione

¹⁸⁶ Kovsted T., *WatsonX AI for Business*, presentazione all'AI Day, 13 novembre 2024. Disponibile su: AI-for-business-AI-Day-13-N <https://aiday.dk/wp-content/uploads/2024/11/AI-for-business-AI-Day-13-November-2024-final-Thomas-Kovsted.pdf>

algoritmica. La posizione dominante di Amazon si scontra, quindi, con la normativa europea, fondata su principi stringenti di *accountability* e diritti della persona. In tale contesto, alcune pratiche aziendali consolidate, fanno fatica a confrontarsi e integrarsi con i principi del Regolamento, soprattutto per quanto riguarda la sorveglianza interna o il riconoscimento biometrico.

Amazon, come già citato, ha avuto difficoltà ad adattarsi all'AI Act ed uno dei casi più emblematici che rappresenta questo, è rappresentato dal caso *Amazon Rekognition*. Quest'ultima è una piattaforma basata su sistemi di *deep learning*, pensata per identificare volti umani, oggetti, scene e attività in contenuti quali foto o video. Inizialmente, il sistema è stato ideato per questioni relative alla pubblica sicurezza e applicazioni commerciali, mentre oggi viene utilizzato da aziende, agenzie governative e forze dell'ordine per il riconoscimento in tempo reale dei volti, il monitoraggio di folle e l'individuazione di comportamenti sospetti, oltre che per il riconoscimento biometrico dell'identità. In particolare *Amazon* ha pensato di svilupparlo per:

- Monitoraggio di strutture e magazzini per identificare attività sospette o non autorizzate;
- Analizzare le immagini dei clienti per personalizzare le offerte e migliorare l'interazione;
- Monitorare i prodotti e le spedizioni attraverso l'analisi visiva.

Tali attività possono essere facilitate dall'uso di *Amazon Rekognition*, proprio attraverso la tecnologia di *cloud* su cui si basa, che consente di aggiungere facilmente funzionalità avanzate di visione artificiale alle applicazioni. Tra le funzionalità principali, oltre al riconoscimento facciale, che identifica volti umani attraverso la determinazione di attributi quali età, genere, emozioni o altro, vi è il riconoscimento di oggetti, scene e contenuti.

Nonostante i benefici e l'innovazione che un sistema come questo può portare, *Rekognition* ha suscitato numerose preoccupazioni legate principalmente alla privacy, alla discriminazione algoritmica e alla trasparenza. Per esempio, sono stati rilevati *bias* sistemici nei tassi di accuratezza, in particolar modo verso individui non caucasici, generando rischi concreti di identificazioni erranee e violazioni di principi di non discriminazione. Nel contesto europeo, tali pratiche si scontrano con diversi articoli del

Regolamento. In particolare, l'articolo 5, il quale vieta l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi pubblici accessibili, salvo determinate autorizzazioni speciali. Inoltre, l'articolo 10 dell'AI Act impone obblighi particolari per la tracciabilità dei dati, la qualità e la rappresentatività, per una ragione legata all'addestramento dei sistemi intelligenti ad alto rischio.

Nel 2018, dopo una prima fase di sperimentazione pubblica iniziata nel 2017, il sistema si è reso protagonista di un'espansione commerciale e dei primi allarmi pubblici. *Rekognition*¹⁸⁷, infatti, venne utilizzato per dei test pilota dell'FBI, dei confronti biometrici da parte di utenti privati e per il riconoscimento facciale durante eventi mediatici, come il matrimonio dei reali inglesi. Nel maggio 2018, l'ALCU¹⁸⁸ denunciò l'uso sperimentale di *Rekognition*, generando forti proteste di dipendenti *Amazon* e organizzazioni civili. Venne evidenziato il rischio di violazione della privacy e sorveglianza ingiustificata. Infatti, un test dell'ALCU, nello stesso anno dimostrò un'erronea identificazione di 28 membri del Congresso come criminali. *Amazon* rispose raccomandando una soglia di affidabilità del 99 % ma i clienti pubblici utilizzavano soglie molto inferiori, violando anche gli standard etici minimi¹⁸⁹. Nel 2020, a fronte delle varie pressioni internazionali, *Amazon* ha annunciato una moratoria sull'uso di *Rekognition* da parte delle forze dell'ordine statunitense, rinnovata negli anni successivi. Nonostante le controversie, il Dipartimento della Giustizia Americano, annunciò nel 2024, che l'FBI adotterà *Rekognition* nell'ambito del progetto “*Tyr*” per analizzare immagini digitali adatte all'identificazione di nudità, armi, esplosivi ed altri contenuti sensibili. Il sistema in questo modo viene rilanciato su contesti ad alta sensibilità costituzionale, aggravando ulteriormente il contrasto con il modello europeo. È chiaro come una tale tecnologia è incompatibile con la normativa europea, e potrebbe aggravare la reputazione regolatoria di *Amazon*, segnando un divario tra la sua *governance* interna e i principi dell'AI Act.

¹⁸⁷ Ngo, Tammy, School of Engineering and Applied Science, University of Virginia, *Amazon Rekognition: Addressing Privacy Concerns and Bias; Exploring Ethical and Legal Complexities of Facial Recognition in Law Enforcement*, 5 maggio 2024. Disponibile su: file:///C:/Users/utente/Downloads/Ngo_Tammy_Sociotechnical_Synthesis.pdf

¹⁸⁸ American Civil Liberties Union

¹⁸⁹ ACLU, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, 2018. Disponibile su: <https://www.aclu.org/ne> <https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28ws/privacy-technology/amazons-face-recognition-falsely-matched-28>

L'adozione di sistemi IA nel contesto lavorativo, ha introdotto, nuove modalità di monitoraggio delle attività di dipendenti, sollevando problematiche etiche e legali. L'utilizzo di algoritmi per la supervisione, la valutazione e gestione del personale prende il nome di *algorithmic management* e spesso avviene senza una regolazione specifica applicata o un'adeguata possibilità di contestazione da parte dei lavoratori. In Europa, il GDPR e la Direttiva (UE) 2024/2831, stabiliscono norme precise sulla trasparenza delle decisioni automatizzate e protezione dei dati personali. Tuttavia, l'applicabilità effettiva nelle aziende o nei contesti pubblici che utilizzano algoritmi è segnata da sfide significative. La sorveglianza pervasiva può avere impatti negativi sul benessere dei dipendenti o in generale sulle politiche aziendali. Oltre a potenziali discriminazioni derivanti da *bias* algoritmici, anche la fiducia tra lavoratori e datori di lavoro può essere erosa. È fondamentale, quindi, per le aziende adottare un uso dell'intelligenza artificiale etico e trasparente.

In tale contesto, il problema principale per *Amazon*, riguarda l'uso di sistemi automatizzati per il monitoraggio dei dipendenti, specialmente nei centri di direzione o logistica, dove algoritmi vengono utilizzati per tracciare, valutare, e a volte anche disciplinare i lavoratori, senza che questi possano essere consapevoli oppure possano anche in minima parte controllare i sistemi. Tra le criticità principali, una delle più importanti riguarda l'assenza di trasparenza *ex-ante*: i dipendenti non venivano informati chiaramente su quali dati venissero raccolti, le tecnologie usate dall'algoritmo, e le conseguenze che ne derivavano in termini di valutazione ed in certi casi anche di penalizzazione. Ciò contrasta non solo gli articoli 13 e 14 del GDPR, ma anche l'articolo 52 dell'AI Act, i quali impongono un'informazione chiara e comprensibile nei confronti degli interessati. Inoltre, gli algoritmi arrivavano ad assegnare automaticamente dei punteggi ai dipendenti, indicatori di produttività, e potevano avviare azioni disciplinari o licenziamenti per "basso rendimento", molte volte senza neanche che i lavoratori ne fossero a conoscenza. Amazon, infine, continuava ad alimentare una cultura aziendale percepita da molti come "iper-sorvegliata", dal momento che venivano creati profili algoritmici, basati anche su temi di inattività, pause e ritmi lavorativi.

Le pratiche adottate da Amazon in materia di monitoraggio algoritmico dei lavoratori appaiono difficilmente compatibili con gli articoli 9 e 10 dell'AI Act, che richiedono una valutazione del rischio, la supervisione umana dei sistemi e la garanzia del rispetto dei

diritti fondamentali. Inoltre, tali pratiche si pongono in potenziale contrasto con il principio di proporzionalità e minimizzazione dei dati sancito dall'articolo 5 del GDPR, evidenziando una tensione tra la gestione algoritmica del personale e la tutela della dignità e della libertà individuale sul luogo di lavoro. In base alla classificazione dell'AI Act, i sistemi di gestione automatizzata dei lavoratori nel contesto delle risorse umane potrebbero rientrare tra i sistemi ad alto rischio (Allegato III), e dunque essere soggetti a obblighi rigorosi di conformità, trasparenza e controllo. L'assenza di una supervisione umana adeguata o di meccanismi di contestazione individuale costituisce un'infrazione sostanziale del quadro normativo europeo. In linea con quanto trattato, il regime sanzionatorio dell'AI Act è strutturato su tre livelli, proporzionali alla gravità delle violazioni¹⁹⁰:

- Fino a 35 milioni di euro o al 7 % del fatturato annuo globale, per violazione su pratiche vietate come l'uso di tecniche manipolative o discriminazioni sistemiche;
- Fino a 15 milioni di euro o al 3 % del fatturato annuo globale, per la non conformità ai requisiti specifici per i sistemi di IA ad alto rischio;
- Fino a 7,5 milioni di euro o all'1 % del fatturato annuo globale, per la fornitura di informazioni inesatte o incomplete alle autorità competenti.

Riguardo al caso *Amazon*, nel dicembre del 2023, la *Commission Nationale de l'Informatique et des Libertés* (CNIL), ovvero l'autorità francese per la protezione dei dati, ha inflitto una multa di 32 milioni di euro ad *Amazon France Logistique*, per aver implementato un sistema di monitoraggio dipendenti troppo intrusivo e non trasparente¹⁹¹. Infatti, il sistema utilizzava scanner portatili per tracciare in tempo reale le attività dei lavoratori, evidenziando periodi eventuali di inattività superiori a 10 minuti e la velocità di scansione. Sebbene la sanzione inflitta dalla CNIL ad Amazon France nel 2023 sia formalmente avvenuta in base al GDPR, il caso rappresenta un'anticipazione

¹⁹⁰ Regolamento 1689/2024, articolo 71, Artificial Intelligence Act, 12 luglio 2024.

¹⁹¹ CNIL, *Surveillance des salariés : la CNIL sanctionne AMAZON FRANCE LOGISTIQUE d'une amende de 32 millions d'euros*, 23 gennaio 2024. Disponibile su : Surv [https://www.cnil.fr/fr/surveillance-des-salaries-la-cnil-sanctionne-amazon-france-logistique-dune-amende-de-32-millionseillance des salariés : la CNIL sanctionne AMAZON FRANCE LOGISTIQUE d'une amende de 32 millions d'euros | CNIL](https://www.cnil.fr/fr/surveillance-des-salaries-la-cnil-sanctionne-amazon-france-logistique-dune-amende-de-32-millionseillance-des-salariés : la CNIL sanctionne AMAZON FRANCE LOGISTIQUE d'une amende de 32 millions d'euros | CNIL)

concreta delle problematiche che l'AI Act mira a prevenire. Le pratiche di monitoraggio algoritmico adottate rientrerebbero oggi nell'ambito dei sistemi di IA ad alto rischio, soggetti a obblighi stringenti in termini di trasparenza, supervisione umana e gestione dei rischi. Il caso Amazon mostra con chiarezza le criticità di adattamento delle big tech al quadro regolatorio europeo.

Il confronto tra IBM e Amazon dimostra come l'AI Act, pur rappresentando una sfida regolatoria complessa, non sia di per sé incompatibile con l'innovazione tecnologica. Piuttosto, evidenzia la necessità di una cultura aziendale improntata alla responsabilità e alla governance, che IBM ha saputo tradurre in vantaggio competitivo, mentre Amazon, in alcuni ambiti, continua a muoversi su un crinale critico di tensione normativa con il quadro europeo.

Conclusioni

La presente tesi ha analizzato l'*Artificial Intelligence Act* mostrandone le finalità, la struttura normativa, le differenze di applicazione potenziali tra gli Stati Membri e le implicazioni per le imprese. Dopo aver evidenziato come sia necessaria una regolamentazione uniforme tra gli Stati dell'Unione Europea in un settore in cui l'utilizzo dell'intelligenza artificiale è critico, si è passati all'analisi dell'applicazione concreta nei principali Paesi europei, come Francia, Germania e Italia, mostrando sia le divergenze interpretative che le problematiche legate alla governance nazionale.

Successivamente, è stato preso in considerazione anche l'impatto del regolamento sulle imprese, analizzando sia i costi di conformità che le opportunità derivanti da una regolazione chiara e definita. Attraverso i casi studio di IBM e Amazon, si è mostrato come le imprese possano reagire in modo molto diverso alla sfida della compliance. IBM si è distinta per un approccio proattivo e strutturato, facendo della conformità all'AI Act una leva strategica. Al contrario, Amazon, pur avendo aderito formalmente all'AI Pact, è stata oggetto di critiche per pratiche che risultano ancora distanti dagli standard imposti dal regolamento, soprattutto in materia di trasparenza algoritmica e tutela dei diritti fondamentali.

L'AI Act rappresenta sicuramente il primo strumento normativo vincolante a livello globale, dedicato interamente all'intelligenza artificiale. Nonostante ciò, la sua efficacia dipenderà da diversi fattori. In primo luogo, risulta di primaria importanza che gli Stati membri implementino in maniera coerente e condivisa le disposizioni, evitando frammentazioni normative. Successivamente, è fondamentale, anche per garantire questa coesione, il ruolo delle autorità di vigilanza, sia a livello nazionale che europeo.

Un'altra criticità che non può essere sottovalutata è la reazione o comunque la resistenza del regolamento ad eventuali evoluzioni tecnologiche. L'approccio adottato dall'AI Act è comunque basato sul rischio ed è orizzontale, quindi facilmente adattabile, ma allo stesso tempo, vi è il rischio che la velocità di innovazione dell'intelligenza artificiale sia superiore ai tempi di aggiornamento della normativa. Un ultimo fattore fondamentale per assicurare il successo dell'AI Act è la coniugazione tra protezione dei diritti fondamentali dell'uomo e la competitività industriale, soprattutto davanti ad altre potenze globali, come la Cina o gli Stati Uniti, che utilizzavano normative diverse. L'AI Act non può risultare

pienamente efficace, infine, se la sua piena applicabilità, non è accompagnata da reali investimenti per le PMI, formazione continua e politiche attive di sviluppo delle competenze digitali, che oggi sono una delle più grandi debolezze per gli Stati europei, ed in particolare per l'Italia.

Nel prossimo futuro, l'AI Act potrebbe evolversi su diversi fronti. Uno dei più interessanti da analizzare è quello relativo alla cooperazione internazionale, in uno scenario, in cui il rischio di arbitraggio normativo, ovvero la delocalizzazione di attività verso Paesi più permissivi in termini di regolazione, resta elevato. L'Unione Europea è la prima entità giuridica ad adottare una normativa vincolante sull'IA, ed in quanto tale, potrebbe rafforzare il proprio ruolo globale in linea con il cosiddetto "*Brussels Effect*", secondo il quale gli standard europei tendono a diffondersi anche al di fuori dei confini dell'Unione per effetto del potere normativo del mercato interno europeo. Inoltre, l'AI Act deve essere ancora attuato tecnicamente, e questo potrà avvenire, per esempio, con atti delegati o linee guida da parte della Commissione Europea, fondamentali per fornire chiarezza ad aspetti ritenuti ancora ambigui, come la definizione di sistema ad alto rischio, o dei modelli di IA generativa. La vicepresidente della Commissione *Margrethe Vestager* ha dichiarato che "l'attuazione dell'AI Act richiederà un dialogo continuo con imprese, autorità nazionali e comunità scientifica, per garantire che le regole siano applicabili anche a tecnologie in rapida evoluzione. Sul piano operativo, gli AI sandbox diventeranno degli strumenti chiave per bilanciare regolazione e innovazione. Sono considerati "un elemento essenziale per testare ex ante la conformità degli algoritmi"¹⁹²". La loro estensione favorirebbe anche la compliance tra le PMI, così che la sperimentazione tecnologica viene resa molto più accessibile, in un ambiente molto assistito a livello normativo. Viene costantemente sottolineata una "convergenza normativa tra i diversi strumenti digitali europei, per evitare frammentazioni e garantire coerenza tra i principi di trasparenza, privacy e accountability", in modo tale da creare come sviluppo futuro una sempre maggiore integrazione tra l'AI Act e altri regolamenti quali il GDPR, il Digital Services Act e il Digital Markets Act. Tutto ciò porterebbe ad un rafforzamento dell'AI Office, istituito presso la Commissione, che coordinerà l'applicazione del Regolamento e

¹⁹² Baccini F., Vestager: "*Identità digitale europea e Digital services act proteggeranno la democrazia dell'UE*", Eunews, 30 ottobre 2020. Disponibile su: Vestager: "Identità digitale europea e Digital services act proteggeranno la democrazia dell'UE" - Eunews

supporterà le autorità nazionali di vigilanza. Probabilmente, l'AI Office evolverà in un'agenzia europea per l'IA con poteri ispettivi ma anche regolatori più ampi. In conclusione, ciò che si può trarre è che è presente un quadro giuridico dinamico e multilivello, dove non vi è semplicemente un'imposizione di vincoli, ma la regolazione diventa uno strumento per governare il cambiamento e l'innovazione tecnologica, in modo etico, sostenibile e competitivo allo stesso tempo.

Bibliografia

.Allio L., Delia R., Andres Amo P., *Multi-Level Regulatory Governance: Policies, Institutions and Tools for Regulatory Quality and Policy Coherence*, OECD Working Papers on Public Governance No. 13, OECD, 2009.

Autorità de la Concurrence, *Intelligence artificielle générative : l’Autorité rend son avis sur le fonctionnement concurrentiel du secteur de l’intelligence artificielle générative*, 28 giugno 2024.

Autoriteit Persoonsgegevens (AP), *Rapporto su IA e Rischi Algoritmici nei Paesi Bassi, inverno 2023–2024*.

Baccini F., Vestager: “*Identità digitale europea e Digital services act proteggeranno la democrazia dell’UE*”, Eunews, 30 ottobre 2020.

Barocas S., Hardt M., Narayanan A., *Fairness and Machine Learning: Limitations and Opportunities*, Fairness and Machine Learning LLC, 2019.

Bradford A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 5 ottobre 2021.

Bundesministerium für Wirtschaft und Klimaschutz (BMWK) und Bundesministerium der Justiz (BMJ), *Referentenentwurf zum KI-Marktüberwachungsgesetz (KIMÜG)*, 2024.

Bundesregierung, *Strategie Künstliche Intelligenz der Bundesregierung, Fortschreibung 2020*, dicembre 2020.

Carrefour Group, *Digital Strategy 2026*..

Chiusi F., Fisher S., Kayser-Bril N., Spielkamp M., *Automating Society Report, Algorithm Watch Bertelsmann Stiftung*, 2020.

Christakis T., Karathanasis T., *Tools for Navigating the EU AI Act: (2) Visualisation Pyramid*, MIAI, 7 marzo 2024.

Chui M., Hazan E., Roberts R., Singla A., Smaje K., Sukharevsky A., Yee L., Zempel R., *The Economic Potential of Generative AI: The Next Productivity Frontier*, McKinsey Global Institute, giugno 2023, p. 15.

CNRS, *Démocratiser l'IA générative en santé : l'Etat, à travers France 2030, sélectionne le projet PARTAGES*, 27 novembre 2024.

Commissione Europea, *Domande e risposte: la legge sull'intelligenza artificiale dell'UE*, 21 aprile 2021.

Commissione Europea, *The Digital Services Act package*, 12 febbraio 2025.

Dal Lago D., *Bias e Discriminazione negli Algoritmi: Come Riconoscerli e Prevenirli*, LinkedIn Plus, 13 febbraio 2025.

Dipartimento per la trasformazione digitale, *Agenzia per l'Italia Digitale, Strategia Italiana per l'Intelligenza Artificiale 2024-2026*, 2024.

European Commission, *AI Watch National Strategies on Artificial Intelligence: A European Perspective in 2019*, JRC Technical Report, 2020.

European Data Protection Board (EDPB), *Guidelines 8/2020 on the targeting of social media users*, versione finale del 13 aprile 2021.

European Parliamentary Research Service (EPRS), *The United Kingdom and Artificial Intelligence*, 2024.

Federal Ministry of Transport, *Federal Government Publishes Strategy for Autonomous Driving in Road Transport, Autonomous Driving Is the Future, Says Federal Minister Wissing*, Press Release, 4 dicembre 2024.

Floridi L., *Artificial Intelligence and the European Union's Artificial Intelligence Act — A Brief Ethical Evaluation*, *Philosophy & Technology*, vol. 35, n. 3, 3 giugno 2021, pp. 411–417.

Floridi L., *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford University Press, 2023.

Floridi L., *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality*, Oxford University Press, 2014.

Fraser H.L., Bello y Villarino J.-M., *Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough*, *European Journal of Risk Regulation*, 27 luglio 2023.

Gasser U., Almeida V.A.F., *A Layered Model for AI Governance*, *IEEE Internet Computing*, 21, 6 novembre 2017, pp. 58–62.

Google Cloud, Intesa Sanpaolo: *Managing Evolving Financial Risk at Speed with Data Analytics and AI*, 2020.

Gruppo di Esperti MISE IA, Ministero dello Sviluppo Economico (MIMIT), Ministero dell'Università e della Ricerca (MUR), Dipartimento per la Trasformazione Digitale, *Proposte per una Strategia Italiana per l'Intelligenza Artificiale*, 2021.

High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, *Commissione Europea*, aprile 2019.

IFO Institute, *Many Companies Are Hesitant About Artificial Intelligence – Germany Nevertheless Performs Well in a European Comparison*, 6 settembre 2024.

Inria, *Building Trust in AI Through a Better Understanding of Algorithms*, 9 aprile 2021.

Intesa San Paolo, *TCFD Report*, 2022.

Kaplan J., *Artificial Intelligence: What Everyone Needs to Know*, Oxford University Press, 2016, p. 25.

Kovsted T., *WatsonX AI for Business*, presentazione all'AI Day, 13 novembre 2024.

McCarthy J., Minsky M.L., Rochester N., Shannon C.E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, AI Magazine, 2006, vol. 27, n. 4, p. 12.

Ministero dell'Economia e delle Finanze, *Nasce Fondazione Ai4Industry. Giorgetti: Presidio sull'Intelligenza Artificiale per Sviluppo Industriale*, 3 maggio 2024.

Mitchell T., *Machine Learning*, McGraw-Hill, New York, 1997, p. 2.

Mueller B., *Center for Data Innovation, How Much Will the Artificial Intelligence Act Cost Europe?*, 26 luglio 2021.

Novelli C., Hacker P., Morley J., Trondal J., Floridi L., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, *European Journal of Risk Regulation*, vol. 4, pp. 1–25, 8 maggio 2024.

Novelli C., Hacker P., Morley J., Trondal J., Floridi L., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, European Liberal Forum, 2023.

OECD, *An Overview of National AI Strategies and Policies*, OECD, 3 agosto 2021

OECD, BCG, INSEAD Business School, *The Adoption of Artificial Intelligence in Firms: New Evidence for Policy Making*, 2 maggio 2025.

OECD, SME and Entrepreneurship Papers, *SME Digitalisation to Manage Shocks and Transitions 2024 OECD D4SME Survey*, 16 settembre 2024.

OECD, *State of Implementation of the OECD AI Principles: Insights from National AI Policies*, OECD Publishing, 2021.

Parlamento europeo, *Il Processo Legislativo Ordinario: Triloghi e Negoziati Interistituzionali, scheda sintetica sul funzionamento dei triloghi*.

Rödl & Partner, *The Draft Bill for the AI Market Surveillance Act: German Implementation of the AI Act*, 26 febbraio 2025.

SAP, Joule: *New Generative AI Assistant*, 26 settembre 2023.

Siemens Healthineers, *Medical Imaging in the Age of Artificial Intelligence*, 2021.

Söderlund K., Larsson S., *Enforcement Design Patterns in EU Law: An Analysis of the AI Act*, *Digital Society*, vol. 3, Articolo 41, 25 luglio 2024.

Steiner F., *AI Regulation: German Government Reveals Supervisory Regime Plan*, Heise Online, 26 settembre 2024.

Stiftung Neue Verantwortung, *AI Talent Flows in Germany*, 14 dicembre 2022.

The European House – Ambrosetti, *AI 4 Italy: Impatti e Prospettive dell'Intelligenza Artificiale Generativa per l'Italia e il Made in Italy*, settembre 2023, p. 24.

UK Government, *AI Regulation: A Pro-Innovation Approach*, Department for Science, Innovation and Technology and Office for Artificial Intelligence, 29 marzo 2023.

UK Government, *National AI Strategy*, Presented to Parliament by the Secretary of State for Digital, Culture, Media and Sport by Command of Her Majesty, settembre 2021.

U.S.-China Economic and Security Review Commission, *CCP Decision-Making and Xi Jinping's Centralization of Authority, Chapter 1*, in 2022 Annual Report to Congress, novembre 2022.

Uuk K., Madiega T., Vigano E., *Operationalising the Definition of General Purpose AI Systems*, Stanford University, Future of Life Institute, 2023.

Veale M., Zuiderveen Borgesius F., *Demystifying the Draft EU Artificial Intelligence Act*, Computer Law Review International, 2021, 22(4), pp. 97–112.

Villani C., *Donner un Sens à l'Intelligence Artificielle: Pour une Stratégie Nationale et Européenne*, Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation, marzo 2018.

World Economic Forum, *Future of Jobs Report*, maggio 2023.

Zew Mannheim, *AI Adoption Stagnates in German Companies*, 28 agosto 2024.

Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2018.

Sitografia

Brookfield Asset Management: <https://bam.brookfield.com>

CNIL: <https://www.cnil.fr/en/topics/artificial-intelligence-ai>

Commissione Europea Digital Strategy: <https://digital-strategy.ec.europa.eu/en/page-not-found>

EU Artificial Intelligence Act: <https://artificialintelligenceact.eu/>

Holistic AI: <https://www.holisticai.com/>

IBM, AI Governance & watsonx.governance: <https://www.ibm.com/it-products/watsonx-governance/model-governance>

Reuters: <https://www.reuters.com/>