



**UNIVERSITÀ
DI PAVIA**

Dipartimento di Scienze Economiche e Aziendali

Corso di Laurea

INTERNATIONAL BUSINESS AND

ENTREPRENEURSHIP – MANAGEMENT

INTERNAZIONALE E IMPRENDITORIALITÀ

**THE ECONOMIC IMPACT OF ARTIFICIAL
INTELLIGENCE REGULATION ON
EUROPEAN COMPANIES**

Relatore:

Chiar.mo Prof. Fabio Marazzi

**Tesi di Laurea
di Crotti Lorenzo**

Matr. n.553508

Anno Accademico 2025-2026

INDEX

INTRODUCTION	5
CHAPTER 1: Artificial Intelligence as a driver of business transformation	8
1.1 Understanding Artificial Intelligence	9
1.1.1 Definition and characteristics of AI	
1.1.2 Machine learning and Deep learning	
1.2 Evolution of Artificial Intelligence	11
1.2.1 Early developments and AI winters	
1.2.2 The rise of Data – Driven AI	
1.2.3 AI in the Fourth Industrial Revolution	
1.3 AI adoption across economic sectors	14
1.3.1 Artificial Intelligence in manufacturing	
1.3.2 Artificial Intelligence in Financial Services	
1.3.3 Artificial Intelligence in Healthcare	
1.3.4 Artificial Intelligence in retail and e – commerce	
1.3.5 Cross - sectoral implications for European businesses	
CHAPTER 2: The European regulatory framework for Artificial Intelligence	22
2.1 The emergence of AI Governance	
2.1.1 Global regulatory approaches	
2.1.2 The European vision of trustworthy artificial intelligence	
2.2 The Development of the EU AI Act	26
2.2.1 Legislative origins	
2.2.2 Policy objectives	
2.2.3 The legislative process	
2.3 The risk – based approach of the AI Act	30
2.3.1 Unacceptable – risk AI systems	
2.3.2 High – risk AI systems	
2.3.3 Limited – risk AI systems	
2.3.4 Minimal – risk AI systems	
2.4 Compliance obligations for businesses	34
2.4.1 Risk management systems	
2.4.2 Data governance requirements	
2.4.3 Transparency and information obligations	

2.4.4	Human oversight requirements	
2.4.5	Documentation and record – keeping	
	2.5 Governance, enforcement and sanctions	39
2.5.1	National supervisory authorities	
2.5.2	The European AI Office	
2.5.3	Administrative fines and penalties	
	2.6 Interaction with other EU digital Regulations	43
2.6.1	General Data Protection Regulation (GDPR)	
2.6.2	Digital Services Act (DSA)	
2.6.3	Digital Markets Act (DMA)	
2.6.4	Data Act	
2.6.5	Cyber Resilience Act	
	CHAPTER 3: The economic impact of AI Regulation on European companies	48
	3.1 Regulation and innovation: theoretical perspectives	
3.1.1	The innovation – inhibiting view	
3.1.2	The innovation – enabling view	
3.1.3	The concept of smart Regulation	
	3.2 Compliance costs under the AI Act	52
3.2.1	Direct compliance costs	
3.2.2	Administrative burdens	
3.2.3	Legal and consultancy costs	
3.2.4	Technological adaptation costs	
	3.3 The impact on small and medium – sized enterprises	56
3.3.1	Structural constraints of SMEs	
3.3.2	Compliance challenges	
3.3.3	Opportunities and support measures	
	3.4 The impact on large companies	59
3.4.1	Corporate governance adjustments	
3.4.2	Internal compliance structures	
3.4.3	Strategic responses to Regulation	
	3.5 Economic benefits of AI regulation	62
3.5.1	Increased consumer trust	
3.5.2	Legal certainty	
3.5.3	Reduction of reputational risks	

3.5.4	Promotion of responsible innovation	
	3.6 AI regulation and business competitiveness	66
3.6.1	Effects on investment decisions	
3.6.2	Effects on innovation capacity	
3.6.3	Effects on market entry and competition	
	3.7 Is Regulation a cost or a competitive advantage?	69
	 CHAPTER 4: Comparative analysis of global AI regulatory models	 73
	4.1 The United States approach to AI regulation	
4.1.1	Market – oriented governance	
4.1.2	Federal and state initiatives	
4.1.3	Regulatory flexibility and innovation	
	4.2 The Chinese approach to AI regulation	77
4.2.1	State – centered governance	
4.2.2	Strategic objectives of AI development	
4.2.3	Regulatory control mechanisms	
	4.3 Comparing the European, American and Chinese models	81
4.3.1	Regulatory philosophy	
4.3.2	Innovation incentives	
4.3.3	Business implications	
	4.4 Strength and weakness of the EU AI Act	85
4.4.1	Legal strengths	
4.4.2	Economic strengths	
4.4.3	Regulatory criticism	
	4.5 Future challenges for AI regulation	89
4.5.1	Generative AI	
4.5.2	Foundation models	
4.5.3	International regulatory coordination	
	 CONCLUSION	 96
	BIBLIOGRAPHY	106
	SITOGRAPHY	110

INTRODUCTION

Artificial Intelligence (AI) has rapidly emerged as one of the most influential technologies of the digital age, reshaping the way businesses operate, compete and create value. Over the last decade, advancements in machine learning, natural language processing, computer vision, and generative AI have enabled firms to automate complex tasks, optimize decision - making processes, and develop innovative products and services. As a result, AI has become a strategic asset for companies seeking to improve productivity, reduce operational costs, and strengthen their competitive position in increasingly globalized and technology – driven markets.¹

The growing adoption of AI systems has generated significant economic opportunities across a wide range of industries. From manufacturing and healthcare to finance and retail, organizations are integrating AI into their business models to enhance efficiency and support innovation. Nevertheless, the rapid diffusion of these technologies has also raised important concerns regarding transparency, accountability, privacy, cybersecurity, and the protection of fundamental rights. The capacity of AI systems to process vast amounts of data and make autonomous or semi – autonomous decisions has created new legal and ethical challenges that traditional regulatory frameworks often struggle to address.²

Against this backdrop, policymakers around the world have begun to develop specific regulatory responses aimed at ensuring that the deployment of AI remains safe, trustworthy, and aligned with societal values. Among the various regulatory initiatives currently under discussion, the European Union has adopted one of the most comprehensive approaches through the introduction of the AI Act. Designed as the first horizontal legal framework specifically dedicated to artificial intelligence, the AI Act establishes a risk – based regulatory model that imposes different obligations depending on the potential risks associated with AI systems.

The adoption of the AI Act represents a significant milestone in the evolution of digital regulation. On the one hand, the European legislator seeks to protect individuals and businesses from the risks arising from the use of AI technologies, while fostering trust and legal certainty within the digital economy. On the other hand, the introduction of new compliance obligations inevitably generates additional costs for firms, potentially affecting their investment decisions, innovation strategies, and overall competitiveness. This tension between regulation and innovation lies at the heart of the contemporary debate on AI governance.

¹ Bassamani et al. (2021), “On the Opportunities and Risks of Foundation Models.”

² Lee, J., Bagheri, B., & Kao, H.-A. (2015): “A Cyber – Physical Systems Architecture for Industry 4.0”

Indeed, the relationship between regulation and economic growth has long been a central issue within both legal and economic scholarship. Supporters of a strong regulatory framework argue that clear rules can encourage responsible innovation, reduce legal uncertainty, and increase consumer confidence, thereby creating favorable conditions for long – term economic development. Critics, however, warn that excessive regulatory intervention may increase compliance costs, slow down technological progress, and place European firms at a competitive disadvantage compared to companies operating in jurisdictions characterized by a more flexible regulatory environment.

Looking at these considerations, this thesis seeks to investigate the economic implications of AI regulation for European companies, with particular attention to the impact of the AI Act. The central objective of the research is to assess whether the European regulatory framework constitutes primarily a constraint on innovation and business growth or whether it can also generate economic benefits through enhanced legal certainty, improved risk management, and greater trust in AI technologies.

More specifically, the study aims to examine the legal obligations introduced by the AI Act and to evaluate their potential effects on business performance. Particular attention will be devoted to the costs associated with regulatory compliance, including governance requirements, risk assessment procedures, documentation obligations, and monitoring mechanisms. Furthermore, the research will explore whether such obligations affect companies differently according to their size and organizational structure, with a specific focus on the distinction between small and medium – sized enterprises and large multinational corporations.

The thesis is guided by the following research question: to what extent does the European Union’s regulatory framework for artificial intelligence, and particularly the AI Act, influence the economic performance and competitiveness of European companies? In addressing this question, the study will also consider whether regulation may produce indirect economic benefits by strengthening consumer trust, reducing legal uncertainty, and encouraging the development of reliable and responsible AI systems.

To answer these questions, the research adopts an interdisciplinary approach combining legal analysis and economic valuation. From a legal perspective, the study examines the AI Act and its interaction with other key components of the European digital regulatory framework, including the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), and the Data Act. From an economic perspective, the analysis focuses on the potential costs and benefits generated by regulatory compliance and their implications for innovation and competitiveness.

The research is primarily based on a qualitative methodology and relies on the examination of

academic literature, legal scholarships, policy papers, institutional reports, and official documents published by European institutions and international organizations. In addition, a comparative analysis of the regulatory approaches adopted by the United States and China will be conducted to evaluate the strengths and limitations of the European model within the broader context of global AI governance.

By combining legal and economic perspectives, this thesis aims to contribute to the ongoing debate concerning the role of regulation in shaping the future of artificial intelligence. Ultimately, the study seeks to provide a better understanding of whether the European approach can successfully balance the need to protect fundamental rights and public interests with the objective of promoting innovation, economic growth, and international competitiveness in the age of artificial intelligence.

CHAPTER 1: Understanding Artificial Intelligence

Artificial Intelligence (AI) has become one of the most influential technologies of the digital age, attracting the attention of governments, businesses, academics, and society. Its growing diffusion across economic sectors has transformed the way organizations operate, make decisions, and create value, while simultaneously raising new legal, ethical, and regulatory challenges.

Despite its increasing relevance, artificial intelligence remains a complex concept. The term encompasses a broad range of technologies, methodologies, and applications that differ significantly in terms of functionality, autonomy and societal impact. As a result, there isn't single universally accepted definition of AI, and different disciplines tend to emphasize aspects of the phenomenon.

In order to understand the rationale behind contemporary regulatory initiatives, particularly the European Union's AI Act, it is first necessary to examine what artificial intelligence is, how it operates, and how it has evolved over time. The following sections therefore analyze the main definitions and characteristics of AI, the technological foundations of machine learning and deep learning and the most significant recent development in the field.³

1.1.1 Definition and characteristics of Artificial Intelligence

Although artificial intelligence has become a central topic in contemporary technological, economic, and legal debates, defining the concept remains a challenging task. The difficulty largely derives from the multidisciplinary nature of AI itself.

One of the most influential definitions within scientific literature was proposed by Russell and Norvig, who describe artificial intelligence as the study of intelligent agents capable of perceiving their environment and taking actions that maximize the probability of achieving specific goals. This definition highlights the ability of AI systems to process information, evaluate alternative courses of action, and autonomously pursue predetermined objectives. More recently, international organizations and regulatory authorities have sought to adopt broader definitions capable of encompassing the wide variety of AI technologies currently in use. The Organization for Economic Cooperation and Development (OECD)⁴ defines an AI system as a machine – based system that can generate predictions, recommendations, or decisions influencing real or virtual environments. Similarly, the European Union has adopted a broad definition within the AI Act, describing AI systems as machine – based systems designed to operate with varying levels of autonomy and capable of producing outputs such as recommendations, or decisions that influence

³ AI Act, art.3 – definition of AI Systems

⁴ OECD (2024), updated OECD Definition of an AI System

environments.⁵

Despite the diversity of existing definitions, most scholars agree that certain characteristics distinguish artificial intelligence from traditional software systems. One of most significant is autonomy; unlike traditional software AI systems can perform tasks and generate outputs with limited human intervention. The degree of autonomy may vary considerably depending on the specific application, yet the ability to operate independently remains one of the defining features of AI technologies.

A second characteristic concerns learning capability. Through advanced computational techniques, AI systems can identify patterns within data and improve their performance over time. This ability enables them to adapt to changing circumstances and produce increasingly accurate results without requiring explicit reprogramming. AI is also characterized by its capacity to process vast quantities of information and generate predictions that support decision – making processes. By analyzing complex datasets, AI systems can identify relationships and correlations that may not be immediately visible to human operators. This capability has become particularly valuable in sectors such as finance, healthcare, manufacturing, and logistics, where data – driven decisions can significantly improve efficiency and performance.

At the same time, these characteristics give rise to important concerns. Many advanced AI systems operate through highly complex models that are difficult to interpret, creating what is commonly referred as the “black box” problem. The lack of transparency associated with certain AI applications raises questions regarding accountability, explainability, and legal responsibility, particularly when automated decisions produce significant consequences for individuals or organizations.

The combination of autonomy, learning capability, predictive power, and opacity explains both the economic attractiveness of artificial intelligence and growing demand for regulatory intervention. As AI systems become increasingly integrated into economic and social activities, policymakers face the challenge of balancing innovation with the protection of fundamental rights, market integrity, and public trust.

1.1.2 Machine learning and Deep learning

The extraordinary progress achieved by artificial intelligence in recent years is largely attributable to the development of machine learning techniques. While traditional software systems operate according to predefined rules programmed by human developers, machine learning allows computers to identify patterns and relationships directly from data. Rather than following a fixed

⁵ Russell & Norvig (2021), “Artificial Intelligence: a modern approach”

set of instructions, these systems learn from experience and improve their performance as the amount of available information increases.

Machine learning has fundamentally transformed the way intelligent systems are designed and developed. Instead of anticipating every possible scenario through manual programming, developers train algorithms using large datasets, enabling them to recognize patterns and generate predictions when exposed to new information. This approach has significantly expanded the range of tasks that computers can perform, particularly in environments characterized by complexity and uncertainty.

The increasing importance of machine learning has been closely linked to the growing availability of digital data. The widespread diffusion of internet services connected devices, social media platforms, and digital transactions has generated unprecedented volumes of information. Combined with substantial improvements in computational power, this abundance of data has created the conditions necessary for the rapid advancement of AI technologies.

Machine learning systems can be broadly classified into three categories. The first is supervised learning, where algorithms are trained using labelled datasets that associate specific inputs with desired outputs. This approach is commonly used in applications such as fraud detection, credit scoring, and medical diagnosis. The second category is unsupervised learning, which involves identifying patterns or structures within data without predefined labels. This technique is particularly useful for customer segmentation, anomaly detection, and data analysis. Finally, reinforcement learning enables systems to improve their performance through continuous interaction with an environment, receiving feedback in the form of rewards or penalties. This approach has been successfully applied in robotics, autonomous vehicles, and strategic decision – making systems.

Among the various branches of machine learning, deep learning has emerged as one of the most influential technological developments of the last decade. Deep learning refers to a subset of machine learning based on artificial neural networks inspired, albeit loosely, by the structure of the human brain. These networks consist of multiple interconnected layers capable of processing increasingly complex representations of information.

The success of deep learning has enabled significantly breakthroughs in areas such as image recognition, speech processing, language translation, and autonomous decision – making. Tasks that were previously considered beyond the reach of machines can now be performed with levels of accuracy that in some cases rival or even surpass human performance. As a result, deep learning has become a key driver of innovation across numerous industries and has contributed substantially to the commercial success of artificial intelligence.

However, the increasing sophistication of deep learning systems has also intensified concerns

regarding transparency and accountability. The internal decision – making processes of neural networks are often difficult to interpret, even for the developers who created them. This lack of explainability has important legal implications, particularly when AI systems are used in contexts involving fundamental rights, employment decisions, financial services, healthcare, or public administration. Consequently, machine learning and deep learning technologies have become central considerations in the development of contemporary AI regulation, including the European Union’s AI Act.

1.2 The evolution of Artificial Intelligence

The current prominence of artificial intelligence is the result of a long and often discontinuous process of technological development. Although AI is frequently perceived as a recent innovation, its origins can be traced back to the middle of the twentieth century, when researchers first began exploring the possibility of creating machines capable of performing tasks associated with human intelligence.

The evolution of artificial intelligence has not followed a linear path. Periods of intense optimism and rapid scientific progress have alternated with phases of disappointment and reduced investment, commonly referred to as “AI winters”. Throughout its history, the development of AI has been influenced not only by technological breakthroughs but also by economic conditions, research funding, and changing societal expectations.

Understanding this historical evolution is essential for appreciating both the opportunities and the challenges associated with contemporary AI systems. The technologies that currently underpin machine learning, deep learning, and generative AI are the result of decades of experimentation, theoretical research, and technological innovation. At the same time, the increasing capabilities of AI systems have progressively amplified concerns regarding accountability, transparency, and governance, ultimately contributing to the emergence of dedicated regulatory frameworks such as the European AI Act.

The following sections examine the major stages in the evolution of artificial intelligence, from its early conceptual foundations to its current role as a transformative technology within the digital economy.

1.2.1 Early developments and AI winters

The foundations of artificial intelligence were established during the 1950s, a period characterized by significant advances in computer science. Early researchers believed that machines could eventually replicate many aspects of human reasoning, problem – solving, and learning. This

ambition culminated in the Dartmouth Summer Research Project on Artificial Intelligence in 1956, widely regarded as the birth of AI as an academic discipline.⁶

During the first decades of research, scientists focused primarily on symbolic AI, an approach based on the assumption that intelligent behavior could be reproduced through the manipulation of logical rules and symbols. Early systems achieved promising results in tasks such as theorem proving, game playing generating considerable enthusiasm among researchers and policymakers. Many experts predicted that human – level artificial intelligence could be achieved within a relatively short period of time. However, these expectations soon proved overly optimistic. Although symbolic systems performed effectively in controlled environments, they struggled to cope with the complexity and unpredictability of real-world situations. Limitations in computational power, data availability, and algorithmic sophistication significantly constrained the practical applications of AI technologies.

As progress slowed and expectations remained unmet, investment in AI research declined. The first major period of reduced funding and interest, later known as an “AI winter”, emerged during the 1970s. A second AI winter occurred in the late 1980s and early 1990s, following the commercial failure of expert systems, which had initially been viewed as a promising application of artificial intelligence.⁷ Despite these setbacks, the periods of reduced enthusiasm played an important role in the long – term development of the field. Researchers continued to refine theoretical models, improve computational methods, and explore alternative approaches to machine intelligence. Many of the concepts developed during these years would later provide the foundation for the breakthroughs that transformed artificial intelligence in the twenty – first century.

1.2.2 The rise of Data – Driven AI

The resurgence of artificial intelligence during the early twenty – first century was largely driven by the convergence of three fundamental factors: the exponential growth of digital data, significant advances in computational power, and the development of increasingly sophisticated machine learning platforms.⁸ Unlike earlier approaches based primarily on symbolic reasoning, modern AI systems rely heavily on data. The widespread diffusion of the internet, mobile technologies, cloud computing, and digital platforms generated unprecedented quantities of information, creating the conditions necessary for training complex machine learning models. Data became the essential resource that allowed algorithms to identify patterns, generate predictions, and continuously

⁶ McCarthy, J. (2007), “What is artificial intelligence?”

⁷ Crevier, D. (1993), “AI: The Tumultuous History of the Search for Artificial Intelligence”

⁸ Agrawal, Gans & Goldfarb (2018), “Prediction Machines”

improve their performance.

At the same time, advances in hardware technologies increased the computational resources available to researchers and businesses. The use of graphical processing units (GPUs), cloud – based infrastructures, and distributed computing systems enabled the training of increasingly large and complex neural networks. Tasks that would previously have required months of computation could now be completed within days or even hours. These technological developments transformed artificial intelligence from a predominantly academic field into a commercially visible technology.⁹ Businesses began adopting AI solutions to improve operational efficiency, optimize supply chains, personalize customer experiences, and support strategic decision – making. Consequently, AI evolved from a specialized research area into a key driver of digital transformation and economic competitiveness.

The rise of data – driven AI also contributed to the emergence of new challenges. As organizations became increasingly dependent on large datasets, concerns regarding privacy, data governance, and algorithmic bias gained prominence. Questions surrounding the ownership, quality, and ethical use of data became central issues within both academic research and public policy discussions.

The transition towards data – driven AI therefore marked a turning point in the history of artificial intelligence.¹⁰ While it enabled unprecedented technological progress, it also highlighted the need for regulatory frameworks capable of addressing the risks associated with the collection, processing, and use of data – intensive technologies.

1.2.3 AI in the Fourth Industrial Revolution

The rapid advancement of artificial intelligence has positioned it at the center of what is commonly referred to as the Fourth Industrial Revolution.¹¹ Unlike previous industrial revolutions, which were driven by mechanization, electrification, and digitalization, the current transformation is characterized by the increasing integration of intelligent technologies into economic and social systems. Artificial Intelligence is often regarded as one of the fundamental technologies of this new era because of its capacity to interact with and enhance other emerging technologies, including the Internet of Things, cloud computing, robotics, blockchain, and advanced data analytics. The convergence of these technologies is creating highly interconnected environments in which intelligent systems can process information, communicate with one another, and make decisions with minimal human intervention.

⁹ Brynjolfsson & McAfee (2014), “The Second Machine Age”

¹⁰ Mayer-Schönberger & Cukier (2013), “Big Data”

¹¹ Klaus Schwab, “The Fourth Industrial Revolution”

From an economic perspective, AI has become a major source of productivity growth and innovation. Firms increasingly utilize AI technologies to automate routine tasks, improve operational efficiency, develop new products and services, and gain competitive advantages in global markets. The ability to generate insights from large datasets has transformed decision – making processes across a wide range of industries, from finance and healthcare to manufacturing and logistics. At the same time, the growing influence of artificial intelligence has generated concerns regarding labor market disruption, market concentration, digital inequality, and the protection of fundamental rights. The increasing autonomy of AI systems has raised questions regarding accountability, transparency, and human oversight, particularly in contexts where automated decisions may significantly affect individuals and organizations.¹²

These concerns have contributed to the emergence of a new regulatory paradigm. Governments and international organizations increasingly recognize that artificial intelligence cannot be governed solely through existing legal frameworks. Instead, dedicated regulatory instruments are required to balance innovation with societal protection and ensure that technological development remains aligned with broader public interests.

Within this context, the European Union has sought to establish itself as a global leader in AI governance. The AI Act represents one of the most ambitious attempts to regulate artificial intelligence, reflecting the broader objective of promoting trustworthy and human – centric innovation. Understanding the historical evolution of AI is therefore essential for understanding why regulation has become such a central component of contemporary technological governance.¹³

1.3 AI adoption across economic sectors

Artificial intelligence has progressively evolved from an emerging technology into a fundamental component of contemporary business strategies. While early AI applications were primarily confined to research laboratories and highly specialized industries, recent technological advancements have enabled organizations of all sizes to integrate intelligent systems into their daily operations. Today, AI is no longer considered a competitive advantage available only to a limited number of innovative firms; rather, it has become an increasingly essential resource for maintaining competitiveness within rapidly evolving digital markets.

The widespread adoption of artificial intelligence reflects a broader process of digital transformation that is reshaping production systems, organizational structures, and value creation

¹² Brynjolfsson, Rock & Syverson (2021), “The Productivity J-Curve”

¹³ European Commission, “White Paper on Artificial Intelligence” (2020).

mechanisms. Companies are using AI not only to automate repetitive tasks but also to improve strategic decision – making, optimize resource allocation, personalize customer experiences, and develop entirely new products and services. Consequently, artificial intelligence is contributing to profound changes in the way firms organize their activities and compete within global markets. Although the pace of adoption differs across industries, AI technologies have become increasingly pervasive in sectors characterized by large volumes of data, complex decision – making processes, and high levels of operational complexity. Manufacturing, financial services, healthcare, and retail represent some of the most significant examples of this transformation. Examining these sectors illustrates both the economic opportunities generated by AI and the diversity of regulatory challenges that emerge from its application.

The following sections analyze the role of artificial intelligence within these industries, highlighting how AI contributes to business performance while simultaneously creating new legal and governance challenges that have become central to contemporary regulatory debates.

1.3.1 Artificial Intelligence in manufacturing

Manufacturing represents one of the sectors in which artificial intelligence has generated some of the most significant economic benefits. The integration of AI into industrial production has accelerated the transition towards smart manufacturing, where interconnected machines, sensors, and intelligent algorithms cooperate to optimize production processes in real time. AI systems are increasingly employed to improve predictive maintenance, quality control, supply chain management, and production planning. By continuously analyzing operational data collected from industrial equipment, machine learning algorithms can detect anomalies before mechanical failures occur, thereby reducing downtime and maintenance costs. Similarly, computer vision technologies enable quality inspection with levels of precision that often exceed traditional manual procedures.¹⁴

Beyond operational efficiency, artificial intelligence is transforming decision – making within manufacturing firms. Managers can rely on predictive analytics to forecast demand, optimize inventory levels, and allocate resources more efficiently. These capabilities contribute to greater organizational flexibility and allow firms to respond more rapidly to changes in market conditions. However, increasing reliance on AI also raises important governance issues. Decisions affecting production quality, workplace safety, and supply chain management are becoming progressively more dependent on algorithmic systems. As a result, manufacturing companies must ensure that AI applications remain reliable, transparent, and compliant with emerging regulatory

¹⁴ Lee, J., Bagheri, B., & Kao, H.-A. (2015). “A Cyber-Physical Systems Architecture for Industry 4.0”.

requirements, particularly when high – risk AI systems are involved under the European AI Act.

1.3.2 Artificial Intelligence in financial services

The financial sector has historically been among the earliest adopters of artificial intelligence. Banks, insurance companies, investment firms, and financial technology providers increasingly rely on AI systems to improve operational efficiency, manage risks, detect fraud, and enhance customer services.¹⁵ One of the most widespread applications concerns credit risk assessment. Machine learning algorithms analyze large quantities of financial and behavioral data to evaluate the creditworthiness of borrowers more rapidly and accurately than many traditional statistical models. AI also plays a crucial role in fraud detection, where intelligent systems continuously monitor transactions to identify suspicious activities and prevent financial crimes.

Investment management has also been profoundly influenced by AI technologies. Algorithmic trading systems process market information at extraordinary speed, while robot – advisory platforms provide automated investment recommendations tailored to individual investors’ preferences and risk profiles.¹⁶ These innovations have increased market efficiency while simultaneously raising concerns regarding transparency, accountability, and financial stability.¹⁷ The extensive use of AI within financial services has significant regulatory implications. Algorithmic decision – making may affect access to credit, insurance coverage, or investment opportunities, making issues such as explainability, fairness, and non – discrimination particularly important. Consequently, the financial sector illustrates how economic efficiency and regulatory oversight increasingly coexist within AI – driven business environments.

1.3.3 Artificial Intelligence in Healthcare

Healthcare represents one of the sectors where artificial intelligence has the potential to generate substantial social and economic benefits. AI technologies support medical professionals in diagnostic procedures, treatment planning, drug discovery, and hospital management, contributing to improved patient outcomes while increasing the efficiency of healthcare systems. Machine learning models can analyze medical images, laboratory results, and clinical records with remarkable accuracy, assisting physicians in the early detection of diseases such as cancer or cardiovascular disorders. AI is also accelerating pharmaceutical research by reducing the time required to identify promising drug candidates and supporting the development of personalized

¹⁵ Financial Stability Board (2017). “Artificial Intelligence and Machine Learning in Financial Services”

¹⁶ OECD reports on AI in finance.

medicine.¹⁸

From an organizational perspective, hospitals increasingly employ AI to optimize resource allocation, predict patient admissions, and improve administrative processes. These applications contribute to reducing operational costs while enhancing the quality of healthcare services.

At the same time, healthcare is one of the sectors most directly affected by legal and ethical considerations. AI systems frequently process highly sensitive personal data, and incorrect algorithmic decisions may have serious consequences for patients. For this reason, many healthcare applications fall within the category of high – risk AI systems under the European AI Act, requiring particularly stringent compliance obligations concerning transparency, data governance, human oversight, and risk management.¹⁹

1.3.4 Artificial Intelligence in retail and e – commerce

The retail sector has undergone significant transformation through the adoption of artificial intelligence. Digital platforms and traditional retailers increasingly employ AI technologies to analyze consumer behavior, personalize shopping experiences, and improve inventory management. Recommendation systems have become one of the most recognizable applications of AI within retail. By analyzing customers' purchasing histories and browsing behavior, intelligent algorithms generate personalized product suggestions that enhance customer satisfaction while increasing sales and customer loyalty. Dynamic pricing systems similarly enable firms to adjust prices in real time according to changes in demand, inventory levels, and competitive conditions.²⁰

Artificial Intelligence also plays a central role in supply chain optimization. Predictive analytics assist retailers in forecasting consumer demand, minimizing inventory shortages, and reducing waste throughout distribution networks. Customer service has likewise been transformed through the introduction of conversational AI systems capable of providing continuous assistance and improving user experience. Despite these advantages, AI – driven retail raises important concerns regarding consumer protection privacy, and algorithmic transparency. The extensive use of personal data for commercial purposes requires firms to comply with data protection legislation while ensuring that automated decision – making processes remain fair and non – discriminatory.²¹ As regulatory frameworks governing AI continue to evolve, retailers must increasingly balance commercial innovation with legal compliance and consumer trust.

¹⁸ Topol, E. (2019). “Deep Medicine”

¹⁹ World Health Organization (2021). “Ethics and Governance of Artificial Intelligence for Health.”

²⁰ McKinsey Global Institute (2023). The Economic Potential of Generative AI.

1.3.5 Cross - sectoral implications for European businesses

The analysis conducted throughout this chapter has shown that the adoption of artificial intelligence is no longer confined to specific industries or technological context. Rather, AI has progressively established itself as a cross – sectoral technology capable of transforming virtually every dimension of business activity. Regardless of whether it is implemented in manufacturing, financial services, healthcare, or retail, artificial intelligence is reshaping organizational processes, strategic decision – making, and value creation. This widespread diffusion confirms that AI should be regarded not merely as another digital innovation but as a general – purpose technology with profound implications for the competitiveness of European businesses and the broader digital economy.

One of the most significant consequences of adoption of AI concerns its contribution to productivity improvements. By automating repetitive tasks, supporting complex decision – making processes, and analyzing large volumes of data in real time, AI enables firms to perform activities more efficiently than traditional digital systems. These capabilities allow organizations to optimize production processes, reduce operational delays, improve forecasting accuracy, and allocate resources more effectively. Consequently, AI has become an increasingly important driver of productivity growth, enabling companies to generate greater value while utilizing resources more efficiently. Closely related to productivity gains is the capacity of AI to reduce operational costs and improve organizational efficiency. Intelligent systems allow businesses to automate administrative procedures, optimize supply chain management, predict equipment failures through predictive maintenance, and streamline customer service operations. Such improvements not only reduce direct operating expenses but also enhance organizational flexibility and responsiveness in highly dynamic markets. As firms continue to operate within increasingly competitive and uncertain economic environments, operational efficiency has become a strategic objective that AI technologies are particularly well suited to support.

Beyond efficiency improvements, artificial intelligence is also fostering innovation and the emergence of new business models. The availability of advanced analytical capabilities enables firms to develop data – driven products and services, personalize customer experiences, and explore innovative forms of value creation. In many industries, AI has transformed traditional business practices by enabling entirely new commercial opportunities, including platform – based services, predictive maintenance solutions, personalized financial products, intelligent healthcare systems, and generative AI applications capable of producing digital content. Rather than simply improving existing processes, AI increasingly functions as an enabler of business model

innovation, allowing firms to redefine the ways in which they create, deliver, and capture value. These developments have important implications for firms' competitive positioning. Companies capable of successfully integrating AI into their operations often benefit from faster decision – making, greater adaptability, improved customer satisfaction, and stronger innovation capabilities. The strategic use of AI may therefore generate sustainable competitive advantages by increasing organizational agility and strengthening firms' ability to respond to changing market conditions. At the same time, organizations that fail to adopt AI technologies risk experiencing declining productivity, reduced innovation capacity, and a progressive loss of competitiveness within both European and global markets.

Nevertheless, the economic opportunities associated with artificial intelligence cannot be considered independently from the risks generated by its widespread deployment. The same characteristics that make AI economically valuable also give rise to significant legal, ethical, and societal challenges. As AI systems become increasingly involved in decisions affecting individuals, businesses, and public institutions, concerns regarding fairness, accountability, transparency, and data governance have become central issues within both academic literature and public policy debates.

Among these concerns, algorithmic bias represents one of the most significant challenges. Since AI systems learn from historical datasets, they may reproduce or even amplify existing social and economic inequalities if the underlying data are incomplete, unrepresentative, or biased. Algorithmic discrimination may affect decisions concerning recruitment, access to credit, insurance, healthcare, or public services, potentially generating unequal treatment of individuals and exposing organizations to substantial legal and reputational risks. Consequently, ensuring fairness in AI systems has become a fundamental objective in both corporate governance and regulatory policy.

A second critical issue concerns the lack of transparency associated with many advanced AI models. Complex machine learning and deep learning systems frequently operate as so – called “black boxes”, producing outputs that are difficult to interpret even by their developers. While these systems often achieve remarkable levels of predictive accuracy, their limited explainability raises important questions regarding accountability and legal responsibility. Businesses increasingly rely on AI to support decisions with significant economic and social consequences, yet stakeholders may find it difficult to understand how these decisions have been reached. This opacity may undermine public trust, complicate regulatory compliance, and reduce organizations' ability to justify automated decisions.

Equally important are the challenges relating to privacy and data protection. Modern AI systems depend heavily on the availability of large quantities of data, many of which may include personal

or commercially sensitive information. The collection, storage, and processing of such data create substantial risks concerning confidentiality, cybersecurity, and compliance with data protection legislation. Organizations must therefore ensure that AI systems operate within robust data governance frameworks capable of safeguarding individual rights while maintaining the quality and reliability of the information used to algorithms. As data increasingly becomes the strategic resource underpinning artificial intelligence, effective data governance has evolved from a purely technical concern into a central component of corporate strategy and regulatory compliance.

Taking together, these opportunities and challenges demonstrate that the adoption of artificial intelligence extends far beyond technological innovation. AI is transforming corporate governance, organizational structures, risk management practices, and strategic decision – making, requiring businesses to develop new capabilities that combine technological expertise with legal, ethical and managerial competences. The successful integration of AI therefore depends not only on technological investment but also on the establishment of governance mechanisms capable of ensuring that intelligent systems remain reliable, transparent, accountable, and aligned with societal expectations. It is precisely this combination of extraordinary economic potential and significant societal risks that has prompted governments around the world to develop dedicated regulatory frameworks for artificial intelligence. As AI increasingly influences markets, organizations, and individuals, regulation becomes essential not only to mitigate potential harm but also to create legal certainty necessary for innovation to flourish. Rather than representing a simple constraint on business activity, an effective regulatory framework can reduce uncertainty, strengthen consumer trust, encourage responsible innovation, and promote fair competition within the digital economy.

Within this broader context, the European Union has adopted one of the most ambitious regulatory strategies currently in force. Instead of regulating AI only with specific industries, the European legislator has introduced a horizontal framework based on the level of risk associated with AI systems, establishing common principles applicable across different sectors of economic activity. This approach reflects the recognition that many of the challenges generated by artificial intelligence, such as algorithmic bias, opacity, inadequate human oversight, and data governance, are intrinsic characteristics of AI technologies rather than sector – specific issues.

Having examined the technological evolution of artificial intelligence, its growing diffusion across economic sectors, and the opportunities and risks associated with its adoption, the discussion can now move from the technological and economic dimensions of AI to its legal governance. The following chapter therefore analyses the emergence of the European regulatory framework for artificial intelligence, focusing on the rationale behind the AI Act, its risk – based approach, the compliance obligations imposed on businesses, and its interaction with the broader

ecosystem of European digital regulation.

CHAPTER 2: The European regulatory framework for Artificial Intelligence

2.1 The emergence of AI Governance

The rapid expansion of artificial intelligence has fundamentally transformed the relationship between technological innovation and public regulation. As AI systems have become increasingly integrated into economic activities, public services, and everyday life, governments around the world have recognized that existing legal frameworks are often insufficient to address the novel risks generated by these technologies. Issues such as algorithmic discrimination, opaque decision – making processes, cybersecurity vulnerabilities, and the extensive use of personal data have challenged traditional legal concepts based on human decision – makers and predictable software systems.²²

Unlike previous waves of digital innovation, artificial intelligence has characteristics that make regulatory intervention particularly complex. AI systems are capable of learning from data, adapting their behavior over time, and operating with varying degrees of autonomy. While these characteristics generate substantial economic benefits by increasing productivity and fostering innovation, they also create uncertainty regarding legal responsibility, accountability, and the protection of fundamental rights. Consequently, AI governance has progressively emerged as a distinct field within technology regulation, combining legal, economic, ethical, and policy considerations. The concept of AI governance extends beyond the adoption of formal legislation. It encompasses the set of legal rules, institutional mechanisms, technical standards, ethical principles, and voluntary guidelines that collectively shape the development, deployment, and use of artificial intelligence.²³ Effective AI governance therefore requires balancing multiple objectives that are not always aligned. Policymakers seek to encourage technological innovation and economic growth while simultaneously ensuring that AI systems remain safe, transparent, accountable, and respectful of fundamental rights.

The balancing exercise has generated different regulatory philosophies across the world. While some jurisdictions have favored flexible governance models centered on innovation and market incentives, others have adopted more interventionist approaches based on comprehensive legal regulation. These differences reflect broader political, economic, and institutional traditions, leading to distinct models of AI governance that increasingly influence international competition and digital policy. Within this evolving landscape, the European Union has pursued a particularly ambitious strategy. Rather than regulating artificial intelligence through sector – specific legislation, the European legislator has sought to establish a comprehensive horizontal framework

²² European Commission (2020) – White Paper on Artificial Intelligence: A European approach to Excellent and Trust

²³ Floridi, L., et al. (2018): “AI4People—An Ethical Framework for a Good AI Society”

applicable across different industries and economic activities. The AI Act represents the most advanced expression of this regulatory vision and reflects the broader European objective of promoting what has been defined as “trustworthy artificial intelligence”.²⁴

Before examining the structure and content of the European AI Act, it is necessary to understand how different approaches to AI governance have emerged worldwide. The following sections therefore analyze the principal regulatory adopted at the global level before focusing on the distinctive characteristics of the European approach.

2.1.1 Global regulatory approaches

The increasing deployment of artificial intelligence has stimulated an unprecedented global debate regarding the appropriate role of regulation in governing emerging digital technologies. As AI systems have become capable of influencing economic activities, labor markets, financial services, healthcare, and public administration, governments have progressively recognized that traditional legal frameworks are often insufficient to address the novel risks²⁵ generated by autonomous and data – driven decision – making systems. Consequently, AI governance has emerged as a strategic priority not only for legal systems but also for economic policy and international competitiveness. Despite this shared recognition, there is no universally accepted model for regulating artificial intelligence. Different jurisdictions have adopted regulatory strategies that reflect their own political priorities, institutional traditions, and economic objectives. While all major economies acknowledge the need to encourage innovation and mitigate the risks associated with AI, they differ substantially in the balance they seek to achieve between technological development, market freedom, and regulatory intervention.

Broadly speaking, three major regulatory models can be identified. The first is the European model, which is characterized by a comprehensive legal framework centered on the protection of fundamental rights, consumer protection, and risk management. The second is the American model, which has traditionally favored a market – oriented approach based on innovation, private – sector leadership, and relatively limited ex ante regulation. The third is Chinese model, where AI governance is closely linked to national industrial policy, technological sovereignty, and extensive state supervision.

The United States has historically adopted a relatively flexible regulatory strategy. Rather than introducing a comprehensive federal law specifically governing artificial intelligence, American policymakers have generally preferred sector – specific regulation supported by existing legal frameworks. This approach reflects the belief that excessive regulatory intervention may

²⁴ High-Level Expert Group on AI (2019): Ethics Guidelines for Trustworthy AI

²⁵ National Institute of Standards and Technology (2023). AI Risk Management Framework.

discourage investment, slow technological progress, and reduce the international competitiveness of domestic firms. Consequently, AI governance in the United States has largely relied on voluntary standards, industry self – regulation, and guidance issued by federal agencies, while leaving significant room for technological experimentation and entrepreneurial initiative.

China has pursued a markedly different strategy. Artificial intelligence is regarded as a strategic technology capable of strengthening national economic development, industrial competitiveness, and geopolitical influence. As a result, the Chinese government has combined substantial public investment in AI research with an extensive regulatory framework that emphasizes state oversight, national security, and social stability.²⁶ Unlike the more decentralized approaches adopted elsewhere, Chinese AI governance is characterized by a high degree of governmental coordination, allowing public authorities to influence both technological development and market deployment. These contrasting approaches illustrate that AI regulation is not merely a legal issue but also an instrument of economic and industrial policy. Decisions regarding the degree of regulatory intervention directly influence investment incentives, innovation ecosystems, and the international competitiveness of domestic firms.²⁷ A regulatory framework that is perceived as excessively restrictive may discourage technological development and reduce firms’ capacity to compete globally. Conversely, an excessively permissive environment may undermine consumer trust, increase legal uncertainty, and generate significant societal risks. The challenge faced by policymakers therefore lies in identifying an appropriate balance between these competing objectives.

Against this international background, the European Union has sought to develop a distinctive regulatory philosophy. Rather than prioritizing either market freedom or state control, the European approach is founded on the idea that technological innovation and the protection of fundamental rights should reinforce one another. This vision has progressively evolved into the concept of “Trustworthy Artificial Intelligence”²⁸, which now constitutes the normative foundation of the European regulatory framework and provides the intellectual basis for the AI Act.

2.1.2 The European vision of trustworthy artificial intelligence

The European Union’s approach to artificial intelligence is founded on the conviction that technological innovation should be developed in a manner that remains fully consistent with the Union’s fundamental values. Rather than viewing regulation as an obstacle to economic growth,

²⁶ Cyberspace Administration of China (2023). Interim Measures for the Management of Generative Artificial Intelligence Services.

²⁷ Cath, C. et al. (2018). Artificial Intelligence and Good Society.

²⁸ OECD (2019) - Recommendation of the Council on Artificial Intelligence

European policymakers have increasingly argued that effective governance can foster innovation by strengthening legal certainty, increasing public trust, and promoting the responsible development of digital technologies. This philosophy has gradually evolved into the concept of “Trustworthy Artificial Intelligence”, which today represents the normative cornerstone of European AI governance. The notion of Trustworthy AI was first systematically articulated by the High – Level Expert Group in Artificial Intelligence established by the European Commission. In its 2019 *Ethics Guidelines for Trustworthy AI*²⁹, the Group argued that AI systems should not be evaluated solely according to their technical performance or economic efficiency. Instead, they should be designed and deployed in ways that respect fundamental rights, democratic values, and the rule of law. According to this perspective, public trust is not simply a desirable consequence of regulation but a necessary condition for the sustainable adoption of artificial intelligence within society and the economy.

The Guideline identify three cumulative conditions that characterize trustworthy AI. First, AI systems must be lawful, meaning that they comply with all applicable legal requirements. Second, they must be ethical, respecting fundamental rights and widely recognized moral principles. Third, they must be technically robust and socially reliable throughout their entire lifecycle. These three dimensions are presented as complementary rather than alternative objectives, reflecting the European conviction that technological progress should not come at the expense of individual rights or societal well – being.

This vision differs significantly from approaches that primarily emphasize economic efficiency or technological leadership. While the European Union fully recognizes the transformative potential of AI for productivity, innovation, and competitiveness, it also considers public confidence to be an essential economic asset. Consumers, businesses and public institutions are more likely to adopt AI technologies when they perceive them as transparent, reliable, and subject to effective legal safeguards. From this perspective, regulation does not merely reduce risks; it also contributes to creating favorable market conditions by reducing legal uncertainty and encouraging investment in trustworthy innovation. The concept of Trustworthy AI has progressively shaped the broader European digital strategy. The 2020 White Paper on Artificial Intelligence translated these ethical principles into concrete policy objectives, proposing a regulatory framework capable of supporting excellence in AI while ensuring adequate protection against its potential risks. This dual objective promoting innovation while safeguarding fundamental rights subsequently became the guiding principle of the AI Act and explains the adoption of its well – known and risk – based regulatory approach.³⁰

²⁹ High-Level Expert Group on AI (2019). *Ethics Guidelines for Trustworthy AI*.

³⁰ European Commission (2020). *White Paper on Artificial Intelligence*.

From an economic perspective, the European model reflects a long – term vision of competitiveness. Rather than competing exclusively through regulatory flexibility, the European Union seeks to position itself as the global leader in reliable and human – centric artificial intelligence. The underlying assumption is that firms capable of developing AI systems that satisfy high standards of transparency, accountability, safety, and data governance will enjoy stronger consumer confidence, lower legal uncertainty, and greater opportunities to operate within international markets where trust increasingly represents a competitive advantage. Nevertheless, the European strategy also attracted criticism. Some scholars argue that imposing extensive compliance obligations may disproportionately affect small and medium – sized enterprises, increase development costs, and slow the commercialization of innovative applications. Others contend that the emphasis placed on fundamental rights and responsible innovation may ultimately strengthen the long – term competitiveness of European firms by encouraging higher – quality technologies and reducing future legal and reputational risks. This debate remains one of the central issues within contemporary AI governance and directly anticipates the analysis developed in the following sections of this thesis.

The emergence of the concept of Trustworthy Artificial Intelligence therefore represents far more than an ethical framework. It constitutes the intellectual and regulatory foundation upon which the entire European approach to AI has been built. Understanding these principles is essential for analyzing the AI Act, whose provisions translate the abstract values of trustworthiness into concrete legal obligations applicable to providers, deployers, importers, and users of artificial intelligence systems throughout the European Union.

2.2 The development of the EU AI Act

The adoption of the Artificial Intelligence Act represents one of the most significant milestones in the evolution of European digital regulation. Rather than constituting an isolated legislative initiative, the AI Act³¹ is the outcome of a broader regulatory strategy through which the European Union has progressively sought to establish a coherent framework capable of governing emerging digital technologies while preserving the values upon which the European legal order is founded. The development of the AI Act reflects the growing awareness that artificial intelligence presents regulatory challenges that differ substantially from those posed by previous digital technologies. The increasing autonomy of AI systems, their dependence on vast amounts of data, and their capacity to influence decisions affecting individuals, businesses, and public authorities have exposed important limitations within existing legal frameworks. As AI technologies became more

³¹ AI Act (Regulation (EU) 2024/1689).

deeply integrated into economic and social activities, European policymakers recognized that relying exclusively on pre – existing legislation would not be sufficient to address the risks associated with these systems. At the same time, the European Union viewed artificial intelligence not only as a source of potential risks but also as a strategic opportunity for economic growth, technological innovation, and international competitiveness.³² Consequently, the development of the AI Act has been characterized by the continuous search for an appropriate balance between encouraging innovation and ensuring that AI systems remain safe, transparent, and respectful of fundamental rights.

Understanding the origins, objectives, and legislative evolution of the AI Act is therefore essential for appreciating both its legal architecture and its potential economic implications for European companies. The following sections examine the principal stages that led to the adoption of the Regulation, beginning with its legislative origins, continuing with the policy objectives pursued by the European institutions, and concluding with an overview of the legislative process that ultimately resulted in the approval of the AI Act.

2.2.1 Legislative origins

The origins of the AI Act can be understood only within the broader context of the European Union’s digital transformation strategy. Throughout the last decade, European institutions have progressively acknowledged that artificial intelligence would become one of the key technologies shaping future economic development. At the same time, policymakers recognized that widespread deployment of AI could generate risks that existing legal instruments (designed for earlier generations of digital technologies) were not fully equipped to address.

The first significant step towards a comprehensive European strategy emerged in 2018, when the European Commission published the *Communication Artificial Intelligence for Europe*. This document identified AI as a strategic priority capable of strengthening productivity, stimulating innovation, and enhancing the competitiveness of European industry. However, it also emphasized that technological progress should remain fully consistent with the Union’s commitment to democracy, the rule of law, and the protection of fundamental rights. The same year, the European Commission established the High – Level Expert Group on Artificial Intelligence, bringing together academics, legal scholars, industry representatives, and civil society organizations. The objective was not merely to assess the technological implications of AI but also to develop a governance framework capable of promoting responsible innovation. The publication of the Ethics Guidelines for Trustworthy AI in 2019 marked a turning point in

³² Smuha, N. A. (2021). From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence.

European AI policy by introducing the concept of trustworthy AI as the normative foundation of future regulation.³³

Building upon these ethical principles, the Commission published the White Paper on Artificial Intelligence in February 2020. The White Paper represented the first comprehensive proposal for a harmonized European regulatory framework specifically dedicated to artificial intelligence. It argued that Europe required a legal framework capable of fostering excellence in AI while simultaneously addressing the risks generated by high – impact AI applications. This document introduced many of the concepts that would later become central features of the AI Act, including the risk – based approach, the distinction between different categories of AI systems, and the importance of compliance obligations proportionate to the level of risk.

The publication of the Proposal for the AI Act in April 2021 therefore represented the natural evolution of a policy process that had already been underway for several years. Rather than introducing an entirely new regulatory philosophy, the proposed Regulation consolidated previous ethical, political, and legal initiatives into a comprehensive legislative framework intended to govern artificial intelligence across the European Union.

From both a legal and an economic perspective, the legislative origins of the AI Act demonstrate that the Regulation was conceived not merely as an instrument for limiting technological risks but also as part of a broader industrial strategy aimed at strengthening Europe’s position within the global AI ecosystem. This dual ambition, to promote innovation while ensuring trustworthy AI, has remained one of the defining characteristics of the European regulatory model throughout the legislative process.

2.2.2 Policy objectives

The policy objectives underlying the AI extend well beyond the regulation of artificial intelligence as a technological phenomenon. Regulation reflects the European Union’s broader ambition to establish a governance model capable of supporting digital innovation while ensuring that technological progress remains compatible with the Union’s legal values, economic priorities, and social objectives. One of the principal objectives pursued by the European legislator is the creation of a harmonized regulatory framework applicable across all Member States. Prior to the AI Act, the absence of common rules risked generating regulatory fragmentation, increasing legal uncertainty for businesses operating within the internal market. By introducing a single set of rules governing AI systems, the Regulation seeks to facilitate cross – border economic activity while reducing compliance complexity for firms developing or deploying AI technologies.³⁴

³³ Floridi, L. (2019). Establishing the Rules for Building Trustworthy AI.

³⁴ Hacker (2023), The European AI Liability Framework.

A second objective concerns the protection of fundamental rights. European policymakers have consistently maintained that artificial intelligence should be developed and deployed in ways that respect human dignity, privacy, equality, non – discrimination, and democratic values. Consequently, the AI Act aims to prevent the deployment of AI systems capable of producing unacceptable risks for individuals while imposing stricter obligations on applications considered particularly sensitive. Closely connected to these legal objectives is the promotion of public trust. European institutions have repeatedly argued that trust constitutes a prerequisite for the successful adoption of artificial intelligence within society and the economy. Consumers, businesses, and public administrations are more likely to embrace AI technologies when they perceive them as transparent, reliable, and subject to effective legal safeguards. In this sense, regulation is viewed not only as a mechanism for limiting risks but also as a catalyst for technological adoption and sustainable innovation. The AI Act also pursues important economic objectives. By providing legal certainty and establishing predictable compliance requirements, the Regulation seeks to create favorable conditions for investment and innovation within the European digital economy. The underlying assumption is that clear and harmonized rules can reduce transaction costs, facilitate market integration, and encourage the development of trustworthy AI solutions capable of competing internationally.

Finally, the Regulation reflects the European Union’s geopolitical ambition to shape the future of global AI governance. Much as the GDPR influenced data protection policies beyond Europe, the AI Act is intended to establish regulatory standards that may become influential at the international level. Through this approach, the European Union seeks not only to regulate its internal market but also to contribute to the development of global principles governing artificial intelligence.

2.2.3 The legislative process

The legislative process leading to the adoption of the AI Act was characterized by extensive political negotiation, institutional dialogue, and stakeholder participation. From its initial proposal in 2021 to its final adoption in 2024, the Regulation underwent significant revisions reflecting the rapid evolution of artificial intelligence technologies and the growing complexity of the issues under consideration.

Following the publication of the Commission’s proposal³⁵, both the European Parliament³⁶ and the Council of the European Union³⁷ introduced numerous amendments concerning the scope of

³⁵ Commission Proposal (2021).

³⁶ European Parliament Amendments (2023).

³⁷ Council of the EU Negotiating Position

the Regulation, the classification of high – risk AI systems, governance mechanisms, enforcement powers, and compliance obligations. Public consultations, expert opinions, academic contributions, and industry feedback played a substantial role in shaping the final legislative text, illustrating the participatory nature of the European legislative process.

The emergence of generative artificial intelligence during the negotiations profoundly influenced the legislative debate. The public release of large language models demonstrated that AI technologies were evolving far more rapidly than initially anticipated when the proposal had first been drafted. Therefore, European institutions introduced specific provisions governing general – purpose AI models and foundation models, ensuring that the Regulation would remain capable of addressing future technological developments. Following the provisional political agreement in December 2023, the AI Act was formally adopted in 2024, becoming the world’s first comprehensive horizontal legal framework specifically dedicated to artificial intelligence. The Regulation introduced a phased implementation schedule, allowing businesses and public authorities sufficient time to adapt their governance structures, compliance procedures, and technological systems before the various obligations become fully applicable.

The legislative process itself reflects one of the defining characteristics of European digital governance: the attempt to reconcile technological innovation with democratic legitimacy, stakeholder participation, and legal certainty. Rather than reacting solely to technological developments, the European Union sought to develop a regulatory framework capable of remaining effective despite the rapid pace of innovation. This objective explains many of the structural choices that characterize the AI Act, particularly its flexible risk – based approach, which will be examined in the following section.³⁸

2.3 The risk – based approach of the AI Act

One of the most innovative aspects of the Artificial Intelligence Act is the adoption of a risk – based regulatory framework. Rather than regulating all AI systems uniformly, the European legislator has chosen to differentiate legal obligations according to the level of risk that each system may pose to individuals, society, and the internal market. This approach reflects the recognition that artificial intelligence encompasses a broad spectrum of technologies whose potential impacts vary considerably depending on their intended purpose, deployment context, and possible consequences. The risk – based model constitutes the conceptual foundation of the AI Act and represents one of its defining features. Instead of focusing exclusively on the technology itself, the Regulation evaluates the degree of risk associated with the specific use of

³⁸ Final AI Act (2024).

an AI system. As a result, regulatory intervention becomes proportionate: the greater the potential harm generated by an AI application, the more extensive the legal obligations imposed on providers, deployers, importers, and distributors.

From an economic perspective, this approach seeks to reconcile two potentially conflicting objectives. On the one hand, the European Union aims to encourage innovation by avoiding unnecessary regulatory burdens for low – risk AI applications. On the other hand, it seeks to ensure that AI systems capable of significantly affecting individuals or society are subject to robust safeguards. Consequently, the risk – based model attempts to balance technological development with legal certainty, consumer protection, and market confidence.

The AI Act distinguishes four categories of AI systems: unacceptable – risk AI systems, high – risk AI systems, limited – risk AI systems, and minimal – risk AI systems.³⁹ Each category is associated with a different regulatory regime reflecting the legislator’s assessment of the potential risks involved. Understanding this classification is essential for analyzing both the legal obligations introduced by the Regulation and their economic implications for European businesses.

2.3.1 Unacceptable – risk AI systems

The highest level of regulatory intervention under the AI Act concerns AI systems that are considered to present an unacceptable level of risk to individuals and society. These applications are regarded as fundamentally incompatible with the values upon which the European Union is founded and are therefore prohibited, except in a limited number of narrowly defined circumstances.⁴⁰ The rationale behind this prohibition lies in the recognition that certain AI applications may seriously undermine fundamental rights, democratic principles, and human dignity. Rather than attempting to regulate these technologies through compliance obligations, the European legislator concluded that the risks they generate cannot be adequately mitigated and therefore require an outright ban.

Examples of prohibited AI practices include systems designed to manipulate individuals through subliminal techniques; exploit vulnerabilities related to age or disability or implement social scoring mechanisms that evaluate individuals based on their behavior or personal characteristics.⁴¹ The Regulation also imposes significant restrictions on certain forms of biometric identification and categorization, reflecting growing concerns regarding surveillance and the misuse of personal data.

³⁹ AI Act (Regulation (EU) 2024/1689), 26–40

⁴⁰ AI Act, Article 5 (Prohibited AI Practices).

⁴¹ Pasquale, F. (2015). *The Black Box Society*

Although the number of prohibited applications remains relatively limited, their inclusion within the AI Act carries important economic implications. By clearly identifying practices considered unacceptable, the Regulation establishes legal certainty regarding the boundaries of permissible innovation. Firms operating within the European market are encouraged to direct investments towards AI applications capable of generating economic value without compromising fundamental rights.

From a governance perspective, the prohibition of unacceptable – risk systems demonstrates that the European Union does not regard technological innovation as an objective that should be pursued without limits. Instead, innovation is expected to remain consistent with broader constitutional values, reinforcing the idea that responsible technological development represents a prerequisite for sustainable economic growth.

2.3.2 High – risk AI systems

High – risk AI systems constitute the core of the regulatory framework established by the AI Act.⁴² Unlike prohibited AI applications, these systems may continue to be developed and deployed within the European Union, if they comply with a comprehensive set of legal obligations designed to reduce potential risks while preserving the benefits associated with technological innovation. The classification of an AI system as high – risk depends primarily on its intended purpose and the context in which it is used. Applications operating in sectors such as critical infrastructure, healthcare, education, employment, financial services, migration, law enforcement, and the administration of justice are considered capable of producing significant effects on individuals' rights and opportunities. Consequently, errors, biases, or failures occurring within these systems may generate substantial legal, economic, and social consequences.

To address these risks, the AI Act introduces extensive compliance requirements covering the entire lifecycle of high – risk AI systems. Providers are required to establish risk management procedures, implement appropriate data governance mechanisms, ensure technical documentation, maintain human oversight, monitor system performance, and guarantee adequate levels of accuracy, robustness, and cybersecurity.⁴³

For businesses, these obligations represent both a challenge and an opportunity. Compliance inevitably generates additional costs related to governance structures, documentation, legal advice, internal controls, and technical adaptation. At the same time, however, these requirements may increase customer confidence, reduce legal uncertainty, and strengthen firms' reputational capital. In this sense, the compliance framework should not be viewed exclusively as a regulatory

⁴² Annex III (High-Risk AI Systems).

⁴³ AI Act, Articles 6–29.

burden but also as a mechanism capable of promoting higher – quality AI systems and facilitating their long – term market acceptance.

The regulation of high – risk AI systems therefore illustrate the broader philosophy underpinning the AI Act: rather than discouraging innovation, the Regulation seeks to ensure that innovation develops within a framework capable of balancing economic competitiveness with the protection of fundamental rights.

2.3.3 Limited – risk AI systems

Not all AI applications generate significant risks requiring extensive regulatory intervention. For this reason, the AI Act establishes a separate category for AI systems presenting limited levels of risk, subjecting them primarily to transparency obligations⁴⁴ rather than comprehensive compliance requirements. The underlying assumption is that users should be aware whenever they interact with artificial intelligence or encounter AI – generated content. Transparency therefore becomes the principal regulatory mechanism governing this category of AI systems. Applications such as chatbots, virtual assistants, deepfake technologies, and certain content – generation systems are generally required to inform users that they are interacting with AI or that the content they are viewing has been artificially generated or manipulated.

These obligations pursue several objectives simultaneously. They protect users from deception, promote informed decision – making, and contribute to strengthening public trust in AI technologies. At the same time, they avoid imposing disproportionate compliance costs on businesses developing relatively low – risk applications.

From an economic perspective, the limited – risk regime illustrates the proportionality principle that characterizes the AI Act. Rather than imposing identical obligations on all AI systems, the Regulation tailors compliance requirements to the actual level of risk generated by each application. This differentiated approach seeks to preserve innovation incentives while ensuring an appropriate degree of consumer protection and market transparency.

2.3.4 Minimal – risk AI systems

Many AI systems currently deployed within the European Union fall within the category of minimal – risk applications. These systems generally present negligible or no significant risks to individuals’ rights, safety, or societal interests and are therefore not subject to specific regulatory obligations under the AI Act.

Examples include spam filters, AI – enabled video games, recommendation engines used for

⁴⁴ AI Act, Article 50 (Transparency Obligations).

entertainment purposes, and various productivity applications that do not significantly affect individuals' legal or economic interests. The European legislator deliberately chose not to regulate these systems extensively to avoid unnecessary barriers to technological development and market innovation. This regulatory choice reflects one of the central principles underlying the AI Act: proportionality. Excessive regulation of low – risk applications could discourage investment, increase compliance costs, and reduce the competitiveness of European firms without generating corresponding societal benefits. By examining minimal – risk AI systems from specific obligations, the Regulation allows businesses to continue developing and deploying a wide range of innovative solutions with minimal administrative burdens.

Nevertheless, the absence of AI Act obligations does not imply the complete absence of legal responsibilities. Depending on the circumstances, providers and users of minimal – risk AI systems remain subject to other areas of European law, including data protection legislation, consumer protection rules, product safety requirements, and contractual obligations. The distinction between minimal – risk applications and more heavily regulated categories demonstrate the flexibility of the European regulatory framework. Rather than adopting a one – size – fits – all approach, the AI Act seeks to calibrate regulatory intervention according to the actual risks generated by different AI applications. This proportionality is one of the reasons why the Regulation has attracted considerable attention internationally and is increasingly regarded as a potential model for future AI governance.

2.4 Compliance obligations for businesses

One of the most distinctive features of the AI Act is that it does not merely prohibit certain AI practices or classify AI systems according to their level of risk. Instead, the Regulation establishes a comprehensive compliance framework that imposes specific obligations on the economic operators involved in the development, deployment, distribution, and use of artificial intelligence systems.

The AI Act adopts a lifecycle to approach AI governance, recognizing that compliance cannot be achieved through a single assessment carried out before an AI system placed on the market. Rather, providers, deployers, importers, distributors, and, in some circumstances, authorized representatives are required to implement continuous governance mechanisms capable of ensuring that AI systems remain compliant throughout their entire lifecycle.⁴⁵ From a business perspective, these obligations represent a significant organizational challenge. Compliance requires firms to establish internal governance structures, adopt risk management procedures, implement

⁴⁵ AI Act (Regulation (EU) 2024/1689), Chapter III (Requirements for High-Risk AI Systems).

appropriate documentation systems, ensure the quality of training data, maintain adequate human oversight, and continuously monitor AI performance after deployment.⁴⁶ Consequently, AI governance becomes an integral component of corporate governance rather than a purely legal or technical function.

While these obligations inevitably generate additional compliance costs, they also contribute to reducing legal uncertainty, strengthening consumer trust, and improving overall reliability of AI systems. The AI Act therefore reflects a broader regulatory philosophy according to which effective compliance should not be regarded exclusively as a legal burden but also a strategic investment capable of supporting sustainable innovation and long – term competitiveness.⁴⁷

The following sections analyze the principal compliance obligations introduced by the AI Act, illustrating both their legal and their practical implications for businesses operating within the European market.

2.4.1 Risk management systems

Risk management constitutes the cornerstone of the compliance framework established by the AI Act. Rather than requiring businesses to delete every possible risk associated with artificial intelligence, the Regulation requires providers of high – risk AI systems to establish a continuous and systematic process capable of identifying, assessing, mitigating, and monitoring risks throughout the entire lifecycle of the system. This obligation reflects the recognition that AI systems are inherently dynamic. Their behavior may evolve over time as a consequence of software updates, changes in operating environments, or interactions with new datasets. Consequently, compliance cannot be limited to a one – time assessment conducted before market placement but must become an ongoing governance activity integrated into the organization's broader risk management processes.

The AI Act therefore requires businesses to identify reasonably foreseeable risks affecting health, safety, and fundamental rights, evaluate their potential impact, implement appropriate mitigation measures, and continuously monitor the effectiveness of those measures after deployment. Risk management⁴⁸ should accompany every stage of the AI system's lifecycle, from design and development to commercialization, deployment, and post – market monitoring.

From an organizational perspective, this requirement encourages firms to adopt governance structures like these already used for cybersecurity, financial risk, or operational risk management. AI risk management therefore becomes a multidisciplinary process involving legal experts,

⁴⁶ AI Act, Chapter IV (Obligations of Providers and Other Operators).

⁴⁷ OECD (2019). OECD AI Principles

⁴⁸ AI Act, Article 9 (Risk Management System).

engineers, compliance officers, data scientists, cybersecurity specialists, and senior management.⁴⁹

Although implementing such systems inevitably requires significant investments in governance, internal controls, and technical expertise, effective risk management may also generate important economic benefits. By identifying potential problems before they materialize, organizations can reduce litigation risks, avoid regulatory sanctions, protect their reputation, and increase stakeholder confidence in AI – enabled products and services. Consequently, the risk management framework established by the AI Act should be understood not merely as a compliance obligation but also as an instrument of strategic corporate governance.

2.4.2 Data governance requirements

Since the performance of artificial intelligence systems depends fundamentally on the quality of the data used throughout their lifecycle, the AI Act introduces specific obligations concerning data governance.⁵⁰ The Regulation recognizes that inaccurate, incomplete, or biased datasets may significantly compromise the reliability, fairness, and safety of AI systems, thereby increasing both legal and economic risks.

For this reason, providers of high – risk AI systems are required to establish appropriate data governance and management practices covering the collection, preparation, validation, storage, and use of training, validation, and testing datasets. Particular attention is devoted to ensuring that data are relevant, representative, sufficiently complete, and, where appropriate, as free as possible from errors and unintended biases. These requirements are closely to one of the principal objectives of the AI Act: reducing the risk of discriminatory or inaccurate algorithmic outcomes. Poor – quality data may produce biased decisions affecting employment, education, healthcare, financial services, and other areas where AI systems have a direct impact on individuals’ rights and opportunities. Consequently, data governance becomes both technical and legal responsibility.

From a business perspective, robust data governance requires organizations to invest in data management infrastructures, quality assurance procedures, internal controls, and interdisciplinary expertise capable of integrating technological, legal, and ethical considerations. Although these investments may increase initial compliance costs, they also contribute to improving model performance, strengthening consumer trust, and reducing exposure to legal liability arising from inaccurate or discriminatory AI outputs.

The emphasis placed on data governance demonstrates that, under the AI Act, compliance begins

⁴⁹ ISO/IEC 23894:2023 – Artificial Intelligence — Guidance on Risk Management.

⁵⁰ AI Act, Article 10 (Data and Data Governance).

long before an AI system is deployed. It starts with the quality of the information on which intelligent systems are trained, highlighting the strategic importance of data as the foundation of trustworthy artificial intelligence.⁵¹

2.4.3 Transparency and information obligation

Transparency represents one of the fundamental principles underpinning the European approach to artificial intelligence governance.⁵² The AI Act therefore introduces a series of obligations designed to ensure that users, regulators, and other relevant stakeholders receive sufficient information to understand the functioning, capabilities, and limitations of AI systems.

The scope of these obligations varies according to the level of risk associated with the AI application. In the case of high – risk AI systems, providers are required to supply detailed instructions for use, technical documentation, information regarding intended purpose, system limitations, performance characteristics, and continuous necessary for safe operation. These requirements are intended to enable deployers to use AI systems appropriately while facilitating effective regulatory supervision.

Transparency obligations also extend to specific AI applications such as chatbots, emotion recognition systems, biometric categorization systems, and AI – generated content. In these situations, users must generally be informed that they are interacting with artificial intelligence or that the content may receive has been generated or manipulated through AI technologies. Such disclosure requirements aim to preserve informed decision – making and reduce the risk of deception. From an economic perspective, transparency contributes to reducing information asymmetries between AI providers, business users, consumers, and regulators. Greater transparency may increase confidence in AI technologies, facilitate market adoption, and strengthen firms’ reputational capital. Although compliance requires additional investments in documentation, communication, and governance processes, transparent AI systems are more likely to gain the trust necessary for widespread commercial adoption.⁵³

Ultimately, transparency should not be understood only as a legal obligation. Within the European regulatory framework, it represents a governance mechanism intended to promote accountability, responsible innovation, and sustainable market development.

2.4.4 Human oversight requirements

One of the defining characteristics of the AI Act is the recognition that artificial intelligence

⁵¹ Floridi, L. (2016). Data Ethics.

⁵² AI Act, Article 13 (Transparency and Provision of Information).

⁵³ AI Act, Article 50 (Transparency Obligations for Certain AI Systems).

should support, rather than replace, meaningful human decision – making in contexts where significant risks may arise. Consequently, providers of high – risk AI systems must ensure that appropriate human oversight mechanisms are incorporated into the design and operation of their systems. The concept of human oversight⁵⁴ does not imply constant human intervention in every automated process. Instead, it requires that qualified individuals remain capable of understanding the functioning of AI systems, monitoring their behavior, interpreting their outputs, and intervening whenever necessary to prevent or minimize potential harm.

This requirement reflects the broader European principle of human – centric artificial intelligence. While AI systems significantly enhance efficiency and productivity, final responsibility for decisions with substantial legal or societal consequences should not rest exclusively with autonomous technologies. Human oversight therefore functions as an essential safeguard against excessive automation and algorithmic overreliance.

For businesses, implementing effective human oversight requires more than assigning formal responsibility to employees. Organizations must ensure that relevant personnel receive appropriate training, understand the capabilities and limitations of AI systems, and possess sufficient authority to override or suspend automated decisions whenever necessary. This obligation has important organizational implications, requiring firms to integrate legal compliance, technical expertise, and corporate governance into a coherent operational framework. Although maintaining human oversight may reduce some of the efficiency gains associated with automation, it also contributes to improving decision quality, reducing legal risks, and strengthening public confidence in AI – enabled decision – making. From this perspective, human oversight represents an investment in trustworthy governance rather than a limitation on technological innovation.

2.4.5 Documentation and record – keeping

Effective compliance depends not only on implementing appropriate governance mechanisms but also on demonstrating that such mechanisms have been correctly applied. For this reason, the AI Act requires providers of high – risk AI systems to maintain comprehensive technical documentation and record – keeping procedures capable of supporting regulatory supervision throughout the AI system’s lifecycle.

Technical documentation serves several important functions. It enables competent authorities to verify compliance with requirements established by the Regulation, facilitates the conformity assessment, and provides deployers with the information necessary to operate AI systems safely

⁵⁴ AI Act, Article 14 (Human Oversight).

and appropriately. Documentation must therefore include information concerning system design, intended purpose, risk management procedures, data governance practices, performance characteristics, and post – market monitoring activities.

In addition to technical documentation, the AI Act requires certain AI systems to generate and retain logs capable of recording relevant events occurring during system operation. These records support traceability, facilitate incident investigations, and strengthen organizational accountability by allowing businesses and regulators to reconstruct the circumstances surrounding particular AI – generated decisions or outcomes.

From a managerial perspective, documentation and record – keeping should not be regarded merely as administrative requirements. Proper documentation enables organizations to demonstrate due diligence, improve internal governance, support auditing activities, and reduce exposure to regulatory sanctions or civil liability. Furthermore, systematic documentation contributes to organizational learning by providing valuable information that can be used to improve future AI development and governance practices.

The documentation obligations introduced by the AI Act therefore illustrate a broader transformation in corporate compliance. As artificial intelligence becomes increasingly integrated into business activities, organizations are expected not only to develop trustworthy AI systems but also to produce verifiable evidence demonstrating that trustworthiness has been achieved and maintained throughout the entire lifecycle of the technology.

2.5 Governance, enforcement and sanctions

The effectiveness of any regulatory framework depends not only on the substantive obligations it establishes but also on the mechanisms through which those obligations are monitored, enforced, and, where necessary, sanctioned. Recognizing this principle, the AI Act introduces a multi – level governance system designed to ensure the consistent application of its provisions across the European Union. Rather than relying exclusively on national authorities or centralized European institutions, the Regulation combines responsibilities at both levels, reflecting the broader governance model traditionally adapted within EU law.⁵⁵

This institutional architecture pursues several objectives simultaneously. It aims to guarantee effective market surveillance, facilitate cooperation among Member States, promote the uniform interpretation of the Regulation, and ensure that AI systems placed on the European market comply with the requirements established by the AI Act. At the same time, the governance framework seeks to provide businesses with greater legal certainty by reducing the risk of

⁵⁵ Regulation (EU) 2024/1689 (AI Act): Chapter VIII – EU Governance of AI

divergent national enforcement practices that could undermine the functioning of the internal market.

The enforcement mechanisms introduced by the AI Act also reflect the increasing complexity of artificial intelligence governance. AI technologies evolve rapidly, often operate across national borders, and involve multiple economic operators participating in global value chains. Consequently, effective supervision requires close cooperation between national regulators, European institutions, standardization bodies, and market participants.

Finally, the Regulation establishes a comprehensive sanctions regime intended to ensure compliance through proportionate, effective, and dissuasive administrative penalties. Together, these governance and enforcement mechanisms reinforce the credibility of the European regulatory framework while encouraging businesses to integrate AI compliance into their broader corporate governance strategies.

2.5.1 National supervisory authorities

The primary responsibility for enforcing the AI Act rests with the competent national authorities designated by each Member State. In line with the principle of shared administration that characterizes much of European Union law, national supervisory authorities are entrusted with monitoring compliance, conducting investigations, supervising market operators, and adopting corrective measures whenever violations of the Regulation are identified.

The AI Act requires Member States to designate both market surveillance authorities and notifying authorities.⁵⁶ Market surveillance authorities oversee AI systems that are placed on the market or put into service, ensuring that providers and deployers comply with the obligations established by the Regulation. Notifying authorities, by contrast, are responsible for assessing and designating conformity assessment bodies, which perform specific evaluation procedures before certain high – risk AI systems can be marketed within the European Union.

The responsibilities of national authorities extend beyond reactive enforcement. They are expected to cooperate with businesses, provide guidance regarding the interpretation of regulatory requirements, exchange information with authorities in other Member States, and contribute to the consistent application of the AI Act across the Union. This cooperative approach reflects the recognition that effective AI governance requires continuous dialogue between regulators and market participants rather than relying solely on punitive enforcement mechanisms.

From a business perspective, national supervisory authorities represent the principal institutional interface through which firms will interact with the AI regulatory framework. Consequently,

⁵⁶ Regulation (EU) 2024/1689 (AI Act): Chapter IX – Post-Market Monitoring, Information Sharing and Market Surveillance

organizations developing or deploying high – risk AI systems will need to establish effective compliance procedures, maintain open communication with competent authorities, and ensure that adequate documentation can be produced whenever requested during supervisory activities.

The decentralized enforcement model adopted by the AI Act offers several advantages, including proximity to national markets and familiarity with domestic legal systems. However, it also raises the challenge of ensuring consistent interpretation across Member States. For this reason, the Regulation complements national supervision with a centralized European coordination mechanism centered on the newly established AI Office.

2.5.2 The European AI Office

While national authorities remain responsible for day – to – day enforcement, the AI Act also establishes a new institutional body intended to strengthen coordination at the European level: the European AI Office.⁵⁷ Created within the European Commission, the AI Office plays a central role in promoting the consistent implementation of the Regulation and supporting the development of a coherent European system of AI governance. The establishment of the AI Office reflects the recognition that artificial intelligence presents challenges extending beyond national borders.

Many AI systems are developed through international supply chains, deployed simultaneously across multiple Member States, and continuously updated through their lifecycle. Under these circumstances, divergent national interpretations could generate legal uncertainty and increase compliance costs for businesses operating within the internal market. The AI Office therefore serves as a coordinating institution capable of promoting regulatory consistency throughout the European Union.

Among its principal responsibilities are supporting cooperation between national supervisory authorities, monitoring the implementation of the AI Act, contributing to the development of the technical guidance, facilitating the exchange of best practices, and coordinating the supervision of general – purpose AI models where provided by the Regulation. The Office also works closely with scientific experts, standardization organizations, and other European institutions to ensure that regulatory implementation remains responsive to technological developments.

For businesses, the creation of the AI Office represents an important source of legal certainty. By promoting harmonized interpretations of the AI Act and encouraging consistent supervisory practices, the Office contributes to reducing regulatory fragmentation and facilitating cross – border commercial activities. This institutional coordination is particularly valuable for firms

⁵⁷ AI Act, Articles 64–67 (European AI Office e governance dei General-Purpose AI Models).

operating across multiple Member States, where inconsistent enforcement could otherwise generate significant compliance burdens.

The AI Office therefore embodies one of the distinctive features of European digital governance: combining decentralized enforcement with centralized coordination in order to preserve both national administrative autonomy and the integrity of the European internal market.

2.5.3 Administrative fines and penalties⁵⁸

To ensure the effective application of its provisions, the AI Act establishes a comprehensive system of administrative fines and corrective measures applicable to organizations that fail to comply with its requirements. Consistent with general principles of European regulatory enforcement, sanctions are intended to be effective, proportionate, and dissuasive, encouraging organizations to integrate compliance into their governance structures rather than treating regulatory obligations as optional recommendations.

The severity of administrative penalties varies according to the nature of the infringement. The most serious violations, including the use of prohibited AI practices, may result in the highest financial penalties established by the Regulation. Lower, but still significant, fines apply to breaches of obligations concerning high – risk AI systems, while the provision of incorrect, incomplete, or misleading information to competent authorities may also trigger administrative sanctions. In determining the appropriate penalty, supervisor authorities are required to consider factors such as the gravity and duration of the infringement, the degree of negligence or intent, previous violations, the level of cooperation demonstrated by the organization, and the measure adopted to mitigate any resulting harm.

Beyond their punitive function, administrative sanctions also pursue broader regulatory objectives. Significant financial penalties encourage firms to invest proactively in compliance systems, internal governance mechanisms, employee training, and risk management procedures. In this respect, enforcement becomes an economic incentive for responsible innovation rather than merely a consequence of regulatory failure.

For businesses, the existence of substantial administrative fines reinforces the importance of adopting comprehensive AI governance frameworks. The potential costs associated with non – compliance extend beyond direct financial sanctions and may include reputational damage, business disruption, litigation risks, and reduced stakeholder confidence. Consequently, effective compliance should be regarded as an essential component of corporate risk management and long – term strategic planning.

⁵⁸ AI Act, Chapter XII – Penalties.

The governance and enforcement architecture established by the AI Act therefore completes the European regulatory model. By combining clear legal obligations with coordinated supervision and credible sanctions, the Regulation seeks to create a regulatory environment in which trustworthy artificial intelligence can develop while maintaining a high level of protection for individuals, businesses, and society. This institutional framework provides the necessary foundation for analyzing, in the following chapter, the broader economic implications of AI regulation for European companies.

2.6 Interaction with other EU digital Regulations

The AI Act does not operate in isolation. Instead, it forms part of a broader legislative framework through which the European Union seeks to regulate the digital economy in a coherent and coordinated manner. Over the past decade, the EU has adopted a series of complementary regulations addressing different dimensions of digital transformation, including data protection, online platforms, digital markets, data sharing, and cybersecurity. Together, these instruments constitute an integrated regulatory ecosystem designed to foster innovation while safeguarding fundamental rights, market fairness, and technological resilience.

Although each regulation pursues distinct objectives, they frequently interact in practice. Organizations developing or deploying AI systems often find themselves subject to multiple regulatory obligations simultaneously. For example, an AI provider processing personal data may need to comply not only with the AI Act but also with the General Data Protection Regulation, while an online platform deploying AI – based recommendation systems may additionally fall within the scope of the Digital Services Act or the Digital Markets Act. Similarly, organizations developing connected AI products may also be required to comply with the Data Act and the Cyber Resilience Act.

From a business perspective, understanding the interaction among these legal instruments is essential. Rather than viewing compliance as a collection of separate obligations, firms increasingly need to adopt integrated governance frameworks capable of addressing multiple regulatory requirements simultaneously. Such an approach reduces legal uncertainty, improves operational efficiency, and supports a more effective implementation of corporate digital governance strategies.

The following sections examine the principal European digital regulations that interact with the AI Act, highlighting both their complementary functions and their implications for organizations operation within the European digital economy.

2.6.1 General Data Protection Regulation (GDPR)

Among the various legal instruments composing the European digital regulatory framework, the General Data Protection Regulation (GDPR)⁵⁹ maintains the closest relationship with the AI Act. Since many artificial intelligence systems rely extensively on the collection and processing of personal data, compliance with AI – specific obligations frequently depend upon compliance with European data protection law.

Despite their close interaction, the two Regulations pursue different objectives. The GDPR governs the processing of personal data, establishing rights for data subjects and obligations for data controllers and processors. The AI Act, by contrast, regulates AI systems according to the level of risk they pose, irrespective of whether personal data is processed. Consequently, the two frameworks should be regarded as complementary rather than overlapping.

Several AI Act requirements reinforce principles that are already embedded within the GDPR. Data quality, fairness, transparency, accountability, human oversight, and risk management all reflect concepts that have long characterized European data protection law. However, the AI Act extends these principles beyond privacy by addressing broader concerns relating to safety, discrimination, and the societal impact of automated decision – making.⁶⁰

For businesses, compliance with the AI Act and the GDPR increasingly requires an integrated governance strategy. Organizations developing AI systems must ensure not only that personal data are processed lawfully but also that AI models satisfy the technical and organizational requirements established by the AI Act. This often requires close collaboration between legal, compliance, cybersecurity, and data science teams.

Rather than creating regulatory duplication, the interaction between the AI Act and the GDPR contributes to a more comprehensive governance model in which the protection of personal data constitutes one component of the broader objective of developing trustworthy artificial intelligence.

2.6.2 Digital Services Act (DSA)

The Digital Services Act⁶¹ complements the AI Act by regulating the responsibilities of providers of intermediary services and online platforms. While the AI Act focuses on the characteristics and risks associated with AI systems, the DSA seeks to create a safer online environment by establishing obligations relating to illegal content, systemic risks, transparency, and platform accountability.

The interaction between the two Regulations becomes particularly relevant for very large online

⁵⁹ Regulation (EU) 2016/679 (GDPR).

⁶⁰ European Data Protection Board (EDPB), Guidelines on Automated Decision-Making and Profiling.

⁶¹ Regulation (EU) 2022/2065 (Digital Services Act).

platforms and search engines that rely extensively on AI – driven algorithms for content moderation, recommendation systems, targeted advertising, and risk assessment. In these contexts, organizations may simultaneously be required to comply with AI Act obligations concerning AI systems and DSA requirements relating to platform governance and transparency. Both Regulations emphasize transparency and accountability, although from different perspectives. The AI Act focuses on the technical characteristics and governance of AI systems, whereas the Digital Services Act addresses the broader societal consequences of algorithmic decision – making within digital platforms. Together, they promote greater user awareness, more responsible platform governance, and improved oversight of automated decision – making processes.

From a business perspective, organizations operating online platforms must increasingly integrate AI governance into their existing compliance structures under the DSA. Instead of treating these obligations separately, firms are encouraged to develop coordinated governance frameworks capable of simultaneously addressing technological risks, platform responsibilities, and regulatory reporting obligations.

2.6.3 Digital Markets Act (DMA)

The Digital Markets Act⁶² addresses a different dimension of the European digital economy by promoting fair competition within digital markets. Unlike the AI Act, which focuses primarily on the risks generated by the artificial intelligence, the DMA seeks to prevent anti – competitive practices adopted by large digital platforms designated as gatekeepers.

Although the two Regulations pursue distinct objectives, they increasingly intersect in practice. Gatekeeper platforms frequently develop and deploy sophisticated AI systems supporting search engines, recommendation algorithms, digital advertising, cloud services, and virtual assistants. Consequently, these organizations may simultaneously be subject to obligations under both the AI Act and the Digital Markets Act.

The interaction between the two Regulations reflects the European Union’s broader strategy of combining innovation governance with competition policy.⁶³ While the AI Act seeks to ensure that AI technologies remain safe and trustworthy, the Digital Markets Act aims to preserve contestable and competitive digital markets by preventing dominant firms abusing their market power.

For businesses, particularly large technology companies, compliance therefore extends beyond technical AI governance and encompasses broader obligations relating to interoperability, data

⁶² Regulation (EU) 2022/1925 (Digital Markets Act).

⁶³ Crémer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019). Competition Policy for the Digital Era.

access, business user rights, and competitive neutrality. This integrated regulatory framework contributes to shaping a digital market in which innovation, competition, and consumer protection reinforce one another.

2.6.4 Data Act

The Data Act⁶⁴ represents another important component of the European digital strategy by establishing rules governing access to and sharing of non – personal and industrial data. As artificial intelligence increasingly depends upon large volumes of high – quality data, the Data Act directly influences the availability of datasets used to develop, train, validate, and improve AI systems.

Unlike the GDPR, which focuses on the protection of personal data, the Data Act seeks to facilitate data accessibility while ensuring fair conditions for data sharing among businesses, consumers, and public authorities. This objective supports innovation by reducing barriers to data availability and encouraging the creation of data – driven business models.

The interaction with the AI Act is particularly significant in relation to data governance. Organizations developing high – risk AI systems require reliable, representative, and high – quality datasets to comply with the AI Act’s requirements. The Data Act contributes to this objective by facilitating lawful access to data while promoting greater interoperability and reducing information asymmetries within the European data economy.

From an economic perspective, the combined application of the AI Act and Data Act illustrates the European Union’s attempt to balance two complementary objectives: ensuring responsible AI development while simultaneously strengthening the availability of data necessary to foster innovation and competitiveness within the European digital market.

2.6.5 Cyber Resilience Act

Artificial intelligence systems increasingly operate within connected digital environments where cybersecurity has become a fundamental prerequisite for trustworthy technological development. Recognizing this challenge, the Cyber Resilience Act (CRA)⁶⁵ introduces horizontal cybersecurity requirements applicable to products containing digital elements throughout their lifecycle.

The interaction between the CRA and the AI Act is particularly evident for AI – enabled products connected to digital networks. While the AI Act primarily regulates risks associated with algorithmic decision – making and fundamental rights, the CRA addresses vulnerabilities that may compromise the confidentiality, integrity, and availability of digital products. The two Regulations therefore regulate different dimensions of technological risk while pursuing

⁶⁴ Regulation (EU) 2023/2854 (Data Act).

⁶⁵ Regulation (EU) 2024/2847 (Cyber Resilience Act).

complementary objectives.

For businesses, this interaction requires the integration of AI governance and cybersecurity governance within a unified compliance framework. Organizations developing AI products must not only ensure that algorithms satisfy the AI Act's requirements concerning transparency, robustness, and human oversight but also implement cybersecurity measures capable of protecting those systems against malicious attacks and unauthorized manipulation throughout their operational lifecycle.

The coexistence of the AI Act and the Cyber Resilience Act demonstrate the European Union's holistic approach to digital regulation. Trustworthy artificial intelligence depends not only on ethical and legal compliance but also on the resilience and security of the technological infrastructures supporting AI systems. Consequently, cybersecurity becomes an essential component of responsible AI governance and a key factor in strengthening public trust, market confidence, and the long – term competitiveness of European businesses.

CHAPTER 3: The economic impact of AI Regulation on European companies

3.1 Regulation and innovation: theoretical perspectives

The relationship between regulation and innovation has long been one of the most debated issues in economics, law, and public policy. While technological innovation is widely recognized as a key driver of productivity, competitiveness, and long – term economic growth, the role of regulation in shaping innovation remains controversial. Some scholars argue that regulation inevitably constrains technological development by increasing compliance costs, limiting entrepreneurial freedom, and discouraging investment. Others maintain that well – designed regulatory frameworks can stimulate innovation by reducing uncertainty, creating market confidence, and encouraging the development of higher – quality technologies.

This debate has become particularly relevant in the context of artificial intelligence. AI is widely regarded as a general – purpose technology capable of transforming virtually every sector of economy. However, its rapid diffusion has also generated concerns regarding privacy, discrimination, accountability, transparency, and cybersecurity. Governments therefore face the difficult challenge of balancing two potentially conflicting objectives: preserving incentives for technological innovation while ensuring that AI systems operate within an appropriate legal and ethical framework.

The European AI Act embodies this tension. By introducing comprehensive compliance obligations for certain AI systems, the Regulation inevitably affects the costs, incentives, and strategic decisions of firms operating with the European market. Whether these effects ultimately hinder or stimulate innovation remains a matter of considerable academic debate. Competing theoretical perspectives offer different explanations regarding the economic consequences of regulation, reflecting broader assumptions about market behavior, technological change, and institutional design.

Understanding this theoretical approach is essential before analyzing the empirical effects of AI regulation on European companies. The following sections examine the principal schools of thought concerning the relationship between regulation and innovation, highlighting both their strengths and their limitations while providing the conceptual framework for the subsequent analysis of compliance costs, competitiveness, and business performance.

3.1.1 The innovation – inhibiting view

One of the most influential perspectives within economic literature argues that regulation tends to reduce innovation by increasing the costs associated with research, development, and market

entry.⁶⁶ According to this view, regulatory intervention imposes administrative burdens, compliance obligations, and legal uncertainty that may discourage firms from investing in innovative technologies, particularly in sectors characterized by rapid technological change such as artificial intelligence.⁶⁷

From a neoclassical economic perspective, regulation may distort market incentives by increasing production costs and reducing the expected return on investment. Firms allocating significant financial and managerial resources to regulatory compliance inevitably have fewer resources available for research and development activities. This effect may be particularly pronounced for start – ups and small and medium – sized enterprises (SMEs), which often operate under more several financial constraints than large multinational corporations.

Several scholars have argued that extensive regulation may also slow technological progress by extending product development cycles and increasing barriers to market entry. AI developers subject to complex documentation requirements, conformity assessment, and continuous monitoring obligations may postpone or even abandon innovative projects due to the uncertainty associated with future regulatory compliance. Critics therefore warn that overly restrictive regulation could reduce Europe’s attractiveness as a destination for AI investment, encouraging firms to relocate research activities to jurisdictions characterized by more flexible regulatory environments.

This argument is frequently supported by theories emphasizing regulatory burden and innovation costs. Excessive legal complexity may discourage entrepreneurial experimentation, reduce venture capital investment, and limit the commercialization of emerging technologies. In highly dynamic industries such as artificial intelligence, where innovation cycles are measured in months rather than years, lengthy compliance procedures may significantly reduce firms’ ability to respond rapidly to technological developments and changing market conditions.⁶⁸

Nevertheless, the innovation – inhibiting perspective should not be interpreted as advocating the complete absence of regulation. Rather, most scholars adopting this approach argue that regulatory intervention should remain limited, proportionate, and technologically neutral, allowing market competition to remain the principal driver of innovation. According to this view, the greatest economic risk lies not in regulation itself but in regulatory frameworks that evolve more slowly than technological progress, thereby generating unnecessary obstacles to entrepreneurship and investment.

⁶⁶ Djankov, S. et al. (2002). *The Regulation of Entry*

⁶⁷ Stigler, G. J. (1971). *The Theory of Economic Regulation*.

⁶⁸ Aghion, P., & Howitt, P. (1998). *Endogenous Growth Theory*.

3.1.2 The innovation – enabling view

An alternative body of literature challenges the assumption that regulation necessarily inhibits innovation. According to this perspective, well – designed regulatory frameworks may actively stimulate technological development by reducing uncertainty, strengthening consumer confidence, and creating incentives for firms to invest in safer, more reliable, and higher – quality innovations.

One of the most influential contributions supporting this view is the Porter Hypothesis⁶⁹, which argues that appropriately designed regulation can encourage firms to improve efficiency, develop new technologies, and enhance long – term competitiveness. Rather than representing a purely economic cost, compliance may stimulate organizational learning, technological upgrading, and process innovation, ultimately generating benefits that partially or fully offset initial regulatory expenditures.

Within the context of artificial intelligence, this argument suggests that AI Act may encourage European firms to invest in explainable AI, robust data governance, cybersecurity, algorithmic transparency, and responsible innovation. Although these investments increase short – term compliance costs, they may also improve product quality, strengthen consumer trust, reduce legal liability, and facilitate access to international markets where trustworthy AI is increasingly valued. Supporters of this perspective further argue that regulatory certainty constitutes an important driver of investment. In the absence of clear legal rules, firms may hesitate to develop or commercialize AI applications because of uncertainty regarding future legal obligations, reputational risks, or potential litigation. By established harmonized requirements applicable across the European Union, the AI Act may therefore reduce transaction costs and create a more predictable environment for long – term investment decisions.⁷⁰

From a broader economic perspective, innovation is increasingly understood as depending not only on technological capability but also on institutional quality. Markets characterized by clear rules, effective governance, and high levels of public trust may provide stronger incentives for sustainable innovation than environments where rapid technological development occurs in the absence of adequate safeguards. Consequently, proponents of the innovation – enabling view regard regulation as in institutional infrastructure capable of supporting both economic growth and responsible technological progress.⁷¹

⁶⁹ Porter, M. E., & van der Linde, C. (1995). Toward a New Conception of the Environment–Competitiveness Relationship.

⁷⁰ Blind, K. (2016). The Impact of Regulation on Innovation.

⁷¹ Ashford, N. A., & Hall, R. P. (2011). Technology, Globalization and Sustainable Development.

3.1.3 The concept of smart regulation⁷²

The apparent opposition between regulation and innovation has gradually given way to more nuanced approaches that seek to reconcile technological development with effective governance. Among these approaches, the concept of smart regulation has emerged as one of the most influential frameworks within contemporary regulatory theory. Rather than asking whether regulation exists, smart regulation focuses on how regulatory systems can be designed to achieve public policy objectives while minimizing unnecessary burdens on innovation.

Smart regulation is founded on several key principles, including proportionality, flexibility, technological neutrality, stakeholder participation, and evidence – based policymaking. Regulatory intervention should be calibrated according to the level of risk generated by different technologies, allowing low – risk innovations to develop with minimal constraints while imposing stricter safeguards only where significant societal risks exist. This philosophy closely resembles the risk – based approach adopted by the AI Act, demonstrating the influence of modern regulatory theory of European digital legislation.

From an economic perspective, smart regulation recognizes that both under – regulation and over – regulation may generate market failures. Insufficient regulation may undermine consumer confidence, create legal uncertainty, and increase the likelihood of harmful outcomes that ultimately reduce market adoption of innovative technologies. Conversely, excessive restrictive regulation may discourage entrepreneurship, limit competition, and slow technological progress. The objective is therefore to identify an optimal regulatory equilibrium capable of simultaneously supporting innovation, protecting fundamental rights, and preserving market efficiency.⁷³

The AI Act may be interpreted as an attempt to operationalize this philosophy within the field of artificial intelligence governance. By differentiating obligations according to the level of risk associated with AI systems, the Regulation seeks to avoid imposing identical compliance requirements on all technologies. Instead, it allocates regulatory burdens proportionately, allowing the majority of low – risk AI applications to remain largely unaffected while concentrating stricter obligations on applications capable of producing significant impacts on individuals and society. Whether the AI Act ultimately succeeds in achieving this balance remains an open empirical question. Some scholars argue that the Regulation represents one of the most sophisticated examples of smart regulation currently adopted worldwide, whereas others contend that its complexity may still generate substantial compliance costs, particularly for smaller firms. This ongoing debate provides the theoretical foundation for the following sections of this chapter, which examine the concrete economic effects of AI regulation on European companies.

⁷² Gunningham, N., Grabosky, P., & Sinclair, D. (1998). *Smart Regulation: Designing Environmental Policy*.

⁷³ Baldwin, R., Cave, M., & Lodge, M. (2022). *Understanding Regulation*.

3.2 Compliance costs under the AI Act

The introduction of the AI Act has generated considerable debate regarding the economic implications of regulatory compliance for European companies. While the Regulation aims to foster trustworthy artificial intelligence and strengthen legal certainty within the internal market, it also requires organizations to allocate significant financial, technological, and organizational resources to satisfy its requirements. Consequently, compliance has emerged as one of the principal factors shaping firms' strategic decisions concerning the development, deployment, and commercialization of AI systems.

Compliance costs encompass a wide range of direct and indirect expenditures associated with implementing the obligations established by the AI Act. These include investments in governance structures, legal expertise, documentation, employee training, technical infrastructure, conformity assessments, cybersecurity measures, and post – market monitoring. Although such costs are particularly significant for providers of high – risk AI systems, they may also affect organizations operating across broader AI value chains, including deployers, importers, distributors, and authorized representatives.

From an economic perspective, compliance costs should not be interpreted solely as additional regulatory burdens. They may also generate long – term benefits by improving organizational governance, reducing legal uncertainty, enhancing product quality, and strengthening consumer confidence. The overall economic impact therefore depends on whether the long – term advantages generated by compliance outweigh the short – term investments required to satisfy regulatory obligations.

The following sections examine the principal categories of compliance costs introduced by the AI Act, highlighting both their economic implications and their potential influence on firms' competitiveness, innovation capacity, and strategic decision – making.

3.2.1 Direct compliance costs

The most immediate economic consequence of the AI Act concerns the direct compliance costs incurred by organizations developing or deploying AI systems. These costs arise from the need to implement the technical and organizational measures required by the Regulation before AI systems can be lawfully placed on the European market or put into service.

For providers of high – risk AI systems, direct compliance costs include the establishment of risk management systems, data governance procedures, technical documentation, conformity assessments, human oversight mechanisms, cybersecurity safeguards, and post – market monitoring activities. In many cases, organizations must also invest in internal compliance

functions, employee training programs, and specialized software capable of supporting regulatory reporting and documentation requirements.⁷⁴

The magnitude of these costs varies considerably according to firm size, industry, and the complexity of the AI applications involved. Large multinational corporations generally possess greater financial resources and more mature compliance infrastructures, enabling them to absorb regulatory costs more efficiently. Conversely, small and medium enterprises (SMEs) and start – ups often face proportionally higher compliance burdens due to limited financial resources and the absence of dedicated legal or compliance departments.

From a strategic perspective, direct compliance expenditures should be viewed not merely as operational costs but as investments in organizational capability. Firms that successfully integrate AI governance into their business processes may benefit from improved risk management, greater investor confidence, stronger customer trust, and easier access to regulated markets. Consequently, although compliance increases short – term expenditures, it may simultaneously strengthen firms’ long – term competitive position.

The economic significance of direct compliance costs therefore depends largely on the balance between immediate financial investments and the broader organizational benefits generated by improved governance and regulatory certainty.⁷⁵

3.2.2 Administrative burdens

Beyond direct financial expenditures, the AI Act also generates substantial administrative burdens associated with regulatory compliance. These burdens arise from the continuous management of internal procedures, documentation, reporting obligations, conformity assessments, and interactions with supervisory authorities throughout the lifecycle of AI systems.

Unlike one – time implementation costs, administrative obligations persist over time. Organizations must continuously monitor AI performance, maintain technical documentation, update risk assessments, retain operational records, report serious incidents where required, and demonstrate ongoing compliance during regulatory inspections. As AI systems evolve through software updates or changes in operating conditions, compliance processes must also be periodically reviewed and adapted.

These administrative activities require dedicated organizational resources, including data compliance officers, legal departments, quality assurance teams, data governance specialists, and technical personnel. In many organizations, AI governance therefore becomes an interdisciplinary function integrated into broader corporate governance structures. This transformation may require

⁷⁴ AI Act, Articles 8–29 (Requirements for High-Risk AI Systems).

⁷⁵ Deloitte (2024). State of Generative AI in Enterprise (for investments in governance and compliance).

substantial organizational restructuring, particularly for firms with limited previous experience in regulatory compliance.

Administrative burdens may also influence managerial decision – making. Firms developing multiple AI applications must allocate resources not only to innovation but also to documentation, internal controls, auditing, and regulatory reporting. Consequently, managers face the challenge of balancing investments in technological development with investments in governance infrastructure.

Nevertheless, administrative obligations may also generate positive organizational effects. Standardized governance procedures improve internal accountability, facilitate knowledge management, strengthen operational transparency, and reduce the likelihood of regulatory violations. Over time, organizations capable of integrating compliance into routine business operations may transform administrative requirements into strategic governance capabilities that enhance overall organizational resilience.⁷⁶

3.2.3 Legal and consultancy costs

Compliance with the AI Act requires organizations to interpret a highly technical regulatory framework that combines legal, technological, and organizational requirements. Therefore, many firms are expected to rely extensively on external legal advisors, compliance consultants, technical auditors, and specialized certification bodies, particularly during the initial implementation phase.⁷⁷

Legal costs arise from several activities, including regulatory interpretation, contractual revision, liability assessment, intellectual property protection, conformity assessment procedures, interactions with supervisory authorities, and the design of internal compliance programs. Organizations developing high – risk AI systems may additionally require multidisciplinary teams capable of integrating expertise in technology law, data protection, cybersecurity, product safety, and corporate governance.⁷⁸

Consultancy costs are likely to be particularly significant for SMEs and start – ups, which frequently lack internal compliance departments or specialized legal expertise. While large corporations may distribute these functions across existing organizational structures, smaller firms often need to outsource substantial portions of the compliance process, increasing both financial expenditures and dependence on external expertise.

However, legal and consultancy services should not be viewed exclusively as regulatory expenses.

⁷⁶ AI Act, Articles 9–15, 17, 19, 20, 72 (risk management, documentation, post-market monitoring e reporting).

⁷⁷ PwC (2024). Responsible AI Survey.

⁷⁸ IBM (2023). Global AI Adoption Index.

Professional advice may help organizations identify compliance risks at an early stage, improve governance structures, reduce future litigation, and avoid costly enforcement actions. Furthermore, external experts often facilitate the implementation of best practices capable of improving organizational efficiency beyond the specific requirements imposed by the AI Act. From an economic perspective, legal and consultancy costs therefore illustrate the broader transformation of AI governance into a specialized professional ecosystem involving lawyers, engineers, auditors, cybersecurity specialists, and regulatory consultants. The emergence of this ecosystem represents not only a source of compliance costs but also a new market for highly specialized professional services.

3.2.4 Technological adaption costs

In addition to legal and organizational expenditures, the AI Act requires many organizations to invest directly in the technological adaption of their AI systems. Existing algorithms, data infrastructures, software architectures, and governance tools may need to be redesigned or upgraded to satisfy the Regulation's requirements concerning transparency, robustness, traceability, cybersecurity, and human oversight.⁷⁹

These technological adaptations frequently involve substantial engineering efforts. Organizations may need to improve data quality, redesign machine learning models to enhance explainability, implement logging mechanisms, strengthen cybersecurity protections, integrate human intervention functionalities, and develop automated monitoring systems capable of supporting continuous compliance throughout the AI system's lifecycle.

The scale of investments varies significantly according to the maturity of existing AI governance infrastructures. Firms that have already adopted responsible AI principles or implemented internal governance frameworks may require relatively limited modifications. Conversely, organizations with highly automated systems developed under less stringent regulatory environment may face considerably higher adaption costs.

Although these technological investments increase development expenditure in the short term, they may simultaneously improve the quality, reliability, and security of AI systems. More robust technologies are less likely to generate operational failures, discriminatory outcomes, cybersecurity incidents, or reputational crises, thereby reducing long – term business risks and enhancing market acceptance.

Ultimately, technological adaptation costs should be understood as investments in future competitiveness rather than merely as regulatory expenses. As global markets increasingly

⁷⁹ AI Act, Articles 10–15 (data governance, technical documentation, transparency, human oversight, accuracy, robustness and cybersecurity).

demand trustworthy and secure AI solutions, firms capable of incorporating regulatory requirements directly into technological design may acquire strategic advantages extending well beyond compliance with European legislation.

3.3 The impact on small and medium – sized enterprises

Small and medium – sized enterprises (SMEs) occupy a central position within the European economy, according for many businesses and making substantial contributions to employment, innovation, and economic growth. At the same time, SMEs are increasingly adopting artificial intelligence to improve operational efficiency, optimize decision – making, and develop innovative products and services. Consequently, the AI Act is expected to have significant implications for this category of firms.

Although the Regulation applies the same legal framework across the internal market, its economic impact is unlikely to be uniform. Large corporations generally possess greater financial resources, established compliance departments, and extensive legal expertise, enabling them to integrate regulatory obligations more efficiently into existing governance structures. By contrast, SMEs often operate with limited financial capacity, smaller workforces, and less specialized knowledge, making compliance proportionally more demanding.

For this reason, the economic debate surrounding the AI Act has increasingly focused on the capacity of SMEs to absorb compliance costs without compromising their ability to innovate and compete. While some scholars argue that regulatory obligations may disproportionately burden smaller firms, others emphasize that harmonized rules, greater legal certainty, and targeted support measures may ultimately strengthen SMEs by creating a more predictable and trustworthy market environment.

Understanding how the AI Act affects SMEs is therefore essential for evaluating its broader economic consequences. The following sections examine the structural characteristics that distinguish SMEs from larger firms, the principal compliance challenges they face, and the support mechanisms introduced to facilitate their participation in the European AI ecosystem.

3.3.1 Structural constraints of SMEs

The economic impact of AI regulation on small and medium enterprises cannot be fully understood without considering the structural characteristics that distinguish them from larger organizations. SMEs typically operate with more limited financial resources, smaller management teams, and less specialized technical expertise. While these characteristics often provide greater flexibility and faster decision – making, they may also reduce firms’ capacity to absorb complex

regulatory obligations.⁸⁰

One of the principal structural constraints concerns financial capacity. Compliance with the AI Act frequently requires investments in governance systems, legal expertise, documentation procedures, cybersecurity, employee training, and technological adaption. For many SMEs, these expenditures represent a significantly larger proportion of available resources than they do for multinational corporations, which benefit from economies of scale and dedicated compliance departments.

A second limitation relates to human capital. Unlike large enterprises, SMEs rarely possess multidisciplinary teams combining legal, technical, cybersecurity, and compliance expertise. As a result, regulatory implementation often depends on a small number of employees who must simultaneously manage business operations, technological development, and compliance activities. This concentration of responsibilities may increase organizational complexity and reduce the time available for innovation.⁸¹

Access to finance also represents a significant structural challenge. Investors and financial institutions may perceive regulatory uncertainty as an additional source of risk, particularly for early – stage AI companies. Consequently, firms facing substantial compliance obligations may encounter greater difficulties in securing the financial resources necessary to support both innovation and regulatory implementation.

These structural characteristics explain why the economic effects of the AI Act are expected to differ substantially according to the firm's size. The Regulation itself does not distinguish between large corporations and SMEs in terms of core legal obligations. However, the relative burden generated by those obligations may vary considerably, depending on the organizational resources available to each firm.

3.3.2 Compliance challenges

The structural limitations affecting SMEs translate directly into a series of practical compliance challenges. While the substantive obligations established by the AI Act are generally identical regardless of firm size, the organizational effort required to satisfy those obligations may be considerably greater for smaller businesses.

One of the most significant challenges concerns the implementation of integrated AI governance systems. Compliance requires organizations to establish risk management procedures, maintain technical documentation, ensure data governance, provide human oversight, monitor AI performance, and interact with supervisory authorities. For SMEs operating with limited

⁸⁰ European Commission. Annual Report on European SMEs.

⁸¹ Deloitte (2024). State of Generative AI in the Enterprise (regarding the gap between large enterprises and SMEs).

personnel and financial resources, simultaneously fulfilling these requirements may divert attention and investment away from research, product development, and market expansion.

The complexity of the regulatory framework itself also represents an important challenge. The AI Act combines legal, technical, and organizational requirements that frequently require highly specialized expertise.⁸² Many SMEs therefore depend on external consultants, legal advisors, or technical auditors to interpret and implement regulatory obligations, increasing overall compliance expenditures and creating additional operational dependencies.

Timing represents another critical issue. Start – ups and innovative SMEs often compete through rapid product development and early market entry. Lengthy conformity assessments, documentation procedures, and ongoing monitoring requirements may delay commercialization, reducing firms’ ability to respond quickly to technological developments and changing customer demands. In highly competitive AI markets, even relatively short delays may influence commercial success.

Despite these challenges, it would be inaccurate to conclude that AI Act necessarily disadvantages SMEs. The Regulation also provides a common legal framework that reduces regulatory fragmentation across Member States, allowing smaller firms to operate within a single European market rather than navigating multiple national regulatory systems. Consequently, while compliance generates significant short – term costs, harmonization may reduce long – term barriers to cross – border expansion and strengthen legal certainty for innovative SMEs.⁸³

3.3.3 Opportunities and support measures

Recognizing the challenges faced by SMEs, the European Union has incorporated several mechanisms within the AI Act and the broader European digital strategy to facilitate regulatory compliance while preserving innovation incentives. These measures reflect the legislator’s awareness that excessively burdensome regulation could undermine one of the principal sources of innovation within the European economy.

Among the most significant support instruments are AI regulatory sandboxes. These controlled testing environments allow companies, particularly SMEs and start – ups, to develop, test, and validate innovative AI systems under the supervision of competent authorities before full market deployment. Regulatory sandboxes aim to reduce legal uncertainty, encourage experimentation, and facilitate dialogue between businesses and regulators, enabling firms to identify compliance issues at an early stage while limiting the risks associated with innovation.

The European Commission has also promoted a broader ecosystem of support through funding

⁸² AI Act, Chapter III (Requirements for High-Risk AI Systems).

⁸³ AI Act, Chapter IV (Obligations of Providers and Other Operators).

programs, digital innovation hubs, guidance documents, and technical assistance initiatives designed to strengthen SMEs' AI capabilities. These measures seek not only to facilitate compliance but also to enhance firms' access to expertise⁸⁴, financing, and technological infrastructure necessary for responsible AI development.

From an economic perspective, these initiatives illustrate an important characteristic of the European regulatory approach. Rather than relying exclusively on prescriptive legal obligations, the AI Act operates within a wider innovation policy framework intended to combine regulation with institutional support. The objective is to ensure that compliance does not become an insurmountable barrier for smaller firms but instead contributes to the development of trustworthy AI capable of competing successfully within both European and global markets.

Whether these support measures will fully offset the compliance costs faced by SMEs remains uncertain and contributes to be debated within academic literature. Nevertheless, they demonstrate that the European Union has attempted to complement regulatory intervention with policies specifically designed to preserve entrepreneurial dynamism and technological innovation. This balance between regulatory oversight and business support represents one of the defining features of the European approach to AI governance.

3.4 The impact on large companies

Large companies occupy a distinctive position with the European AI ecosystem. Unlike small and medium – sized enterprises, they generally possess greater financial resources, specialized expertise, and established governance structures capable of supporting regulatory compliance. At the same time, however, the scale and complexity of their operations mean that the implementation of the AI Act often requires substantial organizational transformation rather than merely the adoption of isolated compliance measures.

Many large corporations develop or deploy AI systems across multiple business units, jurisdictions, and operational contexts. Consequently, compliance with the AI Act cannot be confined to individual projects but must be embedded within enterprise – wide governance frameworks.⁸⁵ This requires coordination among legal departments, compliance teams, data scientists, software engineers, cybersecurity specialists, internal auditors, and senior management. As AI becomes increasingly integrated into core business processes, regulatory compliance evolves into a strategic component of corporate governance rather than a purely legal obligation. From an economic perspective, large firms often benefit from economies of scale that enable them

⁸⁴ European Commission. Digital Europe Programme. European Innovation Council (EIC) Programme. European Digital Innovation Hubs (EDIHs).

⁸⁵ Regulation (EU) 2024/1689 (AI Act).

to distribute compliance costs across broader business activities. Nevertheless, these organizations also face significant implementation challenges arising from the complexity of multinational operations, the need to harmonize internal procedures, and the continuous evolution of AI technologies. As a result, the AI Act may generate profound organizational changes that influence strategic planning, investment decisions, and long – term corporate governance.

The following sections examine how large companies are adapting their governance structures, strengthening internal compliance systems, and developing strategic responses aimed not only at satisfying regulatory requirements but also at leveraging compliance as a source of competitive advantage.

3.4.1 Corporate governance adjustments

The introduction of the AI Act has accelerated the integration of artificial intelligence governance into broader corporate governance frameworks. Rather than treating AI compliance as an isolated legal issue, many large organizations are incorporating it into enterprise – wide risk management systems, board oversight mechanisms, and strategic decision – making processes.

This transformation reflects the growing recognition that AI – related risks extend beyond technical performance. Issues such as algorithmic bias, cybersecurity, reputational damage, regulatory liability, and ethical concerns may significantly affect corporate value, stakeholder confidence, and long – term business sustainability. Consequently, boards of directors and executive management are increasingly expected to supervise AI governance in the same way they oversee financial reporting, cybersecurity, or environmental, social, and governance (ESG) risks.

Corporate governance adjustments frequently include the establishment of dedicated AI ethics committees, cross – functional governance boards, internal AI policies, and enterprise – wide governance frameworks that define responsibilities for AI development, deployment, monitoring, and risk management. These structures promote greater coordination among business units and ensure that regulatory obligations are integrated into strategic planning rather than addressed only after technological development has been completed.⁸⁶

From an economic perspective, these governance reforms require substantial organizational investment. However, they may also improve decision – making quality, reduce regulatory risk, strengthen stakeholder trust, and enhance corporate resilience. In this sense, AI governance increasingly becomes a strategic asset capable of supporting long – term value creation rather than merely a compliance requirement imposed by regulation.

⁸⁶ AI Act, Chapter VIII (Governance).

3.4.2 Internal compliance structures

The implementation of AI Act has encouraged many large companies to strengthen or redesign their internal compliance structures to manage the growing complexity of AI governance. Unlike traditional regulatory compliance, AI regulation requires continuous interaction between legal, technical, operational, and managerial functions throughout the lifecycle of AI systems.

Many organizations are responding by creating multidisciplinary compliance teams composed of lawyers, compliance officers, data protection specialists, software engineers, cybersecurity professionals, data scientists, and internal auditors. These teams collaborate to oversee risk assessments, maintain technical documentation, monitor AI performance, coordinate conformity assessment procedures, and ensure that regulatory obligations remain satisfied as AI systems evolve over time.

Internal compliance structures are also increasingly supported by technological solutions. Companies are investing in governance platforms capable of documenting AI models, monitoring algorithmic performance, managing risk registers, automating compliance reporting, and facilitating internal audits. These digital governance tools reduce administrative complexity while improving traceability, accountability, and operational efficiency.

Although establishing such structures involves considerable financial investment, the long – term organizational benefits may extend beyond regulatory compliance.⁸⁷ Strong internal governance systems improve communication between departments, facilitate knowledge sharing, reduce operational risks, and enable organizations to respond more effectively to future regulatory developments. Consequently, compliance functions are progressively evolving from cost centers into strategic organizational capabilities that support responsible innovation.

3.4.3 Strategic responses to regulation

Beyond organizational adaption, many large companies are increasingly treating the AI Act as a strategic factor influencing competitive positioning, innovation strategies, and long – term investment decisions. Rather than limiting their response to minimum legal compliance, leading organizations are integrating regulatory requirements directly into product design, research and development processes, and corporate innovation strategies.

One increasingly common approach is the adoption of “compliance by design” or “responsible AI by design” principles. Under this strategy, legal, ethical, and technical requirements are incorporated into the earliest stages of AI development, reducing the need for costly modifications

⁸⁷ AI Act, Articles 9–15, 17, 72 (risk management, documentation, monitoring and governance).

after deployment. This proactive approach not only facilitates compliance with the AI Act but also improves product quality, strengthens consumer trust, and reduces exposure to future legal or reputational risks.

Large multinational corporations are also investing in AI governance frameworks that extend beyond European regulatory requirements. Many organizations align their internal policies with globally recognized standards such as the OECD AI Principles, the NIST AI Risk Management⁸⁸ Framework, and ISO/IEC standards on AI management and governance⁸⁹. This enables firms to operate across multiple jurisdictions while maintaining consistent governance practices and reducing fragmentation within global operations.

From a strategic perspective, compliance is therefore increasingly viewed as a source of competitive differentiation. Organizations capable of demonstrating transparency, accountability, cybersecurity, and responsible AI governance may strengthen relationships with investors, customers, regulators, and business partners, particularly in markets where trust has become a decisive competitive factor.

Ultimately, the experience of large companies illustrates that the economic impact of the AI Act extends far beyond the direct costs of regulatory compliance. The Regulation encourages firms to rethink governance structures, organizational capabilities, and innovation strategies, reinforcing the broader transition towards responsible and trustworthy artificial intelligence as a central component of long – term corporate competitiveness.

3.5 Economic benefits of AI regulation

Although much of the academic and policy debate surrounding the AI Act has focused on the compliance costs associated with regulatory obligations, an equally important body of literature emphasizes the potential economic benefits of well – designed AI regulation. According to this perspective, regulation should not be regarded solely as a constraint on innovation but also as an institutional mechanism capable of creating the conditions necessary for sustainable technological development and long – term market growth.

Artificial intelligence is characterized by significant information asymmetries. Consumers, businesses, and public authorities frequently lack the technical expertise required to evaluate the reliability, safety, and fairness of AI systems. This uncertainty may reduce market adoption, discourage investment, and undermine confidence in emerging technologies. Regulatory intervention seeks to address these market failures by establishing common standards that increase transparency, accountability, and legal certainty.

⁸⁸ NIST. AI Risk Management Framework 1.0 (2023).

⁸⁹ ISO/IEC 42001:2023 — Artificial Intelligence Management System (AIMS).

Within this framework, the AI Act may generate economic value beyond its immediate legal objectives. By promoting trustworthy AI, harmonizing regulatory requirements across the European Union, and encouraging responsible technological development, the Regulation has the potential to improve market confidence, reduce business risks, and strengthen the international competitiveness of European firms.

The following sections examine the principal economic benefits associated with AI regulation, highlighting how legal certainty and responsible governance may contribute to innovation, business performance, and sustainable economic growth.

3.5.1 Increased consumer trust

Consumer trust represents one of the most important determinants of the successful adoption of artificial intelligence technologies. Regardless of their technical sophistication, AI systems are unlikely to achieve widespread market acceptance if users perceive them as unreliable, discriminatory, or insufficiently transparent. Consequently, one of the principal economic objectives of the AI Act is to strengthen public confidence by establishing common legal standards governing the development and deployment of AI systems.

The Regulation contributes to this objective through requirements relating to transparency, human oversight, data quality, robustness, and accountability.⁹⁰ By imposing these obligations, the AI Act seeks to reduce the information asymmetries that frequently characterize AI markets, enabling consumers and business users to place greater trust in AI – enabled products and services.

From an economic perspective, higher levels of consumer trust may generate several positive effects. Increased confidence encourages the adoption of AI technologies, expands market demand, reduces resistance to technological innovation, and strengthens customer loyalty. Firms capable of demonstrating compliance with European regulatory standards may therefore enjoy reputational advantages that translate into improved commercial performance and greater market acceptance.

Moreover, trust has become an increasingly important competitive asset within the global digital economy. As concerns regarding algorithmic bias, privacy, misinformation, and cybersecurity continue to grow, organizations able to demonstrate responsible AI governance may differentiate themselves from competitors operating under less rigorous regulatory environments. In this sense, compliance with the AI Act may contribute not only to legal conformity but also to the creation of long – term customer value and sustainable competitive advantage.

⁹⁰ AI Act, Articles 13–15 (Transparency, Human Oversight, Accuracy, Robustness and Cybersecurity).

3.5.2 Legal certainty

Legal certainty constitutes one of the fundamental objectives of European economic regulation and represents a key factor influencing business investment decisions. Before the adoption of the AI Act, organizations developing artificial intelligence systems operated within a fragmented regulatory environment characterized by differing national initiatives, evolving legal interpretations, and considerable uncertainty regarding future obligations. Such uncertainty increased investment risks and complicated long – term strategic planning.

By establishing harmonized rules applicable throughout the European Union, the AI Act seeks to provide businesses with a more predictable regulatory environment. Common definitions, standardized obligations, and coordinated governance mechanisms reduce the likelihood of divergent national approaches, enabling firms to develop AI systems with greater confidence regarding the legal requirements applicable across the internal market.

From an economic perspective, legal certainty contributes to reducing transaction costs and encouraging long – term investment.⁹¹ Firms are generally more willing to allocate financial resources to research, product development, and market expansion when regulatory expectations are clearly defined and consistently enforced. Predictable regulation also facilitates strategic planning, contractual negotiations, and cross – border commercial activities by reducing legal ambiguity and compliance uncertainty.

Although compliance with the AI Act requires significant initial investments, many scholars argue that the benefits generated by regulatory predictability may partially compensate for these costs over time. A stable legal framework encourages responsible innovation by allowing businesses to incorporate regulatory requirements into product design from the earliest stages of development rather than adapting technologies aftermarket deployment.

3.5.3 Reduction of reputational risks

The growing diffusion of artificial intelligence has significantly increased public attention to issues such as algorithmic discrimination, privacy violations, misinformation, cybersecurity failures, and opaque automated decision – making. For businesses, these risks extend beyond legal liability and may seriously damage corporate reputation, consumer confidence, investor relations, and overall market value.

The AI Act contributes to mitigating these risks by establishing governance mechanisms designed to promote transparency, accountability, human oversight, and continuous risk management. Organizations complying with these requirements are better positioned to identify potential

⁹¹ European Commission (2021). Impact Assessment Accompanying the Proposal for the AI Act.

problems before they develop into incidents capable of generating public criticism or regulatory intervention.

From a business perspective, reducing the reputational risk has direct economic value. Corporate reputation represents an intangible asset that influences customer loyalty, access to investment, talent attraction, and relationships with regulators and business partners. Major AI – related controversies may rapidly undermine stakeholder confidence, producing financial consequences that substantially exceed the direct costs of regulatory sanctions.

Compliance with the AI Act therefore functions not only as a legal safeguard but also as a form of reputational risk management. Firms demonstrating responsible AI governance may strengthen stakeholder trust, improve corporate credibility, and reduce the probability of costly reputational crises. In increasingly transparent digital markets, these reputational advantages may become a significant source of long – term competitive resilience.

3.5.4 Promotion of responsible innovation

Perhaps the most ambitious objective of the AI Act is not simply to regulate artificial intelligence but to promote a model of innovation that combines technological progress with legal compliance, ethical responsibility, and social trust. This approach reflects the broader European vision that innovation and regulation should not be regarded as mutually exclusive but as a complementary element of sustainable economic development.

Responsible innovation encourages organizations to integrate legal, ethical, and societal considerations throughout the entire lifecycle of AI systems. Rather than addressing compliance only after products have been developed, firms are encouraged to incorporate principles such as transparency, fairness, accountability, human oversight, and cybersecurity directly into technological design. This proactive approach reduces future compliance costs while improving the overall quality and reliability of AI solutions.⁹²

From an economic perspective, responsible innovation may generate several long – term advantages. Organizations investing in trustworthy AI are more likely to strengthen customer confidence, facilitate access to regulated markets, reduce litigation risks, and attract investors increasingly attentive to environmental, social, and governance (ESG) considerations. Furthermore, integrating governance into innovation processes may improve organizational learning, strengthen interdisciplinary collaboration, and increase firms' capacity to adapt to future technological and regulatory developments.

The AI Act therefore seeks to transform compliance from a reactive legal obligation into a

⁹² UNESCO. Recommendation on the Ethics of Artificial Intelligence (2021).

strategic driver of innovation. Whether this objective will be fully achieved remains subject to empirical verification, particularly as the Regulation is progressively implemented across the European Union. Nevertheless, the European approach illustrates an increasingly influential conception of technological governance in which responsible innovation is viewed not as a limitation on economic growth but as one of its essential preconditions. This perspective provides the conceptual bridge to the final part of this chapter, where the broader implications of AI regulation for the global competitiveness of European companies will be examined.

3.6 AI regulation and business competitiveness

Business competitiveness is one of the central dimensions through which economic impact of AI regulation can be assessed. While previous sections have examined the costs and benefits generated by the AI Act, competitiveness concerns the broader ability of firms to innovate, attract investment, expand into new markets, and maintain sustainable advantages in an increasingly digital global economy. Consequently, evaluating the relationship between regulation and competitiveness requires moving beyond a narrow assessment of compliance costs and considering the long – term effects of the regulatory environment on business performance.

The academic debate offers contrasting perspectives on this issue. Critics argue that stringent regulatory requirements may reduce the attractiveness of the European market, discourage investment, and slow the commercialization of AI technologies. According to this view, companies operating in less regulated jurisdictions may benefit from lower development costs and greater flexibility, enabling them to innovate more rapidly than their European counterparts. Conversely, supporters of the European regulatory approach contend that trustworthy AI constitutes an increasingly valuable competitive asset. By promoting transparency, accountability, improve market acceptance, and encourage sustainable innovation capable of generating long – term economic value.⁹³

Competitiveness should therefore be understood as a multidimensional concept influenced by several interrelated factors. Investment decisions, innovation capacity, market dynamics, access to international markets, and stakeholder trust all contributed to determining firms’ ability to compete successfully. The AI Act may influence each of these dimensions in different ways, producing both short – term costs and long – term strategic opportunities.

The following sections analyze three of the principal channels through which AI regulation affects business competitiveness: investment decisions, firms’ capacity to innovate, and competition within European digital markets.

⁹³ European Commission (2021). Impact Assessment Accompanying the Proposal for the AI Act.

3.6.1 Effects on investment decisions

Investment decisions are strongly influenced by the regulatory environment in which firms operate. Companies developing artificial intelligence technologies must frequently commit substantial financial resources to research and development, data infrastructure, human capital, and technological experimentation long before commercial returns can be realized. Under these circumstances, regulatory certainty becomes an important factor shaping investors' expectations and firms' strategic planning.

The AI Act affects investment decisions in two contrasting ways. In the short term, compliance obligations increase the financial resources required to develop and commercialize AI systems. Expenditures relating to governance, documentation, conformity assessments, cybersecurity, and legal compliance may reduce the expected profitability of AI projects, particularly for firms operating under limited financial constraints. Some investors may therefore perceive regulated markets as involving higher implementation costs and longer investment horizons.

However, a different perspective emphasizes the positive relationship between regulatory certainty and investment confidence. Clearly defined legal requirements reduce uncertainty regarding future regulatory developments, allowing firms to incorporate compliance into long – term business strategies. Investors generally favor predictable regulatory environments because they reduce legal risks, facilitate strategic planning, and improve the reliability of future cash flow projections. From this perspective, the harmonized framework established by the AI Act may strengthen the attractiveness of the European market by providing stable and transparent rules applicable across all Member States.

The overall impact on investment is therefore likely to depend on firms' capacity to transform regulatory compliance into a strategic capability. Organizations that successfully integrate governance into product development may reduce long – term legal risks, improve access to institutional investors, and strengthen relationships with customers and business partners who increasingly value responsible AI practices. Consequently, while the AI Act undoubtedly increases initial investment requirements, it may also improve the quality and sustainability of investment decisions over the long term.

3.6.2 Effects on innovation capacity

Innovation capacity represents one of the most frequently discussed dimensions of AI regulation. Since artificial intelligence evolves through rapid technological experimentation, many scholars have questioned whether comprehensive regulatory frameworks may limit firms' ability to innovate. The answer, however, appears considerably more complex than a simple opposition

between regulation and technological progress.

From a short – term perspective, compliance requirements may reduce the speed of innovation by requiring organizations to allocate financial and human resources to governance activities rather than exclusively to research and development. Technical documentation, conformity assessments, data governance procedures, and ongoing monitoring inevitably increase development timelines, particularly for high – risk AI systems.⁹⁴ These additional requirements may be especially challenging for organizations operating in highly competitive sectors where rapid market entry constitutes a critical success factor.

At the same time, a growing body of literature argues that regulation may improve the quality rather than simply the quantity of innovation. The AI Act encourages firms to incorporate transparency, robustness, explainability, cybersecurity, and human oversight into technological development from the earliest stages of product design. This approach promotes the creation of AI systems that are more reliable, trustworthy, and socially acceptable, thereby facilitating their long – term adoption within regulated markets.

Innovation should therefore be evaluated not only in terms of speed but also in terms of sustainability and market acceptance. AI technologies that generate legal disputes, reputational crises, or widespread public distrust may ultimately prove less economically valuable than innovations developed within robust governance frameworks.⁹⁵ From this perspective, the AI Act may encourage a rapid but potentially risky transition towards more responsible and resilient forms of technological development capable of generating sustainable competitive advantages.

3.6.3 Effects on market entry and competition

The AI Act may also influence the structure of competition within the European digital markets by affecting firms' ability to enter, expand, and compete effectively. Market entry depends upon a wide range of factors, including financial resources, technological capabilities, regulatory compliance, and access to data. Consequently, changes in the regulatory environment may alter competitive dynamics throughout the AI ecosystem.

One concern frequently expressed within the literature is that compliance costs may create higher barriers to market entry, particularly for start – ups and smaller technology companies. Organizations with limited financial and human resources may encounter greater difficulties in satisfying the technical documentation, governance, conformity assessment, and monitoring requirements established for high – risk AI systems. In contrast, large multinational corporations often possess established compliance infrastructures that enable them to absorb regulatory costs

⁹⁴ AI Act, Chapter III (Requirements for High-Risk AI Systems).

⁹⁵ Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a Framework for Responsible Innovation.

more efficiently, potentially reinforcing existing market advantages.

Nevertheless, regulation may also strengthen competition by increasing market confidence and reducing legal fragmentation across the European Union. Prior to the AI Act, businesses faced the possibility of divergent national regulatory approaches that complicated cross – border commercial activities. Harmonized European rules reduce these transaction costs, allowing firms to access a larger and more predictable internal market. For many organizations, particularly those seeking international expansion, regulatory harmonization may offset part of the compliance burden by simplifying market access within the Union.

Furthermore, competition increasingly depends on trust as well as technological capability. Companies able to demonstrate compliance with rigorous European standards may acquire reputational advantages in global markets where concerns regarding AI safety, transparency, and accountability continue to grow. Consequently, the AI Act may reshape competitive dynamics by rewarding firms capable of integrating responsible AI governance into their business models rather than relying on speed or cost minimization.

Ultimately, the relationship between AI regulation and business competitiveness cannot be reduced to a simple trade – off between regulation and innovation. The AI Act introduces new compliance costs and may increase barriers for some market participants, particularly during the initial implementation phase. At the same time, it creates a harmonized legal framework that promotes trust, legal certainty, and responsible technological development. Whether these long – term benefits outweigh the short – term economic costs remain one of the central questions explored throughout this thesis and provides the basis for the conclusions presented in the final chapter.

3.7 Is Regulation a cost or a competitive advantage?

The question of whether AI regulation constitutes a cost or source of competitive advantages lies at the heart of the contemporary debate surrounding the European AI Act. Throughout this chapter, it has become evident that the relationship between regulation and business performance cannot be reduced to a simple dichotomy. Instead, the economic impact of regulation depends on a complex interaction between compliance costs, organizational capabilities, institutional quality, and firms' strategic responses. Consequently, assessing the effects of the AI Act requires moving beyond the traditional view that regulation necessarily constrains economic activity and considering its broader influence on long – term competitiveness.⁹⁶

From a short – term perspective, the introduction of the AI Act undoubtedly generates significant

⁹⁶ Blind, K. (2012). The Influence of Regulations on Innovation: A Quantitative Assessment for OECD Countries. Research Policy.

economic costs for businesses. Organizations developing or deploying AI systems are required to invest substantial resources in compliance programs, risk management systems, legal expertise, technical documentation, cybersecurity, employee training, conformity assessments, and post – market monitoring. These obligations may delay product development, increase operational expenditure, and reduce the financial resources available for research and innovation. The burden is particularly significant for start – ups and small and medium – sized enterprises, whose limited financial and organizational capacities make compliance proportionally more expensive than for larger corporations.

These observations support the innovation – inhibiting perspective discussed earlier in this chapter. According to this view, excessive regulatory intervention may discourage entrepreneurial experimentation, increase barriers to market entry, and reduce Europe’s attractiveness as a destination for AI investment. In global markets characterized by rapid technological progress and intense international competition, firms operating under lighter regulatory frameworks may initially enjoy advantages in terms of speed, flexibility, and lower development costs. From this perspective, regulation appears primarily as an economic cost that may weaken firms’ competitive position, especially during the early stages of implementation.

However, this interpretation captures only part of the broader economic picture. The literature increasingly suggests that focusing exclusively on compliance costs risks overlooking the institutional functions performed by regulation. Markets for artificial intelligence are characterized by significant information asymmetries, uncertainty regarding technological risks, and growing concerns about privacy, discrimination, cybersecurity, and accountability. In the absence of common rules, these factors may undermine consumer confidence, discourage investment, and ultimately limit the diffusion of AI technologies. Regulation therefore performs an important market – building function by establishing the institutional conditions necessary for trustworthy technological development.⁹⁷

From this perspective, the AI Act may generate substantial long – term economic benefits. By harmonizing regulatory requirements across the European Union, the Regulation reduces legal fragmentation and provides firms with a predictable framework for strategic planning and investment. Greater legal certainty facilitates long – term decision – making, reduces transaction costs associated with regulatory uncertainty, and enables organizations to incorporate compliance requirements directly into product development processes. Rather than reacting to evolving legal expectations, businesses can design AI systems that satisfy regulatory standards from the outset, thereby improving planning efficiency and reducing future adaption costs.

⁹⁷ Ashford, N. A., & Hall, R. P. (2011). *Technology, Globalization, and Sustainable Development*.

The promotion of consumer trust represents another important source of potential competitive advantage. artificial intelligence increasingly operates in sectors where public confidence constitutes an essential prerequisite for market adoption. Consumers, investors, business partners, and public authorities are more likely to adopt AI solutions that demonstrate transparency, reliability, fairness, and accountability. By establishing common governance standards, the AI Act contributes to strengthening trust in AI technologies, potentially increasing market demand for compliant products and services. For firms capable of demonstrating responsible AI practices, regulatory compliance may therefore become a valuable reputational asset rather than merely a legal obligation.

The strategic responses adopted by businesses further illustrate this evolving relationship between regulation and competitiveness. As discussed in previous sections, many organizations are no longer approaching compliance as a reactive legal exercise but as an integral component of corporate strategy. Investments in AI governance, internal compliance structures, explainable AI, cybersecurity, and responsible innovation increasingly serve broader business objectives extending beyond regulatory conformity. These investments improve organizational resilience, facilitate stakeholder engagement, strengthen corporate reputation, and enhance firms' ability to respond to future technological and regulatory developments. Consequently, compliance gradually evolves from a cost center into a strategic organizational capability.

The distinction between short – term costs and long – term benefits is particularly important when analyzing competitiveness from a dynamic rather than static perspective. Traditional economic analyzes often evaluate regulation by focusing primarily on immediate compliance expenditures. However, dynamic competitiveness depends not only on current production costs but also on firms' capacity to innovate sustainably, attract investment, maintain stakeholder confidence, and adapt to changing institutional environments. Under this broader perspective, regulation may contribute positively to competitiveness by encouraging the development of more robust organizational structures and higher – quality technological innovation.⁹⁸

Nevertheless, the transformation of regulation into competitive advantage is neither automatic nor guaranteed. The benefits associated with the AI Act largely depend on the proportionality of its implementation, the effectiveness of institutional guidance, and firms' capacity to integrate compliance efficiently into their business models. Excessively complex administrative procedures, inconsistent enforcement across Member States, or disproportionate compliance burdens could reduce many of the anticipated economic benefits, particularly for SMEs and innovative start – ups. Similarly, if competing jurisdictions continue to operate under significantly

⁹⁸ Smuha, N. A. (2021). From a “Race to AI” to a “Race to AI Regulation”.

lighter regulatory frameworks while maintaining comparable levels of technological innovation, European firms may experience disadvantages in certain global markets segments.

The concept of smart regulation provides perhaps the most convincing framework for reconciling these competing perspectives. Rather than interpreting regulations, it seeks to create institutional conditions under which both can reinforce one another. The AI Act's risk – based approach reflects this philosophy by concentrating the most demanding obligations on applications capable of generating significant risks while allowing low – risk AI systems to develop under relatively limited regulatory constraints. Although practical implementation will ultimately determine the effectiveness of this model, the Regulation represents one of the most ambitious attempts to balance technological innovation with the protection of fundamental rights, consumer confidence, and market integrity.

From a broader strategic perspective, the AI Act may also influence the international positioning of European companies. As discussions regarding AI governance continue to expand globally, European firms that develop expertise in regulatory compliance and trustworthy AI may acquire capabilities that become valuable beyond the European market. The so – called “Brussels effect” suggests that European regulatory standards frequently influence international business practices because multinational corporations often choose to adopt a single global compliance strategy rather than maintaining different governance systems across jurisdictions. If this phenomenon extends to artificial intelligence, firms that successfully comply with the AI Act may benefit from first – mover advantages in markets where responsible AI governance becomes an increasingly important competitive criterion.

Ultimately, the evidence examined throughout this chapter suggests that AI regulation should not be interpreted exclusively as either a cost or a competitive advantage. It represents both simultaneously, with the relative importance of each dimension varying according to firms' organizational capabilities, strategic choices, sectoral characteristics, and the maturity of regulatory implementation. Compliance undoubtedly requires significant financial and organizational investments. However, these investments may also strengthen governance, improve technological quality, reduce legal and reputational risks, increase stakeholder trust, and create more sustainable foundations for long – term innovation.

This analysis therefore supports the view that the AI Act should be understood as an institutional investment in the quality of European innovation rather than merely as a regulatory constraint. While its short – term economic effects are likely to be characterized by higher compliance costs and organizational adaptation, its long – term success will depend on whether Regulation succeeds in fostering an ecosystem in which trustworthy artificial intelligence becomes not only a legal requirement but also a distinctive competitive advantage for European companies. The following

chapter builds upon these findings by examining how these theoretical considerations are reflected in practice through selected case studies and empirical evidence concerning the implementation of AI governance within European businesses.

CHAPTER 4: Comparative analysis of global AI regulatory models

4.1 The United States approach of AI Regulation

The regulation of artificial intelligence has evolved differently across the world's major economic powers, reflecting distinct legal traditions, political priorities, and economic strategies. While the European Union has adopted a comprehensive and harmonized regulatory framework through the AI Act, the United States has generally preferred a more flexible and market – oriented approach. Rather than introducing a single federal law governing artificial intelligence, the U.S. regulatory model relies on a combination of sector – specific legislation, existing legal frameworks, voluntary standards, executive actions, and initiatives adopted at both the federal and state levels.⁹⁹

This approach reflects the long – standing American preference for promoting technological innovation through limited ex ante regulation. Policymakers have traditionally emphasized the importance of preserving entrepreneurial freedom, encouraging private investment, and avoiding regulatory constraints that might reduce the competitiveness of the U.S. technology sector. Consequently, artificial intelligence has largely developed within an environment characterized by significant regulatory flexibility, allowing firms to experiment rapidly with emerging technologies while relying on existing legal instruments to address specific risks.

However, the rapid diffusion of generative AI systems, increasing concerns regarding algorithmic discrimination, cybersecurity, misinformation, and national security have gradually intensified the debate surrounding AI governance in the United States. In recent years, federal authorities have introduced several policy initiatives aimed at promoting trustworthy AI without fundamentally abandoning the country's innovation – oriented regulatory philosophy.¹⁰⁰ At the same time, individual states have begun adopting their own AI – related legislation, creating an increasingly complex and fragmented regulatory landscape.

Understanding the U.S. model is essential for evaluating the distinctive characteristics of the European approach. While the European Union prioritizes legal certainty through comprehensive regulation, the United States generally seeks to maximize innovation by allowing regulatory intervention to develop gradually alongside technological progress.

The following sections examine the principal characteristics of the American regulatory model, focusing on its market – oriented philosophy, the interaction between federal and state initiatives,

⁹⁹ Executive Order 14110 (2023), Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

¹⁰⁰ NIST AI Risk Management Framework 1.0 (2023).

and the implications of regulatory flexibility for business competitiveness.

4.1.1 Market – oriented governance

The United States has traditionally adopted a market – oriented approach to technological regulation, grounded in the belief that innovation is most effectively promoted through competition, entrepreneurial freedom, and limited government intervention. Rather than establishing detailed ex ante rules governing the development of emerging technologies, American policymakers have generally favored regulatory frameworks that allow innovation to evolve before introducing comprehensive legal obligations.

This philosophy has strongly influenced the governance of artificial intelligence. Until recently, the United States lacked a comprehensive federal regulatory framework specifically dedicated to AI. Instead, existing legislation relating to consumer protection, civil rights, competition law, product liability, intellectual property, financial regulation, healthcare, and privacy has been applied to AI systems where appropriate. Independent regulatory agencies such as the Federal Trade Commission (FTC)¹⁰¹, the Food and Drug Administration (FDA), and sector – specific authorities have played an increasingly important role in addressing AI – related risks within their perspective areas of competence.

The market – oriented model assumes that excessive regulation may discourage private investment, reduce entrepreneurial experimentation, and slow technological progress. Consequently, regulatory intervention is generally introduced only when concrete risks emerge, allowing businesses greater flexibility during the early stages of innovation. This approach has contributed to the rapid growth of the American AI ecosystem, which continues to host many of the world’s leading technology companies and attracts a substantial share of global venture capital investment.

Nevertheless, critics argue that reliance on existing legal frameworks may leave important regulatory gaps, particularly regarding transparency, accountability, algorithmic discrimination, and systemic AI risks. Unlike the European AI Act, the American model does not establish uniform obligations applicable across all AI systems according to their level of risk. As a result, businesses often operate within a regulatory environment characterized by greater flexibility but also higher legal uncertainty regarding future legislative developments.

From an economic perspective, the market – oriented model illustrates a different interpretation of the relationship between regulation and innovation. Rather than prioritizing precautions through comprehensive ex ante governance, it assumes that market competition and technological

¹⁰¹ Federal Trade Commission (FTC), policy statements on AI.

progress should remain the principal drivers of AI development, with regulatory intervention occurring only where necessary to address clearly identifiable risks.

4.1.2 Federal and State initiatives

Although the United States has not adopted a comprehensive federal AI law comparable to the European AI Act, AI governance has expanded considerably through a combination of federal initiatives and state – level legislation. This decentralized approach reflects the constitutional structure of the United States, where regulatory authority is frequently shared between federal institutions and individual states.

At the federal level, recent years have witnessed increasing governmental attention to artificial intelligence. A significant milestone was the publication of the Blueprint for an AI Bill of Rights by the White House Office of Science and Technology Policy in 2022¹⁰², which identified five guiding principles intended to protect individuals from harmful uses of AI, including safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and human alternatives. Although this document is not legally binding, it has become an influential reference for policymakers and organizations developing AI systems.

Federal governance was further strengthened through Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued in October 2023. The Executive Order instructed numerous federal agencies to develop standards, guidance, reporting mechanisms, and risk management measures relating to AI safety, cybersecurity, national security, and responsible innovation. Rather than introducing directly enforceable obligations comparable to the AI Act, the Executive Order seeks to coordinate federal action while maintaining the flexibility traditionally associated with the American regulatory model.

Alongside federal initiatives, several U.S. states have begun adopting their own AI – related legislation. States such as Colorado, California, Illinois, and New York have introduced or proposed measures addressing algorithmic accountability, employment discrimination, automated decision – making, biometric technologies, and transparency requirements.¹⁰³ While these initiatives demonstrate growing regulatory attention, they also contribute to increasing legal fragmentation, requiring companies operating nationally to comply with multiple regulatory regimes that may differ significantly across jurisdictions.

From a business perspective, this decentralized governance model presents both opportunities and challenges. Firms benefit from the absence of a comprehensive federal compliance framework comparable to the AI Act, thereby preserving greater operational flexibility. At the same time, the

¹⁰² Blueprint for an AI Bill of Rights (2022).

¹⁰³ Colorado AI Act (2024).

proliferation of state – level initiatives may increase legal complexity and compliance uncertainty, particularly for organizations operating across multiple states or providing AI – enabled services nationwide.

4.1.3 Regulatory flexibility and innovation

One of the defining characteristics of the American approach to AI governance is its emphasis on regulatory flexibility. Rather than imposing comprehensive legal obligations before technologies reach the market, the United States generally allows innovation to develop within relatively broad legal boundaries while adapting regulation progressively as new risks emerge. This adaptive philosophy reflects the belief that governments should avoid constraining technological experimentation prematurely, particularly in sectors characterized by rapid innovation and high economic potential.

From an economic perspective, regulatory flexibility may generate several advantages. Lower compliance costs reduced administrative burdens, and fewer ex ante approval procedures enable firms to allocate a larger share of financial and human resources to research, product development, and commercialization. Start – ups and venture capital investors often regard flexible regulatory environments as particularly attractive because they facilitate experimentation, shorten development cycles, and reduce barriers to market entry.

The remarkable growth of the American AI industry is frequently cited as evidence supporting this approach. The United States remains home to many of the world’s leading AI companies, research institutions, and venture capital ecosystems, benefiting from substantial private investment and close collaboration between universities, technology firms, and government agencies. The regulatory environment has historically encouraged entrepreneurial risk – taking and rapid technological scaling, contributing to the country’s global leadership in artificial intelligence.

However, regulatory flexibility also presents significant challenges. The absence of uniform ex ante requirements may increase uncertainty regarding ethical standards, consumer protection, liability, and accountability. Businesses may face evolving legal expectations as new legislation or regulatory guidance is introduced in response to emerging technological developments. Furthermore, the lack of harmonized national rules may reduce public trust in AI systems and compliance international cooperation with jurisdictions that have adopted more comprehensive regulatory frameworks.

Comparing the United States with the European Union highlights two distinct philosophies of technological governance. The American model prioritizes innovation by minimizing regulatory intervention during the early stages of technological development, whereas the European model

seeks to foster innovation within a structured legal framework centered on trust, accountability, and risk management. Neither approach is inherently superior; rather, each reflects different assumptions regarding the appropriate balance between economic competitiveness, technological progress, and societal protection. This comparison provides the foundation for the following sections, which examine how other global powers (most notably China) have developed alternative regulatory models based on different political, economic, and institutional priorities.

4.2 The Chinese approach to AI regulation

China has developed one of the world's most distinctive approaches to artificial intelligence governance. Unlike the European Union, which places the protection of fundamental rights at the center of its regulatory framework, and unlike the United States, which traditionally prioritizes market – driven innovation, China has adopted a state – centered model in which AI regulation is closely integrated with national economic planning, industrial policy, technological sovereignty, and national security objectives.

Artificial intelligence occupies a strategic position within China's long – term development strategy. Over the past decade, the Chinese government has identified AI as a key driver of economic modernization, industrial upgrading, military capability, and global technological leadership. Consequently, regulatory intervention has been designed not only to manage the risks associated with AI but also to accelerate its development in accordance with broader national priorities.

Chinese AI governance is characterized by a strong role played by central government institutions, which actively coordinate technological development through strategic planning, industrial policies, sectoral regulations, and administrative supervision. Rather than relying primarily on market mechanisms or comprehensive horizontal legislation, the Chinese regulatory framework combines targeted legal instruments with extensive governmental oversight, allowing authorities to intervene rapidly as technological developments evolve.

At the same time, China has become increasingly active in regulating specific AI applications. Regulations concerning recommendation algorithms, deep synthesis technologies, and generative artificial intelligence demonstrate the government's intention to balance technological innovation with objectives relating to social stability, cybersecurity, public order, and state security. As a result, the Chinese approach reflects a distinctive model in which innovation promotion and regulatory control are pursued simultaneously under the guidance of the state.¹⁰⁴

Understanding this regulatory philosophy is essential for comparing the three major global AI

¹⁰⁴ Provisions on the Administration of Deep Synthesis Internet Information Services (2023).
Provisions on the Administration of Algorithmic Recommendation Services (2022).

governance models. While the European Union emphasizes trust through legal certainty and the United States prioritizes market flexibility, China seeks to combine rapid technological development with centralized governmental coordination. These different approaches reveal how AI governance has become not only a legal issue but also a strategic instrument of economic policy of international competitiveness.

4.2.1 State – centered governance

The defining characteristic of the Chinese model is the central role of the state in directing the development and governance of artificial intelligence. Rather than relying primarily on market forces to shape technological progress, Chinese authorities actively guide AI development through national strategic planning, industrial policy, regulatory intervention, and close cooperation with leading technology companies and research institutions.

This governance model is rooted in China's broader economic system, where state institutions play a significant role in coordinating long – term industrial development. Artificial intelligence has therefore been incorporated into successive national policy initiatives, including the New Generation Artificial Intelligence Development Plan (2017)¹⁰⁵, which established the objective of transforming China into the world's leading AI innovation center by 2030. Public investment, research funding, infrastructure development, talent cultivation, and technological standardization have all been coordinated within this broader national strategy.

Unlike the European AI Act, which establishes a comprehensive horizontal legal framework applicable across sectors, Chinese regulation frequently adopts a more targeted and adaptive approach. Government agencies issue administrative measures, sector – specific regulations, technical standards, and implementation guidelines that can be updated relatively quickly in response to technological developments. This flexibility enables regulators to intervene rapidly while maintaining strong governmental oversight over strategic technologies.

Another distinguishing feature of the Chinese model is the close interaction between public authorities and private technology companies. Major firms such as Alibaba, Tencent, Baidu, and ByteDance play an important role in implementing national AI strategies while simultaneously operating under extensive regulatory supervision. This relationship differs substantially from the more market – driven approach observed in the United States and the more rights – oriented framework adopted by the European Union.

From an economic perspective, state – centered governance provides significant advantages in terms of strategic coordination, long – term investment planning, and large – scale infrastructure

¹⁰⁵ New Generation Artificial Intelligence Development Plan (2017).

development. At the same time, critics argue that extensive governmental involvement may reduce market autonomy, increase regulatory discretion, and create uncertainty regarding the balance between commercial innovation and state priorities. Consequently, the Chinese model illustrates a fundamentally different conception of AI governance in which economic development and governmental control are viewed as complementary rather than competing objectives.

4.2.2 Strategic objectives of AI development

Artificial intelligence occupies a central position within China's national development strategy because it is regarded not merely as an emerging technology but as a strategic resource capable of reshaping economic growth, industrial competitiveness, scientific leadership, and geopolitical influence. Consequently, AI governance is closely linked to broader state objectives extending well beyond the regulation of technological risks.

The New Generation Artificial Intelligence Development Plan identifies several long – term priorities. These include strengthening China's technological self – sufficiency, accelerating industrial modernization, improving public administration, enhancing national security, and positioning the country as a global leader in AI research and commercialization. AI is therefore viewed as a key component of China's transition towards a high – value, innovation – driven economy capable of competing internationally in advanced technologies.

Industrial policy plays a particularly important role within this framework. Public authorities actively support AI development through investment programs, research funding, preferential policies, national laboratories, research centers, and technology firms. Unlike the European model, where regulation primarily seeks to create trustworthy market conditions, the Chinese approach integrates regulation directly into broader economic planning and industrial strategy.

National security also constitutes a fundamental objective of AI governance. Chinese policymakers increasingly emphasize the importance of maintaining technological sovereignty, protecting critical digital infrastructures, strengthening cybersecurity, and reducing dependence on foreign technologies. These priorities have become even more significant considering growing international competition surrounding semiconductors, advanced computing, and generative AI. From an economic perspective, this strategic approach enables China to mobilize substantial public and private resources towards AI development while maintaining close coordination between technological innovation and national policy objectives.¹⁰⁶ However, it also illustrates how AI regulation in China serves multiple functions simultaneously, combining economic modernization, industrial competitiveness, geopolitical strategy, and governmental oversight

¹⁰⁶ “14th Five-Year Plan for Economic and Social Development and Long – range Objectives Trough the Year 2035 of People's Republic of China (2021–2025).”

within a single policy framework.

4.2.3 Regulatory control mechanisms

While China actively promotes the development of artificial intelligence, it has simultaneously established an increasingly sophisticated system of regulatory control designed to supervise the deployment of AI technologies and ensure that their use remains consistent with broader public policy objectives. Rather than relying primarily on comprehensive framework legislation, Chinese authorities have progressively introduced targeted regulations governing specific categories of AI applications.

Among the most significant regulatory instruments are the *Provisions on the Administration of Algorithmic Recommendation Services* (2022)¹⁰⁷, the *Provisions on the Administration of Deep Synthesis Internet Information Services* (2023)¹⁰⁸, and the *Interim Measures for the Management of Generative Artificial Intelligence Services* (2023)¹⁰⁹. These regulations introduce obligations relating to algorithm registration, content moderation, transparency, cybersecurity, user protection, and provider responsibilities. They also require AI providers to implement mechanisms capable of preventing the generation or dissemination of illegal content while ensuring that AI systems operate in accordance with Chinese legal and policy requirements.

A distinctive characteristic of the Chinese model is the extensive role assigned to administrative supervision. Regulatory authorities possess broad powers to monitor AI services, require algorithm filings, conduct inspections, request information from providers, and adopt corrective measures where regulatory obligations are not satisfied. This administrative approach allows rapid governmental intervention while maintaining considerable flexibility in responding to technological developments.

From a business perspective, these regulatory mechanisms create a governance environment characterized by both opportunities and constraints. On the one hand, firms benefit from strong governmental support for AI development, substantial public investment, and clear strategic priorities. On the other hand, they operate within a regulatory framework where compliance extends beyond technical safety requirements to include obligations relating to cybersecurity, content governance, social stability, and national security. Consequently, business strategies must remain closely aligned with evolving governmental expectations.

Comparing China's regulatory control mechanisms with those adopted by the European Union and the United States reveals three fundamentally different governance philosophies. The

¹⁰⁷ Provisions on Algorithmic Recommendation Services (2022).

¹⁰⁸ Provisions on Deep Synthesis Internet Information Services (2023).

¹⁰⁹ Interim Measures for the Management of Generative Artificial Intelligence Services (2023).

European Union primarily regulates AI according to the level of risk posed to fundamental rights, the United States generally emphasizes market – driven innovation supported by sector – specific regulation, whereas China combines strong industrial promotion with extensive governmental supervision. These differences will provide the analytical foundation for the comparative assessment developed in the following section of this chapter.

4.3 Comparing the European, American and Chinese models

The analysis conducted throughout this chapter demonstrates that the European Union, the United States, and China have developed fundamentally different approaches to the governance of artificial intelligence. Although all three jurisdictions recognize AI as a transformative technology capable of reshaping economic growth, industrial competitiveness, and geopolitical influence, they differ considerably in the legal principles, institutional structures, and policy objectives that guide regulatory intervention.

These differences are not merely legal in nature. They reflect broader economic philosophies concerning the role of the state, the functioning of markets, the protection of individual rights, and the relationship between innovation and regulation. Consequently, each regulatory model creates a distinct business environment, influencing firms’ investment decisions, innovation strategies, compliance costs, and internal competitiveness.

The European Union has adopted a comprehensive regulatory framework centered on the protection of fundamental rights, risk management, and trustworthy AI. The United States has generally relied on market – driven innovation supported by flexible, specific – sector regulation. China, by contrast, has integrated AI governance into a broader state – led strategy aimed at promoting technological leadership while maintaining extensive governmental oversight.

Rather than identifying a universally superior model, comparative analysis seeks to evaluate the advantages and limitations associated with each regulatory philosophy. The following sections compare the three approaches according to three fundamental dimensions: their underlying regulatory philosophy, the incentives they create for innovation, and their implications for businesses operating within increasingly globalized AI markets.

4.3.1 Regulatory philosophy

Perhaps the most significant difference among the three global AI governance models concerns the underlying philosophy that guides regulatory intervention. Although all three jurisdictions seek to promote artificial intelligence while addressing its associated risks, they differ fundamentally in their understanding of the appropriate relationship between innovation, regulation, and public authority.

The European Union adopts a right – based and risk – oriented philosophy. The AI Act is built upon the assumption that technological innovation should develop within a legal framework capable of protecting fundamental rights, ensuring transparency, preventing discrimination, and preserving public trust. Regulation therefore functions primarily as a mechanism for reducing societal risks while simultaneously creating the legal certainty necessary to support sustainable innovation. The European approach reflects the broader constitutional tradition of the Union, where market integration is consistently accompanied by high standards of consumer protection and fundamental rights.

The United States follows a markedly different philosophy based on market – oriented governance. Rather than regulating AI through a comprehensive legislative framework, American policymakers have traditionally relied on competition, entrepreneurial initiative, and sector – specific legal instruments to guide technological development. Regulatory intervention generally occurs only after concrete risks emerge, reflecting the belief that excessive ex ante regulation may discourage innovation and reduce international competitiveness. Within this model, market dynamics remain the principal driver of technological progress, while public authorities intervene selectively to address specific market failures.

China adopts a third and fundamentally distinct regulatory philosophy centered on the strategic role of the state. Artificial intelligence is viewed not only as a source of economic growth but also as an instrument of national development, technological sovereignty, social governance, and national security. Regulatory intervention therefore serves multiple objectives simultaneously, combining industrial policy, economic planning, public administration, and technological supervision within a unified governance framework. Rather than limiting governmental involvement, the Chinese model actively coordinates AI development according to long – term national priorities.

From a comparative perspective, these three philosophies illustrate different conceptions of technological governance. The European model prioritizes trust through legal certainty, the American model prioritizes innovation through regulatory flexibility, and the Chinese model prioritizes strategic coordination through state leadership. Each approach reflects distinct institutional traditions and political values, explaining why AI regulation has evolved differently despite the common technological challenges faced by all three jurisdictions.

4.3.2 Innovation incentives

The three regulatory models also differ significantly in the incentives they create for technological innovation. Although each jurisdiction recognizes artificial intelligence as a strategic driver of economic growth, the mechanisms through which innovation is encouraged vary considerably

according to broader regulatory philosophies and institutional priorities.

Within the United States, innovation incentives are primarily generated through market competition, entrepreneurial freedom, venture capital investment, and relatively limited ex ante regulation. Companies benefit from greater operational flexibility, allowing them to experiment rapidly with emerging AI technologies and commercialize innovations without extensive prior regulatory approval. This environment has contributed to the development of one of the world's most dynamic AI ecosystems, characterized by strong private investment, close collaboration between universities and industry, and the global leadership of major technology companies.

China also places innovation at the center of its AI strategy, but through markedly different mechanisms. Rather than relying primarily on market incentives, Chinese authorities actively promote technological development through industrial policy, public investment, national research programs, strategic planning, and extensive coordination between government institutions and leading technology companies. Innovation is therefore strongly supported by state intervention, reflecting the broader objective of achieving technological self – sufficiency and international leadership in advanced technologies.

The European Union adopts a more balanced approach. Innovation remains an important objective of the AI Act, but it is pursued alongside the protection of fundamental rights, and legal certainty. Rather than maximizing the speed of technological development, the European framework seeks to encourage responsible innovation capable of generating sustainable economic value over the long term. Regulatory sandboxes harmonized legal standards, and risk – based obligations illustrate this attempt to reconcile technological progress with effective governance.

From an economic perspective, each model presents both advantages and limitations. The American approach may facilitate rapid technological experimentation but may also generate greater legal uncertainty. The Chinese model enables coordinated long – term investment but depends heavily on state direction and administrative intervention. The European model imposes higher initial compliance costs but may strengthen innovation quality, market confidence, and international credibility by promoting trustworthy AI. Consequently, the relationship between regulation and innovation cannot be evaluated solely in terms of speed, it must also consider sustainability, institutional stability, and long – term competitiveness.

4.3.3 Business implications

The different regulatory approaches adopted by the European Union, the United States, and China generate distinct implications for businesses operating within domestic and international AI markets. These implications extend beyond legal compliance and directly influence corporate governance, investment strategies, product development, market expansion, and international

competitiveness.

European companies operate within the most comprehensive regulatory framework among the three jurisdictions. Compliance with the AI Act requires significant investments in governance systems, risk management, technical documentation, transparency mechanisms, and human oversight. Although these obligations increase short – term compliance costs, they also provide legal certainty, harmonized market rules, and stronger consumer confidence throughout the European internal market. Firms capable of integrating compliance into their business strategies may therefore transform regulatory obligations into long – term competitive advantages, particularly in sectors where trust represents a decisive market factor.¹¹⁰

American companies generally benefit from greater regulatory flexibility and lower ex ante compliance burdens. This environment supports rapid innovation, attracts venture capital, and facilitates entrepreneurial experimentation. However, businesses also face increasing regulatory uncertainty resulting from the coexistence of federal initiatives, state legislation, and evolving agency guidance. Moreover, the absence of a comprehensive national AI framework may complicate international operations, particularly when companies seek to enter markets governed by stricter regulatory standards such as those established by the European Union.

Chinese companies operate within a regulatory environment characterized by strong governmental support for the technological development combined with extensive administrative supervision. Public investment, industrial policy, and strategic coordination create favorable conditions for rapid AI deployment in priority sectors. At the same time, firms must continuously align business strategies with evolving governmental priorities relating to cybersecurity, content governance, and national security. Compliance therefore extends beyond commercial considerations to encompass broader political and strategic objectives.

For multinational enterprises, these differences create substantial managerial challenges.¹¹¹ Companies operating globally frequently need to design governance frameworks capable of satisfying multiple regulatory systems simultaneously. Many organizations increasingly adopt the highest applicable regulatory standard across all operations rather than maintaining different compliance models for different jurisdictions. This phenomenon is particularly evident among multinational corporations seeking access to the European market, where compliance with the AI Act may become a benchmark for global AI governance.

Ultimately, comparative analysis suggests that no regulatory model offers a universally optimal solution. The American model maximizes flexibility and entrepreneurial dynamism, the Chinese model prioritizes strategic coordination and industrial policy, while the European model seeks to

¹¹⁰ Deloitte (2024). State of Generative AI in Enterprise.

¹¹¹ OECD (2023–2024). Digital Economy Outlook e AI Policy Observatory.

balance innovation with trust, accountability, and legal certainty. Each framework reflects different institutional priorities and generates distinct economic outcomes. Nevertheless, as artificial intelligence becomes increasingly global, successful businesses are likely to be those capable of operating effectively across multiple regulatory environments while integrating responsible AI governance into their long – term corporate strategies. This comparative assessment provides the analytical foundation for the final chapter, which evaluates whether the European regulatory model can ultimately strengthen or weaken the global competitiveness of European companies.

4.4 Strengths and weaknesses of the EU AI Act

The comparative analysis developed throughout this chapter highlights that the European Union has adopted the world’s most comprehensive regulatory framework for artificial intelligence. Unlike the United States, which prioritizes market flexibility, or China, which combines technological development with extensive state coordination, the European model seeks to establish a harmonized legal framework capable of promoting innovation while simultaneously protecting fundamental rights, ensuring transparency, and strengthening public trust.

This ambitious regulatory strategy has attracted considerable international attention. Supporters regard the AI Act as a pioneering legal instrument capable of establishing global standards for trustworthy artificial intelligence and providing businesses with a predictable regulatory environment. Critics, however, question whether the extensive compliance obligations introduced by the Regulation may reduce Europe’s competitiveness in an increasingly dynamic global AI market.

Evaluating the strengths and weaknesses of the AI Act therefore requires a multidimensional analysis. Its effectiveness cannot be measured solely by reference to legal compliance or economic efficiency but must also consider broader objectives such as consumer protection, innovation, international competitiveness, technological sovereignty, and institutional legitimacy. The following sections examine the principal legal and economic strengths of the European framework before addressing the main criticisms advanced within academic literature.

4.4.1 Legal strengths

From a legal perspective, the AI Act represents one of the most ambitious attempts to establish a comprehensive governance framework for artificial intelligence. Rather than regulating isolated technological applications, the Regulation introduces a horizontal legal framework applicable across sectors while differentiating regulatory obligations according to the level of risk generated by individual AI systems. This represents a significant innovation within digital regulation and

distinguishes the European approach from most other jurisdictions.

One of the principal strengths of the AI Act lies in its risk – based methodology. By classifying AI systems according to unacceptable, high, limited, and minimal level of risk, the Regulation seeks to allocate compliance obligations proportionately, avoiding unnecessary regulatory burdens for low – risk technologies while imposing stricter safeguards where fundamental rights or public safety may significantly affect. This proportionality enhances both legal coherence and regulatory legitimacy, ensuring that governmental intervention remains closely connected to the potential risks generated by AI applications.

A second legal strength concerns harmonization. Before the adoption of the AI Act, Member States were increasingly considering rational AI legislation, creating the possibility of regulatory fragmentation within the internal market. The Regulation establishes common legal standards applicable throughout the European Union, thereby reducing legal uncertainty and facilitating the free movement of AI systems across Member States. Harmonization strengthens the functioning of the internal market while providing businesses with greater certainty regarding their legal obligations.

The AI Act also reinforces the protection of fundamental rights by integrating principles such as transparency, accountability, human oversight, non – discrimination, and data governance into the regulatory framework. Rather than addressing these issues solely through ex post liability mechanisms, the Regulation introduces preventive obligations designed to reduce risks before harmful outcomes occur. This preventive approach reflects the broader European constitutional tradition of combining technological innovation with strong safeguards for individual rights.

Finally, the Regulation contributes to the development of international AI governance. Like the influence previously exercised by the General Data Protection Regulation (GDPR), the AI Act may encourage multinational corporations to adopt European standards across global operations, thereby extending its practical influence beyond the borders of the European Union. This phenomenon, frequently described as the “Brussels Effect”¹¹², illustrates how comprehensive European regulation may shape international businesses practices even in jurisdictions where equivalent legislation has not yet been adopted.

4.4.2 Economic strengths

Although public debate frequently emphasizes the compliance costs generated by the AI Act, the Regulation also presents several potential economic advantages capable of strengthening the long – term competitiveness of European businesses. These benefits drive primarily from the creation

¹¹² GDPR (Regulation (EU) 2016/679), for comparison on Brussels Effect.

of a more predictable institutional environment, increased market confidence, and the promotion of high – quality technological innovation.

Perhaps the most important economic strength of AI Act is the legal certainty it provides. Businesses developing artificial intelligence systems require stable regulatory environments to make long – term investment decisions involving substantial financial commitments. By establishing harmonized obligations applicable throughout the European Union, the Regulation reduces legal fragmentation and enables firms to incorporate compliance requirements into strategic planning from the earliest stages of product development. Greater predictability reduces transaction costs associated with regulatory uncertainty and facilitates cross – border commercial activities within the internal market.

A second economic advantage concerns customer trust. Artificial intelligence increasingly operates in sectors involving significant information asymmetries, where users cannot easily evaluate the safety, fairness, or reliability of AI systems. The transparency, accountability, and human oversight requirements introduced by the AI Act may strengthen public confidence in AI – enabled products and services, thereby increasing market acceptance and encouraging broader technological adoption. In this context, regulatory compliance may become a valuable commercial asset rather than merely a legal obligation.¹¹³

Regulation may also contribute to improving the quality of innovation. By encouraging organizations to integrate governance, explainability, cybersecurity, and responsible design into technological development, the AI Act promotes innovation that is not only technically advanced but also socially sustainable and commercially reliable. Such characteristics may prove increasingly important as global markets place greater emphasis on trustworthy AI and responsible digital governance.

Finally, the AI Act may enhance the international competitiveness of European firms by positioning Europe as a global leader in trustworthy artificial intelligence. Companies capable of demonstrating compliance with rigorous European standards may strengthen relationships with international investors, institutional customers, public administrations, and business partners who increasingly value transparent and accountable AI systems. In this sense, regulatory compliance may evolve into a source of competitive differentiation within global markets where trust has become an increasingly valuable economic resource.

4.4.3 Regulatory criticisms

Despite its numerous strengths, the AI Act has also attracted substantial criticism from academics,

¹¹³ Charter of Fundamental Rights of the European Union.

policymakers, industry representatives, and technology companies. Most criticisms do not challenge the legitimacy of regulating artificial intelligence itself, rather question whether the specific regulatory mechanisms adopted by the European Union strike an appropriate balance between innovation, competitiveness, and legal protection.

One of the most frequently expressed concerns relates to compliance costs. The extensive documentation requirements, conformity assessments, governance obligations, and ongoing monitoring procedures introduced by the AI Act may require significant financial and organizational investments, particularly for start – ups and small and medium – sized enterprises. Critics argue that these costs could discourage entrepreneurial experimentation, reduce venture capital investment, and delay the commercialization of innovative AI applications, especially when compared with jurisdictions characterized by lighter regulatory frameworks.

A second criticism concerns regulatory complexity. The AI Act combines legal, technical, organizational, and sector – specific obligations within a highly sophisticated regulatory architecture. Although this complexity reflects the equally complex nature of artificial intelligence, some scholars argue that interpreting and implementing the Regulation may prove challenging even for large organizations possessing substantial legal and technical expertise. Smaller firms may experience difficulties in understanding evolving regulatory expectations, increasing their dependence on external legal and compliance consultants.

Another issue concerns the speed of technological change. Artificial intelligence evolves at a pace that frequently exceeds traditional legislative processes. Critics therefore question whether a comprehensive regulatory framework can remain sufficiently flexible to address emerging technologies without requiring continuous legislative revision. Although the AI Act incorporates a risk – based methodology intended to accommodate future technological developments, concerns remain regarding the Regulation’s capacity to adapt rapidly to innovations such as advanced foundation models, autonomous AI agents, and future generations of generative AI.

The international competitiveness of European businesses also remains the subject of considerable debate. Some commentators argue that higher compliance costs may encourage AI developers to relocate research, investment, or commercialization activities to jurisdictions offering greater regulatory flexibility. Others suggest that multinational corporations may prioritize markets characterized by lower regulatory barriers during the early stages of technological development, potentially reducing Europe’s attractiveness as a destination for AI entrepreneurship.

Nevertheless, many of these criticisms should be interpreted within a broader economic and institutional context. The absence of comprehensive regulation may generate different forms of market failure, including declining consumer trust, legal uncertainty, fragmented governance, and increasing societal resistance to AI adoption. Consequently, the relevant policy question is not

whether regulation should exist but whether it has been designed proportionately and implemented effectively. The AI Act represents an ambitious attempt to reconcile these competing objectives through a risk – based regulatory framework that seeks simultaneously to promote innovation, protect fundamental rights, and strengthen market confidence.

Ultimately, the strengths and weaknesses identified throughout this chapter demonstrate that the European AI Act should neither be idealized nor dismissed as an obstacle to innovation. Instead, it represents a sophisticated regulatory experiment whose long – term success will depend on its practical implementation, the consistency of enforcement across Member States, and the ability of European businesses to integrate compliance into broader strategies of responsible innovation. These considerations provide the basis for the final chapter of this thesis, which will answer the central research question by assessing whether the European regulatory model can transform AI governance into a sustainable source of economic competitiveness.

4.5 Future challenges for AI regulation

The comparative analysis developed throughout this chapter demonstrates that artificial intelligence regulation is not a static policy challenge. The regulatory frameworks adopted by the European Union, the United States, and China have been developed in response to technological developments that continue to evolve at an exceptionally rapid pace. As a result, one of the principal challenges for policymakers is ensuring that regulatory systems remain effective and adaptable without unnecessarily restricting technological progress.

The emergence of generative AI and increasingly sophisticated foundation models has significantly complicated this challenge. Unlike traditional AI applications, which are generally developed for relatively specific purposes, general – purpose models can perform a broad range of tasks and can subsequently be integrated into numerous downstream applications. This creates a more complex distribution of responsibilities between model developers, system providers, deployers, and users.

The European Union has attempted to address this development by incorporating specific obligations for providers of general – purpose AI models into the AI Act. These obligations became applicable on 2 August 2025 and include requirements concerning technical documentation, copyright policies, and the publication of summaries of training content. Providers of GPAI models presenting systemic risk are subject to additional requirements concerning risk assessment and mitigation, incident reporting, and cybersecurity.¹¹⁴

Nevertheless, the rapid evolution of AI technologies raises questions regarding the long - term

¹¹⁴ <https://digital-strategy.ec.europa.eu/en/factpages/general-purpose-ai-obligations-under-ai-act>

adaptability of those provisions. Thresholds, technical standards, definitions, and risk assessment methodologies may become outdated as computational capabilities and model architectures evolve. The European Commission has therefore emphasized the importance of practical guidance and adaptive implementation, while the OECD has similarly highlighted the need for anticipatory governance capable of responding to emerging technological developments.

Three challenges are particularly relevant for the future of AI governance. First, generative AI creates new and rapidly evolving forms of economic and societal risk. Second, foundation models complicate traditional regulatory approaches because a single model may underpin a large and diverse ecosystem of downstream applications. Third, the inherently global nature of AI creates a strong need for international regulatory coordination. These issues are examined in the following sections.

4.5.1 Generative AI

Generative artificial intelligence represents one of the most significant challenges for contemporary AI regulation.¹¹⁵ Unlike conventional AI systems designed to perform relatively specific tasks, generative AI systems can produce text, images, audio, video, software code, and other forms of content. Their versatility has contributed to exceptionally rapid adoption across both consumer and business environments, creating substantial opportunities for productivity, innovation, and the development of new business models.

At the same time, the general – purpose nature of generative AI creates regulatory challenges that are considerably more complex than those associated with traditional AI applications. The same underlying model may be used for harmless productivity applications, high – impact business processes, scientific research, or potentially harmful activities. Consequently, assessing risk solely based on technology itself becomes increasingly difficult. Risk may instead depend on how a model is subsequently integrated, fine – tuned, deployed, and used.

This characteristic has important implications for the allocation of regulatory responsibility. A foundation model developer may have limited knowledge regarding all the downstream applications in which its model will ultimately be used. Conversely, downstream providers may have greater knowledge of the specific context in which an AI system operates but may lack complete visibility into the characteristics of the underlying model. Effective regulation must therefore determine how responsibilities should be distributed across the AI value chain.

The AI Act represents an attempt to address this problem by introducing specific obligations for providers of general – purpose AI models. The framework distinguishes between obligations

¹¹⁵ Regulation (EU) 2024/1689, AI Act, particularly Articles 51–56

applicable to all GPAI providers and additional requirements applicable to models presenting systemic risk. The latter include obligations relating to model evaluation, systemic risk assessment and mitigation, serious incident reporting, and cybersecurity.

Generative AI also raises particularly difficult questions concerning copyright and intellectual property. The AI Act requires GPAI providers to establish a policy for complying with Union copyright law and to publish a sufficiently detailed summary of the content used to train their models. These requirements attempt to increase transparency around training data while preserving the ability of companies to develop and commercialize general – purpose models.

From an economic perspective, the challenge is to prevent regulatory requirements from becoming so burdensome that they discourage investment in European generative AI development. This is particularly important because the development of advanced models requires substantial computational resources, specialized talent, access to data, and large – scale investment. Excessive regulatory costs could therefore affect smaller European developers and reinforce the market position of large technology companies.

At the same time, insufficient regulation could generate significant economic costs through misinformation, copyright disputes, cybersecurity incidents, discriminatory outputs, or loss of consumer trust. The future effectiveness of AI governance will therefore depend on finding an appropriate balance between innovation incentives and risk mitigation.

The regulatory challenge is consequently not simply determining whether generative AI should be regulated, but how regulation can remain sufficiently flexible to accommodate a technology whose capabilities and applications continue to evolve rapidly.

4.5.2 Foundation models

The emergence of foundation models represents a deeper structural challenge for AI regulation. Foundation models are large – scale models trained on extensive datasets and capable of supporting a wide range of downstream applications. Their importance lies not only in their technological capabilities but also in their position within increasingly complex AI value chains. A single foundation model can serve as the technological basis for numerous products and services developed by different companies, making it difficult to identify where responsibility for potential risks should ultimately lie.

This characteristic creates a significant departure from traditional approaches to technology regulation. Conventional regulatory frameworks often assume a relatively clear relationship between a provider, a product, and its user. Foundation models disrupt this structure because the organization developing the underlying model may differ from the organization integrating that model into a specific AI system and from the final entity deploying the system.

The European Union has responded by introducing a dedicated regulatory category for general – purpose AI models. The AI Act requires providers of GPAI models to prepare and maintain technical documentation, provide information to downstream providers, establish copyright policies, and publish summaries of training content. These requirements seek to increase transparency and enable actors further down the AI value chain to understand the capabilities and limitations of the models they incorporate into their systems.

For the most advanced models, the AI Act introduces additional obligations where the model is considered to pose symmetric risk. These obligations reflect the recognition that certain foundation models may generate risks extending beyond individual applications and potentially affecting multiple sectors simultaneously. Providers must therefore implement mechanisms for evaluating and mitigating systemic risks, reporting serious incidents, and ensuring an appropriate level of cybersecurity.

However, the regulation of foundation models remains technically and legally challenging. One difficulty concerns the identification and measurement of systemic risk. Computational thresholds provide an administratively workable method for identifying potentially powerful models, but computational capacity does not necessarily correspond perfectly to real – world risk. A model with substantial computational requirements may pose limited risks in one context, while a less computationally demanding model could create significant risks when deployed in a sensitive environment.

Recent research illustrates this difficulty. Academic analysis has identified cases in which the application of the AI Act’s systemic – risk criteria to advanced foundation models may remain uncertain, demonstrating the potential limitations of relying on fixed regulatory thresholds in a rapidly evolving technological environment.¹¹⁶

Another challenge concerns the economic concentration of the foundation model market. The high cost of training and operating advanced models creates significant economic scale and may favor a relatively small number of large technology companies. If regulatory compliance adds substantial fixed costs, these requirements could unintentionally reinforce market concentration by making it more difficult for smaller European firms to develop competing foundation models. Conversely, appropriate regulation may also improve competition by increasing transparency and reducing information asymmetries between foundation – model providers and downstream businesses. Clear documentation concerning model capabilities, limitations, training practices, and copyright policies can make it easier for companies to compare providers and select models according to their specific business requirements.

¹¹⁶ Arxiv: “The case for ESM3 as a General – Purpose AI Model with Systemic Risk Under the EU AI Act” (<https://arxiv.org/abs/2605.01611>)

The future challenge is therefore to design a regulatory framework capable of addressing systemic risks without transforming compliance into an excessive barrier to entry. The effectiveness of the European approach will depend on whether regulators can adapt technical thresholds and obligations as model capabilities evolve while preserving sufficient incentives for European research, investment, and competition.

4.5.3 International regulatory coordination

The third mayor challenge for the future of AI governance concerns the international coordination of regulatory frameworks. Artificial intelligence is inherently transnational: AI models can be developed in one jurisdiction, trained using data originating from multiple countries, hosted on infrastructure located elsewhere, and ultimately deployed to users around the world. Consequently, purely national or regional approaches may struggle to address the full range of risks and economic consequences associated with advanced AI.

The comparison developed in this chapter demonstrates the extent of the current regulatory fragmentation. The European Union has adopted a comprehensive risk – based framework, the United States continues to rely on a combination of federal initiatives and sectoral or state – level measures, while China combines targeted regulation with strong state – led technological policy. These differences may create significant compliance challenges for multinational companies operating across several jurisdictions.

Regulatory divergence can generate both direct and indirect economic costs. Companies may need to maintain different governance systems, documentation procedures, risk assessments, and reporting mechanisms depending on the jurisdiction in which their products are offered. This increases compliance expenditure and may discourage smaller companies from expanding internationally. Regulatory fragmentation may therefore reduce some of the economic benefits associated with digital markets, particularly economies of scale and cross – border innovation.

At the same time, complete regulatory harmonization may be neither realistic nor desirable. Different jurisdictions possess different legal traditions, political priorities, institutional structures, and approaches to fundamental rights. The objective of international cooperation should therefore not necessarily be to establish a single global AI law, but rather to promote interoperability between regulatory systems.

Several initiatives demonstrate that international cooperation is already developing. The G7 Hiroshima AI Process¹¹⁷ established an International Code of Conduct for organizations developing advanced AI systems, while the OECD has developed a reporting framework designed

¹¹⁷ OECD (2023), G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI.

to monitor the voluntary application of the Hiroshima Code. In February 2025, the OECD launched the reporting framework as a mechanism for encouraging comparable information on AI risk management, incident reporting, and transparency.

More recent developments indicate that international AI governance is increasingly moving towards interoperability and common reporting practices. The OECD's 2025 analysis of the Hiroshima Process Reporting Framework¹¹⁸ examined submissions from organizations across different sectors and countries, demonstrating the potential for voluntary international mechanisms to create greater consistency in AI risk – management practices¹¹⁹. In 2026, the OECD also introduced a streamlined second version of the framework specifically designed to facilitate participation by small and medium – sized enterprises.¹²⁰

From the perspective of European businesses, international coordination could substantially influence the economic impact of the AI Act. If European requirements become interoperable with international standards, firms may be able to use a single governance framework across multiple markets, reducing duplication and compliance costs. Conversely, if regulatory divergence persists, European companies may face higher costs when expanding beyond the EU, potentially weakening their international competitiveness.

International cooperation may also reinforce the European regulatory model. If principles such as transparency, risk management, accountability, cybersecurity, and responsible innovation become increasingly embedded in international standards. European companies' existing compliance capabilities may become valuable assets in global markets. In this scenario, the regulatory requirements imposed by encouraging European firms to develop advanced AI governance capabilities before equivalent requirements emerge elsewhere.

Ultimately, the future of AI regulation is likely to depend on a combination of domestic regulation and international cooperation. The European Union will remain responsible for enforcing its own legal framework, but its ability to maximize the economic benefits of AI governance will partly depend on its capacity to promote interoperability with other regulatory systems. International coordination therefore represents not only a legal challenge but also a strategic economic opportunity.

The future of AI governance should consequently not be understood as a competition between completely isolated regulatory models. Instead, the emerging regulatory landscape is likely to involve a gradual process of convergence around shared principles. Such convergence could reduce regulatory fragmentation while preserving the distinctive legal and political approaches of

¹¹⁸ OECD (2025), Hiroshima AI Process Reporting Framework.

¹¹⁹ OECD (2025), How are AI developers managing risks?

¹²⁰ OECD: https://www.oecd.org/en/publications/how-are-ai-developers-managing-risks_658c2ad6-en.html

individual jurisdictions. In this context, the European Union's challenge will be to preserve the high level of protection established by the AI Act while ensuring that its regulatory framework remains sufficiently flexible, interoperable, and innovation – friendly to support the international competitiveness of European businesses.

CONCLUSIONS

The rapid development of artificial intelligence has fundamentally transformed the relationship between technological innovation, economic activity, and regulation. AI is no longer a technology limited to specialized research environments but has become an increasingly important component of business strategies, production processes, financial services, healthcare, public administration, and consumer markets. The speed and scale of this transformation have created significant opportunities for productivity, innovation, and economic growth, while simultaneously generating new forms of legal, social, and economic risk.

In this context, the emergence of comprehensive regulatory frameworks has become an unavoidable policy challenge for governments and businesses alike.

This thesis has examined this challenge by focusing on the economic impact of artificial intelligence regulation on European companies, with particular attention to the European Union Artificial Intelligence Act. The analysis has adopted an interdisciplinary perspective combining economic, and managerial considerations to determine whether the regulatory framework introduced by the European Union should ultimately be regarded as a constraint on business activity or as a potential source of long – term competitive advantage. The analysis has considered the evolution and characteristics of artificial intelligence, the development of the European regulatory framework, the costs and benefits associated with compliance, the differentiated impact on small and medium – sized enterprises and large corporations, and the implications of regulation for investment, innovation, and market competitiveness. The analysis was subsequently extended to the regulatory approaches adopted by the United States and China to place the European model within the broader international context.

The central research question of this thesis was whether the regulation of artificial intelligence through the EU AI Act is likely to generate a predominantly positive or negative economic impact on European companies. The findings developed throughout the research suggest that this question cannot be answered through a simple binary distinction. The AI Act undoubtedly creates significant economic costs, particularly in the short term, but it also generates potential benefits that may become increasingly important over time. The ultimate balance between these two dimensions depends on the characteristics of individual firms, the type of AI systems involved, the resources available to businesses, the effectiveness of regulatory implementation, and the ability of companies to integrate compliance into their broader strategic and organizational structures.

The first and most evident economic consequence of the AI Act concerns the costs associated with compliance. Companies developing or deploying AI systems may be required to invest in risk management systems, technical documentation, data governance, transparency mechanisms,

human oversight, cybersecurity, monitoring procedures, conformity assessments, employee training, and legal expertise. These obligations inevitably require both financial resources and organizational effort. Compliance may therefore increase the fixed costs associated with the development and commercialization of AI technologies and, in certain circumstances, may extend the time required to bring innovative products and services to market.

These costs are particularly relevant for small and medium – sized enterprises. SMEs represent a fundamental component of the European economy, but they generally operate with fewer financial resources, smaller workforces, and less specialized legal and technical expertise than large corporations. As a result, the same regulatory obligation can have very different economic consequences depending on the size and organizational structure of the company concerned. A compliance system that represents a manageable investment for a multinational corporation may constitute a significant financial burden for a start – up or smaller technology company. This creates a legitimate concern that regulation could increase barriers to entry and unintentionally favor incumbent firms with greater financial and organizational capacity.

The potential effect on innovation must therefore be taken seriously. AI markets are characterized by extremely rapid technological development, and competitive advantage frequently depends on the ability to experiment, iterate, and commercialize new technologies quickly. Compliance requirements may divert financial and human resources from research and development and may potentially slow product development. This concern becomes particularly relevant when European companies compete with firms operating in jurisdictions characterized by less demanding regulatory frameworks. If European businesses are required to devote significantly more resources to compliance than their international competitors, regulation could generate a competitive disadvantage, particularly in highly dynamic areas such as generative AI and foundation models. However, the existence of regulatory costs does not automatically mean that regulation generates a negative economic outcome. One of the central findings of this thesis is that economic impact of regulation needs to be assessed from a dynamic perspective. A purely short – term analysis focuses on the financial resources required to comply with the law. A dynamic analysis, by contrast, considers whether these investments create institutional, organizational, and technological capabilities that generate value over time.

From this broader perspective, the AI Act may generate several important economic benefits. One of the most important is legal certainty. Before the introduction of the AI Act, businesses operating in the European market faced an increasingly complex regulatory environment involving existing data protection rules, consumer protection, product safety requirements, national initiatives, and sector – specific legislation. The introduction of a common European framework provides greater predictability regarding the obligations applicable to AI systems and reduces the risk of significant

regulatory fragmentation between Member States. This can facilitate long – term investment decisions and allow companies to incorporate compliance requirements into product development and strategic planning from the beginning.

Legal certainty is particularly relevant for investment. Businesses are more likely to commit significant resources to research, development, infrastructure, and commercialization when they can reasonably anticipate the regulatory environment in which their products will operate. A harmonized regulatory framework can therefore reduce uncertainty and transaction costs, potentially increasing the attractiveness of the European internal market for businesses seeking to develop and commercialize AI solutions across multiple Member States.

Another potential benefit concerns consumer trust. Artificial intelligence is characterized by significant information asymmetries because users often lack the technical expertise necessary to evaluate the safety, reliability, transparency, or fairness of complex AI systems. If consumers perceive AI technologies as unpredictable, discriminatory, invasive, or unsafe, they may be less willing to adopt them. Regulation can perform an important market – building function by establishing minimum standards and reducing uncertainty. The requirements introduced by the AI Act concerning transparency, human oversight, data governance, risk management, and accountability can contribute to strengthening trust in AI – enabled products and services.

This is economically relevant because trust can influence demand, adoption, customer loyalty, investor confidence, and relationships between businesses and institutional stakeholders. In markets where consumers increasingly care about how technologies are developed and used, the ability to demonstrate responsible AI governance may become a competitive asset. Compliance may therefore evolve from being merely a legal obligation into a reputational and commercial advantage.

The same logic applies to the reduction of legal and reputational risks. AI systems may generate significant consequences when they produce discriminatory outcomes, violate privacy, create cybersecurity vulnerabilities, or generate inaccurate or harmful outputs. Such incidents can result not only in regulatory sanctions but also in litigation, loss of customers, damage to corporate reputation, and deterioration of investor confidence. The preventive approach adopted by the AI Act may reduce the probability of such incidents by requiring organizations to identify and manage risks before they result in significant harm. The economic value of such risk reduction should therefore be considered when assessing the overall impact of the Regulation.

Another important potential benefit is the promotion of responsible innovation. The AI Act does not simply seek to prevent harmful applications of artificial intelligence; it also seeks to establish the conditions for the development of trustworthy AI. This encourages companies to integrate transparency, accountability, cybersecurity, robustness, human oversight, and risk management

into technological development from the earliest stages. In the long term, such an approach may improve the quality and sustainability of innovation by reducing the likelihood that products will encounter serious legal, ethical, or reputational problems after entering the market.

This dynamic perspective is particularly relevant when considering large companies. Large companies generally possess greater financial resources, specialized compliance departments, large expertise, and technological capabilities. They are therefore better positioned to absorb the initial costs associated with the AI Act. Nevertheless, they also face significant organizational challenges because AI governance must increasingly be integrated across multiple business units, jurisdictions, and technological systems. For these companies, the main challenge may therefore be less about the ability to pay for compliance and more about the ability to coordinate it effectively.

The analysis suggests that large companies may ultimately be able to transform compliance into an organizational capability. Companies that establish responsible AI policies, and compliance – by – design processes may reduce future regulatory risks while simultaneously improving their capacity to respond to technological change. In this context, compliance may gradually shift from being a traditional cost center towards becoming part of the firm’s strategic infrastructure.

The question of competitiveness becomes particularly important at this point. The comparison between the European Union, the United States, and China demonstrates that there is no universally optimal model of AI governance. Each jurisdiction has developed a regulatory approach reflecting different economic, political, and institutional priorities.

The United States has historically adopted a more market – oriented and flexible approach. Rather than relying on a single comprehensive federal framework equivalent to the AI Act, the American system has combined existing legislation, sector – specific regulation, federal initiatives, executive actions, voluntary standards, and state – level legislation. This approach has created an environment in which companies can experiment and commercialize technologies with relatively limited ex – ante regulatory constraints. It has also contributed to the development of a highly dynamic AI ecosystem characterized by significant private investment, strong venture capital activity, and the presence of leading frontier AI companies.

The economic strength of the American model is therefore clear: it provides businesses with substantial flexibility and creates powerful incentives for rapid technological experimentation. The principal disadvantage, however, is the potential for regulatory fragmentation and uncertainty. The absence of a single comprehensive federal framework means that businesses may have to navigate different requirements depending on the sector or state in which they operate. Moreover, the flexibility of the regulatory model does not eliminate risks related to consumer protection, discrimination, privacy, cybersecurity, or accountability.

China represents a fundamentally different model. AI is treated as a strategic national technology and is closely integrated into industrial policy, technological sovereignty, national security, and long – term economic planning. The Chinese state plays a central role in directing AI development through public investment, strategic planning, infrastructure development, research programs, and administrative regulation. This model enables substantial coordination of resources and can support rapid technological development on a scale. At the same time, it involves a much greater degree of governmental control over technological development and business activity.

The European Union therefore occupies a distinctive position between these two models. It does not seek to reproduce the market – oriented flexibility of the United States, nor does it adopt the state – centered approach of China. Instead, it seeks to create a regulated environment in which technological development can occur while fundamental rights, consumer interests, transparency, and public trust are protected.

This difference is important when assessing Europe’s competitive position. The United States currently possesses a significant advantage in private AI investment and frontier commercialization. The 2026 Stanford AI Index reports that U.S. private AI investment reached approximately \$285.9 billion in 2025, compared with \$12.4 billion in China, while the United States also recorded substantially more newly funded AI companies. At the same time, China has rapidly strengthened its position in AI research, publications, patents, and frontier model development, demonstrating that the global competitive environment is becoming increasingly intense.

These figures demonstrate an important point for the interpretation of the AI Act: Europe’s competitive weakness cannot simply be attributed to AI regulation. The European competitiveness gap is the result of a broader set of structural factors, including lower levels of private investment, difficulties in scaling technology companies, limited access to growth capital, fragmentation of capital markets, and challenges in translating academic research into commercially successful technologies. Recent OECD analysis similarly emphasizes the difficulty of converting Europe’s strong scientific capabilities into breakthrough innovation and the importance of strengthening productivity, investment, and the European single market.

Consequently, removing or significantly weakening the AI Act would not automatically solve Europe’s AI competitiveness problem. On the contrary, doing so could sacrifice some of the institutional strengths that Europe possesses without addressing the underlying structural weaknesses of its innovation ecosystem.

The more relevant policy question is therefore whether Europe can combine the strengths of its regulatory model with a much stronger innovation and investment strategy. The AI Act should not be viewed as a substitute for industrial policy, but as one component of a broader European

strategy for artificial intelligence. Regulation alone cannot create globally competitive AI companies. Europe also needs stronger investment in research and development, computing infrastructure, digital infrastructure, talent, venture capital, scale – up financing, and mechanisms capable of transforming scientific excellence into commercial innovation.

This distinction leads to an important qualification of the thesis’s central conclusion. The AI Act is positive, but it is not sufficient. Its potential benefits depend on the existence of an economic environment capable of allowing European businesses to exploit them.

The future evolution of artificial intelligence makes this issue even more important. Generative AI and foundation models are already challenging traditional approaches to regulation because the same underlying technology can support many applications with very different levels of risk. The AI Act has responded by introducing specific obligations for providers of general – purpose AI models, including requirements concerning technical documentation, copyright policies, training – data summaries, and, for models presenting systemic risk, additional obligations concerning risk assessment, incident reporting, and cybersecurity. These obligations became applicable from August 2025.

However, the technological environment will continue to evolve faster than traditional legislative processes. Future AI systems may become increasingly autonomous, capable of planning and executing complex sequences of actions, interacting with other systems, and operating with progressively greater levels of independence from direct human supervision. This development could challenge existing assumptions concerning accountability, liability, human oversight, and risk classification.

The future of AI regulation must therefore be adaptive rather than static. A regulatory framework that is excessively rigid risks becoming technologically outdated, while a framework that is excessively vague risks creating legal uncertainty. The European Union will need to rely increasingly on technical standards, regulatory guidance, experimentation, regulatory sandboxes, and evidence - based implementation to maintain the relevance of the AI Act as technology develops.

This adaptability will also be essential for maintaining competitiveness. If compliance requirements become unnecessarily complex or disproportionate, they may reinforce barriers to entry and discourage investment in European AI development. Conversely, if regulation becomes sufficiently predictable and flexible, companies may be able to incorporate compliance into their technological architecture without experiencing excessive delays or costs.

International regulatory coordination will represent another decisive factor. AI development is inherently global: models can be developed in one country, trained on internationally sourced data, hosted on infrastructure located elsewhere, and deployed simultaneously across numerous

jurisdictions. Divergent regulatory requirements can therefore generate significant compliance costs for multinational businesses. The OECD has emphasized the potential economic costs associated with fragmented or overlapping digital regulation and the importance of regulatory coherence in supporting innovation and productivity.

For Europe, international coordination is consequently not merely a diplomatic objective but an economic necessity. If European standards become increasingly interoperable with international standards, European firms may be able to use their AI governance capabilities across multiple markets, thereby reducing duplication and increasing the economic return generated by compliance investments. Conversely, if regulatory divergence between Europe, the United States, China, and other jurisdictions become excessive, European firms may face higher costs when expanding internationally.

The most appropriate European strategy should therefore not necessarily be to impose the AI Act as a global regulatory model in its entirety. Instead, Europe should seek greater regulatory interoperability through common terminology, technical standards, risk management principles, reporting mechanisms, and international cooperation. This would allow the EU to preserve its high level of protection while reducing unnecessary barriers to international business activity.

Taking all these considerations together, the central question can now be answered more explicitly.

Is the EU AI Act positive or negative for European companies?

The answer is that the AI Act is positive overall in the long term, but conditionally so.

It is negative in certain short – term dimensions. It increases compliance costs, creates administrative obligations, requires organizational adaption, and may slow the development or commercialization of certain AI systems. These effects are particularly relevant for SMEs, start – ups, and companies operating in highly competitive areas of AI development. The Regulation may therefore generate a temporary competitive disadvantage compared with firms operating in less regulated environments.

However, the AI Act also creates significant potential benefits. It increases legal certainty, harmonizes the European internal market, promotes consumer trust, reduces certain legal and reputational risks, and encourages responsible innovation. These benefits may become increasingly valuable as AI adoption expands and stakeholders become more concerned about safety, transparency, accountability, and reliability.

The overall assessment can therefore be summarized as follows:

Dimension	Short – term effect	Long – term potential	Overall assessment
Compliance costs	Negative	May decrease through	Negative initially

		organizational learning	
Administrative burden	Negative	Can become integrated into corporate governance	Mixed
Innovation speed	Potentially negative	Responsible innovation may improve quality	Mixed
Legal certainty	Moderate	Strong positive effect	Positive
Consumer trust	Limited initial effect	Strong positive potential	Positive
Reputational risk	Positive	Increasingly valuable	Positive
Market harmonization	Positive	Stronger cross – border opportunities	Positive
SME competitiveness	Potentially negative	Depending on support mechanisms	Risk
Large – company competitiveness	Manageable cost	Potential strategic advantage	Positive
International competitiveness	Potential short – term disadvantage	Potential advantage if standards converge	Mixed/positive
Responsible innovation	Initial compliance cost		

The table illustrates why a simple classification of the AI Act as either “good” or “bad” would be economically misleading. The Regulation produces different effects depending on the time horizon and the characteristics of the firm. The same compliance requirement that represents a cost today may generate an organizational capability tomorrow. The same regulatory standard that initially slows market entry may subsequently increase consumer confidence and market adoption. The same European requirement that appears restrictive compared with the United States may become an international competitive asset if trustworthy AI becomes a global market expectation. The most convincing interpretation is therefore to consider the AI Act as an institutional investment rather than merely a regulatory cost. Like any investment, however, it requires an initial expenditure and does not guarantee a return. The return depends on how effectively the regulatory framework is implemented and on whether complementary economic policies can strengthen Europe’s innovation ecosystem.

This leads to the most important policy implication emerging from this thesis: *the principal risk for Europe is not regulation itself, but regulation without innovation policy.*

If the AI Act is implemented rigidly, generates disproportionate administrative costs, and is accompanied by insufficient investment in research, infrastructure, talent, computing capacity,

and scale – up financing, it could reinforce Europe’s existing competitive weaknesses. Under such circumstances, the Regulation could become a barrier to innovation rather than an enabler of it.

If, on the other hand, the AI Act is implemented proportionately, supported by clear guidance and technical standards, accompanied by effective support for SMEs and start – ups, and integrated into a broader European industrial and innovation strategy, its potential economic benefits become significantly greater.

For European businesses, this also implies a change in managerial perspective. AI compliance should increasingly be understood not simply as a legal function but as a part of corporate strategy. Companies that develop internal AI governance capabilities early may reduce future compliance costs, improve risk management, strengthen stakeholder trust, and become better prepared for future regulatory developments. In this sense, the most successful European companies may be those that move from a model of “compliance as an obligation” towards “compliance as an organizational capability.”

Ultimately, the European Union does not need to choose between regulation and innovation. The real challenge is to demonstrate that regulation can enable sustainable innovation rather than suppress it.

The United States provides an important lesson concerning the value of flexibility, entrepreneurship, private investment, and rapid commercialization. China demonstrates the importance of strategic coordination, infrastructure, long – term investment, and technological policy. Europe possesses different institutional strengths: a large integrated market, a strong legal framework, significant scientific capabilities, and the ability to establish common regulatory standards across Member States. The optimal European strategy should therefore not copy either model but combine elements of their strengths while preserving the principles underlying the European approach.

The final answer to the research question can consequently be formulated as follows:

The EU AI Act is likely to generate a mixed economic impact on European companies in the short term but a predominantly positive impact in the long term, provided that its implementation remains proportionate, flexible, technologically adaptable, and supported by complementary policies aimed at strengthening European innovation and investment capacity. The Regulation creates real compliance costs and may temporarily reduce the speed and flexibility of European AI development. Nevertheless, its contribution to legal certainty, consumer trust, market harmonization, risk reduction, and responsible innovation can generate significant long – term economic value. The AI Act should therefore be regarded not simply as a constraint of European businesses, but as a potential strategic asset whose success depends on Europe’s ability to

transform regulatory compliance into innovation capabilities and competitive advantage.

The future position of Europe in the global AI economy will not be determined by the AI Act alone. It will depend on whether Europe can successfully combine trust with innovation, regulation with investment, and legal protection with economic competitiveness.

The ultimate challenge is not to create the least regulated AI market, nor necessarily the most regulated one. It is to create the most sustainable and competitive AI ecosystem.

If Europe succeeds in achieving this balance, the AI Act may become more than a regulatory instrument. It may become the institutional foundation of a European model of artificial intelligence in which technological innovation, economic value, fundamental rights, and public trust reinforce rather than undermine one another.

In this sense, the long – term success of the AI Act will ultimately depend not on how much regulation Europe has created, but on how effectively Europe converts regulation into trust, trust into adoption, adoption into innovation, and innovation into sustainable economic competitiveness.

BIBLIOGRAPHY

- Bassamani et al. (2021), “On the Opportunities and Risks of Foundation Models.”
- Lee, J., Bagheri, B., & Kao, H.-A. (2015): “A Cyber – Physical Systems Architecture for Industry 4.0”
- AI Act, art.3 – definition of AI Systems
- OECD (2024), updated OECD Definition of an AI System
- Russell & Norvig (2021), “Artificial Intelligence: a modern approach”
- McCarthy, J. (2007), “What is artificial intelligence?”
- Crevier, D. (1993), “AI: The Tumultuous History of the Search for Artificial Intelligence”
- Agrawal, Gans & Goldfarb (2018), “Prediction Machines”
- Brynjolfsson & McAfee (2014), “The Second Machine Age”
- Mayer-Schönberger & Cukier (2013), “Big Data”
- Klaus Schwab, “The Fourth Industrial Revolution”
- Brynjolfsson, Rock & Syverson (2021), “The Productivity J-Curve”
- European Commission, “White Paper on Artificial Intelligence” (2020).
- Lee, J., Bagheri, B., & Kao, H.-A. (2015). “A Cyber-Physical Systems Architecture for Industry 4.0”.
- Financial Stability Board (2017). “Artificial Intelligence and Machine Learning in Financial Services”
- OECD reports on AI in finance.
- Topol, E. (2019). “Deep Medicine”
- World Health Organization (2021). “Ethics and Governance of Artificial Intelligence for Health.”
- McKinsey Global Institute (2023). The Economic Potential of Generative AI.
- European Commission (2020) – White Paper on Artificial Intelligence: A European approach to Excellent and Trust
- Floridi, L., et al. (2018): “AI4People—An Ethical Framework for a Good AI Society”
- High-Level Expert Group on AI (2019): Ethics Guidelines for Trustworthy AI
- National Institute of Standards and Technology (2023). AI Risk Management Framework.
- Cyberspace Administration of China (2023). Interim Measures for the Management of Generative Artificial Intelligence Services.
- Cath, C. et al. (2018). Artificial Intelligence and Good Society.
- OECD (2019) - Recommendation of the Council on Artificial Intelligence
- High-Level Expert Group on AI (2019). Ethics Guidelines for Trustworthy AI.
- European Commission (2020). White Paper on Artificial Intelligence.
- AI Act (Regulation (EU) 2024/1689).
- Smuha, N. A. (2021). From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence.
- Floridi, L. (2019). Establishing the Rules for Building Trustworthy AI.
- Hacker (2023), The European AI Liability Framework
- Commission Proposal (2021).
- European Parliament Amendments (2023).
- Council of the EU Negotiating Position
- Final AI Act (2024).

- AI Act (Regulation (EU) 2024/1689), 26–40
- AI Act, Article 5 (Prohibited AI Practices).
- Pasquale, F. (2015). *The Black Box Society*
- Annex III (High-Risk AI Systems).
- AI Act, Articles 6–29.
- AI Act, Article 50 (Transparency Obligations).
- AI Act (Regulation (EU) 2024/1689), Chapter III (Requirements for High-Risk AI Systems).
- AI Act, Chapter IV (Obligations of Providers and Other Operators).
- OECD (2019). *OECD AI Principles*
- AI Act, Article 9 (Risk Management System).
- ISO/IEC 23894:2023 – Artificial Intelligence — Guidance on Risk Management.
- AI Act, Article 10 (Data and Data Governance).
- Floridi, L. (2016). *Data Ethics*.
- AI Act, Article 13 (Transparency and Provision of Information).
- AI Act, Article 50 (Transparency Obligations for Certain AI Systems).
- AI Act, Article 14 (Human Oversight).
- Regulation (EU) 2024/1689 (AI Act): Chapter VIII – EU Governance of AI
- Regulation (EU) 2024/1689 (AI Act): Chapter IX – Post-Market Monitoring, Information Sharing and Market Surveillance
- AI Act, Articles 64–67 (European AI Office e governance dei General-Purpose AI Models).
- AI Act, Chapter XII – Penalties.
- Regulation (EU) 2016/679 (GDPR).
- European Data Protection Board (EDPB), *Guidelines on Automated Decision-Making and Profiling*.
- Regulation (EU) 2022/2065 (Digital Services Act).
- Regulation (EU) 2022/1925 (Digital Markets Act).
- Cr mer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition Policy for the Digital Era*.
- Regulation (EU) 2023/2854 (Data Act).
- Regulation (EU) 2024/2847 (Cyber Resilience Act).
- Djankov, S. et al. (2002). *The Regulation of Entry*
- Stigler, G. J. (1971). *The Theory of Economic Regulation*.
- Aghion, P., & Howitt, P. (1998). *Endogenous Growth Theory*
- Porter, M. E., & van der Linde, C. (1995). *Toward a New Conception of the Environment–Competitiveness Relationship*.
- Blind, K. (2016). *The Impact of Regulation on Innovation*.
- Ashford, N. A., & Hall, R. P. (2011). *Technology, Globalization and Sustainable Development*.
- Gunningham, N., Grabosky, P., & Sinclair, D. (1998). *Smart Regulation: Designing Environmental Policy*.
- Baldwin, R., Cave, M., & Lodge, M. (2022). *Understanding Regulation*
- AI Act, Articles 8–29 (Requirements for High-Risk AI Systems).
- Deloitte (2024). *State of Generative AI in Enterprise (for investments in governance and compliance)*.
- AI Act, Articles 9–15, 17, 19, 20, 72 (risk management, documentation, post-market monitoring e reporting).
- PwC (2024). *Responsible AI Survey*.

- IBM (2023). Global AI Adoption Index.
- AI Act, Articles 10–15 (data governance, technical documentation, transparency, human oversight, accuracy, robustness and cybersecurity).
- European Commission. Annual Report on European SMEs.
- Deloitte (2024). State of Generative AI in the Enterprise (regarding the gap between large enterprises and SMEs).
- AI Act, Chapter III (Requirements for High-Risk AI Systems).
- AI Act, Chapter IV (Obligations of Providers and Other Operators).
- European Commission. Digital Europe Programme. European Innovation Council (EIC) Programme.
- European Digital Innovation Hubs (EDIHs).
- Regulation (EU) 2024/1689 (AI Act).
- AI Act, Chapter VIII (Governance).
- AI Act, Articles 9–15, 17, 72 (risk management, documentation, monitoring and governance).
- NIST. AI Risk Management Framework 1.0 (2023).
- ISO/IEC 42001:2023 — Artificial Intelligence Management System (AIMS).
- AI Act, Articles 13–15 (Transparency, Human Oversight, Accuracy, Robustness and Cybersecurity).
- European Commission (2021). Impact Assessment Accompanying the Proposal for the AI Act.
- UNESCO. Recommendation on the Ethics of Artificial Intelligence (2021).
- European Commission (2021). Impact Assessment Accompanying the Proposal for the AI Act
- AI Act, Chapter III (Requirements for High-Risk AI Systems).
- Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a Framework for Responsible Innovation.
- Blind, K. (2012). The Influence of Regulations on Innovation: A Quantitative Assessment for OECD Countries. Research Policy.
- Ashford, N. A., & Hall, R. P. (2011). Technology, Globalization, and Sustainable Development.
- Smuha, N. A. (2021). From a “Race to AI” to a “Race to AI Regulation”.
- Executive Order 14110 (2023), Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
- NIST AI Risk Management Framework 1.0 (2023).
- Federal Trade Commission (FTC), policy statements on AI.
- Blueprint for an AI Bill of Rights (2022).
- Colorado AI Act (2024).
- Provisions on the Administration of Deep Synthesis Internet Information Services (2023).
- Provisions on the Administration of Algorithmic Recommendation Services (2022).
- New Generation Artificial Intelligence Development Plan (2017).
- “14th Five-Year Plan for Economic and Social Development and Long – range Objectives Trough the Year 2035 of People’s Republic of China (2021–2025).”
- Provisions on Algorithmic Recommendation Services (2022).
- Provisions on Deep Synthesis Internet Information Services (2023).
- Interim Measures for the Management of Generative Artificial Intelligence Services (2023).
- Deloitte (2024). State of Generative AI in Enterprise
- OECD (2023–2024). Digital Economy Outlook e AI Policy Observatory
- GDPR (Regulation (EU) 2016/679), for comparison on Brussels Effect.

- Charter of Fundamental Rights of the European Union.
- Regulation (EU) 2024/1689, AI Act, particularly Articles 51–56
- OECD (2023), G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI.
- OECD (2025), Hiroshima AI Process Reporting Framework.
- OECD (2025), How are AI developers managing risks?

SITOGRAPHY

Arxiv: “The case for ESM3 as a General – Purpose AI Model with Systemic Risk Under the EU AI Act”

(<https://arxiv.org/abs/2605.01611>)

<https://digital-strategy.ec.europa.eu/en/factpages/general-purpose-ai-obligations-under-ai-act>

OECD: https://www.oecd.org/en/publications/how-are-ai-developers-managing-risks_658c2ad6-en.html

EU AI Act: <https://artificialintelligenceact.eu/>