LUISS

Master's Degree program in Global Management and Politics

Course of Corporate Strategy

The Impact of Artificial Intelligence Regulation in the Tech Sector: The European Union AI Act Case

Prof. Paolo Boccardelli

SUPERVISOR

Prof. Domenico Pauciulo

CO-SUPERVISOR

Simone Pietro Ciccolella - 776191

CANDIDATE

Academic Year 2025/2026

TABLE OF CONTENTS

Ad Antonio, Elena Maria, Marianna, Dominique e Nonna Mimina.

A Nonno Pietro, Nonna Maria, Nonno Renato e Zio Michele.

Alla famiglia che era, è e sarà.

A Wassenaar, Molfetta, Roma, Ginevra e New York.

Dove sono cresciuto.

A Luca e a Marco.
Grazie.

"Principium cuius
hinc nobis exordia
sumet,
nulla rem e nihilo
gigni divinitus
umquam."

(Tito Lucrezio Caro, De rerum natura I, 149 -150)

Introduction

In an era marked by rapid technological developments, a deeply unstable geopolitical climate, and an increasingly evident shift in the global economic balance across world powers, the regulation of artificial intelligence stands as one of the most decisive challenges of the 21st century. In the current global order undergoing transition, the European Union occupies an ambitious and, at the same time, peculiar role. With the entry into force on August 1, 2024, of Regulation (EU) 2024/1689, commonly known as the AI Act, the Union has positioned itself as the first global actor to establish a thorough and binding legal framework governing artificial intelligence systems.

However, the regulatory institutionalization of artificial intelligence establishes a new level of legal and strategic complexity. The AI Act is based on a risk-based approach that classifies AI systems according to their potential impact, establishes documentation obligations, procedural requirements, monitoring mechanisms, and significant penalties for non-compliance. While stating the goal of promoting "trustworthy AI" and supporting innovation, the European regulation is part of an already extremely dense European digital regulatory ecosystem, which includes instruments such as the GDPR, the DMA, the DSA, the Data Act, the Data Governance Act, and the Digital Europe Programme. Furthermore, AI systems are evolving at a pace that may surpass regulatory adaptation: the unpredictability of their evolution poses various difficulties from a legal and corporate perspective, as new technological developments may render existing provisions obsolete. In this new context, companies find themselves immersed in interpretative ambiguities and temporal uncertainties linked to the progressive implementation of the provisions.

The initial reactions from the private sector, particularly from tech companies that develop and deploy AI systems, have highlighted these tensions.

In July 2025, 58 European technology companies requested, through a letter to the European Commission, a temporary two-year suspension of the AI Act before obligations on high-risk AI systems and general-purpose AI models enter into force: "Stop the clock!" According to the signatories, Europe's traditional balance between regulation and innovation is being disrupted by unclear, overlapping, and increasingly complex EU rules, which risk undermining the development of tech companies and limiting firms'

ability to deploy AI at scale, with significant implications for their corporate strategies (EU AI Champions Initiative, 2025).

The technology sector in Europe has risen considerably and is now playing a bigger role in the continent's economy. Europe's growing potential as a worldwide technological leader is demonstrated by the $426 billion that European technology businesses have raised in the last decade (Invest Europe, 2024). This remarkable growth is reflected by the value of the European tech sector, which is close to 4 trillion dollars (Invest Europe, 2025).

In this context, the AI Act is not only a legal instrument but also an institutional intervention capable of influencing companies' innovation strategies.

Despite growing academic and political interest in European digital regulation, gaps remain in how tech companies currently perceive the impact of the AI Act on their corporate strategies.

Previous studies have analyzed the impact of regulations such as the GDPR on business models and investment priorities (Lindgren, 2018; Blind et al., 2024), but there is a lack of empirical evidence on how tech companies are redefining their innovation strategies in response to the AI Act. Furthermore, while previous digital regulatory waves have led to the creation of new internal governance structures (Ullagaddi, 2024), it is still unclear how companies are reconfiguring roles, skills, and organizational capabilities to integrate or anticipate the AI Act's requirements within everyday management practices. Finally, the Institution-Based View, a theoretical framework widely used to explain corporate behavior in regulated contexts (Peng et al., 2009), has not yet been applied to the AI Act as a formal institution in continuous evolution. These gaps show that the AI Act has not yet been investigated as a lived and changing institutional experience within tech companies.

In this regard, the objective of this thesis is to understand how the AI Act shapes strategic innovation within technology companies operating in the European Union. In particular, this study aims to understand the mechanisms through which regulatory pressures interact with organizational structures, managerial choices, and either competitive or innovation strategies in the tech sector.

In line with these objectives, this thesis addresses the following research question: "To what extent does the European AI Act influence strategic innovation in tech companies,

balancing regulatory constraints with opportunities for organizational and managerial transformation?"

To address the research question, the analysis focuses on the relationship between institutions and corporate strategy. On a theoretical level, the thesis adopts the Institution-Based View as its main theoretical framework, which conceives institutions as "rules of the game" and as "independent variables" that reduce uncertainty and ensure stability, often causing companies to adopt similar behaviors (DiMaggio & Powell, 1983; North, 1990; Scott, 1995; Tywoniak & Peng, 2006; Peng et al., 2009). Given the uniqueness of the AI Act in regulating a subject that had never been regulated before, the theoretical framework is refined, extending it with new features adapted to the regulation itself.

For this purpose, this thesis adopts an abductive methodology from Timmermans & Tavory (2012) to answer the research question. In order to produce new theoretical insights, abductive analysis relies on an iterative movement between empirical data and theory. It is based on three methodological operations: "revisiting", which involves a continuous examination of empirical data through various theoretical lenses; "defamiliarization", in which the researcher distances themselves from conventional interpretations; and "alternative casing", which entails reframing empirical situations using alternative theoretical explanations. Theoretical regeneration, which improves current theoretical frameworks to better explain observed empirical patterns, is a crucial result of this process.

In this thesis, empirical data were collected through eleven in-depth interviews with legal experts in digital legislation, EU institutional representatives, an officer from an Italian Ministry, senior managers (including C-level executives), AI governance professionals, and public policy actors within technology companies developing or deploying AI systems and general-purpose AI models under the AI Act. The interview material was analyzed using qualitative data analysis software (MAXQDA) through iterative coding cycles. The "revisiting" phase involved open coding, generating 375 initial codes, which were progressively consolidated through "defamiliarization" into 47 codes and subsequently into 20 parent codes.

The thesis is structured as follows.

Chapter 1 (Literature review) develops the theoretical framework of the thesis, analyzing the conceptual approach of IBV and its fundamental components. The analysis continues

with a critical and structured review of studies that apply the IBV to contexts of technology and digital innovation. In addition, the chapter provides a comprehensive analysis of the EU digital regulation landscape, rebuilding its past evolution and its current and prospective impacts on companies. In particular, it examines the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Act, the Data Governance Act, and the Digital Europe Programme, in order to understand how companies have already perceived the previous regulations.
This reconstruction makes it possible to outline the institutional and regulatory context within which the Artificial Intelligence Act operates.
Chapter 2 is devoted to a brief contextual analysis of the AI Act, reconstructing the reasons that led to the adoption of harmonized regulations at the European level, the objectives, scope of application, and governance structure.
Chapter 3 (Methodology and results) acts as a bridge between the theoretical-regulatory part and the interpretative analysis of the thesis. It transparently describes the qualitative research design based on abductive logic, alongside the sample selection and data collection. Finally, it reconstructs the data analysis through the coding process and presents the results organized into five themes: "Regulatory and institutional capacity gaps," "Uneven innovation environments for tech companies," "The need for collaboration between technical and institutional actors", "Strategic repositioning of European tech companies," and "The AI Act: an enabler of strategic innovation?" with relevant quotes extracted from the interviews.
Chapter 4 (Discussion) revises the empirical results that emerged in Chapter 3 through the "alternative casing" phase typical of abductive methodology, reinterpreting the five themes identified in light of two guiding concepts: AI governance under the AI Act and the Institution-Based View. The chapter shows how the evidence collected confirms the fundamental assumptions of the IBV, clarifying the role of formal and informal institutions in influencing the strategic choices of companies in the tech sector. Secondly, it develops the theoretical contribution of the thesis, arguing that in highly dense regulatory contexts and in the presence of rapid technological change, the AI Act does not necessarily reduce uncertainty and produces uneven impacts. On this basis, the chapter proposes a new process model that explains how the AI Act influences strategic innovation in tech companies through four mechanisms: "Interpretative and operational

uncertainty", "Temporal misalignment and instability", "Asymmetric institutional environments", and "Institutional co-evolution". For each of these mechanisms, the current corporate adaptation innovation strategies are presented. Finally, taking into account the new process model, recommendations are made for EU policymakers and tech company managers, closing with the limitations of the research and possible directions for future research. Lastly, the Conclusion serves as a summary of the work that connects the major takeaway to the research question and the general literature examined.

Chapter 1

Literature review

The institutional context in which firms operate is often overlooked and undervalued in strategic discussions. Institutions are frequently regarded as peripheral to the economic and corporate ecosystem, which is presumed to function independently of them (Olsen, 2009).

However, such an assumption is fundamentally flawed. Institutions do not simply constitute a passive setting; they play an active role in shaping the strategic landscape within which businesses operate. Indeed, an inextricable link exists between institutional frameworks and private enterprises: the regulatory paradigm that dictates the boundaries and conditions of corporate strategic operations.

In recent years, the regulation of technology and digital innovation has emerged as an essential and unavoidable concern for governments and businesses (Bradley - Silverio Donato, 2024).

Regulatory frameworks have become significant factors in competitive dynamics, inducing firms to function within an environment characterized by continual transformation and, at times, substantial uncertainty. As technological advancements accelerate, so do the institutional responses seeking to govern their implications. Recognizing this interaction between institutional forces and corporate strategy is essential for grasping how firms adapt and innovate, thus maintaining a competitive edge.

This chapter is therefore dedicated to exploring the theoretical framework of the Institution-Based View (IBV) in the context of technology and digital innovation. An introductory analysis of IBV and its key components will be conducted, considering that this theory has gained increasing academic credit in recent years (Peng et al., 2023). Subsequently, a methodical literature review will be undertaken to examine the application of IBV to technology and digital innovation, utilizing a theoretical lens supported by empirical examples and case studies. Then, the discussion centers on the critical role of informal networks and lobbying as strategic mechanisms through which firms gain legitimacy, particularly in contexts characterized by weak or underdeveloped formal institutions.

Finally, Chapter 1 concludes with a comprehensive literature review on the regulation of technology within the European Union and its past, present, and anticipated impact on business. Particular attention is devoted to the regulatory context in which tech enterprises operate, what could be called the normative environment shaping corporate behavior, and to how businesses have responded, are currently responding, and are expected to respond to major legislative instruments such as the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Act, the Data Governance Act, and the Digital Europe Programme.

This review is purposeful: it seeks to understand how the business ecosystem, embedded within an evolving normative framework, has metabolized the regulatory pressure of past and present EU digital legislation. Such understanding is indispensable before shifting the lens to the primary subject of this thesis: the Artificial Intelligence Act.

In other words, this chapter lays the groundwork for the following ones. To understand the potential implications of the AI Act, one must first examine the digital regulatory pathways already travelled by European enterprises. This chapter will draw from a broad spectrum of academic sources, including seminar papers, peer-reviewed journal articles, business reviews, and university studies.

1.1 Theoretical framework: Institution-Based View (IBV)

1.1.1 Definition and Components of IBV

The role of institutions cannot be relegated to the backdrop, they are much more. Institutions tell us why companies are different from each other, considering competitive advantage. This is precisely why the need for the theoretical framework of the Institution-Based View has emerged.

The Institution-Based View (IBV) is a theoretical framework that emphasizes the role of institutions in shaping corporate strategies and firm performance. It argues that institutions, both formal (laws, regulations, property rights) and informal (norms, cultures, ethics), are not mere background conditions but active determinants of firm behavior and strategic decision-making (Peng et al., 2009). The IBV, acting as a "third leg", stands in contrast to, yet complements, the other two dominant strategic perspectives: the Industry-Based View and the Resource-Based View (RBV) (Peng et al., 2009). While the Industry-Based View focuses on external competitive forces (Porter,

1998) and the RBV emphasizes internal firm capabilities (Barney, 1991), the third one highlights the importance of the regulatory and sociopolitical environment in which firms operate (Garrido et al., 2020).

In the first two theories, there is a lack of attention to the institutional contexts in which companies find themselves. But sometimes, it is precisely the institutions that facilitate the achievement of competitive advantage for companies. But what is meant by "institutions"?

Institutions are often described as "the rules of the game" that structure economic and social interactions (North, 1990). On the contrary, they were very often seen as "background conditions" (Williamson, 1993).

Scott (1995), instead, categorized institutions into three pillars: the regulative pillar, which includes formal rules, laws, and governance structures that constrain and enable firm behavior; the normative pillar, which consists of social norms, values, and expectations that shape acceptable behavior within industries; and the cognitive pillar, which comprises shared beliefs and assumptions that influence strategic decision-making at a subconscious level (Scott, 1995).

Institutions have the fundamental task of reducing uncertainty and ensuring stability by defining norms of behavior and the boundaries of what is and is not permitted (Peng et al., 2009).

The IBV is rooted in the broader intellectual movement of new institutionalism, which has gained traction across social sciences as many economists like North (1990) and sociologists like Scott (1995) have increasingly acknowledged that market structures and firm capabilities alone cannot fully explain business success or failure (Peng et al., 2009).

The pharmaceutical sector in Japan provides a powerful example of this. Japan's pharmaceutical industry has trailed behind in attaining comparable world-class status, despite the country producing globally renowned inventions in industries like electronics and autos. Institutional factors, such as a national healthcare system that does not provide incentives for the research and commercialization of "novel drugs", are more responsible for this disparity than company capabilities or industry conditions alone (Peng et al., 2009).

This demonstrates how institutional settings can either support or impede strategic innovation in different sectors.

The impact of institutions is particularly visible in emerging markets, where regulatory frameworks are often weak or evolving. Unlike developed economies, where market-supporting institutions are stable and well-defined, emerging economies present high institutional uncertainty, requiring firms to dive into complicated legal landscapes (Garrido et al., 2020).

This has led to increased research interest in IBV as a tool to understand firm behavior under varying institutional conditions. Indeed, the rise of IBV as a dominant strategic framework can be attributed to external and internal forces within strategic management research.

Internal forces stem from criticism of the Industry-Based View and RBV for their lack of attention to the institutional context. The former, for instance, assumes that firms operate within a well-defined market structure, yet it fails to account for institutional voids, government interventions, and informal business practices that significantly impact competitive dynamics (Peng et al., 2009). Similarly, the RBV, which focuses on firm-specific resources and capabilities, has been challenged for its assumption that valuable resources remain valuable across all contexts. However, what constitutes a strategic resource in one institutional environment may not hold the same value in another. Externally, a driver behind the rise of IBV is globalization (Garrido et al., 2020). As firms expand into international markets, they encounter diverse institutional landscapes that affect entry strategies and governance structures. Institutions determine how firms establish operations and engage in partnerships. The IBV provides a framework for understanding how institutional differences shape cross-border investments and strategic alliances (Garrido et al., 2020).

According to Peng et al. (2009), the IBV is based on two core propositions, which we can define as components.

Proposition I assert that "*managers and firms rationally pursue their interests and make strategic choices within the formal and informal constraints in a given institutional framewor*k" (Peng et al., 2009).

Peng et al. (2009) give the example of CEO compensation in the United States during the 2008-2009 economic crisis, when executives were paid $18 billion in bonuses while the average American suffered heavy losses. But the CEOs' decision was rational; they did not break any laws, and they pursued their interests. The basic principle of the IBV is

reflected in this proposition: strategic decisions have roots in an institutional framework. Although managers and businesses behave logically, official regulations and informal norms influence and limit this rationality. As a result, actions that appear illogical or contentious (like the CEO bonuses instance) may be a calculated reaction that fits within the institutional framework.

Proposition II states that "*While formal and informal institutions combine to govern firm behavior, in situations where formal constraints are unclear or fail, informal constraints will play a larger role in reducing uncertainty, providing guidance, and conferring legitimacy and rewards to managers and firm"* (Peng et al., 2009). This explains the constant interaction between formal and informal institutions, which broadens the IBV perspective. It implies that informal institutions take center stage when formal regulations are lax, or there are unclear situations that are frequently present in developing nations or during emergencies. Social norms, relationships founded on trust, religious beliefs, or unspoken rules of behavior are a few examples. In these situations, businesses depend on these unofficial frameworks to lower uncertainty, direct strategic choices, and acquire credibility with stakeholders.

These two propositions demonstrate how businesses negotiate formal and informal institutional limits in order to obtain legitimacy.

Furthermore, isomorphism is one of the renowned theoretical processes that helps to explain this institutional alignment in business behavior. It's a process for understanding how corporations behave strategically in institutional settings. DiMaggio & Powell (1983) introduced the term "isomorphism," which refers to the processes by which organizations look like one another and conform to institutional forces to acquire legitimacy. There are three primary types: normative isomorphism, which comes from common professional ideals and norms; mimetic isomorphism, which happens when businesses copy effective techniques in uncertain situations; and coercive isomorphism, which is produced by legal and regulatory restraints (DiMaggio & Powell, 1983).

These factors support the IBV theory, which holds that businesses are formed to meet both formal and informal institutional expectations rather than operating disconnected from a strategy context.

1.1.2 The role of networks and lobbying in the IBV

The importance of informal institutions, especially networks and interpersonal interactions, is highlighted as a crucial mechanism for strategic adaptation in contexts where formal institutions are inadequate or underdeveloped in the IBV presented by Peng et al. (2009). In these situations, businesses depend more and more on unofficial social connections to support business dealings and maintain continuity, particularly when there is an institutional shift. For example, when official systems collapsed in post-Soviet Russia, entrepreneurs relied on local ties (blat) to sustain commercial operations (Peng et al., 2009). In addition to filling in for the lack of official support, these unofficial networks make it possible to recognize opportunities, even in dubious or grey areas of the economy. Emerging economies are not the only ones that rely on informal techniques. Informal contacts have a big impact on corporate conduct, especially in political arenas, even in sophisticated economies. According to research, U.S. defense companies make a significant profit from lobbying, making $28 for every $1 invested, proving that unofficial political connections can be more profitable than conventional market-based investments (Peng et al., 2009). Additionally, according to the IBV, businesses may still be successful by using unofficial political tactics if they are unable to gain a competitive edge through pricing, differentiation, or product market focus. In the end, the strategic use of networks and alliances, whether referred to as political lobbying in the US or guanxi in China, showcases how informal institutions offer businesses alternate routes to success and growth, lower uncertainty, and provide crucial legitimacy (Peng et al., 2009).

In the case of Acer, which will be analyzed in the next paragraph, the significance of informal institutions, particularly those ingrained in Taiwan's family business culture, is intrinsically related to the company's ascent to prominence as a dragon multinational (Hung & Tseng, 2017). A networked environment where horizontal relationships among enterprises have become structurally institutionalized has been fostered by Taiwan's institutional architecture, which is formed by a mercantile economy dominated by small and medium-sized corporations. In the past, these unofficial networks, which are based on affiliation ties and alumni connections, have made up for market fragmentation and inadequate formal institutions. To secure resources and establish credibility, Acer made use of this network-based approach. These unofficial systems were a major part of founder Stan Shih's business practices; to pursue globalization and innovation, he

depended on reliable management and close family ties (Hung & Tseng, 2017). Shih took charge again and used family logic to pick his oldest son to lead a new business unit, even in times of crisis like the disruption of the tablet industry. In addition to maintaining Acer's strategic adaptability, these unofficial connections provided a long-lasting foundation for utilizing culturally rooted connections in the company's quest for international growth (Hung & Tseng, 2017).

The significance of networks and unofficial connections in the institutional work of digital innovation intermediaries is also emphasized by the study of Colovic et al. (2025): the intermediaries use lobbying and advocacy to change attitudes and establish the legitimacy of digital technology. They lower normative and cognitive barriers to adoption by establishing trusting relationships between businesses, academic institutions, and tech providers. They engage in actions based on informal institutions, such as facilitating connections and coordinating collaboration.

Building coherent digital communities where cooperation and shared ideals foster creativity requires such relational efforts. Through these methods, intermediaries actively construct institutional contexts that facilitate digital change and support policy agendas (Colovic et al., 2025).

1.1.3 IBV on technology and digital innovation

Now that the fundamental ideas of the Institution-Based View (IBV) have been discussed, it becomes essential to look at the specific applications of this theoretical approach to technology and digital innovation. Understanding how institutions affect or limit these trends is crucial, given the growing complexity of institutional environments and the quick spread of digital technologies.

As a result, the following section will offer a critical analysis of the body of research, emphasizing significant works that use IBV to investigate the dynamics of digital innovation.

Considering digitalization as a process of profound institutional change and not only an external technology disruption has been underlined in recent contributions (Schildt, 2022). As new technologies are adopted and backed by changing practices among managers, digitalization involves intricate changes inside institutions and vice versa. The adoption of digital tools is reliant on shifting management attitudes and normative frameworks, a dimension that is frequently disregarded in socio-material approaches.

This shift undermines the notion that companies passively absorb digital technologies from their immediate environment. According to institutional theory, to achieve radical transformation, closely related activities that are in line with long-standing organizational logic must be rearranged (Schildt, 2022). These dynamics are shown, for example, by the EU "Digital Europe Programme", which will be discussed later.

The cultural, cognitive, and regulatory institutions are now seen as malleable to new logics as digitalization allows businesses to quickly scale new practices and cross conventional industry borders (Schildt, 2022).

Hung & Tseng (2017) use the example of Acer to show how the evolution and change of institutional structures have a big impact on the company's ability to innovate technologically and digitally. Taiwan's political-regulatory environment gave Acer access to crucial resources that are necessary for innovation. The Industrial Technology Research Institute (ITRI) and interest-free government loans for strategic acquisitions are two examples of how Taiwan's corporatist state structure offered institutional backing through political-business ties. Through these institutional relationships, Acer was able to establish long-lasting competitive advantages through socially acceptable positions that made it easier to obtain resources, legitimacy, and skills rather than relying just on technological assets (Hung & Tseng, 2017). The authors identify three major institutional systems (cultural, political, and technological) that influence the firm's linkage, leverage, and learning processes. They see Acer as both an institutional entrepreneur and a dragon multinational.

Thus, the institutional approach provides a micro-process explanation of how Acer's embeddedness in, and reflective use of, plural institutional systems allowed it to overcome the disadvantages of being a latecomer, acquire diverse resources, and promote innovation (Hung & Tseng, 2017).

Hinings et al. (2018) show that the Institution-Based View provides a useful lens for examining how digital innovation has changed over time. In their study, it is stressed that isomorphism has historically been used by institutional theory to explain transformation. However, playgrounds within sectors are being reshaped, bringing new organizational forms like Uber and Airbnb that either challenge or coexist with old institutional structures. For example, Uber is a technologically powered organizational form that uses a traditional hierarchical structure to disrupt the taxi sector (Hinings et al., 2018).

Established players like regulators and taxi drivers opposed its entry into the market, demonstrating how digital innovations must compete with preexisting institutional logics. In a similar vein, Apple's platform-based ecosystem regulates participation through uniform guidelines, acting as a digital institutional infrastructure. Emerging proto-institutional infrastructures that challenge centralized institutional logics are represented by technologies such as Bitcoin and blockchain (Hinings et al., 2018).

In the context of digital innovation in emerging economies, Wei et al. (2022) emphasize how institutional contexts significantly influence the interaction between enterprises' IT skills and their knowledge base. The study finds that two institutional factors, government support and enforcement inefficiency, have different moderating impacts on a sample of 170 Chinese enterprises. The association between knowledge depth and IT capability is adversely moderated by enforcement inefficiency, which is common in areas with lax legal enforcement. In these kinds of settings, indiscriminate copying and piracy deter businesses from investing in IT out of concern that their competitive advantages will be quickly undermined. On the other hand, government assistance was supposed to promote IT-based knowledge creation by providing access to limited resources, including subsidies, preferred policies, bank loans, and key technologies. The results, however, provide a surprise: the link between IT competency and knowledge depth is negatively moderated by government funding (Wei et al., 2022). Government support can provide businesses with access to resources more quickly, but it can also cause them to rely too much on administrative help instead of building up their IT-enabled professional knowledge (Wei et al., 2022). These findings highlight the complex function of China's institutional frameworks, where state intervention and regulatory laxity can both impede rather than promote the strategic use of IT for knowledge growth.

According to Colovic et al. (2025), digital innovation intermediaries, in particular, Digital Innovation Hubs (DIHs), play a complex role in establishing and maintaining regulatory institutions that facilitate digital transformation. Intermediaries frequently carry out institutional tasks outside the direct purview of their intermediation operations, such as developing and upholding laws (Colovic et al., 2025). This is particularly true at the ecosystem and higher levels, such as regional or national policymaking, where players like local development agencies actively participate in policy talks, offer comments, and push for regulatory changes. Poles and clusters follow them to a lesser extent. Concerning

regulative institutions, the study defines particular types of institutional work carrying out standard operations and creating regulated infrastructures. DIHs help to maintain operational routines and reshape symbolic and relational systems by operating at the organizational, network, and ecosystem levels. This confirms that institutional activity in digital transitions covers cultural-cognitive and regulative domains (Colovic et al., 2025).

Vecchi et al. (2015) demonstrate how different regulatory frameworks in China and India influence how business groupings innovate. Low-quality regulations and high redundancy costs in China make it difficult to enter new markets and discourage sectoral diversification, which results in cautious R&D spending in established businesses. This conservative approach is further reinforced by government assistance for state-owned businesses, which guarantees access to affordable finance. On the other hand, Indian private company groups are encouraged to seek innovation in more dynamic areas, frequently through international links, by India's more effective regulatory environment, which is characterized by a better rule of law and lower dismissal costs.

The geographic distribution of innovation is also impacted by these institutional variations, with India showing more concentrated and cooperative trends (Vecchi et al., 2015).

Sony & Aithal (2020) argue that institutional forces have a major influence on the Indian engineering sector's adoption of Industry 4.0. With programs like SAMARTH–Udyog Bharat 4.0, the National Manufacturing Policy and the National Programme on Artificial Intelligence, they demonstrate how the Indian government encourages this process rather than imposes it. These initiatives are formal institutional structures that reduce uncertainty and motivate businesses to align with national interests. Digital transformation is further legitimized by normative pressures, such as demands from qualified workers and supply chain partners (Sony & Aithal, 2020). The authors also talk about the continuous validation process, which involves creating new norms and standards to institutionalize Industry 4.0 practices, such as those about labour and the IoT.

In their investigation on the impact of government affiliations on Chinese companies' product innovation, Yang et al. (2025) discovered that companies with closer linkages to higher-level government organizations perform better in terms of innovation. However, the characteristics of the institutional environment, which includes the regulatory landscape, shape this relationship. The writers use the concepts of synchronization and

speed to conceptualize institutional change (Yang et al., 2025). According to their findings, the benefits of government connections for innovation are limited when institutional and regulatory changes happen quickly. On the other hand, these associations more successfully promote product innovation when institutional elements, like regulations, transition more flexibly. The importance of regulatory coherence in augmenting the beneficial impacts of government partnerships on innovation outcomes is confirmed by robustness checks (Yang et al., 2025).

Technology and innovation are fundamentally social processes that are intertwined in institutional contexts, as De la Mothe (2004) highlights. They do not happen in a vacuum but depend on an intricate structure of organizations and concepts that support social progress, economic expansion, and environmental sustainability. Therefore, innovation policy must be viewed as the coordination of knowledge-based activities within political jurisdictions, usually countries or regions, through the use of tools such as institutions. The technological decisions that ultimately define our civil societies are shaped by institutions, ranging from local networks to international organizations like the UN and NATO (De la Mothe, 2004). The author contends that this institutional framing is crucial for developing innovative strategies that may use social learning, governance, and information flow to address global concerns.

Mahto et al. (2022) demonstrate, using the IBV, that companies in financially developed and regulated countries are more innovative because they have easier access to capital, which is essential for expensive innovation activities. Their study indicates a negative moderating effect on performance, presumably due to disclosure risks or decreased appropriability, even though robust patent protection should allow corporations to monopolize returns.

Lu et al. (2008) use an institution-based perspective to describe how the Asian Pacific nations' institutional environment affects businesses' innovation and knowledge management strategies. They point out three important functions: institutions serve as sources of knowledge influenced by regional norms and beliefs, enforce laws for legitimacy, and distribute rewards and resources like intellectual property protection. The Asia Pacific region provides a rich environment for analyzing how institutional dynamics influence knowledge management and innovation practices since many of its nations are rising economies with quickly changing institutions (Lu et al., 2008).

1.2 Regulation of technology in the EU and its business impacts

The technology sector in Europe has grown significantly and is now playing a bigger role in the continent's economy. Europe's growing potential as a worldwide technological leader is demonstrated by the $426 billion that European technology businesses have raised collectively since 2015, which is ten times more than the previous ten years (Invest Europe, 2024). In addition, the technology sector in Europe is predicted to be valued at $8 trillion over the next decade, with an estimated 20 million highly qualified workers (Invest Europe, 2024).

This impressive expansion is mirrored by the value of the European tech sector, which is close to 4 trillion dollars, with some 15% of the EU GDP (Invest Europe, 2025).

Sustained growth is anticipated, with a compound annual growth rate (CAGR) of 5.28% between 2025 and 2029, ultimately generating a market volume of US $589.13 billion by the end of this period (Invest Europe, 2025). In terms of revenue, the US market continues to lead the world, but Europe's IT services industry is expanding rapidly due to changing consumer demands for secure, scalable, and adaptable IT solutions, especially cloud-based and managed services (Invest Europe, 2025). This expansion is further accelerated by the use of advanced technologies like AI, ML, and IoT, which are supported by increasing trends in outsourcing and digital transformation. While Southern European countries mostly concentrate on basic IT infrastructure services, Northern European countries are emerging as early adopters of AI and IoT (Invest Europe, 2025). This reflects the diversified market landscape of Europe. The need for third-party IT service providers is increased by underlying macroeconomic issues such as the need for greater business agility, the increased focus on digital transformation, and the lack of qualified IT workers (Invest Europe, 2025).

Within this context, regulatory frameworks play an increasingly critical role in shaping technological development across Europe. In this regard, this chapter section examines the impact of some of the recent European digital regulations and initiatives, including the General Data Protection Regulation (GDPR), Digital Markets Act (DMA), Digital Services Act (DSA), Data Governance Act (DGA), Data Act, and the Digital Europe Programme, on corporate policies and strategic business strategies on digital innovation. Notably absent from this immediate discussion is the Artificial Intelligence Act (AI Act), which will be addressed comprehensively in a dedicated chapter that follows.

1.2.1 General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679

The 1950 European Convention on Human Rights guarantees the basic right to privacy and serves as the foundation for the GDPR (European Court of HR & Council of Europe, 1950). The EU established baseline protections in 1995 with the introduction of the Data Protection Directive in response to the increasing digitalization of society (Wolford, n.d). But when technologies like social networking, cloud computing, and internet advertising advanced rapidly, it became evident that a more thorough legal framework was required. The General Data Protection Regulation (GDPR), which went into effect on May 25, 2018, has fundamentally changed the way businesses, both inside and outside the European Union, handle personal data. Seven fundamental principles (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability) that are listed in Article 5, serve as the basis for the regulation (Wolford, n.d.).

The main goals of the regulation are to improve consumer trust in the digital economy, increase transparency regarding the use of personal data, and strengthen individual privacy rights. By establishing a consistent standard throughout the EU, often referred to as a "level playing field", it also seeks to streamline the regulatory landscape for global corporations. Any company, regardless of location, that handles the personal data of EU citizens is subject to the GDPR, including businesses that deal with B2C, B2B, and G2C customers (Lindgren, 2018). The principle of responsibility, the requirement to adopt "Data Protection by Design and by Default" (Article 25), and the obligation to keep thorough records of all processing operations (Article 30) constitute significant functional pillars. The regulation also specifies particular rights for individuals, including the right to withdraw consent (Article 7) and the right to be forgotten (Article 17) (Li et al., 2019). Tough breach reporting rules are ingrained in its structure, and regulatory bodies have the authority to sanction non-compliant companies up to 4% of their global yearly turnover (Wolford, n.d.). As a result, businesses in a variety of industries, especially technology companies, have had to drastically change the way they treat data. Leading companies in the sector, like Google, Facebook, and Amazon, have already made the necessary updates to their privacy infrastructures (Wolford, n.d.). The GDPR offers a strategic advantage: companies that adhere to its strict criteria are more likely to gain customer trust and stand out in a privacy-conscious market, even while compliance necessitates significant

organizational adjustments (Wolford, n.d.). In this way, GDPR is a structural and ethical framework that is changing the digital strategy of multinational corporations in addition to being a legal requirement.

The GDPR's complex effects on business models across industries are examined in a study by Lindgren (2018), which emphasizes how important aspects of business models are altered by regulatory compliance. His study shows how GDPR restricts Open Business Model Innovation (OBMI) and creates operational constraints by restricting data flows, which hinders inter-organizational learning and cooperation (Lindgren, 2018).

Moreover, Ullagaddi (2024) illustrates how the GDPR is reshaping business strategy by embedding data protection into organizational structures and practices. Central to this shift is the principle of "data protection by design," which requires data protection to be integrated from the outset into system and service development. This demands cross-functional collaboration among IT, legal, and business units, encouraging innovation and offering a competitive advantage. The GDPR has also driven the implementation of formal data governance frameworks and the appointment of Data Protection Officers (DPOs), who ensure privacy is reflected in strategic decisions, fueling a growing demand for privacy professionals. The "right to be forgotten" necessitates the ability to locate and erase data efficiently, requiring tools for discovery, classification, and flow tracking (Ullagaddi, 2024). The regulation's extraterritorial reach challenges global companies to align data practices across jurisdictions but, despite these complexities, Ullagaddi emphasizes that GDPR compliance fosters trust, accountability, and innovation, positioning data ethics as a strategic asset in the digital economy (Ullagaddi, 2024).

According to Ziegler et al. (2019), the GDPR has a direct and complex effect on corporate operations, especially when it comes to Data-Based Models (DBMs). First of all, because failure to comply with GDPR can result in harsh financial fines, the regulation forces businesses to implement strong risk management plans. This calls for a methodical evaluation of the risks associated with GDPR. Second, DBMs must put people at the center of their data models, particularly when it comes to financial transactions, as the GDPR reinterprets data ownership and control and formally acknowledges the rights of data subjects. Thirdly, businesses must match the use of data to the precise goal specified at the time of consent (Ziegler et al., 2019).

The impact of GDPR on organizations is more complex than the motto “all pain and no gain” implies, according to research by Buckley et al. (2021). Their study shows a variety of direct and indirect benefits, even though many businesses considered compliance to be demanding. By establishing new power bases, particularly in the legal, compliance, and IT departments, that are equipped to promote data protection, GDPR has sparked internal organizational change.

Businesses have been compelled by this change to update their IT infrastructure, strengthen information security, manage risk better, and keep their customer databases cleaner. Furthermore, some businesses have used compliance as a reputational signal to communicate to stakeholders and clients that they are reliable and responsible with data (Buckley et al., 2021).

Blind et al. (2024), using panel data from the German Community Innovation Survey, discovered that the GDPR significantly changed the product innovation landscape from radical to incremental, especially for small enterprises. Businesses were forced to restructure their data management more thoroughly than they otherwise would have, which opened possibilities for enhancing already-existing products. Crucially, their findings demonstrate that the GDPR’s effects were never entirely negative. By improving data management, compliance allowed businesses to find opportunities for incremental innovation even as it consumed resources that could have been used for radical innovation (Blind et al., 2024).

Furthermore, academics highlight how the GDPR has impacted cybersecurity and has forced multinational corporations to restructure their data policies (Amoo et al., 2024). Facebook had to improve user controls and permission procedures to balance innovation and compliance with GDPR, which presented significant obstacles. Microsoft implemented a global compliance approach, working with EU regulators to integrate sophisticated cybersecurity and privacy by design. Siemens incorporated GDPR into its core values, placing a strong emphasis on staff awareness and frequent privacy impact assessments (Amoo et al., 2024).

According to Presidente & Frey (2022), the GDPR has had a major effect on business performance, especially in terms of lowering earnings (by 8%) and, to a lesser degree, sales (by 2%). The main cause of this decline is higher compliance costs rather than lower revenue. Due to their low resources for compliance, smaller businesses have been

disproportionately impacted, but companies like Google and Facebook, which are supported by substantial technical capability and lobbying activities, did not see any appreciable drops in performance. It's possible that Big Tech even improved its market position at the expense of its smaller rivals. Although increasing patenting activity suggests one-time investments in GDPR-compliant technologies, the authors warn that some negative consequences might be temporary (Presidente & Frey, 2022).

According to the European Institute of Leadership and Management (n.d.), "Data Protection by Design and Default" mandates that privacy safeguards be incorporated into all systems and procedures from the beginning. To detect and reduce possible privacy issues as soon as possible, it also requires Data Protection Impact Assessments (DPIAs) for high-risk operations.

By being transparent and taking a great approach to privacy, GDPR strategically increases consumer trust. Additionally, it enhances data governance, which results in higher-quality data and better-informed choices. Additionally, GDPR promotes innovation by pressuring businesses to provide privacy-focused solutions. Thus, compliance turns into a way to stand out from the competition, particularly for multinational corporations looking to establish a reputation for being reliable and privacy conscious (EILM, n.d).

1.2.2 Digital Markets Act (DMA) - Regulation (EU) 2022/1925

The European Commission introduced the Digital Markets Act (DMA), which creates a regulatory framework targeted at big online platforms, or "gatekeepers," that offer Core Platform Services (CPSs) that serve as vital intermediaries between companies and end consumers (Grant Thornton Ireland, 2024). Operating systems, social networking sites, online marketplaces, app stores, and online advertising are some examples of these services. In a proactive move that complements but separates from conventional EU competition law, the DMA enforces several *ex-ante* duties and restrictions, many of which went into effect on May 2, 2023 (European Parliament & Council of the EU, 2022). Revenue, market capitalization, user base, and established market position are among the quantitative and qualitative factors used to identify gatekeepers. Six businesses, Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft, were named gatekeepers as of early 2024 for a variety of CPSs, including Windows OS, TikTok, Instagram, Google Search, and others. The DMA's regulatory scope was further extended in May 2024 when the Commission named Booking Holdings, the parent company of

Booking.com, the seventh gatekeeper (Grant Thornton Ireland, 2024). Although some of these designations have been contested in court, the gatekeepers' duty to abide by the Act is not suspended by these appeals. In addition to avoiding self-preferencing, ensuring interoperability, permitting third-party app downloads, and obtaining explicit user agreement before using personal or corporate data obtained through their platforms, the mandated requirements are extensive. To avoid disproportionate competitive advantages, the DMA also limits the use of non-public data and forbids the bundling of services. Crucially, the DMA does not need proof of market dominance, which is a departure from conventional competition law (Herbert Smith Freehills, 2024). The DMA gives the Commission the power to enforce severe penalties to encourage compliance, including daily penalty payments of up to 5% of daily sales and fines of up to 10% of a gatekeeper's yearly global turnover for a first violation, rising to 20% for successive violations (Herbert Smith Freehills, 2024). To further ensure accountability and transparency in their continuing operations, gatekeepers must provide the Commission with comprehensive annual compliance reports.

According to Solskjaer & Owrenn's (2024) analysis, the Digital Markets Act (DMA) mostly reduces gatekeepers' producer surplus, which promotes a shift from monopolistic to more competitive market structures. This is accomplished through regulatory restrictions that force market leaders to reduce prices and boost production, bringing the market closer to a state of competitive equilibrium. This limits the gatekeepers' capacity to maintain above-competitive pricing and take advantage of their data advantages, even as it improves the welfare of consumers and new entrants through improved access, interoperability, and non-discriminatory practices (Solskjaer & Owrenn, 2024). Gatekeepers, however, are unlikely to be completely overthrown because of their firmly established positions; instead, they might prosper through better integration and innovation. Because the DMA benefits consumers and newcomers at the expense of established producers, it does not provide a truly Pareto optimal result, even though it increases market efficiency and overall welfare (Solskjaer & Owrenn, 2024).

The DMA, according to Coulter (2023), places heavy responsibilities on gatekeepers, changing their business methods and affecting customer preferences. Gatekeepers in advertising must get express user agreement before monitoring and give business clients access to campaign data that Amazon, Google, and Meta had previously withheld.

According to industry experts, Apple and Google will also have to allow third-party app stores on their smartphones, which might lead to several new alternative platforms (Coulter, 2023). The DMA also requires gatekeepers to provide consumers with genuine alternatives to default services like browsers and navigation apps. It will be prohibited for them to give preference to their services on websites such as Google's search results or Amazon's marketplace (Coulter, 2023).

By forbidding gatekeepers from giving their own items priority, SMEs are given more equitable exposure on social media, marketplaces, and search engines. Improved interoperability promotes innovation and customer choice by enabling medium-sized businesses to create products that more readily interact with big platforms (Grignon, 2025). Additionally, by eliminating restrictive behaviors, the DMA improves operational flexibility by allowing SMEs to freely choose partners and products. Businesses are empowered to improve products and make well-informed judgments when they have access to strategic data that gatekeepers previously denied. Additionally, SMEs' competitiveness and market presence are further improved by restricted commissions and improved safeguards against anti-competitive behavior (Grignon, 2025).

In response to DMA's decision to allow other app stores on its operating system in the EU, Apple has announced that it will no longer display its flight search service in its search results within the EU and will instead prioritize rival comparison websites (Financial Times, 2024).

Waldfogel (2024), using data on more than 8 million Amazon search results across 22 Amazon domains worldwide, shows that the company's products have a considerable advantage in search rankings, averaging 24 spots higher than similar non-Amazon products, conditional on fundamental product attributes like price and ratings. Compared to 142 other well-known companies, this rank difference is noticeably greater. Particularly, Amazon's rank difference dropped sharply from a 30-position advantage to a 20-position advantage after being named a "gatekeeper" under the Digital Markets Act in September 2023, while the ranks for other well-known firms stayed constant (Waldfogel, 2024). This timing aligns with when Amazon was supposed to adhere to its DMA responsibilities, which forbade self-preferencing. The observed shift, which took place in both EU and non-EU domains, points to a regulatorily caused decrease in the degree of preferential ranking for products bearing the Amazon brand. This could be in

reaction to both the DMA and related actions like the lawsuit brought by the U.S. FTC (Waldfogel, 2024).

Large IT companies are being forced to use more open and competitive business practices within the EU by the DMA. By allowing customers to select their preferred browser and search engine, displaying third-party options in search results, and providing APIs (Application Programming Interfaces) for data access, Alphabet needs to detach its services from Android (Ciccarelli, 2024). Apple must allow third-party browser engines, support other app stores, and let non-Apple payment firms use its NFC system. Meta must allow third-party advertising within its messaging services and allow messaging platforms to be interoperable. Microsoft needs to make it possible to uninstall Edge, allow third-party widgets, and allow other search engines in Windows Search. In addition to giving publishers and advertisers comprehensive performance indicators and ensuring more equitable product placement on its marketplace without favoring its products, Amazon needs to give consumers more transparent data consent procedures (Ciccarelli, 2024).

The first official non-compliance rulings under the Digital Markets Act were announced by the European Commission on April 23, 2025, fining Apple €500 million and Meta €200 million (European Commission, 2025).

1.2.3 Digital Services Act (DSA) - Regulation (EU) 2022/2065

After being approved by the European Parliament and the Council on October 19, 2022, the Digital Services Act (DSA), officially known as Regulation EU 2022/2065, went into effect on February 17, 2024 (European Parliament & Council of the EU, 2022). It is applied to all digital service platforms that operate within the EU and is enforced in tandem by national authorities and the European Commission. The DSA's primary objective is to stop and prevent harmful and illegal online behaviors, like disseminating false information and illicit content. Additionally, it aims to uphold users' fundamental rights, strengthen security and privacy, and promote an equitable online community. A unified legal framework for hosting and intermediary services, as well as digital platforms, including app stores, social networks, and marketplaces, is introduced under the law (Namirial Focus, 2024). Specifically, the most stringent requirements must be met by Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), which serve more than 45 million people in the EU (European Commission,

2025). These include creating channels of communication between users and law enforcement, reporting criminal activity, upholding user-friendly terms and conditions, and guaranteeing openness in recommendation, advertising, and content control systems. They must also evaluate and reduce hazards associated with electoral integrity, public health, consumer protection, child safety, media pluralism, unlawful content, and discrimination. The DSA introduces strong public oversight, particularly over platforms that reach over 10% of the EU population and greatly enhances procedures for eliminating harmful information and defending rights like freedom of expression (Namirial Focus, 2024). Numerous platforms have proactively modified their systems to comply with these regulations since August 2023, highlighting the DSA's contribution to Europe's regulatory leadership and digital transformation.

Surprisingly, the DSA has sparked the most corporate opposition, as seen by several lawsuits that designated firms have launched against the European Commission (Weigl & Guzik, 2025). These responses highlight the substantial effects of the DSA on business models, especially Articles 38 and 39, which require algorithmic transparency and control over tailored suggestions, endangering platforms that depend on advertising revenue. For example, Amazon claimed that if these rules were followed, it would lose market share and must provide private information, endangering its operations (Weigl & Guzik, 2025). Targeting transparency, risk assessments, and content filtering, the Commission started formal actions to enforce the DSA and sent information requests to several sites, including Amazon, Meta, TikTok, and Pornhub. Businesses that failed to perform risk assessments or guarantee transparent advertising, including Meta, TikTok, and AliExpress, were subject to legal action (Weigl & Guzik, 2025). These changes highlight the DSA's significant strategic and operational effects on digital businesses, which have changed compliance dynamics. As the Digital Services Act was being drafted, Fasel (2025)'s analysis of the Austrian KoPl-G case shows how social media companies strategically utilized EU internal market concepts to fight state regulation, thereby increasing the supremacy of an EU-wide framework. Ironically, these businesses positioned themselves as champions of European integration by successfully contesting Austrian law before the CJEU, which helped them escape more stringent national duties while simultaneously advancing the Commission's objective of avoiding legal fragmentation (Fasel, 2025). This result calls into question the claim that the DSA represents a significant change in

the direction of user protection. Rather, as Fasel (2025) contends, the DSA essentially maintains the liability exemption structure of the E-Commerce Directive, as evidenced by the connection between business litigation strategies and EU regulatory aims. The DSA may strengthen Big Tech's position inside a unified but business-friendly legislative framework rather than undermining it (Fasel, 2025). Intermediary service providers are required by the DSA to explain the rationale for content deletions or account limitations, and hosting companies are legally obligated to provide clear explanations for their moderating choices. Additionally, users have the option to challenge such measures through an out-of-court dispute resolution process under the DSA. Platforms like Facebook, Instagram, and TikTok now let users turn off personalized content feeds by user autonomy (European Commission, 2025). Due to the DSA's ban on targeted advertising to minors, TikTok and YouTube have kept underage accounts private by default, while platforms including Snapchat, Google, YouTube, and Meta's services have stopped doing so (European Commission, 2025). The DSA's dedication to protecting vulnerable consumers online is further demonstrated by the severe prohibition on profiling based on sensitive information, such as sexual orientation, political beliefs, or ethnicity, for advertising purposes (European Commission, 2025).

1.2.4 Data Act - Regulation (EU) 2023/2854

The Data Act, Regulation (EU) 2023/2854, aims to promote equitable access to and use of data in all EU sectors. The regulation, which goes into effect on January 11, 2024, and is applicable since 12 September 2025, tackles the potential problems brought about by the expanding data economy, especially with the growth of the Internet of Things (European Commission, 2024). The Data Act, which clarifies who can access, share, and benefit from data, as well as under what circumstances, serves as a supplement to the Data Governance Act by outlining the rights and responsibilities around data usage (European Commission, 2024).

Ensuring a more equitable distribution of value derived from data is one of the main goals of the Data Act. It requires connected device manufacturers to create items that enable users, whether they are individuals or enterprises, to access, use, and share data created while using them. By allowing third-party service providers to access marketplaces that have historically been controlled by manufacturers, this user-centric model fosters competition, innovation, and transparency (European Commission, 2024).

The Act also increases legal certainty in data transactions, prevents power abuse in data-sharing agreements, and permits public agencies to access private sector data in emergencies or for the public good. It also amends parts of the Database Directive to guarantee consistency with more general EU data policy goals and creates regulations to improve cloud service interoperability (European Commission, 2024).

Mikhail (2025) offers a comprehensive analysis of the EU Data Act, emphasizing the possible harm it could cause to businesses, especially those with U.S. headquarters. In its report, the US Chamber of Commerce contends that the Act penalizes companies that have legitimately expanded within the EU and amassed significant data assets, rather than promoting competition. It cautions that this punishment will deter investment and innovation. The Act places a financial burden on cloud service providers, many of which are US-based, by requiring them to help customers switch to competitors. This may have an impact on client pricing models in addition to raising operating expenses. The Chamber also warns that the burdens imposed on data holders and the ambiguous "FRAND" terminology raise the likelihood of litigation (Mikhail, 2025). As suppliers are under pressure to adhere to "functional equivalency," technological innovation may also decrease, hence decreasing service diversity (Mikhail, 2025).

Restrictions on data flows might harm the US automobile industry, which depends on information from cars made in the EU, affecting innovation and safety. Similar to this, data-sharing requirements in the aviation industry have the potential to jeopardize proprietary information and upset long-standing contractual arrangements. Trade secrets are exposed in the pharmaceutical business, which depends on secure data flow for research and development (Mikhail, 2025). All things considered, the Act seems to help EU companies by undermining US competitiveness, which could lead to the Brussels Effect and alter the dynamics of the world economy.

Shahlaei & Berente (2024) point out that because the Data Act directly governs the use and sharing of IoT data produced by connected cars and the services connected, like mobile apps or electric chargers, it places substantial obligations on automakers. Previously, in the exclusive control of manufacturers, users and any other third party they choose, such as repair services, insurers, or financial institutions, must now have access to this data. According to a key executive of a multinational automaker, "live data sharing" is required by the Data Act, which covers a wide range of data kinds, from raw

sensor outputs to pre-processed, structured information (Shahlaei & Berente, 2024). Furthermore, it is difficult to identify the legitimate data holders because national agencies usually have ownership information about vehicles and do not routinely share it with manufacturers (Shahlaei & Berente, 2024). Despite significant investments made by automakers and their suppliers in creating digital devices for revenue generation, the industry shortages established data analytics cultures and business models. Manufacturers are now forced to share important data with rivals who haven't made comparable investments, which could put them at a competitive disadvantage despite these restrictions (Shahlaei & Berente, 2024).

1.2.5 Data Governance Act - Regulation (EU) 2022/868

Regulation (EU) 2022/868 establishes the Data Governance Act (DGA), which entered into force on June 23, 2022, and became applicable in September 2023 (European Parliament & Council of the EU, 2022). Building trust, removing legal and technical obstacles, and encouraging a more open and competitive data economy are the core goals of this important pillar of the European Data Strategy, which aims to increase the availability and re-use of protected public sector data (CMS Law-Now, 2025). The DGA has extraterritorial effects, forcing non-EU providers of data services within the Union to abide by its requirements, even though it is principally applicable within the EU. Three main pillars form the framework of the DGA (CMS Law-Now, 2025). First, it makes it possible to reuse data from the public sector that is shielded by data protection laws, confidentiality laws, or IP laws. Furthermore, it oversees data intermediation services, which Recital 27 notes are essential to the digital economy (CMS Law-Now, 2025). These services, like data marketplaces, are subject to fines for non-compliance, must register with the appropriate authorities, and must adhere to transparency and neutrality standards. Crucially, the DGA seeks to lessen the power of big digital firms by giving SMEs and start-ups better access to data, particularly through sectoral data spaces. Third, by creating a framework for identifying non-profit organizations that meet structural and legal independence requirements, the legislation encourages data altruism, the voluntary sharing of data for the benefit of the public. Along with complementing current EU laws like the GDPR and the upcoming Data Act, the regulation also includes protections for data reuse, like anonymization and contractual protections. The goal of the DGA is to

create a standardized and reliable data governance framework throughout the Union through initiatives like the European Data Innovation Board (Nagy et al., 2022).

In their critical evaluation of the DGA effects on the EU's data economy, Carovano & Finck (2023) place it within the European Commission's larger data strategy, which aims to create a more reliable and competitive digital environment. They contend that the DGA aims to decentralize data control and promote voluntary data sharing through legally specified neutral actors by establishing a legislative framework for data intermediaries. The authors point out that although the DGA seeks to democratize the data economy and lessen dependency on powerful tech companies, its fundamental presumptions, such as the feasibility of neutrality from an economic standpoint and the efficiency of regulation in reducing network effects, are dubious (Carovano & Finck, 2023). Such expectations run the risk of inhibiting continuous innovation and strengthening inflexible organizational paradigms. Additionally, Carovano & Finck (2023) warn that the DGA's overlap with current and upcoming laws, such as the Data Act, GDPR, and Digital Markets Act, leads to administrative difficulties and legal uncertainty. Therefore, even though the DGA's objectives are admirable, its actual application can unintentionally strengthen centralization and impede the competitive diversification it seeks to foster (Carovano & Finck, 2023).

The DGA has important ramifications for SMEs by encouraging interoperable data sharing to boost the European digital economy, but its impacts are still unclear, especially when it comes to the role of data intermediaries, claim Jackson et al. (2024). Due to a lack of technological and cybersecurity capabilities, SMEs that operate as data holders, users, or DISPs (Data Intermediation Service Providers) must deal with legal ambiguities and compliance concerns (Jackson et al., 2024). Although the DGA offers DISPs a simple application process, oversight protocols are still vague, and compliance expenses vary greatly. DISPs must be distinct legal companies and are not allowed to combine data sharing with ancillary services like storage or anonymization. Instead of maintaining neutrality, this structure can open legal gaps that bigger companies might use to share private information, keeping SMEs out of important markets (Jackson et al., 2024).

1.2.6 The Digital Europe Programme - Regulation (EU) 2021/694

The Digital Europe Programme (DIGITAL) was created by Regulation (EU) 2021/694 to accelerate the digital transformation of Europe's economy and society. On March 16,

2021, the Council and then the European Parliament formally approved the Regulation. On April 29, 2021, the co-legislators signed the Act, and on May 11, 2021, it was published in the Official Journal (Council of the EU & European Parliament, 2021; European Commission, 2021). The initiative addresses the EU's strategic goal of enhancing technological sovereignty and fostering resilience in vital digital domains. Recent worldwide disruptions, such as the COVID-19 pandemic and the war of aggression against Ukraine, have increased this requirement by highlighting the dangers of relying on non-European digital systems and the significance of making investments in cybersecurity and critical digital capabilities (European Commission, n.d.).

DIGITAL offers strategic funding to promote advancements in five key areas: advanced digital skills, cybersecurity, artificial intelligence (AI), supercomputing, and the broad use of digital technologies (European Commission, n.d.). The initiative, which has a total budget of more than €8.1 billion under the Multiannual Financial Framework 2021-2027, is essential to accomplishing the goals of the Policy Programme - Path to the Digital Decade and the EU's 2030 Digital Compass. It functions with other EU tools such as the Recovery and Resilience Facility, Connecting Europe Facility, and Horizon Europe. Additionally, DIGITAL supports the Strategic Technologies for Europe Platform (STEP), which seeks to improve the technological leadership and industrial competitiveness of the EU (European Commission, n.d.).

In line with the goals of Regulation (EU) 2021/694, Article 3(2), and related articles, Ruohonen et al. (2025) discover that more than 30% of the projects funded by the Digital Europe Programme (DEP) focus on strategic priorities like cyber security, innovation hubs, SMEs, AI (including HPC and cloud computing), and education (Ruohonen & Timmers, 2025). This suggests that these hubs provide focused assistance for business-driven digital transformation. Furthermore, the study's regression results demonstrate that economic sectors and technological domains, in particular semiconductors and quantum computing, have a substantial explanatory power for the variation in funding amounts (Ruohonen & Timmers, 2025). The DEP's role in supporting expensive, high-impact technical development is reflected in the relatively bigger financing allocated to these domains, which frequently involve substantial private sector engagement. The results demonstrate that DEP funding is not only in line with the goals of strategic policy but is

also well-designed to provide targeted investments to businesses in important industries (Ruohonen & Timmers, 2025).

According to Biçakci's analysis (2024), the Digital Europe Programme is a complex and dynamic effort whose impact on businesses is still hard to completely assess because of its interdependencies and intricate structure. The quantity and coherence of proposals submitted, as well as the widespread support from European stakeholders, are more important factors in determining DIGITAL's efficacy than the simple distribution of funds. Implementation is severely impeded by member state organizational and cultural differences, as well as disparities in infrastructure capabilities. Furthermore, since programs like fiber deployment, AI, and HPC require close cooperation and rely on shared infrastructure, the program's success depends on nimble management and stakeholder alignment (Biçakci, 2024). This complexity is increased by the interdependencies across programs, such as the need for broadband to build digital skills. The balance between public and private investment is also a source of worry, since there is a chance that certain states would utilize the program to strengthen their position of power rather than to assist SMEs. This implies that implementation strategy, institutional adaptability, and fair resource and benefit sharing will determine digital's long-term impact on businesses (Biçakci, 2024).

This chapter has shown that institutions play a crucial role in defining the strategic opportunities, constraints, and sources of legitimacy available to firms. It has done this by looking at the Institution-Based View and reviewing how it has been applied to technology and digital innovation, as well as examining the impact of digital European regulatory initiatives. In these fields, institutions actively shape the environment in which businesses compete and innovate; this is especially true in the dynamic and heavily regulated digital economy like the European one. The following chapter, which discusses the Artificial Intelligence Act (AI Act), is provided by this foundation. The AI Act, one of the European Union's most ambitious and revolutionary regulatory initiatives, is expected to significantly alter the institutional landscape for companies doing business in Europe, especially tech ones. Beyond compliance, its ramifications force businesses to reconsider their strategic orientation and innovation paths in a way never seen before. In light of this, an examination of the AI Act is pertinent and necessary to comprehend how business strategies will develop in the new AI era.

Chapter 2

The AI Act Regulation (EU) 2024/1689: The regulation of AI in the EU

2.1 The need for the EU AI Act arises

2.1.1 Objectives, scope, and governance of Regulation (EU) 2024/1689

Regulation (EU) 2024/1689, known as the "EU AI Act", is the first legal instrument worldwide to regulate artificial intelligence, reaffirming the European Union's ambition to position itself as "the AI continent". Published in the Official Journal of the European Union on 12 July 2024 and entering into force on 1 August 2024, the AI Act establishes an enforcement timeline expected to extend at least until 2030 (Official Journal of the EU, 2024).

Chapter 2 provides an overview of the EU AI Act, outlining its scope of application and core provisions. This analysis is essential to understanding the broader regulatory framework governing artificial intelligence in Europe, serving as a foundation for examining the practical implications of the Act for firms' compliance obligations.

Before discussing the responsibilities placed on businesses, particularly concerning providers and deployers of AI systems and general-purpose AI models, this chapter first looks at the Regulation's overall goals and justification before exploring its risk-based classification system. The chapter ends with a small review of the Regulation's compliance with the larger EU digital legal framework, as well as monitoring and enforcement procedures. By guiding the reader from fundamental provisions to specific regulatory implications, this "funnel-shaped" chapter strives to show how the AI Act aspires to balance innovation and AI risk reduction in tech companies.

The EU AI Act overview has been conducted through examining the text of the official regulation, with the support of the recent "Handbook on the EU Artificial Intelligence Act" provided by White & Case LLP (Hickman et al., 2025).

Additionally, it is important to acknowledge that the Regulation contains elements of legal uncertainty in its interpretation, which only time will clarify, through interpretative guidance issued by the European Commission, as well as future case law from the courts and decisions by EU regulators.

The need for a regulation governing artificial intelligence arises from the necessity to avoid the possibility that divergent national rules may cause a fragmentation of the internal market, reducing legal certainty for operators who develop, place on the market, or use AI systems.[1] For this reason, it has been essential to ensure a sensitizing regulatory framework at the Union level, which guarantees a high and consistent level of protection for fundamental rights.

According to Recital 1, the Regulation aims to promote human-centric and trustworthy AI, ensure a high level of protection for health, safety, fundamental rights, democracy, the rule of law, environmental protection, and mitigate the harmful effects of AI systems. Additionally, the Regulation seeks to support innovation and secure the free circulation and adoption of AI systems, preventing Member States from introducing national restrictions unless explicitly permitted. It must be applied under Union values, aspiring simultaneously to protect individuals and enterprises and positioning the EU as a global leader in trustworthy AI.[2]

Article 1 reflects Recital 1 by setting out what the Regulation aims to achieve: establishing sensitizing rules for the placing on the market, use, and transparency of AI systems in the EU; forbidding certain AI practices; setting specific requirements for high-risk AI systems and obligations for their operators; regulating general-purpose AI models; ensuring "*rules on market monitoring, market surveillance, governance and enforcement*"; and backing innovation, especially on SMEs and start-ups.[3] Microsoft has implemented a collaborative compliance structure for its European operations with the goal of unified governance, given the EU AI Act. Aligning corporate practices with the Regulation has been the responsibility of committed working groups made up of legal, policy, engineering, and AI governance specialists (Crampton, 2025). Bill Gates' company has revised its documentation, added restricted usage provisions to its GenAI Code of Conduct, and put in place internal review mechanisms to find possible violations, such as social score, in anticipation of its 2025 commitments. As part of its larger Responsible AI mission, the company is also actively collaborating with EU institutions, helping to define technical standards (which are still not established) and the Code of Practice for GPAI providers (Crampton, 2025).

[1] Recital 3 of Regulation (EU) 2024/1689.
[2] Recital 1 of Regulation (EU) 2024/1689.
[3] Article 1 of Regulation (EU) 2024/1689.

Furthermore, the EU AI Act's Articles 64 to 70 establish a governance framework designed to guarantee uniform application throughout the Union.

It consists of the AI Office, an enforcement agency created in January 2024, which is responsible for monitoring the EU AI Act's implementation and potential violations, the Advisory Forum, which brings together stakeholders from academia, industry, and civil society, and the AI Board, an advisory body made up of delegates from Member States. Then, a Scientific Panel is responsible for offering impartial advice on technical issues, including systemic risks and model classification. Regarding EU organizations and bodies covered by the AI Act, the European Data Protection Supervisor (EDPS) also has a supervisory function. National competent authorities must be designated by each Member State for market surveillance and compliance monitoring.

2.1.2 Actors and concepts: their relative interpretative difficulties

Regarding the structure of the regulation, in Article 2, the AI Act immediately identifies its addressees i.e., "providers" (the companies that develop AI systems or GPAI Models), "deployers" (those who utilize AI systems or GPAI models), "importers" and "distributors" of AI systems, along with "product manufacturers", "authorized representatives of providers who are not stabilized in the EU", and "affected individuals who are in the EU"[4].

Since businesses operating outside the EU run the risk of being subject to the Regulation even if they do not intend to conduct operations within the Union, it is imperative to mention the geographical application of the EU AI Act.

Because of a contradiction between Recital 22 and Article 2 of the Regulation, it is unclear whether the Regulation's applicability is dependent on the provider's or deployer's intention to make the AI output available within the EU or just on the fact that the output is used in the EU regardless of any such intent. This creates interpretative complexity regarding the concept of "intent" (Hickman et al., 2025).

Moreover, the regulation has limitations to its applicability; for example, it cannot cover aspects related to national security or AI systems intended for military or defense use and does not apply to AI models or systems that are used exclusively for R&D purposes.

Although the interpretation road is still open to accommodate the sudden advances in AI technologies, Article 3 definitions attempt to clarify the concepts covered by the

[4] Article 2 of Regulation (EU) 2024/1689.

regulation. For instance, there may be ambiguity surrounding the concept of an "AI system," which will be crucial for companies attempting to know if their technologies are covered by the Regulation. AI systems are machine-based tools that can work on their own, learn over time, and produce outputs like predictions, decisions, or recommendations based on the data they receive.[5] Companies might find it challenging to determine if an AI tool meets the Regulation's requirements for becoming an AI system because of the EU AI Act's vague definition, which allows for interpretive ambiguity.

The same is true of "GPAI models," the other significant notion governed by the AI Act after AI Systems. The definition of general-purpose AI models is imprecise, especially when it comes to the point at which fine-tuning turns an existing GPAI model into a new one. Particularly for companies attempting to determine whether their use or development of such models has obligations under the Regulation, this ambiguity adds to the legal confusion (Hickman et al., 2025).

Furthermore, Article 4 of the AI Act asserts that companies that develop and implement AI systems take the necessary steps to guarantee that their employees and other people working on their behalf have a sufficient level of AI literacy. The technical expertise and experience of the individual must all be taken into consideration when making these attempts. However, the fundamental problem is the ambiguity around the practical definition of a "sufficient level" of AI literacy. Businesses are left to interpret and carry out this duty on their own without clear standards or comprehensive guidelines, which raises questions about the extent and sufficiency of compliance, mainly in situations where AI systems may have important ethical consequences (Hickman et al., 2025).

2.2 The risk-based approach: classifying AI systems by threat level

2.2.1 Prohibited AI systems

At the heart of the EU AI Act lies its risk-based approach, which divides AI systems into four risk categories: prohibited, high, limited, and minimal risk.

This strict approach reflects a basic concept of the Regulation, which is that legal requirements ought to be commensurate with the risks that AI systems may pose to fundamental rights, safety, and health (Golpayegani et al., 2025).

[5] Article 3 of Regulation (EU) 2024/1689.

According to Article 5 of the AI Act, prohibited systems are the most extreme category and are categorically forbidden. These include AI systems that are thought to be incompatible with Union principles, such as social scoring, subliminal manipulation, exploiting vulnerable people, real-time biometric surveillance in public areas, and specific types of emotion identification and biometric classification (Neuwirth, 2023). These systems are regarded as an intolerable danger to democracy and human dignity (Deckker & Sumanasekara, 2025). The EU AI Act's bans went into effect on February 2, 2025. It should be emphasized that this list is not definitive and could be modified by the European Commission's yearly reviews, which will take new AI developments into consideration. To maintain compliance, companies must refrain from using any banned AI techniques and keep a close eye on any changes to the law.

2.2.2 High-risk AI systems

Second, under the rigorous guidelines outlined in Article 6 of the AI Act, high-risk AI systems are allowed. Businesses must be certain whether their AI systems are in this category, since doing so entails different compliance requirements. As stated in Annexes I and III of the Regulation, high-risk systems generally cover use cases that could drastically affect people's rights, health, or safety. Examples of these use cases include those implemented in critical infrastructure, education, healthcare, employment, law enforcement, migration, or the administration of justice. An AI system is automatically considered high-risk if it is subject to a third-party conformance review under applicable EU harmonization legislation. However, if an AI system doesn't significantly endanger people's safety, health, or fundamental rights, it might not be classified as high-risk. Examples include tools designed only to improve results previously produced by human work, such as enhancing the tone or intelligibility of a writing, or systems carrying out certain procedural tasks (like classifying documents). The deadline for the European Commission to release useful guidelines to assist companies in identifying high-risk AI systems was February 2, 2026. The European Commission missed this deadline: firms are still unsure about how to comply with the AI Act's obligations. They can, however, start by outlining the design and practical application of their AI systems within their organizational procedures and by attempting to notice if and to what degree those systems might be subject to regulatory requirements under Article 6 (Hickman et al., 2025).

The EU AI Act imposes a severe set of requirements regarding high-risk AI systems. Indeed, Article 9 calls for the use of risk management procedures; Article 10 calls for the use of high-quality and bias-mitigated datasets; Article 11 calls for the creation and continuous maintenance of technical documentation before those systems are placed in the market; Article 12 calls for automated event logging for traceability; Article 13 calls for open and transparent communication with deployers; and Article 14 calls for the inclusion of efficient human oversight mechanisms. In addition, accuracy, robustness, and cybersecurity must be met in the design of high-risk systems (Art. 15). When taken as a whole, these specifications aim at guaranteeing that AI systems used in delicate situations function in a way that protects fundamental rights. Companies should incorporate broad risk management systems, automatic logging mechanisms, and human oversight procedures into their daily operations to comply with the standards for high-risk AI systems. This requires a significant corporate strategy effort. In addition to technical adjustments, this signifies the creation of internal processes and precise compliance checklists.

Then, the EU AI Act imposes several compliance obligations on providers, deployers, and other actors involved, as outlined in Articles 16 to 27, in addition to the requirements outlined previously. These include duties concerning technical documentation and recordkeeping (Articles 18-19), quality management systems (Article 17), remedial measures (Article 20), and collaboration with appropriate authorities (Article 21). Actors like importers, distributors, and authorized representatives based outside of the EU are likewise covered by specific requirements (Articles 22-24). It should be remarked that, in some high-risk situations, deployers are required to carry out effect assessments on fundamental rights and establish proper oversight (Arts. 26-27). The AI Act is anticipated to have a substantial impact on commercial contracting practices in this area as well, leading companies to integrate provisions in their contracts that explicitly assign compliance responsibilities, permit monitoring, and guarantee that parties like subcontractors would fulfil their regulatory duties (Hickman et al., 2025).

Furthermore, high-risk AI system suppliers are required by Articles 49 and 71 of the EU AI Act to register their systems in a database accessible within the EU. Information on the system's operation, inputs, and risk classification must all be included in registrations. Given the high degree of detail required and the overlap with other regulatory duties,

commercial providers must make sure that their registration activities are in line with their entire compliance system, even though public authorities benefit from a more limited disclosure regime.

With its "Watsonx.governance" platform, IBM has operationalized a thorough AI governance framework that is intended to facilitate compliance with the EU AI Act's criteria for high-risk systems (IBM, 2024). To directly translate into duties Articles 9-15, the tool combines risk assessment, documentation, lifecycle monitoring, and bias detection. IBM's technology facilitates traceability and transparency throughout development and deployment through a combination of automatic factsheet generation, ongoing model review, and human oversight activities. These capabilities highlight IBM's dual role as both a compliance implementer and a standardization contributor, as they align with European standards that are presently being developed (IBM, 2024).

The European Commission's Digital Omnibus Package proposal was presented on November 19, 2025.

It proposed specific changes to the EU AI Act and delayed the implementation of high-risk AI obligations until December 2, 2027 (Annex III) and August 2, 2028 (Annex I). The recommendations will now go through the EU legislative process: while the Council drafts its "general approach," the European Parliament has started committee work in late 2025-early 2026, with changes and a final report anticipated by Q1 2026. Unless the Parliament initiates the urgent procedure, which might expedite adoption to Q1 2026, trilogue negotiations are scheduled for spring 2026, with adoption expected by mid- to late-2026 (Santalu et al., 2025).

2.2.3 Limited-risk AI systems

Third, limited-risk systems are mostly governed by the EU AI Act's Article 50 criteria for transparency. These obligations are proposed to ensure that people are informed when engaging with AI systems. They are related to systems that interact directly with people, such as voice assistants and chatbots, create or modify artificial content like text, audio, and video, or are employed for biometric classification, emotion identification, or the production of deepfakes and fake news.

The disclosure of such AI tools must be made explicit by providers and deployers in a way that is recognizable and easily accessible for the user's characteristics, particularly for vulnerable groups. Notifications have to be issued as soon as possible after the initial

point of contact. Additionally, generative AI providers need to make sure that their outputs can be identified as machine-generated, utilizing technical solutions like metadata tagging or watermarking. It is extremely important to identify certain content as being modified or artificially generated, such as deepfakes or texts published on topics of public interest.

Transparency requirements are cumulative and may run with laws concerning high-risk AI systems. For example, creating a deepfake with user input may result in a notice requirement as well as marking (Hickman et al., 2025). Although there are a few specific exceptions (such as for personal use, law enforcement, or editorial content that has undergone human review), they are hardly interpreted. Before these regulations become fully applicable, the European Commission and the AI Office are anticipated to release implementation guidelines and codes of practice to promote uniform application and legal certainty.

Providers and deployers should determine if their systems are covered by Article 50 in the meantime and put in place suitable disclosure procedures. For instance, Instagram's "Made with AI" tags (Clegg, 2024), while not yet mandated by law, represent best practices in line with the Article's transparency goals. A careful approach is nevertheless advised due to the ambiguous definition of terminology like "AI-generated outputs" and the lack of clear technical guidance. These transparency requirements present practical challenges for companies that utilize GenAI in marketing or communication, such as Google (with Gemini or Bard) and Meta (with AI Avatars for social media): how should real-time tagging be used for AI-generated content? Which internal processes need to be changed in order to guarantee appropriate disclosure at the user interface level? These are deliberate choices that impact user trust and reputational risk.

2.2.4 Minimal-risk AI systems

Finally, AI systems that are believed to pose minimal risks are exempt from some regulatory requirements under the EU AI Act. The Act does not impose compliance requirements such as risk management procedures, technical documentation, or conformity assessments on these systems because they are deemed to provide minimal hazards to health and safety. This category includes the great majority of AI systems now in use in the EU, including spam filters, autocorrect tools, and AI-enabled video games. Even though these systems are mainly uncontrolled, providers and deployers are required

to voluntarily follow the general guidelines of trustworthy AI. Furthermore, prudence is always suggested: if minimal-risk systems' functions change or are incorporated into more delicate domains, they can be subject to more stringent standards (European Commission, n.d.).

2.3 General-Purpose AI models

2.3.1 GPAI models and their "systemic risk"

As previously mentioned, General-Purpose AI models are, after AI systems, the other main concept regulated under the EU AI Act. An AI model that has been trained on vast amounts of data using self-supervision at scale and exhibits broad generality and the capacity to carry out a variety of unique tasks across domains is known as a GPAI model, unless it has been created solely for research or prototyping before being released onto the market. Such models may be considered to offer "systemic risk" if they demonstrate "high-impact capabilities," according to the law. GPAI model providers are subject to duties outlined in Articles 51 and 52 of the EU AI Act, which expressly address their regulatory regulation. As stated in Article 51, this classification is based on both quantitative thresholds, such as surpassing 1025 FLOPs of computational capacity, and evaluation using suitable technical tools and procedures, such as indicators and benchmarks (Hickman et al., 2025).

The process for informing the Commission when such thresholds are reached is also outlined in Article 52, which also gives the Commission the authority to declare a model systemic *ex officio* or in response to expert alerts (Hickman et al., 2025).

Providers might challenge this categorization by proving that the unique features of their strategy do not pose systemic risks. However, this creates a matter of legal confusion for providers faced with interpreting and enforcing these regulations due to the lack of clear guidance. Companies like Google and Meta may postpone innovation projects incorporating core models because of this legislative ambiguity. The establishment of internal review boards or AI governance units that can monitor legal interpretations and convert them into workable internal procedures might be necessary from a managerial perspective. Examples of GPAI models include GPT-4 (OpenAI), Claude (Anthropic), Gemini (Google DeepMind), LlaMA (Meta), and Mistral (Mistral AI), which are tools that are now used by almost everyone in everyday life, either for personal or for work use.

2.3.2 Obligations for GPAI models and GPAI models with systemic risk

Article 53 of the EU AI Act outlines obligations that apply to all providers of GPAI models. As part of these responsibilities, providers must create and maintain technical documentation related to the model's testing and training, making sure that the AI Office or other national responsible authorities can access these materials upon request. For downstream developers to fulfil their obligations, providers must also give pertinent information to those developers who want to incorporate the model into their AI systems. Following the law, providers must also establish a copyright compliance policy and publish a summary of the training data they utilized, using a template the AI Office has provided. A partial exemption may be advantageous for open-source GPAI models, as long as the model weights, architecture, and usage information are made openly available (Hickman et al., 2025). However, models that are deemed to pose systemic risk are not covered by this exception. Providers may use standards or recognized codes of practice to help with compliance; alternative strategies may be reviewed by the Commission. The Commission also has the authority to create technical procedures for uniform documentation and enact delegated acts to update Annexes XI and XII.

In addition, focus is placed on obligations that go beyond those that apply to regular GPAI models and are placed on providers of general-purpose AI models with systemic risk (Art. 55 and Annex XI). To identify and reduce risks, these providers must perform thorough model evaluations utilizing standardized and state of the art protocols such as adversarial testing. Throughout the model's lifecycle, they must do accurate risk assessments that address both known and predictable systemic risks. To safeguard the GPAI model, providers must also put strong cybersecurity measures in place. They must also notify the AI Office and the appropriate authorities straight away of any significant occurrences, such as threats to their health or damage to vital systems. Providers may use sensitizing standards or recognized codes of practice to prove compliance; but if these standards are not observed, the Commission must validate alternative methods.

Article 78's confidentiality requirements guarantee the proper protection of private information, including trade secrets (Hickman et al., 2025). The EU AI Act anticipates that codes of practice will be adopted as temporary instruments to assist GPAI model providers in proving compliance with their duties under Articles 53 and 55. Anthropic and OpenAI have already started to modify their internal organizational structures to

comply with these legal mandates. In order to facilitate adherence to the transparency and systemic risk mitigation requirements outlined in Articles 53 and 55 of the EU AI Act, both businesses have built up specialized AI governance systems. In its official briefing on the EU AI Act, OpenAI provided a roadmap for compliance, outlining procedures like pre-deployment model assessments, continuous monitoring, and organized technical documentation to provide accountability and transparency (OpenAI, 2024). On the other hand, Anthropic has also established a dedicated Transparency Hub that offers information about the organization's safety policies and evaluation procedures (Anthropic, 2025). By integrating regulatory compliance into the AI development lifecycle, these governance initiatives reflect a larger industry trend that aims to integrate legal compliance as a strategic competence into organizational innovation processes.

Following the type of systemic risk assessments mandated by Article 55 and Annex XI of the EU AI Act, Google DeepMind has included automatic red teaming (ART) procedures as an essential part of its security approach for the Gemini 2.5 model. ART simulates realistic hostile attacks to find weaknesses like illicit commands encoded in data that the model retrieves, or indirect prompt injection. A technique known as "model hardening," in which Gemini is adjusted to identify and eliminate such embedded dangers, has been added to these assessments. The Regulation's focus on proactive mitigation of systemic AI risks is in line with this layered security strategy, which shows how advanced AI providers are starting to institutionalize adaptive defenses and continuous risk monitoring as part of lifecycle-based governance frameworks (Google DeepMind Security & Privacy Research Team, 2025).

2.4 The AI Act commitment in promoting innovation

2.4.1 Regulatory sandboxes

A fundamental goal established in Article 1 of the regulation, promoting innovation in the AI ecosystem, is reiterated in Articles 57-63 of the EU AI Act. This focus on innovation is closely related to the Institution-Based View (IBV) on technology and digital innovation, which is the theoretical framework examined in Chapter 1 of this thesis. This viewpoint holds that institutional frameworks are crucial in determining how innovation develops in regulated contexts and in determining the technological paths taken by businesses. By creating regulatory sandboxes and requirements for real-world testing, Articles 57 to 63 of the EU AI Act present a specific way to support the testing

and development of AI systems. By August 2026, member states must establish a minimum of one national sandbox, which offers a monitored setting with permissive regulations for AI providers to test their products. As long as they adhere to the precise guidelines decided upon with national authorities, sandbox participants are not subject to administrative fines; however, they are still accountable for any harm they do to third parties. Simultaneously, the Act permits more stringent controls for testing high-risk AI systems in real-world settings, outside of sandboxes. These include competent authorities' supervision, informed permission from all parties involved, and approval of comprehensive testing programs. SMEs and start-ups are given priority access to sandboxes. These clauses aim to preserve regulatory authority and safeguard the public interest while stimulating innovation for companies. Still, a doubt arises: while the AI Act's regulatory sandboxes are intended for stimulating innovation by providing a safe setting for testing AI systems, it is far from clear that they will really encourage technological advancement (Hickman et al., 2025). Companies like IBM or TikTok may occasionally see sandboxes as separate legal experiments that are unrelated to their main R&D or product plan. In others, as might be the case with Amazon's or Microsoft's adaptation efforts, sandboxes might turn into test sites for governance innovations, such as new internal protocols or collaborative risk assessment models that persist outside of the sandbox. Sandboxes run the risk of becoming bureaucratic tools only concerned with regulatory compliance rather than being innovative drivers. Strict eligibility requirements and the little protection they provide from regulatory uncertainty, after the AI system leaves the sandbox setting, make this worry real (Hickman et al., 2025).

2.5 The role of monitoring and penalties

2.5.1 The burdens and privileges of monitoring AI systems

Post-market monitoring and enforcement regarding high-risk AI systems and GPAI models is established by Articles 72 to 94 of the EU AI Act. High-risk AI system providers must put in place continuous monitoring mechanisms for the duration of their products' lifecycles following Articles 72 and 73. For providers to assess compliance with the AI Act, these systems must gather and record pertinent data in a way that is appropriate for the system's risks and characteristics. Additionally, Article 73 mandates that any major events like deaths, significant harm to infrastructure or health, or infringement of basic rights shall be reported right away to the appropriate national

market surveillance body, which is then required to notify the Commission if required. The Commission and national responsible authorities are given supervisory obligations by the enforcement mechanisms outlined in Articles 74 to 84. These authorities have the authority to monitor the market, oversee practical testing, implement remedial actions, and protect fundamental rights. In addition, they might limit or forbid the sale of AI systems that do not comply. Individuals or organizations that want to contest violations or classifications are given recourse. This supervisory approach is extended to GPAI models in Articles 88 to 94. With powers assigned to the AI Office, the Commission maintains primary enforcement authority. These consist of assessing compliance, requesting data, mandating corrective actions, and removing GPAI models that aren't in conformity from the market.

2.5.2 The high price of non-compliance

Member States must create "effective, proportionate, and effective" penalties for infractions of the Regulation following Article 99 of the EU AI Act. The economic feasibility of SMEs, especially start-ups, must be taken into account, and they must be implemented nationally. In cases involving forbidden AI techniques under Article 5, administrative fines can amount to up to €35 million or 7% of the offender's global annual turnover, whichever is larger. Providers, deployers, and other players that violate the Act's other provisions may face smaller but substantial fines of up to €15 million or 3% of global turnover. Non-monetary sanctions, like as warnings and corrective instructions, may also be used in addition to monetary penalties. In addition, providers of GPAI models may be subject to direct administrative fines from the European Commission under Article 101. Depending on whether the infraction was done intentionally, these fines could amount to up to €15 million or 3% of worldwide yearly turnover. Failure to cooperate with requests or documentation requirements (Articles 91-93) and violations of evaluation-related duties (Article 92) are specific reasons for such sanctions. According to this penalty structure, big corporations with significant worldwide revenue will be liable to the Act's penalties regime, even those with little presence in the EU. Because of their limited activity within the EU, companies that operate globally are unable to avoid the rule thanks to this extraterritorial application. Furthermore, compared to the GDPR, which imposes fines of up to EUR 20 million or, for enterprises, up to 4%

of the total yearly global revenue, the AI Act imposes tougher penalties. This shows a strong desire to "convince" businesses to comply.

2.6 Enforcement timeline and integration with the EU digital regulations

2.6.1 Deadlines and transition periods

The EU AI Act's enforcement schedule is purposefully spaced out, with distinct entry dates for each type of obligation and system in question. Despite the Act's official effective date of August 1, 2024, enforcement does not start right away; voluntary compliance is encouraged starting on that date.[6] The first legally binding duties, including the Article 5 bans on specific AI practices, took effect on February 2, 2025. Additionally, clauses on definitions, scope, AI literacy, GPAI model regulations, enforcement methods, and fines (Art. 113) come into effect on this day. As of August 2, 2025, GPAI model providers are subject to legally binding duties. However, enforcement is postponed until August 2, 2027, for GPAI models that were already on the market prior to that date (Article 111). The purpose of this two-year grace period is to allow providers time to be compliant. On high-risk AI systems, we have already mentioned the postponement given the Digital Omnibus.

Lastly, the longest transition period is granted to large-scale IT systems identified in Annex X that were put on the market before August 2, 2027, with enforcement beginning on December 31, 2030 (Article 111). This protracted timetable implies for companies a considerable degree of planning of their activities concerning both AI systems and GPAI models, to avoid, as much as possible, infringements of the law.

2.6.2 Interoperability with GDPR, DMA and DSA

Together with the EU AI Act, laws like GDPR, DMA, and DSA make up the EU's digital regulatory framework, as was covered in Chapter 1. There are a lot of similarities between the GDPR, especially when it comes to automated decision-making and processing personal data. The AI Act expressly states that it applies "without prejudice" to the GDPR, which means that companies creating AI systems that handle personal data must also abide by Article 22 of the GDPR's requirements in addition to AI-specific

[6] Recital 178 of Regulation (EU) 2024/1689.

protections. Similar measures for transparency and risk mitigation that are in line with the AI Act's regulations are introduced by the DSA, which regulates online platforms and AI-based recommender systems. Focusing on big digital platforms known as "gatekeepers," the DMA sets guidelines on the use of AI in services, including personalized advertising and content rating. Particularly for high-risk systems, these responsibilities align with the AI Act's emphasis on responsibility and human oversight. As a result, companies that are subject to these regimes must make sure that all applicable instruments are in parallel and coordinated compliance (Hickman et al., 2025). This entails coordinating AI compliance initiatives with current platform governance and privacy teams or even setting up centralized compliance offices that manage several EU laws at once.

2.7 From regulatory design to managerial behavior

The European AI Act's architecture has been reviewed in this chapter, along with its main goals and guiding principles. It is now evident that the Act is a very intricate regulatory tool that seeks to reduce risks while simultaneously promoting competitiveness and trust in the European AI ecosystem (Balcioğlu et al., 2025).

However, how tech companies, especially those that are providing and deploying AI systems and GPAI models, interpret and absorb the rule inside their managerial processes will determine whether it is seen as a catalyst or a barrier to innovation (Özkiziltan & Landini, 2025; Bignami et al., 2025).

The AI Act's dichotomy as a cautious promoter and a stringent regulator raises crucial concerns about how tech companies might adapt to its obligations. The legislation offers procedures that encourage innovation, including regulatory sandboxes and codes of conduct, even as it imposes substantial duties, particularly for high-risk systems and general-purpose AI models (Fabiano, 2025).

Still, whether these mechanisms are viewed as real opportunities or as extra sources of operational burden is unclear. This ambiguity highlights the necessity of using qualitative field research to supplement the regulatory study in order to understand how tech firms perceive and manage the AI Act's effects for their strategic innovation. This is what this thesis aims to achieve.

To foresee the consequences of the AI Act, one must look beyond its legislative framework and consider how it is influencing businesses' ability to innovate. Although legal documents may specify duties, regulation is put into practice through managerial choices and organizational adaptations.

Thus, it will be necessary to document the experiential and strategic aspects of its reception.

Chapter 3

Methodology and results

3.1 Research gap and research question

3.1.1 Research gap

The previous chapters have examined the AI Act's architecture as well as a more general study on innovation and technology, including analyses of other EU digital laws like the GDPR, Data Act, the Digital Services Act, and the Digital Markets Act, Data Governance Act, and Digital Europe Programme.

There is currently no comparable body of research for the AI Act, and this highlights this lack by observing how this new regulation, which is very intrusive in businesses' internal operations, affects innovation techniques.[7]

The general structure of the regulation, including its risk-based framework, core dispositions, and compliance deadlines, has been described in Chapter 2.

Even at the regulatory level, a large portion of the Act is still ambiguous, and a number of its provisions still need to be clarified through standards and implementation instructions.

Because of this, the regulation is still poorly understood both on paper and in actual application. Moreover, there is still an empirical blind hole on the strategic responses of tech firms to the AI Act.

The literature provides little information about how businesses convert regulatory texts into specific internal procedures and innovative initiatives (Crampton, 2025; IBM, 2024; Clegg, 2024; OpenAI, 2025; Anthropic, 2024; Google DeepMind Security & Privacy Research Team, 2025).[8]

The assessment of the literature in Chapter 1 and the analysis of the AI Act in Chapter 2 reveal three distinct gaps.

There is a strategic gap first. While previous research has shown how companies have modified their business models, investment priorities, and innovation strategies in

[7] Because the AI Act is recent and applies in phases, its business impact cannot yet be observed empirically as extensively as the GDPR (paragraph 1.2.1), a limitation also highlighted by a recent study from Holst et al. (2024). In addition, the obligations for high-risk systems (Arts. 9-15) already indicate internal operational burdens (paragraph 2.2.2).

[8] In addition, cf. paragraph 2.7

response to previous EU digital legislation, particularly the GDPR (Lindgren, 2018; Buckley et al., 2021, Blind et al., 2024), there is no empirical data on how tech businesses reevaluate innovation paths or restructure strategic agendas in reaction to the AI Act. [9]

An organizational gap is the second issue. According to the literature review on EU digital legislation, compliance with laws like the GDPR and DMA has resulted in major organizational transformation, including the establishment of new internal coordination structures and governance responsibilities (Buckley et al., 2021; Ullagaddi, 2024). However, little is known about how businesses are redefining internal roles or creating new organizational capabilities to translate these legal obligations into routine management practices, according to the AI Act. [10]

Third, an institutional gap exists. No previous study has applied the Institution-Based View (IBV) to the AI Act, despite the IBV having been applied to explain firms' strategic behavior under institutional constraints in the context of technology and digital innovation (Peng et al., 2009; Hinings et al., 2018; Hung & Tseng, 2017; Wei et al., 2022; Yang et al., 2025)[11].

Finally, these gaps show that the AI Act has not yet been investigated as a lived and changing institutional experience within tech companies. By combining qualitative data, the current thesis seeks to fill these gaps and capture the voices of those directly affected by this regulation.

3.1.2 Research Question

The research question (RQ) of this thesis asks: "To what extent does the European AI Act influence strategic innovation in tech companies, balancing regulatory constraints with opportunities for organizational and managerial transformation?"

The question explores a field of research that is still entirely new, given the contemporary nature of the regulation, which is constantly under discussion and evolving. The AI Act's conceptual contradiction is reflected in the regulation's format, which aims to promote responsible innovation and improve organizational governance practices while imposing new compliance requirements.

The RQ of this study reflects this sense of conflict.

Indeed, it is necessary to deconstruct this question to analyze it effectively.

[9] Cf. paragraph 1.2.1.
[10] Cf. paragraph 2.7.
[11] Cf. paragraph 1.1.3.

First, the question begins with “to what extent,” suggesting that the objective is to understand through which mechanisms the AI Act affects strategic innovation in tech companies.

Second, the term “strategic innovation” refers to a set of procedures that companies use to review their internal structures and capabilities in reaction to exogenous factors.

Third, the AI Act’s documentary obligations and procedural requirements are examples of regulatory constraints that may impact resource allocation, revenues, and priorities.

Fourth, the mention of opportunities for organizational change and managerial transformation highlights how regulations can also lead to new corporate and institutional roles.

The involvement of tech companies that provide and implement AI systems is a crucial component of the research, as they are particularly vulnerable to the consequences of the AI Act. These businesses frequently incorporate AI into tasks like product development, data governance, R&D, and service delivery, operating in such an ever-changing context.

3.2 Research design and methodology

3.2.1 Research design

This thesis uses a qualitative research design due to the exploratory nature of the research question and the evolving state of the regulation. The study moves iteratively between theoretical frameworks and empirical observations rather than beginning with predetermined hypotheses to be verified. This allows for the refinement or even challenging of initial expectations by emerging insights from the field.

The design is based on an interpretivist perspective, which holds that formal legal analysis or quantitative indicators alone cannot fully represent the AI Act’s impact on strategic innovation. Rather, it must be understood through the interpretations and meanings created by the players operating in this regulatory context, mainly institutional stakeholders and tech corporations engaging in AI governance.

Because of the novelty surrounding the regulation, the design uses a multi-level and multi-actor logic. Its structure is purposefully designed to operate on two levels: the corporate level and the institutional level. This dual focus allows the study to have two perspectives: from the institutional sphere, where experts and regulators articulate the goals of the regulation and anticipate its long-term implications; and from within firms, where tech companies interpret the AI Act and rearrange internal structures.

3.2.2 Methodology

The methodology chosen in this thesis follows an abductive logic. According to Timmermans & Tavory (2012), abductive analysis is a creative inferential process where new interpretive theories are developed in response to unexpected or surprising empirical results. In a broader sense, abduction is a unique way of thinking that aims at creating new theories or extending existing ones.

This approach comes from the interpretive grounded theory. An interpretive and theory-generative logic replaces rigid inductivism in grounded theory, leading to the rise of abductive analysis (Timmermans & Tavory, 2012). According to this point of view, grounded theory serves as the methodological basis for abduction, which makes it possible to develop new theoretical explanations based on empirical data.

The two authors assert that abduction starts when the researcher comes across empirical observations called "breakdowns," "puzzles," or "anomalies" that are not well explained by existing theories. These unexpected data can reevaluate beliefs and look for different explanations (Timmermans & Tavory, 2012).

Additionally, it is different from deductive methods in that the objective is to develop new conceptualizations that better explain the unexpected results rather than to verify pre-existing hypotheses. It also varies from inductive methods, which only use recurrent patterns in data to construct a theory.

Three methodological operations are the foundation of abductive analysis: "revisiting", which involves repeatedly examining empirical material through new theoretical lenses; "defamiliarization", in which the researcher actively distances themselves from common or expected interpretations; and "alternative casing", which entails reframing empirical situations using alternative theoretical possibilities (Timmermans & Tavory, 2012).

One key outcome of the abductive analysis is theoretical regeneration, in which the researcher improves or rearranges preexisting ideas to create a new or better theoretical model that properly describes the observed empirical patterns.

Two sensitizing notions, which function as interpretive lenses, serve as this study's methodological guidelines: AI governance under the AI Act and the IBV (Institution-Based View).

The first sensitizing concept expands on the topic covered in Chapter 2, where artificial intelligence is described as a technical tool that changes how tech businesses will operate.

Adoption of AI is more than just a technological improvement, as demonstrated by examples like Microsoft's specialized AI governance frameworks, IBM's lifecycle-based risk management for high-risk systems, or the restructuring of GPAI governance by companies like OpenAI, Anthropic, or Google DeepMind. Redesigning data governance architectures, integrating AI tools into product development cycles, adding new compliance-focused positions, forming cross-functional teams, and institutionalizing ongoing monitoring, documentation, and risk assessment procedures are all necessary. As a result, AI can promote innovation and cause conflict inside organizations and institutions at the same time.

The second sensitizing concept is based on the theoretical foundations established in Chapter 1, where the Institution-Based View (IBV) is introduced as a framework showing how formal and informal institutions influence organizational behavior and organizations' ability to innovate.

Chapter 1 provided examples of how institutional dynamics affect technology adoption and innovation in a variety of contexts, such as Taiwan's state-industry ties that allowed Acer to become an institutional entrepreneur, China's lax enforcement policies that hinder IT investment, and India's normative and cognitive pressures that facilitate Industry 4.0 transitions. These illustrations demonstrate how institutions actively shape the constraints and benefits that surround technological progress. Thus, here IBV is employed to comprehend how tech businesses react and view the AI Act as a new institutional regime.

These two sensitizing concepts guided the methodology, shaping the in-depth interview guide's design. But in line with abductive reasoning, they were flexible enough to adapt to new empirical discoveries, enabling the analytical framework to change in response to the unexpected results found in the field.

The following sections describe how data were collected and subsequently analyzed via iterative abductive coding cycles.

3.3 Sample selection and data collection

This section of the chapter serves as the empirical work's "research logbook" to certify transparency in line with qualitative research principles.

3.3.1 Sample selection

Qualitative interviews were thought to be the most effective way to approach the research question, as it allows to exploration of opinions of international and European institutional actors involved in regulatory or advisory processes. The sample included legal experts in digital legislation, EU institutional representatives, an officer from an Italian Ministry, senior managers (including C-level executives), AI governance professionals at a global level, and individuals holding public policy roles within big, medium and small technology companies developing or deploying AI systems and GPAI models under the EU AI Act. This diversity was significant in capturing how different institutional and organizational settings with various professional backgrounds perceive the AI Act.

The in-depth, semi-structured interviews were conducted to gather the empirical data for this study between July and August 2025.

An overview of interviewees and their roles is provided in Table 1.

Identification code	Role
INT01_IST	**Policy Officer**
INT02_IST	**Senior Legal Policy Officer**
INT03_IST	**AI Policy Expert**
INT04_IST	**AI Public Policy Officer**
INT05_IST	**Policy Advisor**
INT06_IST	**Digital Policy Officer**
INT07_CORP	**AI Applications Manager**
INT08_CORP	**Chief Technology Officer**
INT09_CORP	**Public Affairs Manager**
INT10_CORP	**AI Policy Manager**
INT11_CORP	**Public Affairs Analyst**

Table 1. Overview of interview participants (role and assigned code)

3.3.2 Data collection

LinkedIn outreach was used to get in touch with the potential interviewees. Although not every candidate contacted was available or willing to participate, the recruitment process followed a structured list of possible interview candidates that was first created. A brief explanation of the study's objectives and confidentiality measures was given to

each participant. Sometimes, several follow-ups or internal approvals before interviews had to be confirmed internally, thus requiring weeks of waiting.

A set of guiding questions was arranged enquiring perceptions of the AI Act's impact on strategic and responsible innovation, organizational and managerial adaptations within tech firms, the clarity and operational burden of compliance requirements, and the role of public institutions.

The questions further addressed whether the AI Act is approached as an opportunity or as a logic of minimal compliance, as well as potential institutional gaps and proposals for regulatory improvement.

As can be seen in Table 2, the first section consisted of six common questions posed to all participants, while the second section included two specific questions tailored to the institutional or corporate nature of the interviewee. A final concluding question was included for all respondents, and so the protocol resulted in a total of nine questions.

Common questions	1. How do you personally perceive the overall impact of the AI Act on responsible and strategic innovation within the tech sector?	
	2. In your opinion, how effective are regulatory sandboxes, corporate codes of conduct or gradual compliance in enabling experimentation and innovation within AI development?	
	3. In what ways, if any, has your organization (or others you observe closely) modified roles, internal processes, or skill profiles in response to the AI Act?	
	4. How clear are the operational and documentation requirements for AI system providers and deployers, including GPAI model providers, under the AI Act?	
	5. In your view, what role should public institutions play in supporting responsible and competitive AI innovation under the AI Act in Europe?	
	6. What do you see as the main benefits and the main challenges posed by the AI Act for tech companies working with AI?	
Specific Questions	7. Do you think full compliance with the AI Act can become a real competitive advantage for your company or industry, or does it pose a risk to innovation agility?	Corp.
	8. Which components of the AI Act pose the greatest complexity or operational burden in your day-to-day business practices?	Corp.
	7. Based on your observation, are tech companies embracing the AI Act as an opportunity to grow and innovate responsibly, or does a logic of minimal compliance prevail?	Ist.
	8. What do you see as the most pressing institutional blind spots or implementation gaps that could undermine the AI Act's long-term credibility and effectiveness?	Ist.
Final Question	9. In your view, are there any reforms or adjustments to the AI Act that could better support tech companies in pursuing innovation while ensuring compliance? If so, what changes would you consider most impactful?	

Table 2. Structure of the interview guide

Participants were invited to indicate their preference concerning anonymity and opted to remain anonymous by signing the informed consent form, which is available in the Appendix A.

In total, eleven interviews were conducted, including six interviews with institutional actors and five interviews with representatives of technology companies.

The average duration of the interviews was 45 minutes, reflecting the complexity of the issues discussed and the willingness of participants to engage in in-depth reflection.

The two sensitizing notions described in the methodology, precisely the AI governance under the EU AI Act and the Institution-Based View, were taken into consideration when creating the interview guide. The purpose of the questions was to investigate respondents' perceptions of the AI Act opportunities and limits, how organizations are changing in response to the regulation, whether public institutions are doing enough to support tech companies, and the practical experiences of compliance and monitoring. Understanding how regulatory uncertainty affects technology companies' strategy reorientation and innovation paths also received special focus.

3.4 Data analysis

Following Timmermans and Tavory (2012), an abductive analytical method was used to analyze the empirical data acquired from the interviews. Qualitative data analysis software (MAXQDA) facilitated the iterative phases of data analysis, which included "revisiting" and "defamiliarization".

The Discussion section, in Chapter 4, will address "alternative casing".

First, all interview notes taken during the interviews were reviewed and rewritten in order. Each transcript was imported into MAXQDA as a separate Word document under a new project named "Tesi_AI_Act_Abductive_spc1.mqda" after being given a distinct anonymous identity (INT01_IST-INT06_IST for institutional actors; INT07_CORP-INT11_CORP for corporate actors).[12]

3.4.1 Revisiting

Open coding, the "revisiting" step of abductive analysis, was the first analytical step.

Interview transcripts were read line by line during this step. One sentence or at most a brief paragraph was classified using interpretive labels that caught the underlying

[12] See Table 1.

meaning of respondents' responses. In the early phases of coding, visual elements such as color coding were sometimes used to support the researcher's orientation. This stage produced a large number of precise single codes, 375, as can be seen from Diagram 1 below.

During the open coding phase, a code structure was gradually developed within MAXQDA. In fact, all single codes were organized hierarchically in the software's code system panel, allowing for constant monitoring of their frequency and internal consistency. This evolving code structure enabled the researcher to observe relationships between codes and distinguish isolated concepts, assessing which codes carried greater analytical weight based on their recurrence.

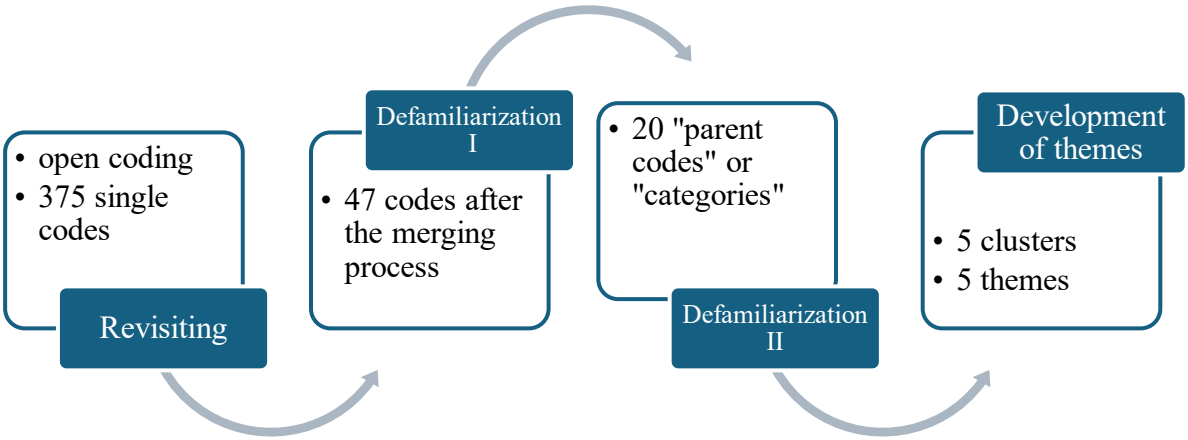

Diagram 1. Iterative coding, categories and the development of themes process

3.4.2 Defamiliarization I

The second phase of analysis involved "defamiliarization", aimed at moving beyond surface-level patterns. Similar codes or overlapping ones were merged using a "drag and drop" method. Initially, this reduces the number of codes to 47, as it can be noted from Table 3.

Codes after the merging process (47)	Number of subcodes
AI Act driving responsible innovation	**5**
AI Act hindering innovation	**11**
AI Act not a starter for resp innovation	**1**
AI Act responds to a trend	**1**
AI evolution outpacing regulatory timing	**17**

AI governance and innovation roles	22
Almost no benefits at all regulation	1
Asymmetric burden between big firms and SMEs	18
Attempts to loosen AI Act obligations	1
Balance challange	1
Calls for reform of the AI Act	22
Competitive advantage full compliance	2
Creation EU sandbox	4
EU competitiveness vs US&China	15
EU safeguards fundamental rights	11
Fragmentation of regulatory authority	10
Fragmented sandbox implementation	9
Full compliance AI Act not a competitive advantage	2
Global deregulatory pressures	5
Innovation via M&A	2
Institutional dialectic conflict	6
Insufficient institutional support and investment efforts	10
Lack of clarity from institutions	2
Lack of regulation's clarity	9
Lack of technical clarity and competence	13
Low impact regulatory sandbox	5
Market decides innovation	3
Minimal compliance prevailing	5
Need for common standards	14
Need for technical experts	3
No stop the clock	2
Overlapping of digital regulations	24
Premature to assess impact	3
Public private synergies	3
Public-sector competence gap	11
Questioned cost/benefit efficiency AI Act	6
Regulating AI mission impossible	1
Regulatory burden on SMEs	14
Sandbox importance for innovation	2
Sector specific sandbox design	1
Stop the clock? Yes!	8
Strong support from public institutions	14
Structural limits of the AI Act	19
Systemic regulatory change needed	3
Technical and legal synergies	6
The AI Act as an opportunity for innovation	18
Trust-building effects	9

Table 3. Defamiliarization I – 47 Codes after the merging process

3.4.3 *Defamiliarization II*

Among the 47 codes, 20 higher-order categories, also known as "parent codes" or "macro-codes," were selected in terms of the number of subcodes and their relevance to the RQ, as can be observed from Table 4.

So, after performing a "similarity test" and then merging or leaving codes separate, the entire set of codes was made even more homogeneous. It was necessary to distance ourselves from the data and theory. This step aimed to separate the analysis from the language used by specific respondents and find greater categories for interpretation.

Categories or "Parent codes" (20)	Number of subcodes
Calls for reform of the AI Act	**22**
Need for common standards	**14**
EU competitiveness vs US&China	**15**
Technical and legal synergies	**6**
The AI Act as an opportunity for innovation	**18**
AI evolution outpacing regulatory timing	**17**
AI governance and innovation roles	**22**
Structural limits of the AI Act	**19**
Lack of technical clarity and competence	**13**
Fragmented sandbox implementation	**9**
AI Act hindering innovation	**11**
EU safeguards fundamental rights	**11**
Insufficient institutional support and investment efforts	**10**
Fragmentation of regulatory authority	**10**
Asymmetric burden between big firms and SMEs	**18**
Public sector competence gap	**11**
Global deregulatory pressures	**5**
Overlapping of digital regulations	**24**
Strong support from public institutions	**14**
Regulatory burden on SMEs	**14**

Table 4. Defamiliarization II – 20 Categories or "Parent codes"

3.4.4 Code map and code structure: the generation of themes

Following the identification of these 20 categories, the Code Map function in MAXQDA (Visual Tools → Code Map) was used to investigate and visualize their interactions.

This step supported a visual inspection of co-occurring categories.

Thus, the visualization was generated by selecting the option "occurrence of codes within the same document"; in this way, the map displayed how often parent codes appeared together across the interview material. In the formatting settings, "node size" was configured to reflect code frequency, while relationships between codes were displayed as connecting lines whose thickness represented the frequency of co-occurrence. A minimum frequency threshold of 1 was applied.

The grid was removed to improve legibility, and five clusters were identified, distinguishable by different node colors and spatial groupings within the map.

The clusters were identified by grouping parent codes that frequently co-occurred across the interviews and shared a common conceptual orientation.

After generating the map, it was saved in MAXMaps format, as can be seen below from Figure 1, and further refined by adjusting graphical elements: connecting lines were displayed in dark grey to reduce visual noise, and the labels of the parent codes were positioned above the lines and highlighted in yellow to improve legibility.

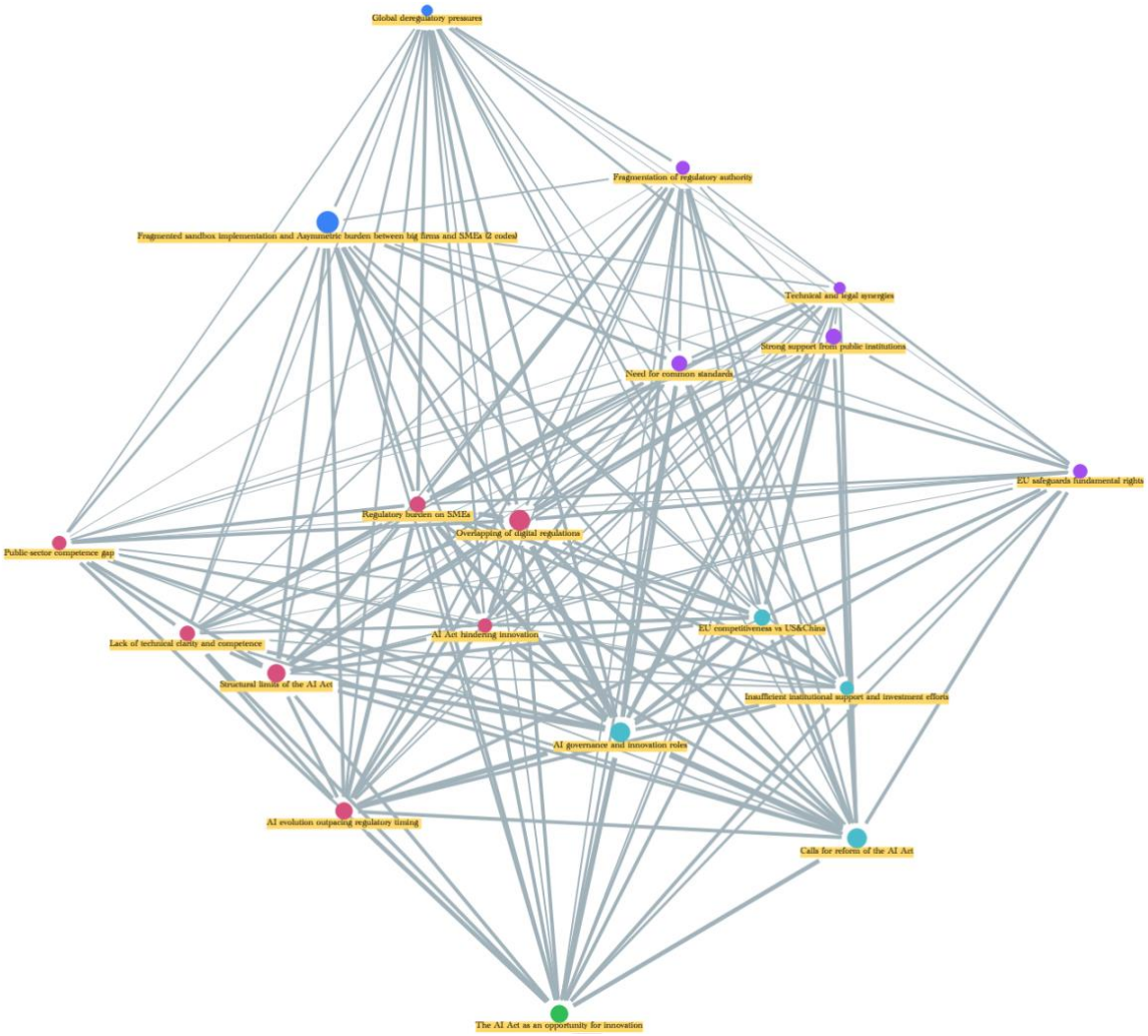

Figure 1. Code map of the 20 categories or "parent codes" emerging from the defamiliarization phase of the abductive analysis

The final step of the data analysis consisted of identifying a limited number of "themes". These themes did not correspond mechanically to individual parent codes. In fact, they emerged from the interpretive aggregation of clusters of interrelated categories, as identified through the code map, the code system and according to the principles of theoretical generation. The identification and naming of five themes were informed first by an analysis of the categories themselves, but above all by a close examination of the "sub-codes"[13] contained within each category. To this end, all quotations associated with

[13] The initial codes developed during the "revisiting" phase and subsequently merged and reorganized during the "defamiliarization" phase.

the categories were carefully reread to construct themes that were coherent with the theoretical framework of the study and aligned with the research question.

Below, Diagram 2 shows the five themes and their corresponding categories or "parent codes" identified (code structure).

The coding process followed a gradual progression: from 375 initial open codes to 47 consolidated codes, then to 20 categories, and finally to 5 themes.[14]

Together, these themes form the analytical structure of the Results section, to which the analysis now turns.

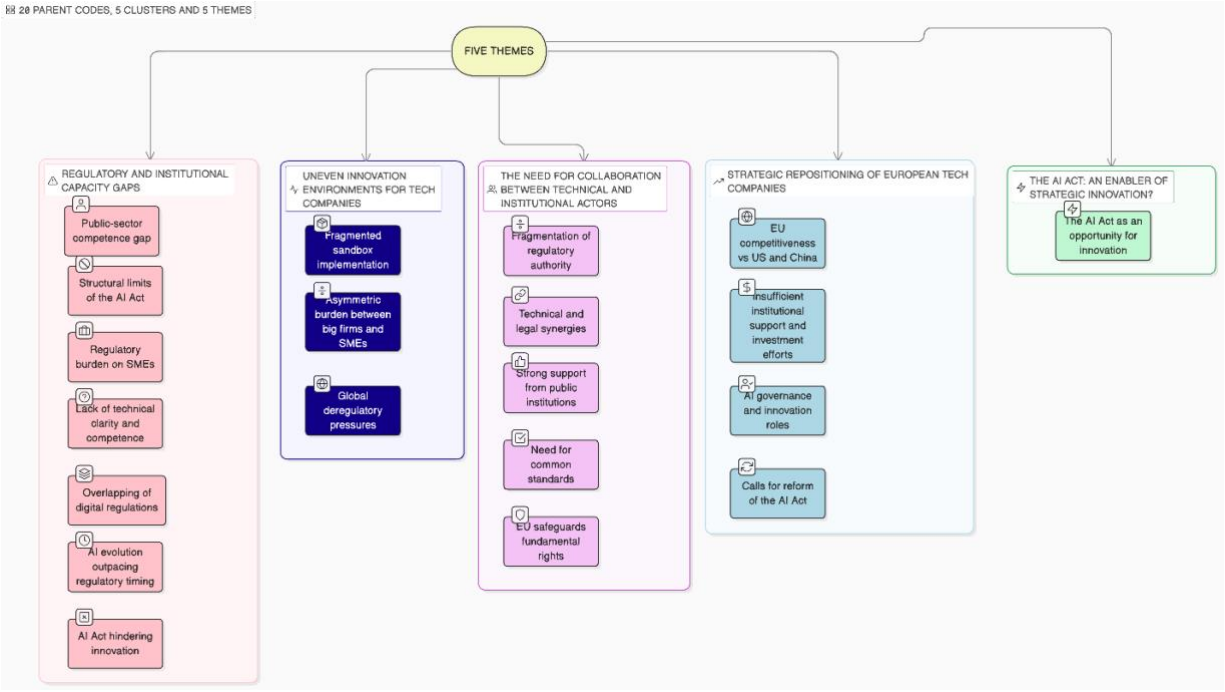

Diagram 2. Code structure linking categories and themes: results of the thesis[15]

3.5 Results of the thesis

As shown in Diagram 2, the clustering of categories resulted in the identification of five themes: "Regulatory and institutional capacity gaps", "Uneven innovation environments for tech companies", "The need for collaboration between technical and institutional actors", "Strategic repositioning of European tech companies", and "The AI Act: an enabler of strategic innovation?".

[14] Cf. Diagram 1.

[15] Sub-codes and quotations underlying each category are not shown for readability. Diagram created thanks to "Eraser.io" program.

They offer an overview of the results and highlight the most significant aspects that emerged from the interviews. They focus on how regulatory constraints interact with strategic innovation practices and changes by revealing how tech companies and institutional players are interpreting and internalizing the dispositions of the AI Act.
Each theme is presented in turn in the subsections that follow, with quotes and interview data serving as the foundation for the analysis.

3.5.1 Regulatory and institutional capacity gaps

The pink cluster brought together the categories "Public sector competence gap", "Structural limits of the AI Act", "Regulatory burden on SMEs", "Lack of technical clarity and competence", "Overlapping of digital regulations", "AI evolution outpacing regulatory timing" and "AI Act hindering innovation", originating the theme of "Regulatory and institutional capacity gaps".
It reflects how interviewees described the implementation of the AI Act as taking place within an institutional and regulatory environment characterized by limited technical expertise among public administration personnel, a high degree of stratification of digital-related regulations, and a temporal lag in adapting regulatory provisions to the extremely rapid development of artificial intelligence systems. Across both institutional and corporate interviews, respondents recurrently referred to difficulties related to the concrete interpretation of the regulation, generating ambiguity regarding how actors should act and behave in practice. Corporate actors admitted a minimal compliance approach towards the AI Act. Moreover, to deal with this uncertainty, companies are creating internal reports to reflect on emerging AI regulatory scenarios and are making awareness campaigns within the companies themselves. Finally, AI tools are more and more being integrated in the companies' workflows.

" Probably the main difficulty lies in the interpretation of the regulation.
Yes, there are some parts that, well, will likely become clearer over time, but at first glance, our initial impression - and some issues were actually raised to us - was the difficulty in understanding, for instance, the difference between provider and deployer, as I mentioned before, which is quite important." - INT02_IST

Public sector competence gap

From the interviews, it emerges that there is a difficulty in recruiting individuals with adequate AI-related expertise within the public sector, both due to salary differences between the public and private sectors and because specialists often move outside the EU, where remuneration is higher. Interviewees also reported that when the regulation was drafted, the AI technological boom had only just begun, and that the regulation was therefore written by policymakers with limited competence in this field. Concerns regarding a public sector lacking sufficient technical expertise emerged from both institutional and corporate perspectives.

An institutional interviewee explicitly stated:

"X Italian government agency has difficulty in understanding how an AI system is built, I mean - they're basically discovering it these days." - INT03_IST

A corporate respondent noted:

"So, and in fact now they've set up the AI Office with the goal - basically with the goal of bringing in experts, obviously underpaid ones who will never come, because they get paid seven times more in companies that do AI, maybe overseas." - INT09_CORP

Structural limits of the AI Act

This category covers interviewees' assertions describing the AI Act as structurally limited and, at times, confusing, with the presence of several grey areas. From the interviews, it emerged that these limitations are perceived as rooted in the way the AI Act is designed, particularly in its treatment of AI through a product-safety regulatory approach. In fact, as noted by an institutional interviewee, AI systems are regulated as if they were a product, even though AI is a component of a product. Additionally, the fact that the regulation simultaneously addresses several digital-related issues was another point raised by interviewees.

Indeed, an institutional actor noted:

"Surely, the fundamental thing is that the Act tries to pursue too many objectives, probably even ones that are sometimes far apart from one another." - INT01_IST

On the other side, a corporate respondent emphasized how formal exclusions within the Act do not eliminate compliance challenges for dual-use technologies:

"And the AI Act, in Article 2.3, explicitly excludes military applications from the provisions and limitations deriving from the Act itself.
But this does not mean that companies like mine have "no constraints",
especially in the case of dual-use technologies - the so-called dual use - with civil applications.

In fact, all technologies related to surveillance, robotics, or cybersecurity, which may also have civil uses, still fall within the regulatory constraints of the AI Act.
And this creates important challenges for compliance and for internal governance." - INT09_CORP

Regulatory burden on SMEs

From both institutional and corporate interviews, it emerged that SMEs face significant difficulties dealing with the continuous production and constant updating of documentation needed for compliance. From a corporate perspective, SMEs' low organizational and administrative resources made gradual compliance difficult for them. Moreover, SMEs are deciding to postpone their entry into the market. Finally, it emerged that firms are testing and commercializing AI products outside the EU market since many national sandboxes are not ready.

An institutional respondent explained:

"Tech companies, especially SMEs, may face difficulties in meeting detailed compliance obligations, particularly in the absence of harmonized global frameworks. Risk classification, documentation, and monitoring requirements may impose disproportionate burdens without corresponding benefits if not implemented in a balanced and scalable way." - INT06_IST

Another institutional actor noted:

"[…] some companies have decided to wait for the full approval of the Act, and they're still waiting for the technical developments before entering the European market. So, they're already testing - even selling -in third countries but not in Europe. - INT05_IST

Lack of technical clarity and competence

This category reflects interviewees' references to uncertainty regarding how the technical requirements of the AI Act will be applied. Respondents described difficulties in understanding which technical tests, thresholds, or evaluation criteria should be considered acceptable.

In addition, it emerged that this uncertainty is shared by both regulated actors and public authorities, contributing to an opaque regulatory environment in which the practical meaning of technical requirements remains unclear. Thus, corporations are pursuing

awareness campaigns on AI and are increasing the hiring of technically specialized personnel.

One institutional actor stated:

"[…] That the uncertainty about how the technical requirements of the regulation will be applied is so huge that in the end it will end up exactly like privacy, where everything is personal data, but nobody knows what that actually means." - INT03_IST

An institutional actor noted:

" […] First and foremost - and this is probably the most important point - awareness campaigns are starting from the top of the company." - INT02_IST

Another institutional actor highlighted:

"What I see is that there is definitely a rush - let's say, a growing attention - to hire specialized profiles in these fields." - INT01_IST

Overlapping of digital regulations

From both institutional and corporate perspectives, interviewees unanimously referred to the overlapping nature of digital regulations, describing difficulties in identifying which regulatory framework should be followed to be compliant with the provisions of the AI Act.

From the interviews, referencing the Draghi Report, it emerged that the European Commission continuously produces a large number of regulatory instruments, and that Europe suffers from this regulatory excess. But this is coherent with the strong European regulatory culture, said an institutional actor.

A corporate interviewee observed:

" […] And the fragmentation of EU digital regulation doesn't help: GDPR, DMA, DSA, the Data Act, the Data Governance Act, the Digital Europe Programme… everything overlaps. Some companies have literally told me: "If this process is non-compliant, which law do I choose to violate? The one with the lower penalty?" - INT08_CORP

Indeed, an institutional actor shared this opinion and mentioned how challenging it is to deal with several regulatory layers at once:

" […] And there, we've observed - at least at the national level, though the rules are of European origin, an extreme regulatory complexity: there are norms from here and there, all tied to privacy, consumer protection, the AI Act… there are even provisions on profiling in the Digital Services Act, in the Digital Markets Act - there's a huge number of overlapping rules, and putting them all together is extremely difficult." - INT02_IST

AI evolution outpacing regulatory timing

From most corporate interviews, regulating AI was described as a very challenging issue. Respondents asserted that technology evolves too rapidly to keep pace with EU regulatory timelines. From the corporate interviews, it emerged that interviewees perceive the current technological shift as unprecedented in terms of speed, making regulation particularly difficult.

There was a shared view that there has never been a technological transformation moving at such a pace, and that this temporal mismatch complicates the formulation and application of regulatory rules.

From the institutional perspective, interviewees stressed that when the technology itself is so new, it presents intrinsic challenges where regulatory sandboxes alone are not enough. Corporate actors stated that, even if it is tough, they are trying to constantly monitor the AI systems development, updating systematic risk assessment procedures and regular updating of internal legal documentation.

An institutional respondent stated:

"[…] because it risks generating obsolescence of the norms before they even become effective." - INT01_IST

Corporate actors highlighted how difficult it is to keep up with the evolution of technology and the applicability of the regulation:

"The problem, of course, is that all of this is happening while the technology is evolving absurdly fast.
And that, in my view, makes a truly accurate regulation almost impossible at this stage.

So yes, for now I think it's essentially impossible to regulate this technology "correctly"." - INT08_CORP

"[…] And something I've also seen in how the regulation itself is written - right, inside the regulation, there are actual definitions, about what an AI system is, who the deployers are, who the providers are - they are already obsolete. It's normal." - INT08_CORP

"Changes are so fast that if you create, let's say, a monolithic regulation that cannot be updated and modified and kept aligned with the speed of development of a sector like this, you cut your legs off yourself.
The regulation becomes - and the definitions inside the regulation become - obsolete in…

Well, two days later.
Two days later.
That's how it is. It is how it is." - INT09_CORP

AI Act hindering innovation

From a corporate perspective, interviewees reported that compliance with the AI Act has led to slowdowns in research and development cycles. From the institutional side, it emerged that the regulatory regime is considered strictly tight, a characteristic that was described as potentially constraining innovation, above all for AI providers subject to extensive compliance obligations.

A corporate interviewee noted:

"[…] However, from a strategic standpoint, it could act as a brake, not so much because of its content, but rather due to the difficulties it poses for all actors throughout its implementation process." - INT07_CORP

Another corporate respondent added:

"[…] However, achieving compliance may also slow down innovation agility, especially in the short term, due to complex or unclear requirements. Much will depend on how the outstanding parts of the regulation are implemented and whether they strike the right balance between legal certainty and flexibility." - INT11_CORP

3.5.2 *Uneven innovation environments for tech companies*

The dark blue cluster revealed a connection between "Fragmented sandbox implementation", "Asymmetric burden between big firms and SMEs" (it's curious to point out that these two codes have the same position in the map) and "Global deregulatory pressures", from which the theme of "Uneven innovation environments for tech companies" emerged.

It illustrates how interviewees described innovation conditions under the AI Act, which are unevenly distributed across different contexts. One issue raised by respondents was the diverse establishment of regulatory sandboxes in Member States with different possibilities for experimentation according to national rules. Then, interviewees stressed that not all businesses face the same legal and economic burden related to AI Act compliance, with big tech and SMEs not having equal limitations and capacities for adaptation. Finally, interviewees stated that a deregulatory wind from the United States might influence decision-making in the European Union.

"I mean, if everyone has their own sandbox - as we say in Rome, *"se la suona e se la canta"* - right? Meaning: everyone does their own thing." - INT09_CORP

Fragmented sandbox implementation

The fact that each Member State has the possibility to establish its own regulatory sandbox risks creating an environment in which everyone does whatever they want, as stated by a corporate interviewee. From the institutional perspective, concerns were raised because this is perceived as a lack of harmonization and also a contradiction: although the AI Act is intended to create a single regulatory framework for the internal market, allowing each Member State to create its own sandbox produces the opposite effect. According to interviewees, the volume of paperwork required to access regulatory sandboxes makes SMEs more hesitant to take part.

A corporate interviewee noted:

"[…] My only fear - the only one - as an Italian, is that we get there after other countries have already created them, consolidated them, tested them, and then we arrive last and set up a very, very restrictive sandbox, and so we end up limiting our companies compared to the competitors from neighboring countries." - INT08_CORP

Similarly, an institutional actor stated:

"[…] Therefore, I'd say that disparities will definitely arise, and perhaps even specific innovation hubs or poles may form. Some Member States might be much more driven toward innovation in artificial intelligence compared to others." - INT05_IST

Another institutional interviewee highlighted:

"[…] meaning that if they ask you for a ton of paperwork and you are a startup, you won't enter the sandbox, and the sandbox will be ineffective." - INT04_IST

Asymmetric burden between big firms and SMEs

From both the institutional and corporate sides, it emerged that big tech companies have greater structural capacities than SMEs to bear the compliance costs deriving from the regulation.

In particular, it emerged that big tech companies have stronger economic resources to deal with potential infringements of the regulation compared to SMEs.

Moreover, from some corporate interviews, it emerged that there is also a disparity in the allocation of human resources, with big tech companies having the possibility to hire big

legal teams and being able to find appropriate professional figures more easily, often from other SMEs, providing higher wages.

An institutional actor noted:

"Big American tech companies are augmenting budget to engage in lobbying activities with regulators." - INT01_IST

As highlighted by an institutional interviewee:

"[…] And for a Big Tech company, which might have a strong team of lawyers, that's manageable - they can pay attention to every detail - but for SMEs and startups, they have to be mindful of ten different regulations at once." - INT02_IST

This perspective was echoed by a corporate interviewee, who stated:

"[…] All the bureaucratic requirements become even heavier if you're an SME compared to a big tech company.
A big tech usually has people fully dedicated to compliance, entire legal teams, specialists who do only that.
We don't.

So, what happens is that the burden weighs much more on us." - INT08_CORP

Another institutional actor observed:

"Now Big Tech are hiring everyone from X company with quadruple salaries." - INT04_IST

The same institutional interviewee noted:

"[…] For which the interpretation of the AI Act that will be given in Italy will be different from the one given in France. This, for example, will be a problem for startups if they want to scale across more than one market instead of remaining in the national market." – INT04_IST

Global deregulatory pressures

From the institutional side only, it emerged that there is currently a push toward deregulation. Interviewees stated that this trend is linked to negotiations with the United States, which are described as seeking a loosening of certain regulatory constraints. In this context, the United States was described as having a lighter regulatory environment aimed at promoting innovation.

An institutional interviewee observed:

"[…] So if, in the negotiations with Trump, they include some sort of reduction - formal or informal - of the weight of digital regulation in Europe, then the first thing that will be conceded is stop-the-clock for the AI Act." - INT03_IST

3.5.3 The need for collaboration between technical and institutional actors

The purple cluster included the categories “Fragmentation of regulatory authority”, “Technical and legal synergies”, “Strong support from public institutions”, “Need for common standards”, and “EU safeguards fundamental rights”, giving rise to the theme of “The need for collaboration between technical and institutional actors”.

It reflects how interviewees described the need for closer coordination between technical expertise and institutional decision-making. Respondents referred to a fragmented regulatory authority landscape where responsibilities are distributed across multiple actors. At the same time, interviewees underlined the importance of technical and legal synergies to ensure that regulatory requirements are scientifically and legally coherent. Furthermore, this need for collaboration was linked to the role of public institutions, which is emerging as a strong provider of support in the implementation of the AI Act, in fact there is a spread in the participation in voluntary regulatory initiatives. Interviewees also referred to the necessity of common standards as a shared reference point between institutions and technical actors. Finally, it emerged a wide hiring of cross-functional expertise combining legal, technical and ethical competencies.

“This sector is so highly technical and, at the same time, so regulated, that it really requires synergy between the legal sector and the more engineering-oriented side.” - INT05_IST

Fragmentation of regulatory authority

From the institutional side only, it emerged that there are difficulties in dealing with a set of authorities that intervene at the same time, often with different outcomes. From the interviews, it also emerged that coordination between national authorities and the AI Office is not simple. Concerns emerged regarding the fact that each body may end up certifying, or not certifying, based on its own “feeling”.

In the words of an institutional interviewee:

“[…] This is a fundamental issue because, if I’m developing a system and I have to go through hundreds of certifications, dealing with Agency X, Agency Y, the national one, the European one - I’ll never get out of it.

And instead of developing and selling my product, I’d be stuck managing paperwork.” - INT05_IST

Technical and legal synergies

From both the institutional and corporate sides, it emerged that there is a need to bring together technical competencies, talking about the knowledge of the technology, and legal competencies. Interviewees referred to the need for engineers and legal experts to find points of convergence.

It also emerged that support is provided by public affairs teams, which try to encourage collaboration between these different professional profiles. Moreover, it is highlighted how many corporations are developing AI systems aligned with compliance-by-design approaches.

A corporate interviewee noted:

"So obviously this means that at our level there is a team of people - of which I am part - mainly legal or government affairs, that tries to help, tries to put together what may be the company's responses to the compliance requirements." - INT10_CORP

An institutional actor pointed out:

"[…] And let's say that, in my view, it suffers from what all these innovation-related topics suffer from - namely, the fundamental need to create a dialogue among policymakers, between the classical profile of a policymaker (who might be a political scientist, a jurist, or an economist) and the computer scientist who can explain how the system actually works."- INT01_IST

Another institutional interviewee stated:

"[…] However, some organizations are moving toward compliance by design, meaning they already design their AI systems to be compliant from the start." - INT05_IST

Another institutional actor highlighted:

"[…] An emerging trend is the creation of cross-functional expertise that combines legal, technical, and ethical competencies." - INT06_IST

Strong support from public institutions

From both the corporate and institutional sides, it emerged that public institutions are recognized as playing a strong supporting role for companies. In particular, interviewees referred to the European Commission and its AI Office as key actors in supporting firms in the implementation of the AI Act. It also emerged that guidelines help companies with compliance, as well as tools such as the AI service desk, which give those who are not

able to interpret certain AI regulations internally the possibility to ask for what can be described as institutional advice.

In addition, interviewees referred to the acknowledgement that there have been delays with respect to the original timeline for some provisions of the regulation, and to the hypothesis of a derogation, which was ultimately introduced for high-risk models.

As noted by a corporate interviewee:

"[…] Already the fact that they are considering a possible derogation shows that the idea of providing support is there." - INT10_CORP

From the institutional perspective, one interviewee noted:

"The market is also starting to perceive AI as a fundamental, essential element. And I must say that, through all these initiatives, the Commission - especially under this new legislature - is now giving significant attention to the industrial side of artificial intelligence." - INT05_IST

The same institutional actor highlighted:

"[…] the European Commission is doing an incredible job. Regardless of everything, the AI Office is doing something truly big and complex. Let's say it clearly, because honestly, they keep getting criticized by everyone, but they're doing an outstanding job. - INT05_IST

Need for common standards

From both the corporate and institutional perspectives, it emerged that there is a need for harmonization of testing methodologies and for the standardization of conformity-assessment procedures. Interviewees also referred to the fact that these elements are still under negotiation between experts and EU officials.

From the interviews, it emerged that the lack of standards creates disorientation among companies, which are still uncertain about how to behave. This is limiting their R&D activities, also in dual projects.

A corporate interviewee noted:

"[…] And then there is the issue of standards.
In industry - particularly industries like defense - a large part of their R&D and production relies on technical standards. Technical standards are obviously fundamental in order to make products operable at the level of the armed forces or the end user.
And so obviously the AI Act and compliance with its obligations essentially create a set of new standards that companies and products will have to follow, and this of course adds another layer of complexity." - INT09_CORP

This concern was echoed by an institutional interviewee, who stated:

"The real issue is that we completely lack standards." - INT03_IST

From an institutional perspective, another interviewee added:

"First, embedding references to international, market-driven standards can help provide a common operational foundation and reduce implementation complexity. These standards offer practical tools for managing risk, promoting transparency, and ensuring accountability in AI development." - INT06_IST

EU safeguards fundamental rights

From both the institutional and corporate sides, satisfaction emerged regarding the role of the European Union in protecting the fundamental rights of its citizens and consumers. From the interviews, it emerged that gradual compliance helps protect citizens from the risks associated with improper use of AI by companies.

Interviewees also referred to the existence of a good level of agreement and collaboration aimed at guaranteeing responsibility and attention in the development and use of AI systems, especially in order to avoid emulating models such as the Chinese system of social scoring. Furthermore, responsible practices are embedded throughout the AI development lifecycles.

A corporate interviewee observed:

"Broadly speaking, I believe the greatest benefits of the AI Act will concern the protection of citizens' fundamental rights. If we look at the list of prohibited practices - such as social scoring or real-time biometric identification for example - we find systems that could seriously endanger individual rights and yet are still legal in other parts of the world." - INT11_CORP

In the words of an institutional interviewee:

"[…] But yes, this is really a big issue. I'm personally very convinced that the value of the European approach -the one centered on putting the human being at the core (man-in-the-loop, etc.) - will, in the long run, prove to be the winning one.
Because, really, the protection of fundamental rights is a distinctive element that should not be, let's say, sold off. - INT02_IST

Another institutional interviewee noted:

"[…] companies are not building AI tools that can cause physical or psychological harm to a vulnerable group." - INT04_IST

Lastly, an institutional interviewee highlighted:

"Many companies are embracing the AI Act as an opportunity to embed responsible practices into their development lifecycles […]" - INT06_IST

3.5.4 Strategic repositioning of European tech companies

The light-blue cluster grouped "EU competitiveness vs US&China", "Insufficient institutional support and investment efforts", "AI governance and innovation roles" and "Calls for reform of the AI Act", highlighting the theme of "Strategic repositioning of European tech companies".

It mirrors how interviewees described the current phase of AI governance as one in which European tech companies are striving to reposition themselves strategically in a competitive global context. Respondents referred to the competitive pressure exercised by the United States and China, while at the same time highlighting perceived shortcomings in institutional support and public investment at the European level. Within this context, interviewees emphasized that AI is transforming business structures through the creation of new corporate roles.

Finally, a common willingness emerged to revise the AI Act in light of the problems identified.

"We are beginning to see that the AI Act indeed gives the possibility, for example, to reduce or modify the description of high-risk uses, and therefore an open approach to the possibility of increasing but also reducing the list of high-risk uses would probably be the best way to ensure companies' ability to continue innovating in Europe - not because one always wants to be outside a regulatory instrument, but because it is not necessarily the case that what four or five years ago was seen as a possible concern has actually materialized into a real concern." - INT10_CORP

EU competitiveness vs US&China

From both the institutional and corporate perspectives, it emerged that the European Union is positioned behind the United States and China in private investment and venture capital in the AI sector. Interviewees also referred that the European market is fragmented because Member States tend to rely on their national markets, unlike the United States, which operates as a single market.

In this context, a corporate actor referred to a saying often repeated in Brussels, described like a joke: "the United States invents, China copies, and the European Union regulates."

From an institutional perspective, one interviewee stated:

"[...] Well, for the moment - I mean, if we have to think very simply - just look at Stargate and the investments announced by von der Leyen in February. We're talking about completely different figures.
Again, I'm not going into how that money is being spent or how it's been allocated - I'm only talking about the figures, purely in numerical terms.

And even if we look at the market capitalization of American or Chinese companies in the AI sector - just think of DeepSeek, which in January entered the market with such force that it actually scared people." - INT05_IST

From the corporate perspective, an interviewee stated:

"[…] Because they want an extremely competitive internal market, where no favoritism is created through state aid for one company over another, or through aggressive merger & acquisition strategies…
but at the same time they want Europe to be competitive externally, against global players.

And these two things are… well, inversely proportional.
You cannot be extremely competitive internally and at the same time externally.
You have to compromise: either you allow state aid, allow consolidation - one big company acquiring 15 smaller ones and thus creating a champion able to compete with external players - or you don't.
If you don't, you will have the most competitive internal market in the history of humanity, but you will not be competitive externally." - INT09_CORP

Insufficient institutional support and investment efforts

From both the institutional and corporate sides, it emerged that there is a need for stronger investment strategies and additional support measures. Interviewees referred to a limited volume of investment derived from a lack of willingness to invest in European AI.

In this context, respondents also mentioned the lack of European unicorns. From the interviews, it emerged that there are expectations for funding initiatives and collaborative projects among EU countries to sustain technological development.

From the corporate perspective, one interviewee stated:

"[…] However, we believe that more agile and easily accessible instruments are needed to further stimulate innovation - for instance, the possibility of accessing the resources of HPC infrastructures located in Italy, developing AI systems within technological sandboxes that already comply with regulatory criteria." - INT07_CORP

Another corporate interviewee emphasized:

"[…] The first is operational support:
they should, in my view, promote the creation of competence centers, technical advisory units, and risk assessment tools - basically systematize their know-how and their administrative and bureaucratic capacities to give operational support to the actors developing these things, to companies, and I'm especially thinking about SMEs and startups." - INT09_CORP

AI governance and innovation roles

From both the institutional and corporate sides, it emerged the creation of new roles and teams dedicated to AI governance within companies like Chief AI Governance Officers. Interviewees referred to a shared push to train staff on how to use AI tools appropriately. It also emerged that new professional figures are expected to develop, in a way similar to the emergence of the Data Protection Officer following the GDPR. Corporate interviewees reported that AI training has been made mandatory across their companies. A corporate interviewee referred to the establishment of dedicated organizational units:

"On the product-development side, I'm also setting up an "AI Business Unit". I'm hiring more senior people because I want to remove myself from the operational AI lead - I'm the CTO, so I have many other responsibilities - and put someone fully dedicated to running the BU, which will then have developers and a proper structure." - INT08_CORP

The same corporate interviewee illustrated that there is an implementation of mandatory internal training program within the company:

"We made AI training mandatory for the entire company - both technical and non-technical roles."- INT08_CORP

A further corporate interviewee noted the emergence of new professional figures:

"These figures called AI ethicists also emerged - they're people who maybe don't have a technical background but a humanistic one, and they try to investigate the ethical aspects of using this kind of system." - INT09_CORP

Finally, another corporate interviewee stated:

"I believe that in the coming years we will see a growing presence of internal committees or designated figures responsible for AI within companies, aimed at ensuring compliance with transparency, accountability, and risk management requirements.
At present, from what I can observe, we are still in a preparatory phase in which professionals with related expertise - such as Data Protection Officers - are increasingly taking on responsibilities linked to AI development." - INT11_CORP

Calls for reform of the AI Act

From both the corporate and institutional sides, calls emerged for a reform of the AI Act as it is right now. Interviewees referred above all to the need to simplify bureaucratic requirements.

In particular, from the corporate side, requests emerged for the establishment of gradual adaptation timelines for currently unregulated sectors and, above all, for SMEs that choose to adopt AI systems. Interviewees also referred to the introduction of tax

incentives for AI systems developed in collaboration with universities and innovative startups.

In addition, respondents mentioned the possibility of modifying the definition of high-risk uses, as well as the need for greater attention to emerging AI phenomena.

From the institutional perspective, one interviewee stated:

"Second, the AI Act should adopt a more dynamic and proportionate approach to compliance, particularly for lower-risk applications and smaller firms. Tools such as simplified reporting templates, capacity-building support, and modular implementation pathways can make a meaningful difference." - INT06_IST

From the corporate side, another interviewee noted:

"[…] Whereas there are problems that to me are much more relevant - such as disinformation tools, deepfakes that could be used, and which should receive slightly different treatment or at least be stimulated to be more strictly controlled from a technical point of view." - INT10_CORP

Finally, an institutional interviewee added:

"[…] Another thing - I hope that startups and SMEs can have privileged access to structures such as not only the Gigafactories and AI Factories, where there is already significant industrial development, but also, as far as the AI Act is concerned, that they can have a privileged entry point to structures like the AI Desk. - INT05_IST

3.5.5 The AI Act: an enabler of strategic innovation?

Finally, the green cluster, composed of the only "The AI Act as an opportunity for innovation", has been interpreted as "The AI Act: an enabler of strategic innovation?" theme.

Despite being composed of a single category, this cluster is particularly relevant as it captures interviewees' views on the role of the AI Act in relation to strategic innovation and because it has strong connections with each of the other clusters.

The theme is framed *ad hoc* as a question in order not to provide a definitive answer, and because it emerged as a divisive issue among respondents. Indeed, this theme reflects the coexistence of different perceptions regarding the innovative potential of the AI Act, also in relation to what emerged in other themes, such as "Regulatory and institutional capacity gaps".

"[…] So, obviously - I repeat - the AI Act represents an attempt made by the European Commission, the European Union, to promote responsible innovation that takes into account safety, fundamental rights, transparency, and all that." - INT09_CORP

The AI Act as an opportunity for innovation

The AI Act has the ability to stimulate innovation within businesses and increase their strategic competitiveness, according to institutional and corporate actors.

This is because the regulation clarifies and defines a legal space in which artificial intelligence is regulated and within which companies can operate, as stated by an institutional respondent.

From both perspectives, the regulation was described as a starting point.

According to an institutional interviewee:

"[…] there's the topic of the model life cycle, data collection, clinical trials, synthetic data, consent management, these are all… these are all things that surely, probably, the AI Act has given an impulse to organize." - INT04_IST

An institutional interviewee noted:

"It has the potential to establish a benchmark for trustworthy AI globally, enhancing user confidence and international collaboration." - INT06_IST

Similarly, a corporate interviewee added:

"We believe that the AI Act represents an important starting point for responsible innovation, fully reflecting the
ethical spirit that the EU places at the core of every form of innovation" - INT07_CORP

After presenting the empirical results in Chapter 3, the analysis shifts to Chapter 4 (Discussion), which involves a process of theoretical building and regeneration.

The identified themes are reexamined through "alternative casing" to provide new theoretical meanings, placing the study's emergent insights within current theory and in conversation with the two sensitizing concepts: the Institution-Based View (IBV) and AI governance under the AI Act.

Now let's turn the page.

Chapter 4

Discussion

4.1 From empirical results to theoretical generation: alternative casing

Following the *iter* of abductive methodology, after the phases of "revisiting" and "defamiliarization", the analysis now moves to "alternative casing", in which the results are reread and rearticulated through the lens of the two sensitizing concepts: AI governance under the AI Act and the Institution-Based View (IBV). This step is undertaken to explore alternative interpretations of the same empirical material and to generate new theoretical explanations when, and if, existing ones prove insufficient (Timmermans & Tavory, 2012).

Before going further, it is important to make two clarifications: the first is that in this chapter, the IBV is extended and viewed from a broader perspective concerning the social paradigm of AI; therefore, it never fully contradicts it, but it is largely supported, as will be argued in the following paragraphs. After interviewing institutional and corporate actors, the researcher attempts to contribute by adding aspects that enrich IBV as a theory, seeking to discover new phenomena that are occurring at this historic moment in the management of AI governance in the European Union.

The second clarification concerns the fact that only a few provisions of the AI Act have come into force and that, therefore, the statements made are based exclusively on the results of the interviews. The European regulation on artificial intelligence is subject to continuous changes and, therefore, it can be defined as a regulation that is still incomplete in its implementation.

Thus, the goal of this chapter is to explain how organizational opportunities and regulatory constraints interact in shaping tech companies' strategic responses to the AI Act, generating a new theoretical model.

4.2 What the results confirm: alignment with existing literature

It is important to consider how the results of this study confirm the theoretical foundations of the Institution-Based View proposed by Peng et al. (2009), also through its two core

Propositions, demonstrating coherence with the theoretical framework adopted in this thesis.

The results clearly show that the role of institutions is indispensable, since market structure and firms' internal resources alone are insufficient to explain how tech companies undergo strategic innovative transformations.

At the same time, a consistent *fil rouge* emerges that remains faithful to the theory, as the AI Act, taken as a formal institution, proves to generate significant constraints for technology firms, shaping and influencing their corporate strategies. The following subsections build on this alignment with the Institution-Based View by looking at how formal and informal institutions function under the AI Act and how tech companies strategically still pursue their interests in these institutional pressures. In doing so, the analysis also confirms the insights emerging from the literature review of the EU digital regulation.[16]

Following an abductive logic, confirmation is a necessary step before theoretical regeneration. Without establishing alignment, any attempts at extension would be weak.

4.2.1 The role of formal and informal institutions under the AI Act

Recalling the Institution-Based View, formal and informal institutions define the "rules of the game" within which managerial decisions are made and delimit the playground within which firms can operate (North, 1990).

Indeed, among the main functions of institutions is that of reducing uncertainty and defining what is considered legitimate, conditioning strategic choices. Regulatory uncertainty is partially reduced since this *ad hoc* framework has been established, creating a dedicated law concerning artificial intelligence.

Based on the results obtained from the interviews, it can be argued that the European regulation on artificial intelligence represents, and will continue to represent, a central institutional reference for technology companies.

Building on this, and in line with De la Mothe (2004), technology and innovation should be viewed as essentially social processes that are tightly connected to their institutional context rather than as only technical phenomena. Therefore, institutional structures and actors, including IOs, mediate technological decisions that define modern civil societies. In this way, the European Union becomes a constitutive institutional actor that uses its

[16] Cf. Chapter 1, paragraph 1.2

legal framework to actively shape the course of artificial intelligence development on the European continent.

This raises the question of how tech companies are experiencing, in practice, the conditioning role of institutions, whether formal or informal, under the AI Act context in the EU.

The EU regulatory trend involves an international institutional opposition, where external actors, especially the United States, are perceived as attempting to lessen the weight of the AI Act, possibly through negotiations that could result in delays like the "stop-the-clock". The IBV assumption that company behavior is shaped within a multi-level institutional framework (Tywoniak & Peng, 2006), where global power inequality and competing overseas regulatory models impact European norms, is strengthened by this external institutional pressure. Similar perceptions had already emerged during the debate surrounding the Data Act, which was interpreted by Mikhail (2025) as being structured in a way that could disadvantage firms headquartered in the United States by constraining data-driven business models and potentially slowing innovation, while comparatively favoring European companies.

Moreover, the lack of a significant presence of European unicorns and structural disadvantages in venture capital and market size, when compared to the US and China, are the reasons for contrasting the EU's regulatory ambitions with what respondents described as inadequate institutional support and limited investment capacity. In this case, formal institutions can simultaneously create a robust governance framework while failing to offer complementary enabling conditions, influencing businesses' strategic decisions in a setting where institutional support for scaling innovation is seen as relatively weak, but compliance requirements are high.

Furthermore, the institutional design of experimentation tools is another aspect.

Although the AI Act seeks to establish a unified framework for AI systems in the internal market, the option for Member States to establish national sandboxes poses the risk of creating differentiated innovation plans and competitive distortions across countries. This makes the fragmented sandbox implementation a particular tool through which formal institutions can shape innovation in tech companies differently from Member State to Member State.

This fragmentation may result in unequal chances for testing and developing AI systems, which could disadvantage businesses operating in more restrictive national environments or in ecosystems that are still in the early stages of development. From an IBV perspective, this means that formal institutions can influence strategic innovation through administrative and geographical modalities that structure regulatory flexibility (Vecchi et al., 2015).

However, sometimes formal institutions, especially those run by the European Commission, can facilitate strategic innovation by offering institutional support in well-defined areas. The creation of the AI Office and the AI service desk was characterized as a concrete type of institutional support that aids businesses in adapting to the new AI landscape, decreasing uncertainty and providing direction that is particularly pertinent in situations where businesses lack the internal capacity to independently interpret requirements.

In this case, the Commission's supportive architecture is consistent with the IBV concept that institutions grant legitimacy and minimize uncertainty (Tywoniak & Peng, 2006; Peng et al., 2009; North, 1990). According to Yang et al. (2025), stronger innovation performance is linked to closer ties between businesses and high-level governmental organizations because institutional proximity offers coordination and strategic guidance. In this regard, the EU case reflects these already seen processes in the literature. Similar to this, solid institutional support from the public encourages innovation by lowering uncertainty and demonstrating long-term commitment, as noted by Sony & Aithal (2020). In addition, this aspect is also connected to the EU's normative orientation: the protection of fundamental rights was presented as a unique institutional characteristic of the European approach, defining what constitutes acceptable AI innovation and setting EU governance distinct from non-democratic models.

Furthermore, considering Peng et al.'s (2009) Proposition II[17], a particular focus should be given to the role of informal institutions and, in this case, informal constraints.

Under the AI Act, several formal constraints are unclear in an operational and strategic sense. While the regulation formally defines obligations and risk categories, firms face persistent uncertainty regarding how technical requirements will be concretely applied

[17] II Proposition - "*While formal and informal institutions combine to govern firm behavior, in situations where formal constraints are unclear or fail, informal constraints will play a larger role in reducing uncertainty, providing guidance, and conferring legitimacy and rewards to managers and firms"* (Peng et al., 2009).

and how fast-evolving AI systems will be assessed against static legal definitions. This uncertainty is reinforced by the structure of the AI Act itself, such as its product-safety logic and the coexistence of multiple regulatory objectives, which collectively limit firms' ability to translate formal rules into stable strategic expectations.

From an Institution-Based View perspective, this situation produces a gap between formal constraint and practical guidance. Exactly here, informal constraints acquire a larger role. Tech firms are increasingly relying on non-codified mechanisms, precisely "informal constraints" such as the creation of dialogue between policymakers and engineers and the expansion of public and government affairs functions to understand how to cope with uncertainty about how to behave.

These practices help firms "make sense" of the regulation while it is still evolving and unevenly interpreted, confirming a continuous exchange between formal and informal institutions.

Informal constraints re-channel regulatory pressure into organizational routines aimed at avoiding penalties and complying with the regulation as much as possible, since formal institutions are technologically challenged and continuously evolving, and since several interviewees stated that AI is impossible to regulate.

4.2.2 Strategic interests under the AI Act

If Section 4.2.1 shows why institutions still matter in this context, this paragraph shows how Proposition I of Peng et al. (2009)[18] is reflected in the way tech companies are trying to pursue their own interests despite the difficulties involved. The aim here is not to map the full set of corporate responses; this can be visualized and conceptualized in the process model (Section 4.4).

First, the results show that the AI Act's regulatory burden is unequally allocated among businesses, mirroring patterns seen in earlier EU digital legislation.[19] Due to their smaller organizational capacity and greater relative administrative costs, SMEs typically face more resource-intensive compliance requirements under the GDPR and the Data Governance Act than do bigger companies (Lindgren, 2018; Jackson et al., 2024). This complexity is further increased by the AI Act's coexistence with other EU digital frameworks. Thus, companies change their innovation objectives and scale-up choices in

[18] I Proposition - *"Managers and firms rationally pursue their interests and make strategic choices within the formal and informal constraints in a given institutional framewor*k" (Peng et al. 2009).
[19] Cf. Chapter 1, paragraph 1.2

accordance with their resource limitations and risk exposure, resulting in different strategic responses.

Second, companies rationally reallocate resources and make internal organizational changes in response to institutional pressure. In order to maintain operational continuity and competitive positioning under the AI Act, deliberate strategy decisions are reflected in investments in specialist competencies and internal governance capability. According to earlier studies on digital transformation, these organizational adjustments are logical reactions to a changing institutional context (Hinings et al., 2018; Ullagaddi, 2024).

Lastly, companies prioritize compliance efforts and schedule adaptation over time when faced with complex obligations, balancing prospective sanctions against innovation and market objectives. While smaller organizations employ more defensive and selective tactics, larger firms are typically better equipped to absorb compliance expenses through specialized legal and institutional capacities.

These trends support Proposition I of the Institution-Based View, which states that businesses logically modify their resource allocation and compliance targets to further their goals under the AI Act.

4.3 What the results extend: a theoretical regeneration

Despite the literature confirmations covered in the previous section, results also draw attention to features that are missing in the corpus of existing research and can be explained from a different perspective. In particular, they reveal several anomalies that, when applied to rapidly evolving, technically complex regulatory frameworks such as the European AI Act, broaden and innovate the Institution-Based View (IBV).

Yet the empirical evidence emerging from the five themes[20] suggests that the AI Act operates through additional mechanisms that can extend the existing IBV theory. On purpose, this section directly addresses the research question by articulating the study's theoretical contribution, asserting that the AI Act, as a formal institution, does not necessarily reduce uncertainty, and it challenges stability given the rapid evolution of AI technologies. Moreover, the AI Act shapes different behaviors for tech firms; thus, this regulation cannot be considered as an "independent variable".

[20] "Regulatory and institutional capacity gaps"; "Uneven innovation environments for tech companies"; "The need for collaboration between technical and institutional actors"; "Strategic repositioning of European tech companies"; "The AI Act as an enabler of strategic innovation?".

Indeed, the AI Act acts on the strategic innovation of tech companies through four fundamental mechanisms: “Interpretative and operational uncertainty,” “Temporal misalignment and instability,” “Asymmetric institutional environments,” and “Institutional co-evolution.” Tech companies, in turn, are responding with strategies for adaptation and business innovation.

The output of these reflections will result in a new theoretical process model.

4.3.1 Interpretative and operational uncertainty

By adopting an abductive approach and focusing on the interaction between formal regulation and firms’ interpretative practices, this study extends the IBV, providing insights into how the EU AI Act affects strategic innovation in tech companies through an “Interpretative and operational uncertainty” mechanism. Classical IBV theory argues that one of the most important roles of institutions is to reduce uncertainty (North, 1990; Tywoniak & Peng, 2006; Peng et al., 2009), whereas Scott (1995) argues for a clear distinction between the normative and cognitive pillars.

The empirical results of this study go beyond these concepts, demonstrating that this function is not always satisfied.

In the context of European artificial intelligence regulation, IBV appears to be partially applicable because the theme of “Regulatory and institutional gaps” gives rise to a concept where uncertainty comes from the difficulty of understanding its operational meaning and not from the absence of rules, since there is a written and approved regulation.

Actually, this finding extends the IBV by showing that the difficulty of converting legal principles into specific organizational and technological practices creates uncertainty.

Thus, the AI Act is perceived as operationally ambiguous by both institutional and corporate actors, suggesting that formal rules alone are insufficient to guide behavior clearly.

From this perspective, the AI Act should be seen as an incomplete institution that shifts the work of reducing uncertainty within the companies themselves. The public sector competence gap (at least initially) shows how the ability of public institutions to reduce uncertainty is limited by a lack of adequate technical expertise in AI.

This shortage is perceived at its source as structural, affecting then the quality of the interpretations provided to companies: it can be noted from the example of dual-use

technologies quoted in INT 09 in the category "Structural limits of the AI Act"[21], which illustrates how these limitations translate into ambiguity regarding corporate behavior.
In this way, the institution fails to fully perform its cognitive reference function, generating uncertainty about how companies should act in practice.
The category of "Lack of technical clarity and competence" further supports the idea that uncertainty is technical and not exclusively regulatory. The results show that both regulated actors and competent authorities encounter difficulties in understanding which technical requirements, tests, or evaluation criteria should be acceptable for compliance purposes. This difficulty is linked to the fact that defined standards are still lacking, contributing to the incompleteness of the regulation.
Furthermore, uncertainty is accentuated by overlap between the AI Act and other European digital regulations. The category of "Overlapping digital regulations" highlights how regulatory stratification complicates compliance processes, where companies admit difficulty in identifying which set of rules prevails or which provisions of which regulation are being violated. Here too, firms face a layered regulatory environment that undermines interpretative clarity, since there are now more than 10 EU digital regulations (Marinello, 2023).

4.3.2 Temporal misalignment and instability

By engaging with the temporal dimension of the regulation, this study reveals how the AI Act is interacting with the rapid evolution of AI technologies, affecting the strategic innovation of tech companies through a mechanism of "Temporal misalignment and instability".
As observed in Chapter 1, Scott (1995) views institutions as "*regulatory, normative, and cognitive structures and activities that provide stability and meaning to social behavior*."
On the other hand, the results show that in the presence of evolving technologies such as AI, it is a real challenge to maintain regulatory stability, as this translates into strategic instability. AI is a set of technologies that are unpredictable and evolving, from one day to the next. Regulatory frameworks find it difficult to keep up with technological advancements due to the rapid speed of change. A demonstration of this dynamic occurred on November 30, 2022, when ChatGPT was launched. At that moment, it was a type of technology that did not fall within the definitions given in the AI Act, so the draft

[21] Cf. p. 67.

text was quickly amended to try to be ready for the European Parliament's proposal in March 2023.

In the context of the AI Act, the findings reveal a temporal and structural misalignment between regulation and technology, making the temporal dimension a crucial variable for understanding institutional influence on innovation. Thus, the effects of institutions on innovation depend on the timing between regulation and technology.

This mechanism is also associated with the category "AI evolution outpacing regulatory timing," which explains how an environment in which the pace of technological development makes it extremely difficult for regulation to maintain consistency over time, meaning that what is defined and regulated at an early stage risks losing relevance in relation to market practices[22]. In this scenario, instability directly affects companies' strategic choices as well as regulatory planning: regulation cannot be treated as a stable reference point, making it difficult for tech companies to plan innovation according to medium to long-term logic. With this in mind, tech companies find themselves immersed in a context where regulation is perceived as subject to sudden and continuous revisions. This situation helps to interpret the results associated with the theme "Strategic repositioning of European tech companies", in particular from the category "AI governance and innovation roles". The results suggest that the lack of regulatory stability in the AI Act is pushing tech companies to adopt anticipatory innovation strategies, in which the ability to respond to regulatory and institutional changes becomes part of the corporate architecture, as reflected in the emergence of positions dedicated to AI governance.

This anticipatory logic is further reinforced by recent institutional developments. 3265 companies, including MNCs and SMEs, have signed the European Commission AI Pact (European Commission, 2025), which was announced in September 2024, committing to voluntary promises before the full implementation of the AI Act. The Pact pushes businesses toward anticipatory compliance and adaptive innovation strategies by encouraging them to create AI governance policies and identify high-risk systems before formal legal obligations apply. Before the EU AI Act's requirements for general-purpose AI models beginning on August 2, 2025, nearly all significant US Big Tech companies, including Amazon, Google, Microsoft, and OpenAI, voluntarily signed the Code of

[22] Cf. Category "Structural limits of the AI Act".

Conduct (Haeck, 2025). Twenty-six enterprises have already signed on, including European firms like Aleph Alpha and Mistral AI. While xAI only signed the safety chapter, Meta is the only significant exception. (Haeck, 2025)

These dynamics highlight how strategic reactions to the AI Act are determined by temporal misalignment and instability, turning time itself into an essential component through which institutions impact innovation.

4.3.3 Asymmetric institutional environments

This study identifies an "Asymmetric institutional environments" mechanism through which the AI Act influences strategic innovation because the regulation interacts with existing organizational and territorial differences, creating innovation opportunities in uneven ways.

According to DiMaggio & Powell (1983), isomorphism is a process that causes organizations to behave homogeneously or similarly in a given institutional context to gain legitimacy. Furthermore, more generally, IBV recognizes that institutions strongly influence competition and innovation, as illustrated by Peng et al.'s (2009) analysis of the pharmaceutical industry in Japan[23]. However, the empirical findings of this study demonstrate that institutional impact fails to produce uniform consequences in the context of the AI Act.

The data show that not all companies can innovate and behave in the same way: large tech companies manage, albeit with difficulty, to absorb compliance costs, while SMEs, despite the formal existence of incentives for entering sandboxes, experience a significant limitation in their capacity for experimentation. In the AI domain, compliance is seen as a capability that enables or hinders innovation. Thus, the influence of the AI Act on innovation is also conditioned by the organizational capacity of companies to sustain compliance requirements.

This asymmetry emerges particularly clearly from the theme "Uneven innovation environments for tech companies," especially through the category "Fragmented sandbox implementation."

As previously discussed, the results show that the obligation for each Member State to establish its own national sandbox introduces competitive discrepancies both across EU countries and among companies operating within them. This situation risks producing a

[23] Cf. paragraph 1.1.1

contradiction: while the AI Act was created to establish a single regulatory framework for the internal market in the field of AI, the emergence of numerous national sandboxes ends up further fragmenting the institutional ecosystem. There are some countries, such as Spain, for example, that have managed to create sandboxes more quickly, while there are other countries that are lagging or adopting more restrictive criteria that risk limiting the opportunities for experimentation for their companies. For this very reason, some respondents expressed concern that, in Italy, the late and overly cautious implementation of sandboxes could translate into a competitive advantage for companies located in other Member States.

It is likely that these disparities will arise and that specific centers or hubs of innovation may even form. Some Member States may be much more innovation-oriented in artificial intelligence than others. However, this is also part of the very nature of the economies of individual Member States.

A second level of asymmetry concerns the different ability of companies to remain compliant, as highlighted by the category "Asymmetric burden between big firms and SMEs". Large technology companies, with their strong teams of lawyers, have the necessary resources to analyze the regulation in detail and support alternative interpretations, including through litigation at the Court of Justice in Luxembourg. The ability to draw on a large number of technical and legal experts allows them to "cover their backs" both legally and in terms of interpreting the regulation. It is also important to note that, in terms of public affairs budget allocation, many large technology companies have allocated more funds to specialists or experts in the field, preferring to follow the development of the AI Act from 2021, or even earlier, rather than focusing on other digital regulations or directives under discussion. On the contrary, for SMEs and startups, the situation appears radically different. In "Regulatory burden on SMEs," under the theme "Regulatory and institutional capacity gaps," results indicate that these companies face a particularly heavy burden in maintaining complete process traceability and extended document retention. Often, the need to produce large amounts of documentation is a real obstacle to accessing sandboxes, which risk becoming ineffective precisely for the players who should benefit most from them.

4.3.4 Institutional co-evolution

After the mechanism of uncertainty, temporal instability, and asymmetry discussed above, the results highlight how institutions and regulated actors appear to adjust to one another through ongoing processes of "Institutional co-evolution."

In the context of the AI Act, the traditional conception of institutions as external factors influencing business strategies can be expanded, as a more intense and structured dialogue emerges between regulators and regulated entities, preventing institutions from being considered mere "independent variables" (Peng et al., 2009).

As we saw in Chapter 2, the AI Act is a work in progress because many provisions have yet to become mandatory, and it is in the early stages of implementation. In this phase, whether companies see the regulation as a constraint or as an opportunity for innovation depends on the ability to reach the best possible "good rule". A "good rule" provides a clear and effective framework for the functioning of the AI sector and encourages investment rather than hindering it. If the rules provide clarity, they become an asset. The results suggest that innovation and regulation must go hand in hand, according to a by-design logic. In this sense, regulation can generate added value by guiding technological development in a sustainable and predictable way, not limiting business activities. Innovation and regulation can be seen as complementary elements that must be kept together and not as antinomies. For this to happen, regulation must be of high quality and capable of addressing the complexity generated by technological innovation. Effective governance cannot be indifferent to the technical and social implications of innovation; on the contrary, it must integrate these dimensions and simultaneously coordinate development and control requirements. The path to achieving this form of governance emerges from a joint effort between institutions, businesses, and universities. It is precisely in this circumstance that the mechanism of co-evolution between rules and innovation, and between different stakeholders, becomes visible. This mechanism is based on the theme of "The need for collaboration between technical and institutional actors." In fact, the category of "Technical and legal synergies" shows that effective regulation of AI systems requires a deep understanding of how the technologies work, which can be achieved only through continuous exchanges between legal and technical expertise. These exchanges become an integral part of the institutional and regulatory process itself. Similarly, the "Need for common standards" reflects the concept of co-

evolution between regulation and innovation, in which constant coordination between AI experts and policymakers contributes to the development of standards, leading to a compromise for "good regulation." Institutional co-evolution is further supported by the role of public institutions at the European level. The category "Strong support from public institutions" highlights how these actors remain attentive to the needs of businesses during the implementation phase. Indeed, the AI Office is moving in a direction that favors providers and deployers of AI systems by informing them about regulatory developments, thus engaging in dialogue with the industry through clarifications and guidelines, also taking into account the AI desk. In this way, the European Commission's action emerges as a concrete attempt to transform the AI Act from a regulatory constraint into a governance infrastructure, sometimes trying to help companies understand and gradually integrate regulatory requirements into their organizational models. Finally, institutional co-evolution is confirmed by the theme "Strategic repositioning of European tech companies," particularly through the category "Calls for reform." Businesses play a key role in making their voices heard and communicating their ideas for regulatory changes to institutions. Calls for greater flexibility and less bureaucracy have led the European Commission to put forward proposals that, among other things, involve simplifying and revising the AI Act. The "Digital Omnibus", among other things, proposes to make the obligations on high-risk AI systems mandatory only when technical standards for testing their compliance are in place, setting a maximum period of 16 months from their adoption for effective implementation. In this way, companies are partially relieved of compliance costs, allowing them to explore adjustments over time and plan resources (LCA Lex, 2025).

4.4 A new theoretical model

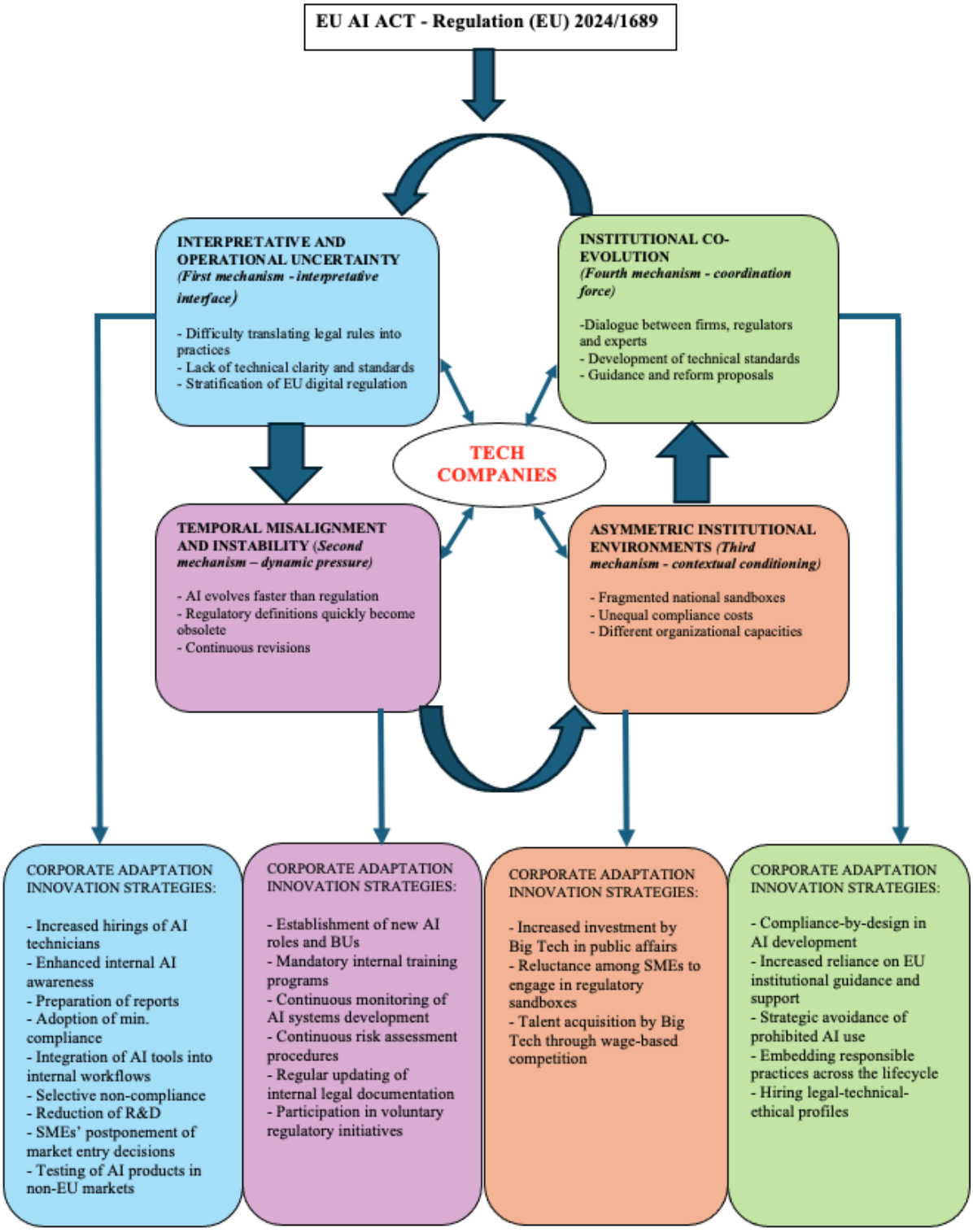

Diagram 3. A Process Model of Institutional Influence and Tech Corporate Adaptation under the EU AI Act

4.4.1 Institutional influence and tech corporate adaptation under the EU AI Act

Diagram 3 illustrates the theoretical model labelled "A Process Model of Institutional Influence and Tech Corporate Adaptation under the EU AI Act."

The model integrates the abductive reasoning carried out through the "alternative casing" phase of Timmermans and Tavory's (2012) methodology and visually synthesizes how the European AI Act influences strategic innovation in technology companies through four interrelated mechanisms operating in a logical, circular order.

Building on the discussion in Sections 4.2 and 4.3, extending the IBV, this model views the AI Act as a formal institution immersed in an incomplete and evolving regulatory regime.

First, the process begins with "Interpretative and operational uncertainty," which constitutes the primary interface between the AI Act and firms' organizational practices. This mechanism comes from the theme "Regulatory and institutional capacity gaps", where categories such as the "Public-sector competence gap", "Lack of technical clarity and competence", "Structural limits of the AI Act", "Regulatory burden on SMEs", "Overlapping digital regulations" and also from the theme "The need for collaboration between technical and institutional actors", category "Need for common standards".

This shows that uncertainty is given by the difficulty of translating formal obligations into operative technical and organizational practices. In this setting, firms are currently in a state of confusion; they are unsure how to proceed, given that the regulation remains "in progress" and since there is excessive regulation in the digital domain, making it difficult to understand the legal boundary between one law and another.

To adapt to this mechanism, tech companies activate a set of corporate adaptation innovation strategies aimed at restoring internal controllability over an uncertain regulatory environment.

Firms are increasing their recruitment of highly specialized technical figures who have in-depth knowledge of artificial intelligence systems. In this case, this is primarily pointing to experienced computer engineers who can clarify how programs work and how they should be used correctly.

In addition, awareness campaigns on AI are being carried out within organizations, from the board of directors down to interns. This is because there is a need to be aware, especially among senior figures, of the importance of all the implications that this set of

technologies can bring, of the opportunities they offer us today, and of how essential it is to interact with them as soon as possible. In fact, companies are preparing internal reports to share their thoughts on possible scenarios concerning both the evolution of the text of the regulation in question and the evolution of technologies that may have an impact on their industry.

Furthermore, given the lack of operational certainty, tech companies are favoring a minimal compliance approach to the AI Act, not seeing full compliance as a factor that can bring competitive advantage. They seek to interpret the law in such a way as to respect its fundamental principles without really going into depth: there is a tendency to adopt a more conservative, compliance-oriented stance.

Moreover, there is a growing trend towards adopting AI tools such as Copilot, Claude, Gemini, Grammarly, and ChatGPT in their workflows. This applies to all business departments, and in many cases, it is no longer optional: they must start using them immediately because they are helpful tools for everyday operations, saving time and costs.

In a context characterized by a strong stratification of countless European digital regulations, such as GDPR, DSA, DMA, Data Act, DGA, and Digital Europe Programme, many companies, especially SMEs, not knowing which provisions and rules could be violated in their business operations, choose to break laws that carry minor penalties and fines. This type of opportunistic adaptive strategy is based on a comparative assessment of regulatory risks, thus revealing a tendency to favor selective compliance with regulations. In this way, companies seek to maintain operational continuity and economic sustainability in an uncertain institutional environment.

Due to a continuing lack of standards, tech companies are temporarily freezing or scaling down experimental projects whose legal status remains ambiguous. This tendency is especially pronounced in dual-use contexts, where AI systems developed for civilian purposes may also generate security and surveillance issues. Thus, limiting their R&D activities, firms are prioritizing low-risk applications that can be more aligned with existing compliance interpretations. Finally, many SMEs adopt a wait-and-see strategy, postponing market entry until the AI Act is fully operationalized through certifications and technical standards. During this phase, several firms redirect testing and selling

products towards third-country markets, outside the EU, where regulatory frameworks are less demanding.

The initial uncertainty is subsequently intensified by “Temporal misalignment and instability”, which introduces a dynamic dimension into the institutional influence process. Deriving from the category “AI evolution outpacing regulatory timing”, this mechanism shows the reason why the AI Act affects innovation through timing: the rapid obsolescence of definitions and the perceived impossibility of regulating “correctly” in real time undermine the stabilizing function attributed to institutions, pushing firms toward anticipatory and adaptive innovation strategies. This aspect is empirically reinforced by the theme “Strategic repositioning of European tech companies” with the category “AI governance and innovation roles”.

To counteract this mechanism of instability, tech companies are redesigning their corporate architecture with the creation of new roles dedicated to AI governance, such as Chief AI Innovation Officers, Chief AI Officers, Chief AI Governance Officers, and AI Ethicists. These new roles are responsible for continuously monitoring regulatory and technological developments, coordinating internal adaptation processes, and integrating regulatory requirements into the development of AI systems. On the product development side, this is reinforced by the creation of AI Business Units, which are designed as semi-autonomous organizational structures tasked with managing the development and commercialization of artificial intelligence systems. These units are composed of cross-functional teams that identify and plan specific actions resulting from the adoption of AI tools, taking into account all regulatory aspects.

Therefore, there is a trend in making AI training mandatory within companies, both for technical and non-technical staff. Firms are searching for courses, both free and paid, identifying which ones are useful and dividing them by level and then assigning accountability to one person who oversees the training paths for different departments, from finance to sales.

This is crucial because, for example, salespeople need to be able to sell a product with AI, and if they don’t fully understand what they are selling, it’s a problem.

The courses range from basic theory, such as what an LLM is, to highly advanced modules such as fine-tuning techniques. This is also becoming compulsory for companies along the supply chain, which are underneath them and deal with hardware tools.
Finally, in order to detect changes that can impact a system's risk profile, tech organizations are putting continuous monitoring of AI system development into practice. This entails the tracking of AI models throughout their whole lifecycle (from design and training to deployment and post-market use). This makes it possible for firms to identify new compliance problems early on and take action before regulatory thresholds are exceeded. The implementation of constant risk assessment methods, which use iterative risk assessment frameworks that are updated on a regular basis in response to the European Commission clarifications or technical advancements, complements this practice. Then, companies regularly update their internal legal documents, which primarily include guidelines, internal policies, technical documentation, and contractual terms that must be aligned with the rules and decisions that the European Commission will make. Finally, tech businesses are becoming more involved in voluntary regulatory initiatives, like the Code of Practice, which serve as soft-law tools to operationalize the AI Act and explain expectations prior to legally enforceable implementation steps. Participation is still unequal, though, as some businesses have supported these voluntary commitments while others, like Meta, have decided not to join (Haeck, 2025), indicating different strategic evaluations of the advantages and disadvantages of early regulatory harmonization.

The effects of uncertainty and instability are then filtered through "Asymmetric institutional environments", determining how firms are able to respond to the AI Act.
This mechanism derives from the theme "Uneven innovation environments for tech companies" and highlights how fragmented sandbox implementation and asymmetric regulatory burden generate different innovation conditions across firms and territories.
In this context, compliance capacity becomes a strategic resource, enabling larger firms to deal more easily with complexity through dedicated legal teams while constraining SMEs' experimentation due to disproportionate bureaucratic demands. Thus, instead of creating uniform effects, asymmetry in the model influences the distribution and intensity of strategic innovation.

Following this mechanism, companies, especially Big Tech, as noted previously, are making large investments in lobbying and legal teams to bear the cost of compliance imposed by the regulation. This strategy allows these companies to internalize the compliance costs, making regulatory compliance a stable organizational function.

The more consultants you can afford, the more institutional affairs you can manage, the greater will be your overall weight in the market. In addition, Big Tech companies are pursuing an aggressive hiring strategy, recruiting highly skilled personnel from other tech companies by offering significantly higher salaries and more competitive contract terms. This rapidly strengthens Big Tech's already impressive capabilities by integrating specialist skills that are difficult to develop in the short term.

In contrast, SMEs are taking more defensive adaptation strategies under asymmetric institutional environments. Many SMEs show strong reluctance to participate in regulatory sandboxes, perceiving them as non-convenient due to extensive documentation requirements and administrative complexity. Sandboxes are interpreted by SMEs as expensive compliance exercises that divert limited organizational resources away from core innovation activities.

Furthermore, SMEs tend to avoid scaling their operations across multiple European markets, preferring to remain within national boundaries. Structural differences in regulatory interpretation and institutional structures across Member States increase the costs and risks associated with cross-border expansion.

In conclusion, "Institutional co-evolution" represents the mechanism where regulation and innovation co-develop through constant interaction over time. It is grounded in the theme "The need for collaboration between technical and institutional actors" and reinforced by categories such as "Technical and legal synergies", "The need for common standards", "Strong support from public institutions", "Calls for reform of the AI Act", and "EU safeguards fundamental rights".

In the model, co-evolution serves as a coordinating function, turning the AI Act from a source of uncertainty into a developing governance framework shaped by dialogue and reform ideas, especially in the case of the development of standards.

In conformity with this mechanism, a growing number of organizations are moving towards the development of AI systems aligned with compliance-by-design approaches.

Some organizations are moving towards compliance by design, meaning that they are already designing their AI system to be compliant from the start. So basically, they ensure the highest standard for their consumers, creating trust. In this way, they communicate this sense of safety in using AI; they may become a driver for consumers themselves.

Businesses' growing reliance on institutional support mechanisms offered by the European Commission and the AI Office is another indication of this co-evolutionary force. In the context of the AI Act, these organizations are increasingly seen as crucial tools for support, providing direction, explanation, and interpretive aid. By interacting with these institutional actors, businesses participate in a feedback loop that gradually clarifies regulatory expectations through continuous communication with market players.

Additionally, businesses are avoiding developing AI applications that can hurt people physically or psychologically, as this is forbidden by Article 5. Tech businesses are including ethical practices and fundamental rights safeguards throughout the whole AI development lifecycle in accordance with the concept of a "trustworthy AI". This involves paying more attention to matters like accountability procedures, openness, human monitoring, and bias mitigation, which strengthens the connection between technological advancement and the EU's value-based regulatory framework.

Lastly, the increased hiring of cross-functional experts with legal, technological, and ethical capabilities coincides with these changes. Businesses are looking for hybrid profiles who have knowledge of management, engineering, and law.

Specifically, businesses are hiring more academic talent, such as researchers and technical specialists with extensive expertise in AI systems and ethics. In addition to strengthening their ability to interact with institutional actors and changing regulatory expectations, this interaction between academia and industry enables businesses to internalize the latest technological knowledge and normative competence.

These four mechanisms and their relative corporate adaptation innovation strategies explain how the AI Act influences strategic innovation in tech companies through a mediated institutional process model that includes interpretation, temporal adaptation, structural asymmetries, and interactive governance. In this sense, the influence of the AI Act on strategic innovation is yet non-deterministic. Thus, strategic innovation emerges as a negotiated outcome determined by uncertainty, instability, uneven institutional

environments and progressively reoriented through co-evolutionary interactions among firms and institutions.

4.5 Policy suggestions and managerial implications

This section presents a set of policy suggestions for EU policymakers and managerial implications for managers of tech companies, building on the empirical findings and the theoretical regeneration, extending the Institution-Based View. The four institutional mechanisms that emerged in the theoretical model, "Interpretative and operational uncertainty", "Temporal misalignment and instability", "Asymmetric institutional environments", and "Institutional co-evolution", are the direct source of these recommendations. In light of how businesses and institutions are already acting, this part seeks to translate these mechanisms into further operational insights to guide the actions of core institutional and corporate actors.

To create more favorable conditions for technology companies to thrive within the new regulatory framework, institutions should establish a single EU regulatory sandbox, establish an EU Fund for AI Standard Setting, and work towards the creation of a European Centre for AI Regulation. On the other side, managers should favor M&A between start-ups, form an "AI Organizational Design Lab" in partnership with universities, and create within their organizational design an "AI Act Monitoring Unit".

4.5.1 Implications for EU policymakers

First, policymakers should establish a single EU regulatory sandbox governed by a centralized European authority, rather than relying on 27 different national sandboxes and their respective national authorities.

This EU sandbox would function as a single point of entry for experimentation, possibly integrated into or closely directed by the AI Office. It would establish uniform common documentation templates and compatible testing and reporting procedures. Consistent regulatory guidance that is applicable across Member States would be advantageous to firms accepted to the sandbox, and the associated documentation may be utilized to prove compliance across the internal market. This will greatly reduce administrative paperwork and legal ambiguity, especially for SMEs.

Within a common European framework for sandboxes, national competent authorities would be incorporated as supervisory partners. Coordination of regulatory discretion would be achieved in this way, maintaining contextual expertise while preventing competitive distortions from divergence.

According to the process model established in this study, a single European sandbox would directly reduce "Asymmetric institutional environments" while also promoting "Institutional co-evolution" by establishing a common area for experimentation and regulatory learning under the Union's governance umbrella.

Second, EU policymakers should establish a dedicated European Fund for AI Standard Setting to reduce the delays associated with AI standard development.

Due to significant financial constraints, stakeholders' unequal ability to engage in standards development is a major structural limitation of the existing European standardization system. Non-industry actors are not sufficiently involved today, especially members of SMEs businesses and academic specialists. These actors lack the funding necessary for ongoing participation in technical committees (Future of Life Institute, 2025).

The fact that participation is primarily unpaid under the current system is a significant aspect: experts are usually not paid for their work or reimbursed for participation and travel expenses. Committees run the risk of being controlled by wealthy industrial players who can commit full-time staff to the drafting process, augmenting the mechanism of "Asymmetric institutional environments".

By giving specific financial support to independent specialists serving on committees entrusted with creating standards related to the AI Act, the creation of a European Fund for AI Standard Setting would directly address these disparities. Compensation for expert time, reimbursement for participation and travel costs, and administrative assistance for technical secretariats should all be covered by the Fund.

To ensure that funds are distributed fairly, funding allocation should depend on quantifiable contributions to committee activities. This would allow a more motivated group of experts to participate and contribute to the development of standards within a reasonable timeframe. In the AI Act context, accelerating this process is essential to provide businesses with regulatory clarity and synchronize institutional adaptation with the pace of innovation.

Within the framework of "A Process Model of Institutional Influence and Tech Corporate Adaptation under the EU AI Act", a European Fund for the definition of AI standards would reduce "Interpretative and operational uncertainty" by finally providing tech firms with reference standards, mitigate "Temporal misalignment and instability" by aligning regulatory implementation with business innovation cycles, and promote "Institutional co-evolution" by strengthening collaboration between public institutions and technical expert communities.

Third, EU policymakers should establish a European Centre for AI Regulation as a permanent joint initiative between the European Commission and the European University Association (EUA), designed as an institutional hub dedicated to integrating technical and legal expertise on artificial intelligence into EU policymaking.

The Centre would be organized through a network of affiliated university laboratories and research units throughout Member States and would be managed by a central coordinating office, situated in Brussels.

In order to ensure high scientific standards and geographic balance throughout Europe, universities would take part through a formal accreditation system run in cooperation with the Commission and the EUA.

Polytechnic universities would be in charge of constantly tracking and evaluating advancements in AI systems under this arrangement, and law faculties would counsel legislators on the best legal language and regulatory frameworks to guarantee that new technological ideas could be successfully incorporated into future AI laws.

With consultation cycles aligned with the EU legislative calendar, the Center would operationally generate updated, quick technical-legal evaluation reports for EU institutions. Academic specialists would work closely with Commission directorates during these cycles to evaluate proposed regulations against the most recent advancements in AI technologies.

A biannual cycle of conferences held by universities member of EUA would then be organized by the Centre, bringing together representatives of civil society, industry, academic researchers, and Commission officials. The purpose of the conferences is to summarize the input that has been sent to the European Commission in the meantime, with exchanges of views and feedback from participants.

Finally, the Centre, through its network of universities, would provide executive training programs for national and EU regulators. To ensure that policymakers stay up to date on the development of AI technology and its governance consequences, these programs would offer in-depth modules on the latest AI models.

According to the theoretical model, the Centre would guarantee constant access to combined engineering and legal expertise, reducing "Interpretative and operational uncertainty". Its executive training programs and reporting cycles would also help to reduce "Temporal misalignment and instability", keeping policymakers themselves informed and up to date on AI advancements. Then, the Centre would improve "Institutional co-evolution" by formalizing a consistent line of communication between EU institutions and the EUA.

4.5.2 Implications for tech firms

First, managers of European technology start-ups and SMEs should pursue M&A strategies or structured joint ventures with other SMEs, where allowed by European competition law.

Technical and managerial expertise, if confined to small businesses, can be detrimental to the organizations themselves; this type of sharing is also necessary in order to compete with the rest of the European AI industry market. Thus, mitigating the "Asymmetric institutional environments" mechanism.

In this way, by expanding their structure, they would be able to more easily engage with both national and European institutions, increasing their visibility and credibility, supporting the "Institutional co-evolution" mechanism.

The integration of complementary competencies should serve as a basis for consolidation. For example, two specialized start-ups can form a joint venture to create a shared compliance unit while maintaining separate product lines, or a product company can merge with a data or machine-learning engineering firm to strengthen documentation and testing capacity.

By establishing a centralized compliance and documentation unit in charge of templates or risk assessments, businesses may concentrate on compliance-related tasks. A uniform testing and evaluation environment that includes model monitoring tools, validation datasets, stress tests, benchmarks, and audit trails should be included. This constitutes an

effective strategy to deal with the "Interpretative and operational uncertainty" mechanism.

Second, managers should reach agreements with universities (both polytechnics and social science universities) to create specialized master's degrees with the aim of training managers with high technical skills in AI. Companies need hybrid figures, who are now increasingly in demand, who know how to deal with rapidly developing technological contexts from an organizational standpoint and who have in-depth knowledge of the technology itself. The program is primarily intended, but not exclusive, for those with an engineering background.

The partnership would take the form of an "AI Organizational Design Lab", in which participants would be involved in training-experimentation-evaluation cycles within universities, working under both managerial and academic supervision.

During the training phase, participants update their technical skills on AI systems alongside modules focused on business organization, i.e., learning how certain technical choices have both economic and sometimes ethical impacts. In addition, there are specific legal modules on the AI Act.

During the experimentation phase, participants would be tested on real-world problems: what happens if a new AI system is discovered? How should we deal with the regulations? How does a compliance-by-design process work? How do we manage the relationship between risk and innovation?

In the evaluation phase, the solutions are analyzed jointly by university professors and business managers according to an evaluation grid that takes into account whether the choices made are consistent with the relevant strategic business objectives.

By anchoring to the new theoretical model, this would reduce "Interpretative and operational uncertainty" and "Temporal misalignment and instability" as this academic-business path leads to the creation of a managerial-engineering figure of "AI Governance Architect." This would allow companies to create corporate roles that are ready for the technical and strategic challenges of AI and not leaving companies with the task of having to undertake external training courses independently, without the guarantee of university excellence.

Third, managers should establish "AI Act monitoring units" within their organizational designs in order to keep track of ongoing regulatory developments at both the European

and national level, with the AI Office and national competent authorities as their points of reference. Indeed, these new units would become the main interlocutors with the institutions.

This new unit should be composed of legal managers with specific expertise in European digital regulation, engineers with in-depth knowledge of the technicalities of AI systems, managers responsible for maintaining the company's clear strategic direction, taking into account risk management and business objectives, and institutional affairs managers tasked to engage with European Commission officers and with officers of the relevant national ministries.

On a practical level, the unit would have the opportunity to constantly monitor developments in the regulatory framework of the AI Act, including all relevant guidelines, the status of updates to standards, opportunities to participate in sandboxes, and notices regarding temporary suspensions of legal obligations. In addition, it would assess the impact of regulatory changes on AI systems that have been developed or are in the design phase and work on defining internal compliance-by-design procedures, with support for audit and conformity assessment functions.

Keeping the theoretical model as a reference point, the creation of this new unit allows companies to avoid fragmented approaches to the AI Act within the company itself, concentrating all their energies in a single area. This reduces "Interpretative and operational uncertainty." In addition, continuous monitoring of regulatory developments allows for better alignment with technological innovation cycles, reducing "Temporal misalignment and instability". Finally, by acting as a stable interface with institutional actors, this unit strengthens the mechanism of "Institutional co-evolution", also affecting the clarity of communication and what they really want to communicate to institutions. Having an *ad hoc* unit could really make firms more likely to be heard.

4.6 Limitations of the study

This paragraph is dedicated to highlighting the limitations of this research work.

First of all, as already mentioned in the chapters above, the AI Act is a regulation that is subject to sudden changes or the suspension of certain provisions; therefore, it is not easy to deal with a law that is constantly evolving and not yet fully implemented.

Some of the dynamics observed and interpreted in this study may change in the medium term, once the implementation framework is fully stabilized.

Furthermore, eleven interviews represent a limited number, even though they were conducted in depth and allowed for the collection of highly detailed qualitative data. In addition, the anonymous nature of the interviews, necessary to ensure the freedom of expression of the interviewees and access to sensitive institutional and corporate positions, limits the possibility of fully contextualizing certain statements in relation to the specific role or organization of the individuals involved.

A further limitation concerns the composition of the sample and the sectoral approach adopted. The sample includes representatives of both SMEs and large technology companies; however, during the analysis, the tech sector is considered as a single entity. This choice is dictated by the comparability of the data and the construction of the theoretical model, but it does not capture the high internal heterogeneity of the tech industry.

4.7 Future research

Given the large number of results, future research could investigate aspects not covered in this study.

Firstly, new research could further adopt a comparative perspective, comparing the European regulatory framework on AI with those in China and the United States. This would assess how different institutional structures (the former more state-centric, the latter more market-oriented) create mechanisms that impact strategic innovation in tech companies. Furthermore, future studies could focus on specific industries, such as pharmaceuticals, finance, defense, or space. This would allow for a more accurate assessment of regulatory exposure levels, observing whether and to what extent the impact of the AI Act varies across industries with different risk profiles.

Finally, another line of research could focus exclusively on start-ups, analyzing how they address the challenges posed by the AI Act in terms of market access and innovation capacity. Such an in-depth study would provide a better understanding of the strategic adaptation dynamics typical of start-ups, comparing them with those of large technology companies.

Conclusion

This thesis has examined the impact of Regulation (EU) 2024/1689 (EU AI Act) on strategic innovation in technology companies. As the first binding regulatory framework in the world designed to govern artificial intelligence, the AI Act emerges in a context where firms operate within an already overloaded digital regulatory environment (GDPR, DMA, DSA, Data Act, DGA, DIGITAL), while AI technologies continue to evolve rapidly.

By adopting and extending the Institution-Based-View (IBV) (DiMaggio & Powell, 1983; North, 1990; Scott, 1995; Tywoniak & Peng, 2006; Peng et al., 2009) and relying on an abductive qualitative methodology (Timmermans & Tavory, 2012), this study has shed light on how regulatory constraints and organizational opportunities interact in shaping corporate innovation strategies under the AI Act.

Through eleven in-depth interviews and the respective coding process, the results led to the identification of five core themes: “Regulatory and institutional capacity gaps”, “Uneven innovation environments for tech companies”, “The need for collaboration between technical and institutional actors”, “Strategic repositioning of European tech companies”, and “The AI Act: an enabler of strategic innovation?”.

Together, these themes provide an overview of how corporate and institutional actors are interpreting and responding to the new European AI regulatory framework.

Building on these empirical results, the study made it possible to theorize four institutional mechanisms that explain to what extent the AI Act is affecting tech firms’ innovation paths: “Interpretative and operational uncertainty”, “Temporal misalignment and instability”, “Asymmetric institutional environments”, and “Institutional co-evolution”.

Thanks to these mechanisms, this thesis elaborates a new theoretical process model called “A Process Model of Institutional Influence and Tech Corporate Adaptation under the EU AI Act”, that extends the IBV in four main ways. First, it shows that the stratification of EU digital laws, together with a lack of clarity in regulatory provisions, means that formal regulation does not necessarily reduce uncertainty: indeed, uncertainty persists because it is difficult to translate legal principles into corporate behavior, especially in the absence of standards.

Second, it introduces a temporal dimension into the IBV logic by demonstrating that since AI is evolving faster than regulation, regulatory definitions quickly become obsolete, providing instability for firms and pushing them to anticipatory governance and continuous organizational adaptation. Third, it illustrates that firms do not behave uniformly under a single institutional regime like the AI Act because large firms are in a better position to amortize regulatory burdens, while SMEs face disproportionate constraints on experimentation and scaling, with differences depending on the national context.

Fourth, institutions are not seen as mere "independent variables" since the relationship is not one-directional: regulated actors actively engage with institutions through continuous dialogue and interaction, to reach the most possible "good rule".

The model provides a map for both policymakers and managers to deal with the ambiguous context of the AI Act. For policymakers, it clarifies how choices regarding implementation design, such as the fragmentation of sandboxes among Member States and delays in creating standards, amplify uncertainty and asymmetries, leading to differences in how tech companies can innovate differently within the 27 countries.

For managers of tech firms, the model offers an opportunity to understand what aspects can change strategic innovation and what some companies are already doing to address them. It also provides guidance on how to align investments in light of this regulation, indicating why the creation of new AI governance roles, technical and legal coordination, ongoing monitoring, and compliance by design approaches are becoming key strategies for keeping pace and not being overwhelmed by the unpredictability of the regulation.

If the European Union truly wants to become the "AI Continent," it is not enough to claim regulatory primacy; it must also address the regulatory and structural fragmentation that characterizes its governance system.

An efficient and innovative European artificial intelligence ecosystem requires greater central steering capacity. Without deeper political and institutional integration, moving closer to a federal model, the European Union risks producing sophisticated rules without uniform implementation across Member States.

Greater institutional cohesion is essential to establish itself as a powerhouse for innovation, where the tech sector is among the primary beneficiaries.

Appendix A. Informed Consent - Interview

This appendix contains the informed consent and the semi-structured interview guide adopted for the empirical phase of the research.

INFORMED CONSENT – INTERVIEW

I, the undersigned _____

in the capacity of (role and/or position) _____

declare that I understand the objectives of the master's thesis, conducted by the student **Simone Pietro Ciccolella** at **LUISS Guido Carli University**, under the supervision of **Rector Paolo Boccardelli**, with the provisional title:

"The AI Act between constraint and opportunity: strategic innovation in the tech sector from public and private perspectives"

I confirm that I have received a set of questions to which I have chosen to respond. These responses will be transcribed, and I authorize the use of my answers exclusively for academic purposes. The interview duration is approximately 15 minutes.

I confirm that I have received explanations regarding the purpose and nature of the study, and I have had the opportunity to ask questions about it.

I also declare that I am aware that the content of my responses may be cited in the thesis, and:

[] I authorize the use of my name and role within the thesis.

[] I prefer to remain anonymous, requesting that neither my name nor my role be mentioned in any part of the thesis.

I have been assured of the right to request at any time the correction or removal (even partial) of my contributions, should I deem it appropriate, up until the official submission of the dissertation.

Signature: _____
Place: _____
Date: _____

INTRODUCTION

I would like to thank you in advance for your time and for the support you will provide for this research.

Let me start by introducing the research:

The European Union has recently adopted the AI Act, the world's first comprehensive regulation on artificial intelligence, aiming to ensure that AI systems developed and used in the EU are trustworthy, human-centric, and safe. While much has been written on the legal and ethical implications of the Act, there is still limited understanding of how tech companies are adapting strategically and organizationally to these new rules.

My name is **Simone Pietro Ciccolella**, and I am a second-year master's student in **Global Management and Politics** at **LUISS Guido Carli**. Under the supervision of **Rector Paolo Boccardelli**, I am writing a thesis that explores the following research question:

"*To what extent does the European AI Act influence strategic innovation in tech companies, balancing regulatory constraints with opportunities for organizational and managerial transformation in the adoption of AI technologies*?"

The study focuses on institution and industry perspectives and aims to investigate how the AI Act is being interpreted, internalized, and operationalized within tech firms. Through expert interviews, I hope to gain insights into how innovation paths are reshaped, whether constrained or enabled, by this new regulatory environment.

The privacy of the information is ensured according to the choices made in the signed consent.

I would like to remind you that you always have the right to withdraw or to ask for a reformulation of any previous response until the final submission of the thesis.

Section 1- Common questions

1. **How do you personally perceive the overall impact of the AI Act on responsible and strategic innovation within the tech sector?**

2. **In your opinion, how effective are regulatory sandboxes, corporate codes of conduct or gradual compliance in enabling experimentation and innovation within AI development?**

3. **In what ways, if any, has your organization (or others you observe closely) modified roles, internal processes, or skill profiles in response to the AI Act?**

4. **How clear are the operational and documentation requirements for AI system providers and deployers, including GPAI model providers, under the AI Act?**

5. **In your view, what role should public institutions play in supporting responsible and competitive AI innovation under the AI Act in Europe?**

6. **What do you see as the main benefits and the main challenges posed by the AI Act for tech companies working with AI?**

Section 2 - Specific questions

INSTITUTIONAL ACTORS

7. **Based on your observation, are tech companies embracing the AI Act as an opportunity to grow and innovate responsibly, or does a logic of minimal compliance prevail?**

8. **What do you see as the most pressing institutional blind spots or implementation gaps that could undermine the AI Act's long-term credibility and effectiveness?**

CORPORATE ACTORS

7. **Do you think full compliance with the AI Act can become a real competitive advantage for your company or industry, or does it pose a risk to innovation agility?**

8. **Which components of the AI Act pose the greatest complexity or operational burden in your day-to-day business practices?**

CONCLUSION

As we come to the end of the interview, I would like to ask a final question:

- **In your view, are there any reforms or adjustments to the AI Act that could better support tech companies in pursuing innovation while ensuring compliance? If so, what changes would you consider most impactful?**

The next steps in the research will involve using and analyzing the information collected during this and other interviews to write the thesis in an exploratory and comprehensive manner.

Thank you for your time.
Your contribution to this research is greatly appreciated.

Wishing you a good day,

Best regards.
Simone Pietro Ciccolella

References

Anthropic. (2025). "Introducing Anthropic's Transparency Hub", anthropic.com. official website: https://www.anthropic.com/news/introducing-anthropic-transparency-hub

Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), 1338-1347.Official website: https://ijsra.net/sites/default/files/IJSRA-2024-0220.pdf.

Balcioğlu Y.S., Çelik A. A., Altindağ E. (2025). "A turning point in AI: Europe's human-centric approach to technology regulation". *Journal of Responsible Technology,* vol. 23, 100128, ISSN 2666-6596, https://doi.org/10.1016/j.jrt.2025.100128

Barney, J. B. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17, 99-120. https://doi.org/10.1177/014920639101700108

Bıçakçı, A. S. (2024). Digital Europe Program: Nurturing Technological Sovereignty for a Resilient European Digital Ecosphere. *Ankara Avrupa Çalışmaları Dergisi*, *23*(Özel Sayı-Future of Europe: Reflections from Türkiye), 135-174. Official website: https://dergipark.org.tr/en/pub/aacd/article/1439811

Bignami, E. G., Russo, M., Semeraro, F., & Bellini, V. (2025). Balancing Innovation and Control: The European Union AI Act in an Era of Global Uncertainty. *JMIR AI*, *4*, e75527. https://doi.org/10.2196/75527

Blind, K., Niebel, C., & Rammer, C. (2024). The impact of the EU General data protection regulation on product innovation. *Industry and Innovation*, 31(3), 311–351. https://doi.org/10.1080/13662716.2023.2271858. Official website: https://www.tandfonline.com/doi/full/10.1080/13662716.2023.2271858

Bradley-Silverio Donato, J. (2024). *The impact of tech regulation on innovation, society and competition*. Forbes. Officiall website: https://www.forbes.com/councils/forbesbusinesscouncil/2024/10/22/the-impact-of-tech-regulation-on-innovation-society-and-competition/

Buckley, G., Caulfield, T., & Becker, I. (2021). " It may be a pain in the backside but..." Insights into the impact of GDPR on business after three years. *arXiv preprint arXiv:2110.11905*. official website: https://arxiv.org/abs/2110.11905.

Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. *Computer Law & Security Review*, *50*, 105830. Official website: https://www.sciencedirect.com/science/article/pii/S0267364923000407

Ciccarelli, L. (2024). *The Digital Markets Act and its impact on digital marketing*. Intarget. Official website: https://www.intarget.net/en/the-digital-markets-act-and-its-impact-on-digital-marketing/

Clegg, N. (2024). “Labeling Ai-Generated Images on Facebook, Instagram and Threads”, meta.com. official website: https://about.fb.com/news/2024/02/labeling-ai-generated-images-on-facebook-instagram-and-threads/

CMS Law-Now. (2025). *The Data Governance Act – Overview*. Official website: https://cms-lawnow.com/en/ealerts/2023/02/the-data-governance-act-overview

Colovic, A., Caloffi, A., Rossi, F., & Russo, M. (2025). Institutionalising the digital transition: The role of digital innovation intermediaries. *Research Policy, 54*(1), 105146. https://doi.org/10.1016/j.respol.2024.105146

Coulter, M. (2023). *How the EU's Digital Markets Act challenges Big Tech*. Reuters. Official website: https://www.reuters.com/technology/how-eus-digital-markets-act-challenges-big-tech-2023-09-06/

Council of the European Union & European Parliament. (2021). *Regulation (EU) 2021/694 establishing the Digital Europe Programme.* Official website*:* https://eur-lex.europa.eu/eli/reg/2021/694/oj/eng

Crampton, N. (2025). “Innovating in linewith the EU’s AI Act”, blogs.micrsoft.com. official website: https://blogs.microsoft.com/on-the-issues/2025/01/15/innovating-in-line-with-the-european-unions-ai-act/?_

Digital Europe Programme. European Sources Online. Official website: https://www.europeansources.info/record/proposal-for-a-regulation-establishing-the-digital-europe-programme-for-the-period-2021-2027/

De la Mothe, J. (2004). The institutional governance of technology, society, and innovation. *Technology in Society, 26*(2–3), 523–536. https://doi.org/10.1016/j.techsoc.2004.01.009

Deckker, D., Sumanasekara, S. (2025). “Safeguarding human dignity: A narrative review of prohibited practices under the EU AI Act”. *World Journal of Advanced Research and Reviews,* 26(03), 243-250. DOI: https://doi.org/10.30574/wjarr.2025.26.3.2193

DiMaggio, P. J., & Powell, W. W. (1983). “The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields.” *American Sociological Review, 48*(2), 147–160. DOI:10.2307/2095101
EU AI Champions Initiative. (2025). “Stop the Clock - Open Letter”. Official website: https://aichampions.eu/

European Commission. (2025). “AI Pact marks one year of progress on trustworthy AI in Europe”. Official website: https://digital-strategy.ec.europa.eu/en/news/ai-pact-

marks-one-year-progress-trustworthy-ai-europe#:~:text=The%20AI%20Pact%20now%20counts,community%20engagement%20and%20knowledge%20sharing.

European Commission. (2021). *Digital Europe Programme (2021–2027)*. EUR-Lex. official website: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4526703

European Commission. (2024). *Data Act – Shaping Europe's digital future*. official website: https://digital-strategy.ec.europa.eu/en/policies/data-act.

European Commission. (2025). *Data Governance Act – Shaping Europe's digital future*. official website: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

European Commission. (2025). *Supervision of the designated very large online platforms and search engines under DSA*. Official website: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

European Commission. (2025). *The impact of the Digital Services Act on digital platforms*. official website: https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

European Commission. *The Digital Europe Programme*. official website: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

European Commission. *Digital Europe Programme (DIGITAL) | EU Funding & Tenders Portal*. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital

European Commission, Press Release. (2025). *Commission finds Apple and Meta in breach of the Digital Markets Act*. official website: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085 European Commission+6European Commission+6European Commission+6

European Court of Human Rights & Council of Europe. (1950). European Convention of Human Rights.

European Institute of Leadership and Management. (n.d.) The Effect of GDPR on European Business Management. Official website: https://eilm.edu.eu/blog/the-effect-of-gdpr-on-european-business-management/

European Parliament and Council of the European Union. (2022, May 30). *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*. Official Journal of the European Union, L 152, 1–44. Official website: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

European Parliament and Council of the European Union. (2022, October 19). Regulation (EU) 2022/2065... *(Digital Services Act)*. *Official Journal of the European Union, L 277*, 1–102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 12 July 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. Official Journal of the European Union.

Fasel, M. (2025). *Is the Digital Services Act here to protect users? Platform regulation and European single market integration*. University of Lausanne. Official website: https://serval.unil.ch/resource/serval:BIB_D51A412AD3FD.P001/REF.pdf

Fabiano, N. (2025). "Subject Roles in the EU AI Act: Mapping and Regulatory Implications". Studio Legale Fabiano – Affilitation: IIS. Official website: https://arxiv.org/html/2510.13591v1

Financial Times. (2024). *What impact is the Digital Markets Act having?. Official website:* https://channels.ft.com/en/tech/what-impact-is-the-digital-markets-act-having/

Future of Life Institute, FLI. (2022). Standard Setting Overview. EU Artificial Intelligence Act. Artificialintelligenceact.eu. Updated 21 July 2025. Official website: https://artificialintelligenceact.eu/standard-setting-overview/

Garrido, E., Gomez, J., Maicas, J. P., & Orcos, R. (2020). The Institution-Based View of Strategy: How to Measure It. BRQ Business Research Quarterly, 17(2), 82-101. https://doi.org/10.1016/j.brq.2013.11.001 (Original work published 2014)

Golpayegani, D., Pandit, H. J., & Lewis, D. (2025). Semantic Patterns of Prohibited AI Systems in the EU AI Act. In *NeXt-generation Data Governance workshop 2025*.

Google DeepMind Security & Privacy Research Team. (2025). "Advancing Gemini's security safeguards"., deepmind.google.com. official website: https://deepmind.google/discover/blog/advancing-geminis-security-safeguards/

Grant Thornton Ireland. (2024). *Digital Markets Act: An overview of the new EU regulation*. Official website: https://www.grantthornton.ie/insights/factsheets/digital-markets-act-an-overview-of-the-new-eu-regulation/

Grignon, J. (2025). *What the EU's Digital Markets Act means for the middle market*. (RSM Global). Official website: https://www.rsm.global/insights/what-eus-digital-markets-act-means-middle-market

Haeck, P. (2025). Commission publishes list of signatories to AI code of practice. Politico.eu. Official website: https://www.politico.eu/article/eu-signatories-ai-code-practice-amazon-google-ibm-microsoft-ai/

Herbert Smith Freehills. (2024). *Digital Markets Act – Overview*. Official website: https://www.herbertsmithfreehills.com/notes/crt/2024-03/digital-markets-act-overview

Hickman, T., Lorenz, S., Rennie, J., Hainsdorf, C. (2025). *Handbook on the EU Artificial Intelligence Act*. White & Case LLP. Official website: https://www.whitecase.com/insight-alert/white-case-launches-eu-ai-act-handbook

Hinings, B., Gegenhuber, T., & Greenwood, R. (2018). Digital innovation and transformation: An institutional perspective. *Information and Organization, 28*(1), 52–61. https://doi.org/10.1016/j.infoandorg.2018.02.004

Holst, L., Lämmermann, L., Mayer, V., Urbach, N., & Wendt, D. (2024). The Impact of the EU AI Act's Transparency Requirements on AI Innovation. *Wirtschaftsinformatik 2024 Proceedings. 92.* Official website: https://aisel.aisnet.org/wi2024/92/

Hung, S.-C., & Tseng, Y.-C. (2017). Extending the LLL framework through an institution-based view: Acer as a dragon multinational. *Asia Pacific Journal of Management, 34*(4), 799–821. https://doi.org/10.1007/s10490-016-9494-8

IBM (2024). *High-quality standards and good governance tools for compliance with the AI Act*. Dr. Jochen Friedrich, eu-LISA Industry Roundtable, Budapest. Official website: https://eulisaroundtable.eu/eulisa_content/uploads/2024/11/ibm-ai-act-standardisation-and-tools-jochen-friedrich.pdf

Invest Europe. (2024). State of European Tech 2024: A decade of progress and the road ahead. Official website: https://www.investeurope.eu/news/newsroom/state-of-european-tech-2024-a-decade-of-progress-and-the-road-ahead/

Invest Europe. (2025). State of European Tech 2025: A roadmap to unlock further tech growth. Official website: https://www.investeurope.eu/news/newsroom/state-of-european-tech-2025-a-roadmap-to-unlock-further-tech-growth/

Jackson, E., Weck, M., Pappel, I. (2024). The Role of Data Intermediaries for Small- and Medium-sized Enterprises in the Innovation Ecosystems of the Nordic-Baltic Silver Economy. In: Vesa Salminen (eds) Human Factors, Business Management and Society. AHFE (2024) International Conference. AHFE Open Access, vol 135. AHFE International, USA. Official website: https://openaccess.cms-conferences.org/publications/book/978-1-964867-11-3/article/978-1-964867-11-3_15

LCA LEX website. "Digital Omnibus". Official website: https://www.lcalex.it/digital-omnibus/

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22(1), 1–6. Official website: https://ideas.repec.org/a/taf/ugitxx/v22y2019i1p1-6.html

Lindgren, P. (2018). GDPR regulation impact on different business models and businesses. *Journal of Multi Business Model Innovation and Technology*, *4*(3), 241-254.

Official website:
https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-456X_434.pdf

Mahto, R., Singhal, C., & Kraus, S. (2022). Technological Innovation, Firm Performance, and Institutional Context: A Meta-Analysis. *IEEE Transactions on Engineering Management*, 69(6), 2976-2986. https://doi.org/10.1109/tem.2020.3021378

Marinello, F. (2023). "11 norme UE per la sovranità digitale: testi in vigore e novità future". Delli Ponti Studio Legale. Official website:
https://www.studiolegaledelliponti.eu/11-norme-ue-per-la-sovranita-digitale-testi-in-vigore-e-novita-future/

Mikhail, M. A. (2025). *A holistic overview of the Data Act, its implications on the economy and interplay with the GDPR*(Student thesis). Seton Hall University. Official website:
https://scholarship.shu.edu/cgi/viewcontent.cgi?article=2571&context=student_scholarship

Nagy, A., Mikes, A., Flakoll, R. (2022). *An overview of the newly adopted EU Data Governance Act*. Clifford Chance. Official website:
https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/09/an-overview-of-the-newly-adopted-eu-data-governance-act.html

Namirial Focus. (2024). *What is the Digital Services Act 2024?* Official website:
https://focus.namirial.com/en/digital-services-act/

Neuwirth, R. J. (2023). Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). *Computer Law & Security Review*, *48*, 105798.

North, D. C. (1990). Institutions, institutional change and economic performance. *Cambridge University press*

Olsen, J. P. (2009). Change and continuity: an institutional approach to institutions of democratic government. *European political science review*, *1*(1), 3-32.

OpenAi. (2024). "A Primer on the EU AI Act", openai.com. Official website:
https://openai.com/global-affairs/a-primer-on-the-eu-ai-act/

Özkiziltan, D., Landini, P. (2025). "Trustworthy and human-centric? The new governance of workplace AI technologies under the EU's Artificial Intelligence Act". *ETUI,* Transfer, Vol. 31 (4) 503-517. Official website:
https://journals.sagepub.com/doi/pdf/10.1177/10242589251336193

Peng, M. W., Sun, S. L., Pinkham, B., & Chen, H. (2009). The institution-based view as a third leg for a strategy tripod. *Academy of management perspectives*, *23*(3), 63-81.

Peng, M. W., Wang, J. C., Kathuria, N., Shen, J., & Welbourne Eleazar , M. J. (2023). Toward an institution-based paradigm. *Asia Pacific Journal of Management*, *40*(2), 353–382. https://doi.org/10.1007/s10490-022-09861-6

Porter, M. E. (1998). *Competitive strategy: Techniques for analyzing industries and competitors*. Free Press. (Original work published 1980)

Presidente, G., Frey, C.B. (2022). The GDPR effect: How data privacy regulation shaped firm performance globally, *Centre for Economic Policy Research*. Official website: https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally

Reviewed by himself Scott, W.-.-R. (2014). W. Richard Scott (1995), Institutions and Organizations. Ideas, Interests and Identities. Paperback: 360 Pages Publisher: Sage (1995) Language: English Isbn: 978-142242224. M@n@gement, . 17(2), 136-140. https://doi.org/10.3917/mana.172.0136.

Ruohonen, J., & Timmers, P. (2025). Early Perspectives on the Digital Europe Programme. *arXiv preprint arXiv:2501.03098*. official website: https://arxiv.org/pdf/2501.03098

Santalu, N., Bond T., Ballhausen M. (2025). "AI Act 2.0: The Commission's regulatory remix proposal", *Bird&Bird.* Official website: https://www.twobirds.com/en/insights/2025/ai-act-2,-d-,0-the-commission's-regulatory-remix-proposal

Schildt, H. (2022), "The Institutional Logic of Digitalization", Gegenhuber, T., Logue, D., Hinings, C.R.(B). and Barrett, M. (Ed.) *Digital Transformation and Institutional Theory* (*Research in the Sociology of Organizations, Vol. 83*), Emerald Publishing Limited, Leeds, pp. 235-251. https://doi.org/10.1108/S0733-558X20220000083010

Shahlaei, C. A., & Berente, N. (2024). *An analysis of European data and AI regulations for automotive organizations* (arXiv:2407.11271). arXiv. Official website: https://arxiv.org/abs/2407.11271 Ibidem.

Solskjær, A. M., & Owrenn, E. L. (2024). *The role of the Digital Markets Act in promoting fairness and competitiveness in the digital economy: A legal and economic analysis on how the DMA impacts market dynamics and consumer welfare, its regulatory effect on gatekeepers and its role in closing the loophole in competition law within digital markets* (Master's thesis, Copenhagen Business School). Official website: https://research-api.cbs.dk/ws/portalfiles/portal/108042689/1818782_The_Role_of_the_Digital_Markets_Act_in_Promoting_Fairness_and_Competitiveness_in_the_Digital_Economy.pdf

Sony, Michael and Aithal, P. S., A Resource-Based View and Institutional Theory-Based Analysis of Industry 4.0 Implementation in the Indian Engineering Industry (September 20, 2020). International Journal of Management, Technology, and Social Sciences

(IJMTS), 5(2), 154-166. (2020). ISSN: 2581-6012. , Available at SSRN: https://ssrn.com/abstract=3695750

Timmermans, S., & Tavory, I. (2012). Theory construction in qualitative research: From grounded theory to abductive analysis. *Sociological theory*, *30*(3), 167-186.

Tito Lucrezio Caro. De Rerum Natura - Liber Primus. Thelatinlibrary.com. The Latin Library.

Tywoniak S. Mike W. Peng (2006) Global Strategy Thomson South-Western ISBN: 0-324-31649-6. *Journal of the Australian and New Zealand Academy of Management*. 2005;11(2):59-61. doi:10.5172/jmo.2005.11.2.59

Ullagaddi, Pravin. (2024). GDPR: Reshaping the landscape of digital transformation and business strategy." *International Journal of Business Marketing and Management* 9.2, 29-35. Official website: https://ijbmm.com/paper/Mar2024/8340436609.pdf

Vecchi, A., Della Piana, B., Vivacqua, E. (2015). An Institutional-Based View of Innovation - An Explorative Comparison of Business Groups in China and India. *INTERNATIONAL JOURNAL OF INNOVATION MANAGEMENT*, 19(5), 1-30 [10.1142/S1363919615500516].

Waldfogel, J. (2024). *Amazon self-preferencing in the shadow of the Digital Markets Act* (NBER Working Paper No. 32299). National Bureau of Economic Research. Official website: https://www.nber.org/system/files/working_papers/w32299/w32299.pdf

Wei, S., Xu, D. and Liu, H. (2022), "The effects of information technology capability and knowledge base on digital innovation: the moderating role of institutional environments", European Journal of Innovation Management, Vol. 25 No. 3, pp. 720-740. https://doi.org/10.1108/EJIM-08-2020-0324

Weigl, L., & Guzik, A. (2025). In Brussels we trust? Exploring corporate resistance in platform regulation. Law, Innovation and Technology, 17(1), 335–365. Official website: https://www.tandfonline.com/doi/full/10.1080/17579961.2025.2470588

Williamson, O. E. (1993). Transaction cost economics and organization theory. *Industrial and corporate change*, *2*(2), 107-156.

Wolford, B. (n.d) What is GDPR, the EU's new data protection law?, *gdpr.eu.* official website: https://gdpr.eu/what-is-gdpr/

Yang, C., Bossink, B. and Peverelli, P. (2025), "The influence of government affiliations on firm product innovation in a dynamic institutional environment: insights from China", *International Journal of Emerging Markets*, Vol. 20 No. 1, pp. 187-208. https://doi.org/10.1108/IJOEM-04-2021-0622

Yuan Lu & Eric Tsang & Mike Peng, 2008. "Knowledge management and innovation strategy in the Asia Pacific: Toward an institution-based view," *Asia Pacific Journal of Management*, Springer, vol. 25(3), pages 361-374, September.

Ziegler, S., Evequoz, E., Huamani, A.M.P. (2019). The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities. In: Aagaard, A. (eds) Digital Business Models. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-96902-2_8