UNIVERSITY OF THE AEGEAN

Department of Information and Communication Systems Engineering

Regulatory Framework for the Responsible Development of Artificial Intelligence and Robots: A Comparative Analysis between EU, the USA, Singapore and China and an Ideal Model

Abstract

This thesis examines the regulatory frameworks governing artificial intelligence and robotics in the European Union, the United States, China and Singapore. The European and Singaporean models are its main axes of analysis, while the US and China serve as points of reference and contrast. Through a comparative analysis guided by eight research questions, it identifies the fundamental differences in regulatory philosophy, governance structure, legal instruments and policy priorities of the four jurisdictions. The state of the frameworks is reflected up to October 2026.

The findings show that there is no single, globally accepted model of governance. Instead, there are four substantially different regulatory philosophies, each rooted in its own political traditions and institutional capacities:

European Union: the AI Act offers legal certainty and strong protection of fundamental rights. It is constrained by high compliance costs, slow adaptation and regulatory overlaps, as the postponement of high risk obligations through Regulation (EU) 2026/1744 confirmed.

United States: the model favours innovation but suffers from political instability and growing tension between federal and state competence.

China: the model achieves remarkable regulatory speed through successive vertical rules, at the cost of individual rights and democratic legitimacy.

Singapore: a quasi regulatory model combines flexibility, practical tools such as AI Verify and a binding data protection basis. Its external verifiability and its transferability to larger jurisdictions remain limited.

The thesis also shows that non bindingness does not mean an absence of consequences. Compliance pressure shifts towards market reputation, supervisory assessment and the threat of future legislation.

The main contribution of the thesis is an ideal regulatory model that combines the strengths of the four approaches. It has five interrelated layers: a binding horizontal core,

proportionate risk based escalation with rapid technical updating under democratic control, quasi regulation instruments institutionally linked to compliance, sectoral specialisation with a priority rule and strengthened ex post enforcement.

All five layers are underpinned by international interoperability. The thesis also sets out the preconditions for implementing the model: institutional capacity, timely technical standards, a stable legislative basis, democratic legitimacy, trust between the state and industry, and international coordination.

The thesis concludes that a model with all the strengths and none of the weaknesses is not feasible, because certain advantages and disadvantages are aspects of the same institutional feature. A hybrid model that significantly reduces these trade offs is, however, attainable. The partial convergence of the four jurisdictions observed in 2026 suggests that regulatory practice is already moving in this direction.

Contents

1 Chapter 1: Introduction 8

1.1 Introduction 8

1.2 Theoretical Background and Ethical Dimensions of Artificial Intelligence and Robotics .. 11

1.2.1 Definitions and Key Concepts 11

1.2.2 The Ethical Dimension: Key Concerns 13

1.2.3 Privacy, Surveillance and Human Dignity 14

1.2.4 Theoretical Frameworks of Artificial Intelligence Governance 15

2 Chapter 2: The Regulatory Framework for Artificial Intelligence and Robotics in the European Union 16

2.1 The Regulatory Philosophy of the EU 16

2.2 The Artificial Intelligence Act (EU AI Act) 16

2.3 The GDPR and Data Protection 18

2.4 The Ethics Guidelines and the New Machinery Regulation 18

2.5 Recent Developments: The Digital Omnibus on AI Regulation and the Implementation Tools of the AI Act 20

3 Chapter 3: The Regulatory Approach to Artificial Intelligence and Robotics in the United States 23

3.1 The Regulatory Philosophy of the US 23

3.2 Federal Agencies and Sectoral Regulation 23

3.3 Policy Initiatives and National Strategies up to 2022 24

3.4 The Policy Shift of 2025 25

3.5 Overall Assessment 27

4 Chapter 4: The Regulatory Approach to Artificial Intelligence and Robotics in China 28

4.1 China as a Global Artificial Intelligence Power 28

4.2 National Artificial Intelligence Strategy 28

4.3 Artificial Intelligence Regulatory Framework 29

4.4 Social Control and Surveillance 32

5 Chapter 5: Singapore, Modern History and AI Regulatory Framework 33

5.1 Singapore, from Colonialism to the Twenty First Century 33

5.1.1 Historical and Geopolitical Context 33
5.1.2 The Economic Transformation: From Unemployment to High Technology 34
5.1.3 The Digital Turn: Smart Nation and the National Artificial Intelligence Strategy 35
5.1.4 The Regulatory Ethos as a Legacy of History 36
5.2 The Regulatory Framework for Artificial Intelligence in Singapore 36
5.2.1 The Regulatory Philosophy: Innovation with Responsibility through Quasi Regulation 36
5.2.2 The Artificial Intelligence Governance Framework 38
5.2.3 The AI Verify Tool 39
5.2.4 Data Protection as a Binding Basis: The Role of the PDPA 40
5.2.5 The Financial Sector and the MAS 41
5.2.6 International Orientation and Singapore's Role in International Artificial Intelligence Governance 42
5.2.7 The Practical Consequences of Non Compliance 43
6 Chapter 6: Comparative Analysis of the Regulatory Models of the EU, the US, China and Singapore 46
6.1 Comparative Analysis: EU and US 46
6.2 Comparative Analysis: EU and China 47
6.2.1 Regulatory Philosophy and Structure 47
6.2.2 Speed of Regulatory Response 48
6.2.3 The Role of the State in Relation to Technology 49
6.2.4 Industrial Policy and Regulation 49
6.3 Comparative Analysis: EU and Singapore 50
6.3.1 Regulatory Philosophy 50
6.3.2 Governance Structure, Horizontal Framework versus Multi Layered Ecosystem 50
6.3.3 Risk Categorisation 51
6.3.4 Transparency, Accountability and Human Oversight 52
6.3.5 Generative AI and Emerging Technologies 52
6.4 Four Way Comparison: Axes of Convergence and Divergence 53
7 Chapter 7: Challenges and Ideal Regulatory Model 55
7.1 Challenges and Future Regulatory Developments 55
7.1.1 Challenges of the European Model 55
7.1.2 Challenges of the American Model 56
7.1.3 Challenges of the Chinese Model 57

7.1.4 Challenges of the Singaporean Model *58*
7.1.5 Future Developments *59*
7.2 Towards an Ideal Regulatory Model: Combining the Strengths of the Four Approaches. 60
7.2.1 Criteria for Selecting the Positive Characteristics *60*
7.2.2 The Architecture of the Ideal Model *62*
7.2.3 Characteristics Deliberately Excluded *65*
7.2.4 Preconditions for Implementation *65*
7.2.5 Inherent Tensions and Limits of the Ideal Model *67*
8 Chapter 8: Conclusions 68
8.1 Answers to the Research Questions 68
8.2 Conclusions, Ideal Model and Limitations 73
9 Bibliography 75

1 Chapter 1: Introduction

1.1 Introduction

Modern societies are facing one of the most radical technological transformations in their history. The rapid development of artificial intelligence and robotics is redefining the way in which economies, industries, public services and the everyday lives of citizens function. From autonomous vehicles and surgical robots to automated decision making systems and digital assistants, artificial intelligence systems are penetrating ever more deeply into sectors such as healthcare, education, industrial production, financial services and transport (Russell & Norvig, 2020).

Despite the undeniable benefits that these technologies offer, such as increased productivity, improved accuracy and the reduction of human error, they simultaneously give rise to complex legal, ethical and social concerns. Issues such as liability for algorithmic decisions, algorithmic bias, the violation of privacy, the lack of transparency in black box systems and the risks posed by autonomous weapon systems highlight the need for a coherent regulatory framework (Floridi et al., 2018).

This reality has prompted governments and international organisations around the world to develop legislative and regulatory frameworks aimed at ensuring that artificial intelligence and robotic systems are developed and used in a responsible, safe and ethical manner. However, there is no single, global model of governance. Different societies, with their particular political traditions, economic priorities and social values, have chosen different approaches to the regulation of these technologies.

The European Union, the United States, China and Singapore represent four characteristic and, to a large extent, conflicting regulatory paradigms. The European Union, with the adoption of the AI Act in 2024, adopted a precautionary and rights based approach, namely a comprehensive legislative framework that categorises artificial intelligence systems according to their level of risk and establishes binding obligations for manufacturers and users (European Commission, 2024). This approach is complemented by pre existing legal instruments, such as the General Data Protection Regulation, and by the ethics guidelines developed by the High Level Expert Group on AI (HLEG AI, 2019). The United States, by contrast, follows a more decentralised and reactive model, based on a combination of sectoral regulations, voluntary standards and guidelines issued by federal agencies such as the FTC, NIST and the FDA (Calo, 2017),

reflecting a political philosophy that prioritises innovation, economic competitiveness and private sector self regulation over precautionary state intervention (White House, 2019). China, for its part, combines strong state guidance and the strategic promotion of innovation with the parallel development of social surveillance systems, in a model where technological development systematically precedes regulation (Roberts et al., 2021). Finally, Singapore has chosen an intermediate, essentially voluntary model of governance, which seeks a balance between innovation and responsible use, without the adoption of a single binding piece of legislation of the AI Act type. The analysis reflects the state of the four frameworks up to October 2026, a period during which all four jurisdictions undertook significant changes, such as the amendment of the AI Act through Regulation (EU) 2026/1744, the finalisation of the MAS Guidelines on artificial intelligence risk management in Singapore, the attempt at federal preemption of state laws in the US and the adoption of new specific rules in China.

The juxtaposition of these models has direct and practical consequences for technology companies operating at a global level, for the citizens who interact with these systems, and also for the shaping of international standards for the governance of artificial intelligence and robotics. As competition between the major regulatory powers in the technology sector intensifies, regulatory choices acquire geopolitical dimensions, a phenomenon that some scholars call the "Brussels Effect", denoting the tendency of European regulations to influence global standards (Bradford, 2020).

The purpose of this thesis is the analysis and comparative evaluation of the regulatory frameworks governing artificial intelligence and robotics in the European Union, the United States, China and Singapore, with an emphasis on the European and Singaporean models, which constitute the main axes of analysis of the thesis, while the US and China are examined complementarily as points of reference and contrast. More specifically, the thesis seeks to highlight the fundamental differences in the regulatory philosophy, the governance structure, the legal instruments used and the policy priorities of each system. Through this comparative analysis, an attempt will be made to identify the strengths and weaknesses of each model, as well as to outline an ideal regulatory model, which combines the positive characteristics of the European, Singaporean, Chinese and American experience, together with the preconditions and limits of its implementation.

The above analysis is guided by eight specific research questions. First, what are the fundamental differences in regulatory philosophy, governance structure, legal instruments and policy priorities among the four jurisdictions under examination. Second, how the apparent non binding nature of voluntary and quasi regulatory frameworks operates in practice, and what consequences are faced by those actors who

choose not to comply. Third, which factors explain the significant differences in the speed of regulatory response to rapidly evolving technologies such as generative artificial intelligence. Fourth, how the historical and institutional legacy of a country influences its regulatory philosophy towards artificial intelligence. Fifth, which regulatory model most effectively manages the tension between the protection of fundamental rights and economic or technological competitiveness. Sixth, to what extent the regulatory model of Singapore is transferable to jurisdictions of much larger scale and institutional heterogeneity, such as the European Union. Seventh, how the treatment of artificial intelligence as an instrument of state power affects the possibility of international harmonisation of standards and cross border trust in imported artificial intelligence systems. Eighth, to what extent it is feasible to design an ideal regulatory model that combines the positive characteristics of all four jurisdictions without inheriting their weaknesses, and what preconditions its implementation would require. The answers to these questions are summarised in the eighth chapter, on the basis of the findings of the preceding analysis.

As regards the structure of the thesis, the first chapter, to which the present section belongs, presents the theoretical background and the main ethical concerns associated with artificial intelligence and robotics. The second chapter analyses the regulatory framework of the European Union, with an emphasis on the AI Act, the GDPR, the ethics guidelines and the New Machinery Regulation, as well as on the recent amendments of 2026. The third chapter examines the corresponding regulatory approach of the United States. The fourth chapter analyses the regulatory approach of China. The fifth chapter focuses on Singapore, examining both the historical and geopolitical background of the country and its contemporary regulatory framework for artificial intelligence. The sixth chapter carries out a comparative analysis between the European Union and the United States, between the European Union and China, and between the European Union and Singapore, and proceeds to a four way comparison of the four models. The seventh chapter discusses the common and the specific challenges of each system and future regulatory developments, and concludes with the outline of an ideal regulatory model that combines the positive characteristics of the four jurisdictions, as well as with the analysis of the preconditions and limits of its implementation. The eighth and final chapter summarises the conclusions of the thesis.

1.2 Theoretical Background and Ethical Dimensions of Artificial Intelligence and Robotics

1.2.1 Definitions and Key Concepts

In order to understand the regulatory landscape governing artificial intelligence and robotics, it is necessary to clearly define the key concepts that will be used in this thesis. The term artificial intelligence refers to computational systems designed to perform tasks that traditionally require human intelligence, such as perception, learning, decision making and problem solving (Russell & Norvig, 2020). At the legal level, the original proposal for the AI Act of the European Union defined an artificial intelligence system as software developed using specific techniques and approaches, capable of generating, for a given set of objectives, outputs such as content, predictions, recommendations or decisions that influence the environment with which it interacts (Nobile, 2023). In the final text of the Regulation the definition was reformulated, and an artificial intelligence system is defined as a machine based system designed to operate with varying levels of autonomy, which may exhibit adaptiveness after deployment and which, for explicit or implicit objectives, infers from the input it receives how to generate outputs, such as predictions, content, recommendations or decisions, that can influence physical or virtual environments (European Commission, 2024, Article 3(1)). This definition is deliberately broad, so as to cover a wide range of technologies and to prevent the circumvention of the legislation through artificial conceptual distinctions.

Of importance for the regulatory debate is the distinction between narrow and general artificial intelligence. Narrow artificial intelligence, also known as Artificial Narrow Intelligence or weak artificial intelligence, refers to systems that perform specific tasks with high performance, but without the ability to transfer these capabilities to other fields of knowledge (Nobile, 2023). General artificial intelligence, which remains largely theoretical, would be capable of displaying broad cognitive flexibility comparable to human intelligence (Bostrom, 2014). Current regulatory frameworks refer exclusively to narrow artificial intelligence, while nevertheless recognising the need for adaptation in view of future technological developments.

Robotics, on the other hand, concerns the design, construction and operation of mechanical systems that interact with the physical environment. According to the High Level Expert Group on AI of the European Commission, robotics can be defined as artificial intelligence in action in the physical world, that is, as embodied artificial

intelligence, where a robot is a physical machine that has to cope with the dynamics, the uncertainties and the complexity of the real world, incorporating capabilities of perception, reasoning, action, learning and interaction (Nobile, 2023). Modern robotic systems increasingly incorporate artificial intelligence algorithms, enabling them to operate with increased autonomy (Siciliano & Khatib, 2016).

From a legal point of view, the European Parliament has set specific conditions for characterising a system as a smart robot. According to the 2017 resolution on civil law rules on robotics, a system meets these conditions if it acquires autonomy through sensors and the exchange of data with its environment, has at least some physical support, adapts its behaviour to the environment and is not alive in the biological sense, while it may optionally be capable of self learning through experience (Nobile, 2023). However, as Nobile points out, this definition remains incomplete, since it may include systems without any element of artificial intelligence, while at the same time leaving outside its scope certain intelligent systems that have no physical presence.

In this context, a broader concern also emerges regarding the ethical dimensions of the development of artificial intelligence. Society views with ambivalence the ever increasing presence of robots and artificial intelligence in everyday life, since the very technologies that improve productivity and the quality of services simultaneously raise issues of employment, dependence on technology and deeper questions of identity and human dignity (Floridi et al., 2018). These social dimensions make it clear that the regulation of artificial intelligence is not exclusively a technical or legal matter, but a deeply social and ethical one, a fact that must be taken into account by legislators when shaping regulatory frameworks.

1.2.2 The Ethical Dimension: Key Concerns

The development and use of artificial intelligence and robotic systems raise a wide range of ethical issues, which constitute the foundation of every regulatory approach. These concerns are not merely abstract or philosophical, but have direct practical consequences for citizens and societies.

One of the most central issues is algorithmic bias. Artificial intelligence systems are trained on datasets that reflect historical inequalities and social prejudices. As a result, these systems can reproduce and reinforce existing forms of discrimination, particularly in fields such as the administration of justice, the recruitment of employees and creditworthiness assessment (O'Neil, 2016). Addressing bias requires both technical solutions and regulatory interventions that ensure the fairness and impartiality of automated decisions.

A second critical issue is the transparency and interpretability of artificial intelligence systems. Many modern machine learning models, particularly deep neural networks, operate as black boxes, that is, they produce outputs without it being possible to understand the internal process that led to them (Doshi-Velez & Kim, 2017). This lack of interpretability creates serious problems for the principle of accountability, as it becomes difficult to identify responsibility when an artificial intelligence system makes erroneous or harmful decisions. This issue acquires particular seriousness in the case of so called smart collaborative robots, which combine the opacity of machine learning with the risks arising from direct physical interaction with humans in the working environment (Segate & Daly, 2024).

The issue of liability also constitutes a central challenge for legal systems worldwide. When an autonomous robot or an artificial intelligence algorithm causes damage, the question arises as to who bears responsibility: the manufacturer, the programmer, the user or the system itself. Traditional legal frameworks were not originally designed to deal with such cases (Delvaux, 2017). The search for harmonised solutions remains partial even in the EU, which, despite the initial intention of harmonisation through a dedicated directive, ultimately left the matter largely to the national laws of the Member States, as will be analysed in the seventh chapter. Especially in collaborative robotic systems, the challenge remains acute, since their behaviour evolves through machine learning in ways that are not predictable in advance, not even by the programmers themselves (Segate & Daly, 2024).

A particularly important ethical dimension highlighted in the contemporary literature concerns the impact of robotics on the mental health of workers. The close collaboration of humans and robots in the working environment raises concerns that go beyond physical safety and touch on deeper psychological and social dimensions. The risk of alienation, the sense of a downgrading of the human role, the stress arising from constant competition with high performance machines and so called automation bias, that is, the tendency to place excessive trust in algorithmic decisions, constitute ethical challenges that legislators must take into account when shaping regulatory frameworks (Segate & Daly, 2024). At the same time, the observed tendency to humanise robots through anthropomorphic appearance and behaviour may create misleading perceptions of trust and dependence among users, which raises additional ethical questions regarding transparency and honesty in the design of technological systems.

1.2.3 Privacy, Surveillance and Human Dignity

The widespread use of artificial intelligence systems for the collection and processing of data raises serious concerns regarding privacy and human dignity. Technologies such as facial recognition, behavioural analysis and surveillance through robotic systems can be used for purposes that threaten individual freedoms, particularly in authoritarian regimes (Zuboff, 2019). Even in democratic societies, mass surveillance through artificial intelligence raises questions about the limits of state power and the protection of fundamental rights. This issue, as will be analysed in more detail in the fourth chapter, becomes particularly acute in the case of China, where artificial intelligence systematically also operates as an instrument of social control.

In this context, the notion of artificial intelligence as an instrument of power acquires particular significance. The concentration of powerful artificial intelligence technologies in a few large companies or states creates new forms of inequality and dependence, both at the national and at the international level (Crawford, 2021). This dimension of artificial intelligence governance goes beyond the narrow confines of technology policy and enters the field of geopolitics and international relations.

1.2.4 Theoretical Frameworks of Artificial Intelligence Governance

Two dominant theoretical approaches to the governance of artificial intelligence can be identified in the literature, which largely reflect the differences between the regulatory models under examination.

The first approach is the precautionary principle, which holds that, in the face of uncertainty about the consequences of a technology, precautionary measures must be taken to prevent possible harm, even if there is no full scientific certainty (Sunstein, 2005). This principle constitutes a foundation of the European regulatory philosophy.

The second approach is that of risk based regulation, which focuses on addressing risks proportionately according to their severity and likelihood, avoiding excessive regulation that could hinder innovation (Baldwin, Cave & Lodge, 2012). Elements of this approach can be found in all the models examined in this thesis, although they are applied with differing degrees of stringency and through different legal instruments, from the binding risk categorisation of the AI Act to the voluntary risk self assessment provided for by the Singaporean MAIGF.

Understanding these theoretical frameworks is necessary for interpreting the regulatory choices that will be analysed in the following chapters, since every legislative text or policy initiative reflects specific values and assumptions about the role of the state, the rights of citizens and the relationship between technology and society.

2 Chapter 2: The Regulatory Framework for Artificial Intelligence and Robotics in the European Union

2.1 The Regulatory Philosophy of the EU

The European Union has positioned itself as a global leader in the regulation of emerging technologies, adopting a precautionary and rights based approach aimed at ensuring that technological innovation develops in a manner that respects fundamental rights, safety standards and social values (European Commission, 2020). The regulatory strategy of the EU also aims at creating harmonised rules across all Member States, ensuring that technological development takes place on the basis of consistent legal standards throughout the European single market.

This regulatory effort does not start from scratch. The EU already had a body of legislation indirectly concerning robotics and artificial intelligence, such as the Machinery Directive, the Product Liability Directive and the Framework for Safety and Health at Work. The problem, as Segate and Daly (2024) point out, is that these legislative texts were designed for an earlier era, in which robots operated in isolated environments, without direct physical collaboration with humans and without the capabilities of autonomous learning that characterise modern artificial intelligence systems. The existing framework was unable to adequately address the challenges posed by smart collaborative robots, with the result that significant regulatory gaps were created in the fields of both safety and liability.

2.2 The Artificial Intelligence Act (EU AI Act)

The most important legislative initiative of the EU in this field is the Regulation on Artificial Intelligence, known as the AI Act, which entered into force in 2024 and constitutes the first comprehensive regulatory framework for artificial intelligence systems worldwide. The regulation adopts a risk based approach, categorising artificial

intelligence applications according to the level of risk they pose to individuals and society (European Commission, 2024).

As Nobile (2023) points out, the definition of an artificial intelligence system adopted by the original proposal for the AI Act was deliberately broad, including techniques known for decades, with the aim of preventing the circumvention of the legislation through artificial conceptual distinctions. The definition itself has nevertheless been criticised as excessively broad, since it may cover systems that present minimal or no risk.

The AI Act establishes four risk categories. Unacceptable risk includes artificial intelligence systems that constitute a clear threat to fundamental rights and democratic processes and are therefore expressly prohibited. High risk concerns systems in sensitive sectors such as healthcare, transport, education and law enforcement, which are subject to strict regulatory requirements. Limited risk concerns applications with transparency obligations, such as informing users of their interaction with artificial intelligence systems. Minimal risk concerns systems with little or no risk, which remain largely unregulated (European Commission, 2024, Nobile, 2023).

Robotic systems used in sectors such as autonomous vehicles, medical robotics or industrial automation usually fall within the high risk category, requiring manufacturers to comply with strict obligations relating to safety testing, documentation, risk assessment and human oversight mechanisms. Segate and Daly (2024) note, however, that the AI Act, although an important first step, does not delve sufficiently into the particularities of collaborative robots that use machine learning, leaving open critical issues regarding algorithmic opacity and the allocation of responsibility. Moreover, following Regulation (EU) 2026/1744, the obligations for high risk systems embedded in Annex I products apply from 2 August 2028, while the definition of a safety component has been narrowed, so that systems serving exclusively functions of user assistance, performance optimisation or convenience are no longer considered safety components (Orrick, 2026), as analysed in section 2.5.

2.3 The GDPR and Data Protection

Robotic systems frequently collect, process and analyse large volumes of data, including personal information. For this reason, manufacturers and operators of robotic technologies must comply with the General Data Protection Regulation, which establishes strict rules governing data protection and privacy within the EU (GDPR, 2016).

The GDPR requires organisations to ensure that personal data are processed lawfully, transparently and for specified purposes. In the context of robotics and artificial intelligence systems, this means that manufacturers must apply the principles of privacy by design, ensuring that data protection safeguards are integrated directly into the design of technological systems (Kuner, Bygrave & Docksey, 2020). Nobile (2023) further emphasises that black box machine learning models may not be compatible with the GDPR requirements for interpretability and transparency in automated decision making, which creates additional regulatory challenges for the manufacturers of artificial intelligence systems.

2.4 The Ethics Guidelines and the New Machinery Regulation

Beyond formal legislation, the EU has also developed a framework of ethical governance for artificial intelligence and robotics. The European Commission, through the High Level Expert Group on AI, introduced guidelines promoting trustworthy artificial intelligence, placing emphasis on principles such as transparency, accountability, fairness and human oversight (HLEG AI, 2019). These principles cover issues such as human agency and oversight, technical robustness and safety, privacy protection, transparency, non discrimination and the accountability of manufacturers.

At the level of occupational safety, the New Machinery Regulation, Regulation (EU) 2023/1230, which replaced the old Machinery Directive, represents a step forward, as it introduces for the first time a Regulation instead of a Directive, achieving direct and uniform application in all Member States without the need for national transposition.

Segate and Daly (2024) nevertheless argue convincingly that the New Machinery Regulation remains inadequate for the needs of smart collaborative robotics, since it does not adequately address the challenges of machine learning, algorithmic opacity and the allocation of responsibility in human and robot environments. They propose the adoption of a new, binding Regulation on Occupational Health and Safety that would specifically address the challenges of collaborative robotics, incorporating both technical standards and legal safeguards for workers and manufacturers. This critique acquires additional significance following Regulation (EU) 2026/1744, which moved the Machinery Regulation from Section A to Section B of Annex I of the AI Act, reducing the number of AI Act obligations that apply to machinery (European Union, 2026, Orrick, 2026). Consequently, the requirements for robotic systems falling under the Machinery Regulation will be shaped to a greater extent through the sectoral framework itself, that is, precisely through the legislative instrument whose adequacy Segate and Daly (2024) call into question.

The issue of liability remains, as noted in the first chapter, incompletely regulated at EU level, since the specific proposal for an Artificial Intelligence Liability Directive was formally withdrawn in October 2025, leaving the matter largely to the national laws of the Member States, despite the partial coverage offered by the revised Product Liability Directive, Regulation 2024/2853 (Bird & Bird, 2025a). This issue will be analysed in more detail as one of the central challenges of the European model in the seventh chapter.

Overall, the regulatory framework of the EU represents the most ambitious and comprehensive attempt at governing artificial intelligence and robotics at the global level. Despite the existing gaps, the EU's commitment to the protection of fundamental rights, transparency and human oversight creates a model that influences regulatory choices in other jurisdictions as well, the so called Brussels Effect (Bradford, 2020).

2.5 Recent Developments: The Digital Omnibus on AI Regulation and the Implementation Tools of the AI Act

The most important change to the European framework since the adoption of the AI Act is Regulation (EU) 2026/1744, known as the Digital Omnibus on AI. The European Commission submitted the proposal on 19 November 2025, the political agreement between the European Parliament and the Council was reached on 7 May 2026, the Parliament approved the text on 16 June 2026 and the Council on 29 June 2026. The Regulation was published in the Official Journal on 24 July 2026 and entered into force on 27 July 2026, a few days before the original date of application of the obligations for high risk systems (European Union, 2026). The Regulation retains the risk based categorisation, but amends in a targeted manner the timetable and certain substantive provisions of the AI Act.

First, the application of the obligations for high risk systems is postponed. For stand alone systems under Annex III, such as those used in employment or biometrics, the obligations apply from 2 December 2027 instead of 2 August 2026, while for systems falling under the Union harmonisation legislation of Annex I, which also covers many robotic systems, they apply from 2 August 2028. For systems intended to be used by public authorities, the compliance deadline is set at 2 August 2030 (European Union, 2026, Orrick, 2026). The Regulation itself justifies the extension by the delayed availability of standards, common specifications and alternative guidance, as well as by the delayed establishment of national competent authorities (European Union, 2026, recital 40). By contrast, the transparency obligations of Article 50, such as informing users that they are interacting with an artificial intelligence system and labelling deepfakes, apply as scheduled from 2 August 2026, with the sole exception of a transitional period until 2 December 2026 for the machine readable marking of content by systems that had already been placed on the market before that date (Orrick, 2026).

Second, the Regulation extends the prohibited practices of Article 5 with two new prohibitions, which concern systems that generate or manipulate realistic intimate material of identifiable persons without their consent, as well as child sexual abuse material, and which apply from 2 December 2026.

Third, in order to address overlaps with sectoral legislation, the Machinery Regulation is moved from Section A to Section B of Annex I, while a mechanism is introduced whereby the Commission may, by means of implementing acts, limit the application of

the AI Act where sectoral legislation contains equivalent requirements for artificial intelligence. At the same time, the definition of a safety component is narrowed to systems whose intended purpose is to prevent or mitigate risks to health and safety, without, however, excluding systems whose failure would endanger human health and safety (Orrick, 2026). For robotics, these changes mean that the regulation of embedded artificial intelligence systems is partly shifted from the horizontal regulation towards sectoral product safety legislation.

Fourth, the simplification measures provided for small and medium sized enterprises, such as simplified technical documentation templates, more proportionate quality management requirements, priority access to regulatory sandboxes and tailored penalty caps, are extended to a new category of small mid cap enterprises (small mid caps), namely enterprises with fewer than 750 employees and an annual turnover of up to 150 million euros or a balance sheet total of up to 129 million euros.

Fifth, central supervision is strengthened, as the AI Office acquires exclusive competence for systems based on a general purpose model of the same provider, as well as for systems integrated into very large online platforms and search engines under the Digital Services Act.

Sixth, the Commission is required to request from the European standardisation organisations unified technical standards covering both the AI Act and the existing harmonisation legislation simultaneously, while the legal basis for the processing of special categories of data for the purpose of detecting and correcting bias is extended, subject to the condition of strict necessity and mandatory safeguards (Orrick, 2026).

Finally, the deadline for the operation of at least one regulatory sandbox in each Member State is postponed to 2 August 2027 (European Union, 2026).

In parallel with this Regulation, the Commission issued two important implementation tools. On 19 May 2026 it published draft guidelines on the classification of high risk systems under Article 6, in three documents concerning the general principles, classification through Annex I and classification through Annex III (European Commission, 2026a). These guidelines, which according to the AI Act should have been issued by 2 February 2026 (European Commission, 2024, Article 6(5)), are not legally binding, since the authoritative interpretation of the Regulation rests with the Court of Justice of the European Union. In addition, on 10 June 2026 the Commission published the final Code of Practice on the marking and labelling of content generated by artificial

intelligence. The Code is voluntary, but, once it is assessed as adequate by the Commission and the European Artificial Intelligence Board, signatories will be able to rely on it to demonstrate their compliance with the binding obligations of Article 50 (European Commission, 2026b).

These developments are of twofold significance for this thesis. On the one hand, they confirm that the implementation of a horizontal binding framework depends critically on the availability of technical standards and institutional capacity, since their absence led to a postponement of the central deadlines by approximately sixteen months. On the other hand, they show that the EU now makes use, within its binding framework, of non binding instruments, such as guidelines and voluntary codes of practice, which are functionally similar to the quasi regulation instruments that characterise Singapore, as will be analysed in sections 6.3 and 7.2. The European model, therefore, is not static, but evolves under the pressure of practical implementation difficulties.

3 Chapter 3: The Regulatory Approach to Artificial Intelligence and Robotics in the United States

3.1 The Regulatory Philosophy of the US

In contrast to the European Union, the United States follows a more decentralised and innovation oriented approach to the regulation of artificial intelligence and robotics. Instead of adopting a single comprehensive legal framework, the US regulatory system is based on a combination of sector specific regulations, voluntary standards and guidance issued by federal agencies (Calo, 2017). This approach reflects a broader political tradition that prioritises technological innovation, economic competitiveness and private sector leadership in technological development (White House, 2019).

The US regulatory philosophy tends to focus on encouraging innovation, addressing risks as they emerge, rather than applying extensive ex ante regulatory controls. As a result, the governance of artificial intelligence and robotics in the US often involves flexible regulatory instruments, such as guidelines, risk management frameworks and industry best practices, rather than binding legislation (Cath, 2018).

3.2 Federal Agencies and Sectoral Regulation

Several federal agencies play an important role in overseeing the use of robotics and artificial intelligence in specific sectors. Because these technologies are used across multiple industries, regulatory responsibility is distributed among various government bodies. The Federal Trade Commission, known internationally as the FTC, is responsible for addressing issues related to consumer protection, deceptive practices and the unfair use of artificial intelligence technologies, applying mainly Section 5 of the FTC Act on unfair or deceptive practices, as well as laws such as the Equal Credit Opportunity Act and the Fair Credit Reporting Act. The agency has intensified its activity in recent years

around algorithmic accountability and the potential risks associated with automated decision making systems, through a combination of guidance documents and enforcement cases (Holland & Knight, 2023).

The National Institute of Standards and Technology, known as NIST, plays a central role in the development of technical standards and risk management frameworks for artificial intelligence. The Artificial Intelligence Risk Management Framework, known as the AI RMF, provides voluntary guidance to organisations on how to design and develop trustworthy artificial intelligence systems while managing potential risks (National Institute of Standards and Technology, 2023).

In sectors such as healthcare and medical technologies, the Food and Drug Administration, known as the FDA, regulates robotic and artificial intelligence based medical devices, assessing their safety and effectiveness before they are approved for use in clinical settings (Food and Drug Administration, 2021).

3.3 Policy Initiatives and National Strategies up to 2022

In the years preceding 2025, the United States government had introduced several policy initiatives aimed at strengthening national leadership in artificial intelligence. An important example was the American AI Initiative, which emphasised investment in artificial intelligence research, workforce development and international cooperation (White House, 2019).

Another key policy document was the Blueprint for an AI Bill of Rights, introduced in 2022 by the White House Office of Science and Technology Policy. This framework set out principles designed to protect individuals from potential harms caused by automated systems, including protections relating to privacy, discrimination and transparency (White House Office of Science and Technology Policy, 2022). These principles were not legally binding, but provided guidance to government agencies and private organisations developing artificial intelligence technologies.

3.4 The Policy Shift of 2025

The American approach changed significantly from 2025 onwards. On 23 January 2025, President Trump signed Executive Order 14179, entitled Removing Barriers to American Leadership in Artificial Intelligence, which revoked the previous Executive Order 14110 of the Biden administration on the safe and trustworthy development of artificial intelligence and directed the preparation of a national action plan within one hundred and eighty days (Federal Register, 2025). This plan, entitled Winning the Race: America's AI Action Plan, was published on 23 July 2025 and focuses on deregulation, the promotion of ideologically neutral artificial intelligence systems, investment in infrastructure and international competitiveness, while it directs a revision of the NIST AI RMF itself (Seyfarth Shaw, 2025).

In December 2025, the administration issued a new executive order, Executive Order 14365 of 11 December 2025, aimed at limiting the fragmentation of state laws on artificial intelligence, attempting to establish a single federal framework in the face of growing legislative activity at state level, such as in Colorado and California (White House, 2025). This development highlights an inherent characteristic of the American model, namely the tension between federal and state competence, which remains an open issue.

The implementation of this order during 2026 turned the tension into an open institutional and judicial confrontation. On 9 January 2026 the Attorney General established the AI Litigation Task Force of the Department of Justice, tasked with challenging state artificial intelligence laws before the federal courts, while the evaluation of state laws that the Department of Commerce was required to publish by 11 March 2026 had not been made public by the end of April 2026 (Jenner & Block, 2026). On 20 March 2026 the White House published the National Policy Framework for Artificial Intelligence, a short document of non binding legislative recommendations to Congress, organised around seven thematic axes, including the protection of children, intellectual property, freedom of speech and innovation, with the central proposal of preempting state laws that impose undue burdens, so as to establish a single and minimally burdensome national standard (White House, 2026).

A characteristic example of the new dynamic is the Colorado artificial intelligence law, the first comprehensive state law on high risk systems, which had borrowed concepts from the EU AI Act. Following the lawsuit filed by the company xAI against the law, the

Department of Justice intervened on 24 April 2026, arguing that the law violates the Equal Protection Clause of the Constitution (U.S. Department of Justice, 2026). A few weeks later, on 14 May 2026, Colorado repealed and replaced the law before it took effect, with a new, narrower statute that applies from 1 January 2027 and shifts the approach from proactive risk management obligations towards a limited framework of transparency and consumer rights in relation to automated decisions (Eckert Seamans, 2026). At the same time, on 1 July 2026 the FTC published, in implementation of the same executive order, a proposed Policy Statement according to which state laws may be preempted when they require companies to engage in conduct contrary to the prohibition of deceptive practices in Section 5 of the FTC Act (Arnold & Porter, 2026).

State legislative activity, however, has not been halted. California's SB 53 on the transparency of advanced (frontier) models has applied since 1 January 2026 as the first state law requiring standardised safety and transparency disclosures from the developers of such models, while in March 2026 New York amended the corresponding RAISE Act, aligning it to a large extent with the California law, with application from 1 January 2027 (Cooley, 2026).

Overall, the transition from the 2022 framework, with its emphasis on the protection of rights through non binding principles, to the 2025 framework, with its emphasis on deregulation and global dominance in artificial intelligence, reflects the structural instability of the American model, which depends to a large extent on the presidential administration in office rather than resting on a stable legislative basis. At the time of writing, Congress has not enacted a federal law on artificial intelligence, with the result that the desired uniformity is being pursued through executive acts, non binding recommendations and judicial interventions rather than through legislation.

3.5 Overall Assessment

The US approach to the governance of artificial intelligence and robotics is characterised by decentralised governance, with multiple agencies responsible for oversight in different sectors, by flexible regulatory mechanisms, including voluntary standards and industry guidelines, by a strong emphasis on innovation and economic competitiveness, and by a greater reliance on private sector self regulation compared with the EU (Cath, 2018). While this regulatory strategy encourages rapid technological development, the absence of a comprehensive federal framework creates regulatory gaps and inconsistencies between sectors, while the shift in policy between administrations adds further uncertainty for businesses operating in the market over the long term. The developments of 2026 reinforce this assessment, since the uncertainty no longer concerns only the content of federal policy, but also which state laws will ultimately remain in force. Nevertheless, the US model continues to influence global debates on balancing technological innovation with regulatory oversight.

4 Chapter 4: The Regulatory Approach to Artificial Intelligence and Robotics in China

4.1 China as a Global Artificial Intelligence Power

China is one of the leading powers worldwide in the field of artificial intelligence. According to the AI Index 2025 Report of Stanford HAI, China ranks second worldwide in the number of notable artificial intelligence models, with fifteen models in 2024 compared with forty for the US and three for Europe, while it holds first place worldwide in publications and patents in the field (Maslej et al., 2025). At the same time, China dominates industrial robotics, accounting for 51.1% of global industrial robot installations in 2023 (approximately 54% in 2024 according to the IFR), according to the International Federation of Robotics (Maslej et al., 2025).

China's regulatory model differs fundamentally from those of the EU, the US and Singapore, since it combines strong state guidance, the strategic promotion of innovation and the parallel development of social surveillance systems (Roberts et al., 2021). China's regulatory philosophy is characterised by a model in which development precedes regulation, allowing rapid technological development under state guidance with the gradual introduction of regulatory measures when deemed necessary (Roberts et al., 2021). This approach reflects the broader political philosophy of the country, in which the state plays a central role in shaping technological development guided by national strategic objectives (Ding, 2018).

4.2 National Artificial Intelligence Strategy

In 2017, the Chinese government published the New Generation Artificial Intelligence Development Plan, which sets the goal of China becoming the leading global power in artificial intelligence by 2030 (State Council of China, 2017). The plan unfolds in three phases, the first being the achievement of an international level by 2020, the second significant research breakthroughs by 2025, and the third global leadership by 2030 (State

Council of China, 2017). This strategy is complemented by the Made in China 2025 initiative, which designates artificial intelligence and robotics as central pillars of industrial development (Ding, 2018).

In terms of investment, private investment in artificial intelligence amounted to 9.3 billion dollars in 2024, significantly lower than the 109.1 billion of the US. The Chinese government nevertheless offsets this private shortfall through state funding and through the active alignment of large technology companies such as Baidu, Alibaba and Tencent with national strategic objectives (Maslej et al., 2025).

In August 2025, the State Council of China issued the AI Plus Action Plan, the most recent national plan for the integration of artificial intelligence into six priority areas: science and technology, industrial application, consumer services, public welfare, governance and security, and international cooperation (State Council of China, 2025). The targets set are particularly ambitious, with artificial intelligence penetration of seventy per cent in the six key areas by 2027, ninety per cent across the entire economy by 2030, and a full transition to an intelligent economy and society by 2035 (IAPP, 2025).

4.3 Artificial Intelligence Regulatory Framework

In recent years, China has developed a progressively expanding regulatory framework for artificial intelligence, a characteristic feature of which is its vertical and iterative logic, since each new regulation builds on the previous one, correcting gaps and broadening the scope of application (Sheehan, 2023). In 2022, regulations were introduced on recommendation algorithms, which oblige companies to provide transparency on the operation of algorithms with public influence, as well as regulations on deep synthesis technologies (Deep Synthesis Provisions), which regulate deepfakes and synthetic content (CAC, 2022). Both regulations introduced the algorithm registry, a central transparency tool through which companies are required to declare to the government how their algorithms operate and are trained (Sheehan, 2023).

The most significant step came in August 2023, when the Interim Measures for the Management of Generative Artificial Intelligence Services entered into force, making

China one of the first jurisdictions worldwide with binding regulations on generative artificial intelligence (Generative AI) (CAC, 2023). These regulations require providers of artificial intelligence services to ensure that the content generated complies with core socialist values, to submit their models to security assessments before their public release, and to cooperate with the regulatory authorities during inspections (Mazzini & Simonelli, 2024).

In March 2025, the CAC issued the Rules for Labelling Content Generated by Artificial Intelligence, which entered into force on 1 September 2025 (CAC, 2025). These rules impose dual labelling, visible labels for users and invisible labels embedded in the metadata of every text, image, audio or video generated by artificial intelligence, making China one of the few jurisdictions worldwide to have established mandatory labelling of artificial intelligence content at national level (Bird & Bird, 2025b). Since 2 August 2026 corresponding, although not identical, labelling obligations also apply in the EU through Article 50 of the AI Act, as analysed in section 2.5.

During 2026 the Chinese framework was further expanded with four critical texts. First, the amendment of the Cybersecurity Law, which was approved by the Standing Committee of the National People's Congress on 28 October 2025 and entered into force on 1 January 2026, introduced for the first time a specific provision on artificial intelligence into a fundamental law on cyberspace. The provision combines state support for research, algorithms and data and computing power infrastructure with the improvement of ethical rules and the strengthening of monitoring, risk assessment and safety supervision, while the amendment also significantly increases the penalties for violations (Haynes Boone, 2026). This provision is of a framework nature and does not constitute a horizontal regulatory framework equivalent to the AI Act.

Second, on 20 March 2026 the Ministry of Industry and Information Technology (MIIT), jointly with other government departments, adopted the Trial Measures for the Ethics Review and Services of Artificial Intelligence Science and Technology, which apply to artificial intelligence research and development activities that may entail ethical risks to human dignity, public order, life and health (MIIT et al., 2026).

Third, on 10 April 2026 the CAC and four other departments issued the Interim Measures for the Administration of Anthropomorphic Interactive Artificial Intelligence Services, which entered into force on 15 July 2026 and constitute the first departmental regulation dedicated exclusively to services that simulate human personality and emotional interaction, such as digital companions, with a requirement to clearly inform

users that they are interacting with an artificial intelligence system and not with a human being, and with special protection for minors and the elderly (Bird & Bird, 2026a).

Fourth, on 8 May 2026 the CAC, the National Development and Reform Commission (NDRC) and the MIIT jointly issued Implementation Opinions on the standardised application and innovative development of intelligent agents (AI agents), which are defined as intelligent systems capable of autonomous perception, memory, decision making, interaction and execution (CAC, NDRC & MIIT, 2026). In this way agents are treated as a distinct category and not merely as an application of generative artificial intelligence, which confirms the vertical and iterative logic of the Chinese model, in which each new technological category acquires its own regulatory text.

As regards the policy making process, Sheehan (2023) analyses how Chinese artificial intelligence regulations are shaped through a four layer policy funnel: technological reality, the ideology of the Chinese Communist Party, the world of ideas and the bureaucracy. A central role in coordinating the regulations is played by the CAC, which has emerged as the main artificial intelligence regulator, although its dominance is expected to be challenged as regulation extends beyond the control of online content (Sheehan, 2023). This prediction appears to be partly confirmed by the texts of 2026, since the ethics review measures were issued under the lead of the MIIT, while the texts on anthropomorphic services and on intelligent agents were issued by the CAC jointly with other bodies, including the NDRC and the MIIT (MIIT et al., 2026, Bird & Bird, 2026a, CAC, NDRC & MIIT, 2026).

4.4 Social Control and Surveillance

One of the most characteristic and controversial elements of the Chinese approach is the use of artificial intelligence as an instrument of state governance and social control. The Social Credit System makes use of facial recognition, data analysis and artificial intelligence technologies to assess the behaviour of citizens and businesses (Roberts et al., 2021). The use of artificial intelligence for surveillance purposes has been documented particularly in the autonomous region of Xinjiang, provoking strong international criticism for violations of fundamental rights (Roberts et al., 2021, Ding, 2018). This dimension highlights a fundamental difference in values between the Chinese model and Western regulatory frameworks, in which the protection of fundamental rights constitutes an explicit design principle of artificial intelligence regulations.

5 Chapter 5: Singapore, Modern History and AI Regulatory Framework

5.1 Singapore, from Colonialism to the Twenty First Century

5.1.1 Historical and Geopolitical Context

Understanding Singapore's contemporary regulatory framework for artificial intelligence and robotics presupposes an examination of the country's particular historical and geopolitical trajectory, which largely explains the particular way in which Singapore approaches the governance of technology.

Singapore is an island state southeast of the Malay Peninsula, with a total area of approximately 725 square kilometres and a population of just over 6.1 million inhabitants, making it one of the most densely populated states in the world (Britannica, 2024).

The British colonial presence in Singapore dates back to 1819, when Sir Stamford Raffles established a trading post on behalf of the British East India Company. The geographical position of the island, at the point of convergence of the maritime trade routes between the Indian and Pacific Oceans, gave it strategic importance from the outset as a transhipment port. For more than a century Singapore was a landmark of the British imperial presence in Asia, developing into one of the most important trading hubs of the region. After its occupation by Japan during the Second World War, from 1942 to 1945, and its recapture by the British, there followed a period of gradual transition towards self government. In 1959 Singapore acquired self governing status within the British Commonwealth, with Lee Kuan Yew and the People's Action Party (PAP) assuming power (SG101, 2024).

In 1963 Singapore was incorporated into the Federation of Malaysia; however, political and ethnic tensions between the Singaporean leadership and the central government led, on 9 August 1965, to Singapore's separation from the Federation and its proclamation as an independent republic (Britannica, 2024). This independence was not the result of a national liberation process but, according to Lee Kuan Yew, was imposed involuntarily on a country without natural resources, without a hinterland and without an army. He

himself chose From Third World to First as the title of the second volume of his memoirs, eloquently capturing the transformative development trajectory that the country followed (Lee Kuan Yew, 2000).

5.1.2 The Economic Transformation: From Unemployment to High Technology

During the first years of its independence, Singapore faced acute problems of unemployment, housing and a weak industrial base. The economy relied almost exclusively on entrepôt trade, while two out of three inhabitants lived in slums (ANZ, 2015). The PAP government responded to these challenges with a programme of accelerated industrialisation, establishing in 1961 the Economic Development Board as a body for attracting foreign investment and developing infrastructure (Minshawi, 2025).

During the 1960s and the early 1970s, the strategy focused on labour intensive industrialisation with low cost labour, attracting multinational companies mainly in the textile and assembly sectors. From the mid 1970s onwards, the government turned to sectors of higher added value, including the electronics industry. At the same time, the financial sector was developed, with the aim of making Singapore a regional centre for financial services.

An unwavering commitment to public integrity, an effective independent anti corruption policy and the meritocratic staffing of the public administration were central features of Singaporean governance and gave the country a strong regulatory character, which it also maintained in the field of technology governance. From the 1980s onwards, Singapore completed its transformation, focusing on excellence, innovation and the advanced services sector (Minshawi, 2025).

5.1.3 The Digital Turn: Smart Nation and the National Artificial Intelligence Strategy

Singapore's technology policy gradually took shape into a comprehensive national strategy during the 2010s and the 2020s. In 2014 the government announced the Smart Nation initiative, a comprehensive digital transformation programme aimed at harnessing technology to improve citizens' quality of life, create economic opportunities and develop a more connected and inclusive society (GovTech Singapore, 2024). The then Prime Minister Lee Hsien Loong presented the Smart Nation Initiative (SNI) as an ambitious whole of government programme, with the aim of making Singaporean society a digitally connected city which "enables meaningful and fulfilling lives, seamlessly connected through technology" (Prime Minister's Office Singapore, 2014, via Das & Kwek, 2024).

The Smart Nation Initiative was structured around three strategic pillars: Digital Government, the Digital Economy and Digital Society. Indicative applications include SingPass, the national digital identity that provides access to more than 1,700 digital services, as well as autonomous vehicles, robotic systems in public safety and artificial intelligence systems in healthcare (IEREK, 2025).

In 2019 Singapore published its National Artificial Intelligence Strategy, known as NAIS, which describes how the country aims to become a global leader in artificial intelligence by 2030, focusing on nine sectors: transport and logistics, manufacturing, finance, safety and security, cybersecurity, smart cities and estates, healthcare, education and government (IMDA, 2019). In December 2023, in recognition of the rapid evolution of generative AI, Singapore revised its strategy with the release of NAIS 2.0, which allocates more than one billion Singapore dollars over five years to strengthen artificial intelligence capabilities, digital trust and workforce readiness (MDDI, 2026). At the end of 2024, the government announced Smart Nation 2.0, in which the new Prime Minister Lawrence Wong described generative artificial intelligence as a "once in a generation" technology (GovTech Singapore, 2024), while 120 million Singapore dollars were allocated to fund related initiatives through the AI for Science programme.

5.1.4 The Regulatory Ethos as a Legacy of History

This brief historical examination reveals certain characteristics that are necessary for understanding Singapore's regulatory philosophy in the field of artificial intelligence. First, Singapore is a small state without natural resources, which has depended on its institutional capacities, its human capital and technological excellence as the main driving forces of economic development. This makes technology governance a matter of existential importance for the country and not merely a regulatory issue. Second, the strong state with an effective bureaucracy and low levels of corruption created a framework of trust between government, businesses and citizens, which enables the rapid implementation of technology policies (Minshawi, 2025).

These historical legacies explain why Singapore has adopted an artificial intelligence governance model that differs both from the binding European model and from the decentralised American model: a model characterised by flexibility, collaborative governance between the public and private sectors, and an aspiration to balance innovation and responsibility, always within the framework of a strong state with clear strategic priorities.

5.2 The Regulatory Framework for Artificial Intelligence in Singapore

5.2.1 The Regulatory Philosophy: Innovation with Responsibility through Quasi Regulation

Singapore's regulatory framework for artificial intelligence differs fundamentally both from the binding legislative model of the European Union and from the decentralised, sectoral model of the United States. Instead of adopting a single legally binding regulatory text of the AI Act type, Singapore has deliberately chosen a model characterised by the combination of national strategies, voluntary governance frameworks, sectoral guidance and practical implementation tools (Duane Morris & Selvam, 2026).

This approach falls within what the regulatory literature calls quasi regulation, that is, a set of rules and standards which the government shapes, endorses or actively

encourages, but without incorporating them into a formal legislative act with legally binding force (Australian Government Best Practice Regulation Handbook, as cited in ALRC, 2019). It is a distinct category of regulatory instrument, deliberately placed between binding legislation and pure industry self regulation, which draws from the former its institutional legitimacy and state guidance, and from the latter its flexibility and lower administrative burden. The significance of this category for this thesis is central, since almost all of the instruments examined below, the MAIGF, AI Verify, the FEAT Principles and the MAS Guidelines on Artificial Intelligence Risk Management, fall precisely within this intermediate category, and not within simple voluntary self regulation, with which they are often confused.

This choice reflects a distinct political philosophy, since responsibility for the responsible adoption of artificial intelligence is allocated primarily to the organisations that develop and use it, within a framework of principles shaped by the state, but without the imposition of binding ex ante obligations. Regulatory theory explains why a state with strong institutional capacity, such as Singapore, consciously chooses this intermediate path instead of full legislation. Quasi regulation allows faster adaptation to technological developments without the delay of the formal legislative process, while retaining significantly greater steering power than pure market self regulation, precisely because these instruments are designed, published and monitored by state bodies such as the IMDA, the PDPC and the MAS (Duane Morris & Selvam, 2026). Such an approach allows Singapore to maintain a "responsible optimism" towards artificial intelligence, harnessing the dynamism of the free market within clearly defined limits, while simultaneously retaining the capacity for immediate legislative intervention should this be deemed necessary.

However, this flexibility does not mean an absence of governance, as will be analysed in section 5.2.7. Singapore has created a multi layered ecosystem of instruments, guidance and institutions which, although non binding in their general form, constitute de facto reference standards both within the country and in the wider region of Southeast Asia. This positioning allows Singapore to avoid direct regulatory incompatibility with the dominant regulatory powers (EU, US, China) and to position itself as a regulatory pole for the small and medium sized jurisdictions of the region facing similar challenges (Allen et al., 2025).

5.2.2 The Artificial Intelligence Governance Framework

The central instrument of the Singaporean approach is the Model Artificial Intelligence Governance Framework, known as the MAIGF, which was first issued in January 2019 by the Personal Data Protection Commission (PDPC) and the Infocomm Media Development Authority (IMDA). The second edition was published in January 2020 at a meeting of the World Economic Forum (Data Protection Report, 2020). The MAIGF is expressly non binding and aims to provide organisations with practical guidance for the responsible development and use of artificial intelligence.

The framework is based on two fundamental principles: first, that the decisions of artificial intelligence systems must be explainable, transparent and fair, and second, that all artificial intelligence solutions must be human centric in their design and application. Governance is organised into four key and interrelated areas. The first concerns institutional organisation and internal control, that is, the restructuring of the internal mechanisms of organisations through a clear allocation of responsibilities, the establishment of risk management protocols and the continuous training of staff on algorithmic decisions. The second concerns the calibration of human involvement, through clarifications around the "human over the loop" model, in which the human retains a supervisory and controlling role over the algorithmic process, with the level of human oversight being determined by the nature and reversibility of the potential harm as well as by the operational feasibility of the intervention itself. The third concerns the operational management of models and data, through a risk based approach that prioritises the impacts on stakeholders, introducing quality specifications such as robustness, reproducibility and auditability. The fourth concerns strategic communication and transparency, through guidelines for determining the appropriate level of information according to the stakeholder group.

Complementing the MAIGF, the IMDA and the PDPC have developed the Implementation and Self Assessment Guide for Organisations, known as ISAGO, which translates the principles of the framework into practical tools and industry examples, designed to help businesses align their artificial intelligence governance practices through market best practices. It was developed in collaboration with the World Economic Forum's Centre for the Fourth Industrial Revolution and with input from more than sixty organisations, promoting innovation (Lexology, 2024). In subsequent years, the MAIGF was expanded to address new categories of artificial intelligence, with the Model AI Governance Framework for Generative AI in 2024, which concerns the

risks of large language models, and the Model AI Governance Framework for Agentic AI in January 2026, which addresses the challenges of autonomous or semi autonomous artificial intelligence systems. These developments place Singapore among the first jurisdictions to formulate structured governance guidance for advanced artificial intelligence systems (Duane Morris & Selvam, 2026).

The framework for agentic AI was already updated on 20 May 2026 on the basis of industry feedback, introducing new best practices and real world case studies on multi agent systems, third party agents and automation bias, while safety and reliability mechanisms, such as access controls, guardrails, human approvals and logging and monitoring, were added as core components of an agent (Baker McKenzie, 2026a). This update, only four months after the first edition, is a characteristic example of the flexibility that quasi regulation allows.

5.2.3 The AI Verify Tool

One of the most innovative elements of the Singaporean approach is AI Verify, which was launched in May 2022 by the IMDA and the PDPC as a Minimum Viable Product for international pilot testing. It was developed in consultation with companies of different sizes and sectors, while more than fifty local and multinational companies participated in the pilot, among them Dell, IBM and Hitachi. AI Verify combines technical tests with process checks, allowing organisations to assess their artificial intelligence systems against eleven internationally recognised governance principles within their own internal environment, resulting in the production of verifiable governance reports (Allen et al., 2025, IMDA/PDPC, 2022).

In June 2023, the establishment of the AI Verify Foundation was announced at Asia Tech x Singapore; the Foundation took over the stewardship of the tool and made it available to the global open source community, with the participation of large technology companies such as Google, IBM, Microsoft and Salesforce (Engler & Doyle, 2024). The Foundation aims to develop artificial intelligence testing tools for responsible use and to promote governance best practices, operating as a neutral platform for international cooperation (AI Verify Foundation, 2024). The AI Verify testing framework is aligned with international standards, including the NIST Risk Management Framework and ISO/IEC 42001 (AI Verify Foundation, 2024).

5.2.4 Data Protection as a Binding Basis: The Role of the PDPA

Despite the generally voluntary nature of the artificial intelligence regulatory framework, there is a clear binding basis, the Personal Data Protection Act, known as the PDPA, which constitutes the main legally enforceable framework for artificial intelligence systems that process personal data in Singapore. The PDPA applies throughout the artificial intelligence life cycle, from data collection and model training to deployment and monitoring (Duane Morris & Selvam, 2026). In contrast to the voluntary MAIGF, a breach of the PDPA entails penalties of one million Singapore dollars or ten per cent of annual turnover for companies with an annual turnover exceeding ten million, or up to two hundred thousand in the case of a natural person (PDPA, 2022).

In March 2024, the PDPC issued the Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems, which clarify how the PDPA applies at three key stages of the implementation of an artificial intelligence system. The first concerns development, testing and monitoring, that is, cases where organisations act as system developers and use personal data to train and test the systems, as well as to monitor their performance after deployment. The second concerns deployment, that is, cases where organisations deploy systems that collect and use personal data at the level of retail to the end consumer ("business to consumer", B2C). The third concerns procurement, that is, service providers that develop bespoke systems on behalf of other companies ("business to business", B2B), using the personal data held by those companies.

It is worth noting that these Guidelines do not cover generative artificial intelligence (generative AI), the regulation of which is addressed separately within the framework of the MAIGF for Generative AI (Data Protection Report, 2024). Although they are not legally binding, the PDPC is likely to take positions on the basis of them, thereby giving them substantial regulatory weight (Bird & Bird, 2024).

This gap was filled in 2026 when, following a public consultation from 2 June to 1 July 2026, the PDPC published on 20 July 2026 the Advisory Guidelines on Use of Personal Data in Generative AI (Allen & Gledhill, 2026a). According to these Guidelines, model providers that process personal data for the development and operation of generative artificial intelligence models are considered organisations within the meaning of the PDPA and are subject to all of its obligations, even when they collect data from downstream systems, such as user prompts. In addition, organisations that use user data to train models must provide specific notification of this use, so that consent is meaningful, and may not make the provision of a product or service conditional on

consent to such use (PDPC, 2026). In this way, generative artificial intelligence is now directly linked to the binding basis of the PDPA and not only to the voluntary MAIGF for Generative AI.

5.2.5 The Financial Sector and the MAS

Of particular importance for understanding the Singaporean model is sectoral regulation in the financial sector, where the Monetary Authority of Singapore, known as the MAS, has developed one of the most extensive artificial intelligence frameworks in the financial industry worldwide. On 12 November 2018, the MAS published the FEAT Principles (Fairness, Ethics, Accountability, Transparency), which provide financial institutions with guidance on the responsible use of artificial intelligence and data analytics (AIDA), focusing on fairness, ethics, accountability and transparency (MAS, 2018). The FEAT Principles are formally non binding and are considered the first artificial intelligence principles issued by a central bank or financial regulator worldwide (Cleary FinTech Update, 2018).

Towards the effective implementation of FEAT, the MAS announced in November 2019 the launch of the Veritas Initiative, a consortium of financial institutions and technology companies, which developed assessment methodologies and open source tools for the practical application of the principles (MAS, 2023). The Initiative completed three phases, with Phase 1 completed in January 2021 and focusing on fairness assessment for use cases in the banking sector, Phase 2 completed in February 2022, developing assessment methodologies for all four principles through a consortium of twenty seven companies, and Phase 3 completed in June 2023 with the release of Veritas Toolkit 2.0 through a consortium of thirty two companies, including DBS, HSBC, Standard Chartered Bank, Google Cloud and IBM (MAS, 2023).

In November 2025, the MAS issued a consultation paper on proposed Guidelines on Artificial Intelligence Risk Management, with a consultation period until 31 January 2026 (MAS, 2025a). The proposed Guidelines concerned all supervised financial institutions and covered three axes: first, oversight of risk management at board and senior management level; second, the obligation to maintain an up to date inventory of artificial

intelligence systems and to assess the materiality of their risk; and third, controls across the entire artificial intelligence life cycle, covering data management, transparency, human oversight, third party risk management and post deployment monitoring (Allen & Gledhill, 2025). The MAS expressly clarifies that the new Guidelines do not replace the FEAT Principles but complement them, extending the scope to cover generative artificial intelligence (generative AI) and autonomous agents (AI Agents), technologies that were not adequately addressed by the 2018 FEAT Principles (MAS, 2025a).

Following the completion of the consultation, on 7 October 2026 the MAS issued the final Guidelines on Artificial Intelligence Risk Management, which apply to all financial institutions and to all forms of artificial intelligence, with controls proportionate to the nature, scale and materiality of the risk (MAS, 2026). The Guidelines take effect on 7 October 2027 with phased implementation: the expectations on oversight and on key risk management systems, policies and procedures apply from 7 October 2027, while the expectations on life cycle controls and on the capabilities and capacity of institutions apply by 7 October 2028 (Allen & Gledhill, 2026b, Baker McKenzie, 2026b). Compared with the consultation text, the final text strengthens proportionality, allowing the use of existing governance structures without an obligation to set up a dedicated artificial intelligence committee, while expressly retaining the institution's responsibility for artificial intelligence systems of third party providers (MAS, 2026). The MAS also announced that during 2027 it will consult the industry on additional guidance concerning agentic AI (Allen & Gledhill, 2026b).

5.2.6 International Orientation and Singapore's Role in International Artificial Intelligence Governance

A distinctive feature of the Singaporean framework is its strong emphasis on international interoperability and alignment with international standards. Singapore was a founding member of the Global Partnership on Artificial Intelligence at its establishment in 2020, being the only Southeast Asian country in this arrangement (OECD.AI, 2024). In October 2023, Singapore and the United States made their artificial intelligence governance frameworks interoperable, establishing a bilateral Governance Group and committing to strengthen research cooperation. Specifically, AI Verify was

mapped to the NIST Risk Management Framework and to the ISO/IEC 42001:2023 standard, reducing compliance costs for organisations operating in multiple jurisdictions (Global Legal Insights, 2026).

In the context of international alignment, in May 2024 Singapore was among the ten countries that signed the Seoul Declaration for safe, innovative and inclusive artificial intelligence, which commits the signatories to cooperation on the interoperability of regulatory frameworks (Saif et al., 2025). The alignment of AI Verify with multiple international standards serves a strategic purpose, since the choice not to adopt binding horizontal regulation allows Singapore, as a small state, to avoid direct regulatory incompatibility with any of the three major regulatory powers that have adopted different strategies, the US, the EU and China. At the same time, the Singaporean approach has already exerted influence on the wider region, as shown by the fact that the ASEAN Guide on AI Governance and Ethics, published in early 2024, adopts a risk and principle based framework similar to that of Singapore. The same authors point out, however, that whether the Singaporean approach can be transferred to other jurisdictions and economies of different scale, with different regulatory environments and cultures, remains an open question (Allen et al., 2025).

5.2.7 The Practical Consequences of Non Compliance

The repeated description of the Singaporean framework as non binding raises a reasonable question: what exactly happens when an organisation simply chooses not to follow the relevant guidelines. The answer differs depending on the specific instrument and reveals the operational logic of quasi regulation in practice.

In the case of the MAIGF and AI Verify, non compliance does not entail any direct sanction on the part of the IMDA or the PDPC, provided that the PDPA is not breached at the same time. An organisation may lawfully develop and make available an artificial intelligence system in Singapore without having adopted any of the principles of the MAIGF and without having submitted its system to testing through AI Verify. The absence of a direct sanction does not, however, mean an absence of consequences. First, an indirect market pressure mechanism operates, since certification through AI Verify

has become a de facto prerequisite for participation in certain public procurement tenders and in partnerships with large multinational organisations that have already adopted the tool, such as IBM and Microsoft, which participate in the AI Verify Foundation (Engler & Doyle, 2024). Second, non compliance deprives the organisation of the possibility to invoke alignment with international standards, such as the NIST risk management framework or ISO/IEC 42001, which has direct consequences for organisations that operate in multiple jurisdictions and wish to demonstrate compliance without repeating audit procedures in each market (Global Legal Insights, 2026).

The case of the FEAT Principles and the MAS Guidelines on Artificial Intelligence Risk Management is different, since, although formally non binding, they concern organisations that are already subject to licensing and supervision by the MAS under other, binding legislation. In this case the MAS applies what regulatory theory describes as responsive regulation or the regulatory pyramid, that is, a system of escalating intervention in which voluntary compliance constitutes the first and preferred tier, while binding intervention remains available as a last resort if voluntary compliance proves inadequate (Ayres & Braithwaite, 1992). In practice this means two things. First, non compliance with the MAS guidelines, without in itself incurring a fine, is taken into account in assessing the fitness of senior managers and the overall corporate governance of a supervised institution under the fit and proper criteria, which the MAS applies on a binding basis to all licensed financial institutions (MAS, 2025b). Second, the MAS itself has expressly stated in an analogous context, that of outsourcing risk management, that it retains the possibility of converting guidelines into a binding regulatory instrument in the future if voluntary compliance is deemed insufficient, making it clear that the non binding nature is an initial policy choice and not a permanent inability to enforce. With the issuance of the final Guidelines in October 2026, the MAS expressly presents them as supervisory expectations with specific implementation timelines, an element that further strengthens their practical weight in the context of supervisory assessment (MAS, 2026).

Finally, in the case of the PDPA, there is no margin for non compliance without consequences, since it constitutes the main horizontal binding basis of the Singaporean framework, with legal penalties of up to one million Singapore dollars or ten per cent of annual turnover, as analysed in section 5.2.4.

The binding basis of the Singaporean framework is not, however, limited to the PDPA. Singapore has enacted targeted legislation for specific risks associated with artificial intelligence, such as the 2024 amendment to the legislation on the integrity of online

election advertising, which prohibits manipulated election deepfakes and was the first time the term artificial intelligence appeared in Singaporean legislation, as well as the Online Safety (Relief and Accountability) Act 2025, which provides for a statutory tort of inauthentic material abuse, including material generated with generative artificial intelligence (Chambers and Partners, 2026). The latter was passed on 5 November 2025, and since 29 June 2026 the Online Safety Commission has been operating, while specific provisions on the relevant civil claims have entered into force, allowing victims of online harms to seek redress before the courts (Ministry of Law Singapore, 2026). This is targeted binding legislation concerning specific harms and not horizontal regulation of artificial intelligence, which nevertheless supplements the system of sanctions beyond the PDPA.

The overall picture that emerges is that the non binding nature of the Singaporean model does not mean an absence of consequences, but a shift of the main source of pressure from direct legal sanction towards a combination of market reputation, institutional assessment and the lingering threat of future legislation, which is supplemented by targeted binding legislation for the most serious harms. This is a deliberate regulatory architecture and not a regulatory gap, a distinction that is critical for the correct assessment of the model in the context of the comparative analysis of the sixth chapter.

6 Chapter 6: Comparative Analysis of the Regulatory Models of the EU, the US, China and Singapore

6.1 Comparative Analysis: EU and US

The regulatory approaches adopted by the European Union and the United States reflect two different philosophies regarding the governance of emerging technologies such as artificial intelligence and robotics. While both jurisdictions recognise the need to address potential risks associated with autonomous systems, their strategies differ significantly in terms of regulatory structure, legal instruments and policy priorities.

The European Union adopts a precautionary and rights based approach, emphasising the protection of fundamental rights, safety standards and ethical oversight. Through legislative initiatives such as the AI Act, the EU seeks to establish a comprehensive and harmonised regulatory framework that applies in all Member States, ensuring that artificial intelligence and robotic technologies are developed in a manner consistent with European values, particularly with regard to transparency, accountability and human oversight (Veale, 2021). By contrast, the United States prefers a more flexible and innovation oriented regulatory model. Instead of adopting a single comprehensive law, regulatory oversight is distributed among various federal agencies and sector specific regulations, a decentralised structure that allows regulators to address risks in specific industries while maintaining a relatively open environment for technological experimentation.

A key difference lies in the use of binding regulations versus optional guidelines. The EU framework relies largely on legally binding obligations imposed on developers and deployers of artificial intelligence systems, particularly in high risk cases. By contrast, many US governance initiatives focus on guidance documents, standards and best practices, such as those developed by NIST through the AI Risk Management Framework. This distinction is no longer absolute, since the EU also makes use of voluntary instruments, such as the Code of Practice on Transparency of AI-generated Content, which nevertheless function as means of demonstrating compliance with binding obligations (European Commission, 2026b). These differences reflect broader policy priorities, as the EU regulatory strategy emphasises risk prevention, consumer protection and ethical oversight, while the US model prioritises technological leadership,

economic growth and global competitiveness, a priority that intensified further after the 2025 policy shift analysed in the third chapter, as well as with the attempt at federal preemption of state laws in 2026. This contrast has nevertheless been partly softened, since the EU, through Regulation (EU) 2026/1744, postponed the obligations for high risk systems and extended the simplification measures, without however abandoning the binding character of its framework (European Union, 2026). This comparison will be examined further, together with China and Singapore, in the four way analysis of section 6.4.

6.2 Comparative Analysis: EU and China

6.2.1 Regulatory Philosophy and Structure

The comparison between the EU and China reveals the most radical contrast in regulatory philosophy among all the jurisdictions under examination. The EU adopts a single, horizontal and legally binding framework, the AI Act, which applies ex ante to all sectors and all categories of artificial intelligence systems, aimed primarily at the protection of fundamental rights (European Commission, 2024). China, by contrast, does not have a single horizontal law, despite the incorporation of a general provision on artificial intelligence into the Cybersecurity Law from 1 January 2026 (Haynes Boone, 2026), but develops its regulatory framework through successive, vertical regulations targeting specific technological categories, such as recommendation algorithms in 2022, Generative AI in 2023 and synthetic content labelling in 2025, as well as anthropomorphic interactive services and intelligent agents in 2026 (Sheehan, 2023, Mazzini & Simonelli, 2024). Both jurisdictions thus arrive at binding regulation, but through opposite methodologies: the EU through a comprehensive piece of legislation with a lengthy preparatory process, China through rapid, targeted regulations issued administratively by the CAC without the need for a parliamentary legislative process equivalent to the European one (Sheehan, 2023).

6.2.2 Speed of Regulatory Response

The vertical and iterative logic of the Chinese model gives China remarkable speed in adapting to new technological developments. By way of illustration, China issued binding rules on generative artificial intelligence (generative AI) as early as August 2023, with content labelling following by 2025, while the corresponding regulation of general purpose models in the EU AI Act became applicable in August 2025, two years later (Mazzini & Simonelli, 2024), with the Commission's powers to impose fines on the providers of these models applying from August 2026 (European Commission, 2024, Article 113). This difference is not due to a lack of will on the part of the EU, but to the structural difference between a legislative process that requires the consensus of twenty seven Member States and the European Parliament, and an administrative process under a single state authority.

The developments of 2026 confirm the same difference. Within a few weeks, China issued specific texts on anthropomorphic artificial intelligence services and on intelligent agents (Bird & Bird, 2026a, CAC, NDRC & MIIT, 2026), while the EU postponed the application of the obligations for high risk systems by approximately sixteen months, precisely because of the delay in the availability of standards and in the establishment of national authorities (European Union, 2026). Nevertheless, the completion of the amending procedure itself in approximately eight months from the submission of the proposal shows that the European legislative process can be accelerated when there is sufficient political will.

6.2.3 The Role of the State in Relation to Technology

The most essential difference, however, is not procedural but one of values. In the EU, the regulation of artificial intelligence aims primarily at protecting the individual from potential harms caused by the technology, with the state acting as a guarantor of rights (European Commission, 2024). In China, artificial intelligence functions additionally as an instrument for the exercise of state power and social control, as reflected in the Social Credit System and in the use of surveillance technologies in Xinjiang (Roberts et al., 2021). The requirement of Chinese regulations that content generated by artificial intelligence comply with core socialist values reflects the same logic, namely the use of regulation not only to prevent harm but also to ensure the ideological conformity of content (Mazzini & Simonelli, 2024). This fundamental difference renders the two models essentially incompatible in terms of their guiding values, despite certain procedural similarities, such as the common use of binding rules and transparency obligations.

6.2.4 Industrial Policy and Regulation

A final dimension of comparison concerns the relationship between regulation and industrial policy. The EU treats regulation and industrial strategy as relatively distinct policy fields, with the AI Act aimed primarily at risk management. This distinction has, however, been blurred, since Regulation (EU) 2026/1744 simplifies compliance and extends the relief measures to a wider range of businesses, which shows that competitiveness considerations now directly influence European regulation as well (Orrick, 2026). China integrates the regulation of artificial intelligence directly into the framework of national industrial objectives, as reflected in the New Generation Artificial Intelligence Development Plan and the recent AI Plus Action Plan, which sets specific quantitative targets for the penetration of artificial intelligence into the economy (State Council of China, 2017, 2025). Regulation in China thus functions less as a brake and more as an instrument for steering technological development towards national strategic objectives. It is characteristic that the 2026 Implementation Opinions on intelligent agents were issued jointly by the CAC, the MIIT and the NDRC, that is, the country's central economic planning body (CAC, NDRC & MIIT, 2026).

6.3 Comparative Analysis: EU and Singapore

6.3.1 Regulatory Philosophy

The most fundamental difference between the two systems lies in their regulatory philosophy. The AI Act constitutes the first legally binding and horizontal legislative framework for artificial intelligence at the global level. The EU adopted a precautionary approach based on ex ante risk categorisation, imposing binding compliance obligations on providers and deployers of high risk systems before they are placed on the market, with fines of up to thirty five million euros or seven per cent of global annual turnover for the most serious infringements (European Commission, 2024, Article 99).

Singapore follows the opposite philosophy. The MAIGF, AI Verify and sectoral frameworks such as FEAT and the MAS Guidelines are as a rule voluntary, with binding obligations confined to the PDPA where personal data are involved. The objective is not ex ante compliance but the cultivation of responsible optimism through organisational maturity and the voluntary adoption of standards (Allen et al., 2025). This difference is not merely technical but reflects deeper policy choices, since the EU places the protection of fundamental rights as a non negotiable precondition, while Singapore places economic competitiveness and flexibility as priorities, with the ethical dimension shaped through guidelines and voluntary cooperation.

6.3.2 Governance Structure, Horizontal Framework versus Multi Layered Ecosystem

The AI Act adopts a horizontal structure: it applies to all sectors and all categories of artificial intelligence systems, with a single four tier risk classification, unacceptable, high, limited and minimal, and a single enforcement mechanism through national competent authorities and the AI Office of the European Commission. This offers legal clarity and harmonisation across the internal market of twenty seven Member States, but at the same time creates a high administrative burden, particularly for smaller organisations. Regulation (EU) 2026/1744 further strengthened the central character of

supervision, assigning to the AI Office exclusive competence for systems based on general purpose models of the same provider and for systems integrated into very large online platforms, while extending the simplification measures to small mid cap enterprises, partly mitigating the administrative burden (Orrick, 2026).

Singapore operates with a multi layered ecosystem, in which the horizontal MAIGF is implemented by the IMDA and the PDPC, FEAT and the Guidelines on Artificial Intelligence Risk Management, which were finalised in October 2026 (MAS, 2026), are implemented by the MAS for the financial sector, while the PDPA constitutes the common binding basis. Although this structure is more flexible and less burdensome in terms of compliance costs, it raises questions about a lack of regulatory clarity, since the absence of a single enforcement authority for artificial intelligence may create uncertainty for organisations as to their precise obligations (Allen et al., 2025, MAS, 2025a).

6.3.3 Risk Categorisation

The EU introduces a formal four tier risk classification, which determines ex ante which systems fall into which categories, with detailed lists in Annexes I and III of the AI Act. This provides legal certainty but may face difficulties in classifying new, hybrid or emerging technologies. Indicative of this difficulty is that the Commission published the draft guidelines on high risk classification in May 2026, after the February 2026 deadline, and that these guidelines are not legally binding (European Commission, 2026a). The EU thus itself resorts to interpretative guidance in order to make its classification workable. Singapore does not introduce a formal risk classification for artificial intelligence systems at the horizontal level. Instead, the MAIGF guides organisations to carry out an internal risk assessment based on the nature of their application, with human oversight adjusted accordingly (PDPC/IMDA, 2020). This flexibility may be an advantage for rapid adaptation to new technologies, but it makes systematic comparison and external control difficult.

6.3.4 Transparency, Accountability and Human Oversight

Both frameworks regard transparency and human oversight as fundamental principles, but they differ radically in the way they are implemented. The AI Act imposes specific legally binding obligations of transparency, documentation, registration in a European database and human oversight for high risk systems (Articles 13 to 14). The MAIGF recognises the same principles but implements them through internal organisational commitment, without external verification or binding procedural requirements, unless the organisation chooses to use AI Verify (Allen et al., 2025). The distance between the two approaches has, however, been partly reduced, since the transparency obligations of Article 50 of the AI Act apply from 2 August 2026, while for their implementation the Commission published a voluntary Code of Practice on content labelling, adherence to which, once assessed as adequate, may be used as a means of demonstrating compliance (European Commission, 2026b). The EU thus makes use of instruments that are functionally similar to Singaporean quasi regulation, which, however, operate within a binding framework.

6.3.5 Generative AI and Emerging Technologies

One area in which the comparison is particularly revealing is the treatment of Generative AI. The AI Act regulates General Purpose Models through Articles 51 to 56, with binding obligations that entered into force in August 2025, including the assessment of systemic risk for the most advanced models (European Commission, 2024). In May 2024 Singapore issued the MAIGF for Generative AI, which covers nine dimensions of risk, from accountability to content safety, while in January 2026 it issued the MAIGF for Agentic AI, making it one of the first jurisdictions worldwide to address this category of systems explicitly (Duane Morris & Selvam, 2026). This framework was described as the first in the world designed specifically for agentic AI systems (Bird & Bird, 2026b) and was already updated in May 2026 (Baker McKenzie, 2026a), while in July 2026 the PDPC issued specific guidelines on the use of personal data in generative artificial intelligence (PDPC, 2026). It is worth noting that in May 2026 China also issued a specific text on intelligent agents (CAC, NDRC & MIIT, 2026), while in the EU artificial intelligence agents fall under the general categories of the AI Act. Singapore's speed of response in

these new fields is attributed precisely to the absence of binding legislation that would require broad consultation and a legislative process for each update, a characteristic that Singapore partly shares with the Chinese model, as analysed in section 6.2.2, albeit through an entirely different regulatory logic, voluntary in the one case and binding in the other.

6.4 Four Way Comparison: Axes of Convergence and Divergence

The examination of the four jurisdictions reveals one central axis of convergence and three axes of fundamental divergence. As regards convergence, all four systems recognise that artificial intelligence systems give rise to risks that require some form of governance, and to some extent use international standards as reference points, although China shows here a clearly lower commitment to multilateral arrangements such as the OECD.

The first axis of divergence concerns the degree of bindingness. The EU opts for legally enforceable horizontal obligations, with now postponed timetables for high risk systems, Singapore opts for voluntary governance with a binding basis mainly through the PDPA and targeted legislation for specific harms, the US operates with voluntary standards and sectoral regulation, in the face of growing state legislation which the federal government seeks to restrict, and China applies binding regulations for specific categories of artificial intelligence, such as algorithms, Generative AI and content labelling, as well as anthropomorphic services and intelligent agents, without a single horizontal law, while maintaining strong state oversight (Sheehan, 2023, Mazzini & Simonelli, 2024).

The second axis of divergence concerns regulatory philosophy. The EU prioritises fundamental rights, Singapore economic competitiveness within a framework of responsible use, the US technological leadership and private sector innovation, and China national strategic development under party guidance, while ranking social stability above individual freedom (Roberts et al., 2021, Ding, 2018).

The third axis of divergence, which China's inclusion brings out with particular clarity, concerns the relationship between artificial intelligence and the state. While the EU, the

US and Singapore treat artificial intelligence as a technology requiring regulation in order to protect individuals and societies from potential harm, China additionally treats it as an instrument of state governance and social organisation, using its capacity for surveillance, assessment and control in a manner that raises fundamental concerns from a human rights perspective (Roberts et al., 2021).

Beyond these axes, the developments of 2026 reveal a dynamic of partial convergence. The EU postponed timetables, extended simplification measures and makes use of voluntary codes and guidelines within its binding framework (European Union, 2026, European Commission, 2026b). Singapore, without adopting a horizontal law, linked generative artificial intelligence to the binding basis of the PDPA and gave the supervisory expectations of the MAS specific timelines (PDPC, 2026, MAS, 2026). China continued its vertical regulatory practice, while at the same time incorporating a general provision on artificial intelligence into a fundamental law (Haynes Boone, 2026), while in the US the federal government is pursuing a single national standard against state fragmentation (White House, 2026). This convergence does not negate the fundamental differences in values described above, but it suggests that each jurisdiction is seeking, in its own way, combinations of binding and flexible instruments, which constitutes the starting point for exploring an ideal regulatory model in section 7.2.

7 Chapter 7: Challenges and Ideal Regulatory Model

7.1 Challenges and Future Regulatory Developments

7.1.1 Challenges of the European Model

Despite its pioneering nature, the AI Act faces certain structural challenges in its implementation. The first and foremost is the cost of compliance for small and medium sized enterprises. Research has shown that the requirements for extensive testing, documentation and certification of high risk systems impose a disproportionate burden on smaller organisations that lack sufficient financial and technical resources (Gutierez et al., 2026). Regulation (EU) 2026/1744 sought to partly mitigate this burden by extending the simplified compliance measures to small mid cap enterprises as well, without however changing the substantive requirements for high risk systems (Orrick, 2026). The literature had also pointed out that the delayed publication of technical standards for high risk systems left providers with particularly narrow margins for compliance, increasing uncertainty for the organisations concerned (European Journal of Risk Regulation, 2025, Hacker et al., 2025). This assessment was confirmed, since the delay in the availability of standards and in the establishment of national authorities ultimately led to the postponement of the relevant deadlines to 2 December 2027 and 2 August 2028 (European Union, 2026, recital 40). The postponement offers additional preparation time, but does not eliminate uncertainty, which now shifts to whether the unified technical standards provided for by the amended Article 40 will be available in time (Orrick, 2026).

A second challenge is the risk of delayed regulation in the face of rapidly evolving technologies, as already highlighted in the comparison with the Chinese model in section 6.2.2. The legislative process in the EU, although it guarantees democratic legitimacy, makes rapid adaptation to new risk categories difficult. Generative AI is a characteristic example: although it was incorporated into the AI Act through the provisions on GPAI models, their complex implementation continues to create uncertainty. The need to postpone the deadlines for high risk systems by means of a new regulation in 2026 is a further indication of the difficulty the legislative model has in keeping pace with the practical reality of implementation.

A third challenge is regulatory overlap. Organisations operating in regulated sectors, such as medical devices or financial services, face the problem of overlapping obligations under the AI Act and under sectoral legislation, which increases cost and complexity. A characteristic example is the GDPR obligation of data minimisation, which is in tension with the AI Act requirement for representative and complete data in order to properly train high risk models (Clark, 2026). Regulation (EU) 2026/1744 partly addresses both issues. On the one hand, it introduces a mechanism for limiting the application of the AI Act where sectoral legislation contains equivalent requirements and moves the Machinery Regulation to Section B of Annex I. On the other hand, it extends the legal basis for the processing of special categories of data for the purpose of detecting and correcting bias, under a regime of strict necessity and mandatory safeguards (Orrick, 2026). The full resolution of the overlap nevertheless depends on the acts that will follow, with a deadline of 2 August 2028 for the relevant delegated act of the Commission.

A fourth challenge, as analysed in the first chapter, is the issue of liability for damage caused by artificial intelligence, which remains incompletely regulated following the withdrawal of the Artificial Intelligence Liability Directive in October 2025, leaving the matter fragmented among the national laws of the Member States, with only partial coverage by the revised Product Liability Directive (Bird & Bird, 2025a).

7.1.2 Challenges of the American Model

The American model faces challenges of a different nature, which stem mainly from its decentralised structure itself. The absence of a single federal law creates fragmentation among sectoral regulations, resulting in inconsistent levels of protection depending on the sector of activity (Calo, 2017). This tension is exacerbated by growing legislative activity at state level, which the federal government attempted to restrict with the executive order of December 2025, as analysed in the third chapter, thereby creating an open constitutional and political confrontation between federal and state competence. Moreover, the heavy reliance on voluntary standards, such as the NIST AI RMF, means that compliance depends largely on the goodwill of organisations, without an external control mechanism comparable to that of the EU (Cath, 2018). Finally, the abrupt policy reversal between administrations, such as the complete overturning of the 2022 approach

by the 2025 approach, adds significant regulatory uncertainty for businesses planning long term investments. This confrontation moved to the courts in 2026, with the intervention of the Department of Justice against the Colorado law and its subsequent replacement by a narrower statute (U.S. Department of Justice, 2026, Eckert Seamans, 2026), while uniformity is being pursued through non binding legislative recommendations, without a federal law (White House, 2026). The result is that regulatory uncertainty now stems not only from changes between administrations, but also from the uncertain outcome of the conflicts between the federal and state levels.

7.1.3 Challenges of the Chinese Model

The Chinese model, despite its effectiveness in terms of speed of regulatory response, faces its own category of challenges. The fragmented, vertical character of regulation, although it allows rapid adaptation, creates ambiguities regarding the overlap between successive regulations and uncertainty for providers as to the full set of their obligations (Sheehan, 2023). This challenge intensified in 2026, since the addition of specific texts on ethics review, anthropomorphic services and intelligent agents, combined with the general provision of the amended Cybersecurity Law, increases the density of the framework, with the result that a single product may fall under more than one regime at the same time, such as a digital companion that also operates as an intelligent agent. A more serious challenge is the fundamental tension between the use of artificial intelligence as an instrument of social control and international standards for the protection of rights, an issue that limits the possibility of international harmonisation of the Chinese model with Western governance standards and raises serious concerns when other jurisdictions assess imported artificial intelligence systems of Chinese origin (Roberts et al., 2021).

7.1.4 Challenges of the Singaporean Model

The Singaporean model in turn faces challenges of a different nature. Its central weakness concerns the question of whether reliance on voluntary and quasi regulatory governance will continue to provide adequate safeguards as artificial intelligence becomes ever more widespread, particularly in light of the new risks introduced by Generative AI, such as disinformation and privacy issues (Allen et al., 2025). The same authors point out that the absence of strict regulatory mechanisms raises questions about long term accountability, and that a stronger framework could ensure that artificial intelligence remains aligned with ethical standards as it continues to evolve.

A second challenge lies at the level of coverage of regulatory processes. A comparative analysis of six jurisdictions cited by Allen et al. (2025) shows that the Singaporean Generative AI model displays partial coverage in five of the fifteen critical governance processes, including model development and the management of distribution and access control, while significant gaps are identified in another five critical processes, such as the safeguarding of user rights and control (Luna et al., 2024). These gaps concern in particular the safeguarding of individuals' autonomy over their personal data and over the decisions produced by Generative AI models.

Some of these concerns, which were formulated before the developments of 2026, have been partly addressed. The PDPC Guidelines on generative artificial intelligence strengthen individuals' control over the data used to train models (PDPC, 2026), the final MAS Guidelines give specific timelines to supervisory expectations in the financial sector (MAS, 2026), and the Online Safety Act provides judicial protection against harms from material generated with generative artificial intelligence (Chambers and Partners, 2026, Ministry of Law Singapore, 2026). These developments show a gradual strengthening of institutional oversight without a horizontal law, but they do not remove the central reservation regarding the external verifiability of voluntary instruments.

A third challenge is the transferability of the model. Although the Singaporean approach has already influenced the ASEAN Guide on AI Governance, whether it can be adopted by other jurisdictions with a different scale, regulatory culture and institutional framework remains an open question (Allen et al., 2025). This matters for its comparative assessment as a model for the EU, since certain of its features, such as the high degree of trust between the state and industry and centralised decision making in a small state, may not transfer directly to a heterogeneous system of twenty seven Member States.

7.1.5 Future Developments

All four models are evolving. In the EU, the simplification measures for the AI Act that the European Commission was considering (Hacker et al., 2025) were enacted through Regulation (EU) 2026/1744, and the next critical milestones are 2 December 2027 for Annex III systems, 2 August 2028 for Annex I systems and the finalisation of the guidelines on high risk classification (European Union, 2026, European Commission, 2026a), while the regulatory sandboxes of Article 57 are expected to function as a mechanism of regulatory learning (Future of Privacy Forum, 2025), with the deadline for the operation of at least one sandbox per Member State now set at 2 August 2027 (European Union, 2026). In Singapore, the finalisation of the MAS Guidelines on Artificial Intelligence Risk Management in October 2026, with application from 2027 and consultation on agentic AI during 2027 (MAS, 2026), and the establishment of the Singapore AI Safety Institute in 2025 suggest a gradual shift towards more intensive institutional oversight, particularly in high risk sectors (Allen et al., 2025). In the US, political uncertainty as to the degree of federal intervention remains the dominant feature, with the tension between federal and state competence expected to intensify further. The next milestones include the entry into application of the new Colorado law and of the New York RAISE Act on 1 January 2027, as well as the possible introduction of federal legislation based on the recommendations of March 2026 (Eckert Seamans, 2026, Cooley, 2026, White House, 2026). In China, the 2025 AI Plus Action Plan reveals a strategic shift from the defensive control of artificial intelligence content towards the aggressive integration of artificial intelligence across the entire economy, with binding quantitative targets for the coming years (State Council of China, 2025), while the 2026 texts on anthropomorphic services and intelligent agents show that regulatory attention is shifting towards the most autonomous and interactive forms of artificial intelligence (Bird & Bird, 2026a, CAC, NDRC & MIIT, 2026). This development has direct implications for international regulatory dynamics, since China is expanding its artificial intelligence into international markets through the export of technology and infrastructure, with the result that the mode of governance accompanying these exports becomes an important factor for the EU, which is called upon to determine which artificial intelligence is imported into its internal market and under what conditions (Roberts et al., 2021, Mazzini & Simonelli, 2024).

7.2 Towards an Ideal Regulatory Model: Combining the Strengths of the Four Approaches

The preceding comparative analysis shows that each of the four jurisdictions has features that work effectively, but also weaknesses that often stem from those very features. This section attempts to outline an ideal regulatory model, which combines the strengths of the four approaches while limiting their weaknesses. It must be clarified that this model is an analytical and normative construct of this thesis, based on the findings of the previous chapters and on regulatory theory, and not an empirically validated proposal. The model is not addressed to a specific jurisdiction, but describes the structural elements that a regulatory system would need in order to meet simultaneously the requirements of rights protection, speed of adaptation, innovation and legal certainty.

7.2.1 Criteria for Selecting the Positive Characteristics

Positive characteristics are understood here as those elements which, according to the analysis of chapters two to six, contribute to at least one of the competing objectives identified in section 6.4, without necessarily presupposing the negative characteristics of their jurisdiction of origin. From the EU are drawn legal certainty, harmonisation and the protection of fundamental rights through a binding core of rules (European Commission, 2024). From Singapore are drawn the flexibility of quasi regulation, practical implementation tools such as AI Verify and sectoral specialisation through supervisory authorities with strong expertise (Allen et al., 2025, MAS, 2026). From China is drawn the capacity for rapid, targeted regulation of new technological categories through vertical, iterative rules (Sheehan, 2023). From the US are drawn the emphasis on innovation, the use of technical standards such as the NIST AI RMF and ex post enforcement through existing consumer protection legislation (National Institute of Standards and Technology, 2023, Holland & Knight, 2023).

The theoretical link between these elements is provided by the regulatory pyramid of Ayres and Braithwaite (1992), according to which voluntary compliance constitutes the first tier of a system of escalating intervention, with binding sanctions remaining available as a last resort, as well as by risk based regulation, which requires the

proportionate allocation of regulatory burdens according to the severity and likelihood of risks (Baldwin, Cave & Lodge, 2012). In the same context, the notion of quasi regulation, as an intermediate category between binding legislation and self regulation (Australian Law Reform Commission, 2019), allows the theoretical integration of voluntary instruments into a system with a binding core.

7.2.2 The Architecture of the Ideal Model

The ideal model is organised into five interrelated layers and one cross cutting principle, which are summarised in Table 1.

Table 1: The layers of the ideal regulatory model

Layer	Content	Jurisdiction of origin	Weakness to be avoided
1. Binding horizontal core	Prohibitions of unacceptable risk practices, minimum transparency obligations, binding data protection	EU (AI Act, GDPR), Singapore (PDPA)	Absence of enforceable rights protection in purely voluntary models
2. Proportionate escalation with rapid technical updating	Risk categories in the law, technical specifications and new categories of systems through administrative acts under democratic control	EU (risk categorisation), China (vertical, iterative regulation)	Slowness of the full legislative process, concentration of power
3. Quasi regulation instruments linked to compliance	Governance frameworks, codes of practice, open testing tools, regulatory sandboxes	Singapore (MAIGF, AI Verify), EU (Code of Practice)	Limited enforceability of pure self regulation, high compliance costs
4. Sectoral specialisation with a priority rule	Supervisory expectations of specialised authorities, application of equivalent sectoral regulation	Singapore (MAS), US (FDA, FTC), EU (Regulation 2026/1744)	Overlap between horizontal and sectoral regulation
5. Ex post enforcement and accountability	Consumer protection, civil liability, judicial remedies, escalating supervisory intervention	US (FTC), Singapore (OSRAA, fit and proper criteria)	Excessive ex ante burden, liability gaps
Cross cutting principle: international interoperability	Mapping of tools and unified technical standards	Singapore (AI Verify, NIST AI RMF, ISO/IEC 42001), EU (unified standards)	Fragmentation and multiple compliance costs

The first layer is a limited but binding horizontal core, following the EU model. It includes the prohibitions of unacceptable risk practices, minimum transparency obligations, such as informing users of their interaction with an artificial intelligence system and labelling synthetic content, and a binding data protection basis, such as the GDPR and the PDPA. These elements are chosen because they concern fundamental values, which do not change at the pace of technology, and therefore the stability of legislative regulation is not a disadvantage here but a guarantee. Indicatively, even during the simplification of 2026, the EU not only retained but also extended the prohibited practices, while maintaining the timetable of the transparency obligations (European Union, 2026, Orrick, 2026). At the same time, Singapore's experience shows that the binding basis of data protection can be extended to new technologies, such as generative artificial intelligence, through interpretative guidance without new legislation (PDPC, 2026).

The second layer concerns the proportionate escalation of obligations on the basis of risk, combined with a mechanism for rapid technical updating. The law defines the risk categories and the substantive requirements, while the technical specifications and new specific categories of systems, such as intelligent agents or digital companions, are regulated through administrative or delegated acts. This element borrows from China the vertical, iterative logic, which allowed the regulation of generative artificial intelligence in 2023 and of intelligent agents in 2026 within a short time (Sheehan, 2023, CAC, NDRC & MIIT, 2026), but detaches it from the concentration of power. Rapid updating must be subject to public consultation, parliamentary scrutiny and periodic review clauses, so that speed does not come at the expense of democratic legitimacy.

The third layer is a set of quasi regulation instruments, following the Singaporean model: governance frameworks, codes of practice, open technical testing tools of the AI Verify type and regulatory sandboxes. The critical element, which distinguishes this layer from pure voluntary self regulation, is its institutional link to the binding core, since adherence to an approved code or successful testing through an official tool should function as a means of demonstrating compliance. The EU already follows this logic with the Code of Practice on content labelling, which, once assessed as adequate, allows signatories to demonstrate compliance with Article 50 (European Commission, 2026b). In this way the flexibility of quasi regulation is preserved, as shown by the updating of the Singaporean framework for agentic AI within four months (Baker McKenzie, 2026a), without sacrificing enforceability. Open testing tools also reduce compliance costs for

smaller businesses (Engler & Doyle, 2024), responding to one of the central challenges identified in section 7.1.1 (Gutierez et al., 2026).

The fourth layer is sectoral specialisation through supervisory authorities with specialised expertise, following the model of the MAS in Singapore and of sectoral agencies in the US, such as the FDA (Food and Drug Administration, 2021). Sectoral authorities translate general requirements into specific supervisory expectations, as the MAS did with the FEAT Principles and with the 2026 Guidelines, which set specific timelines and proportionate requirements for all financial institutions (MAS, 2018, 2026). In order to avoid the overlap identified as a challenge of the European model, an explicit priority rule is required, according to which, where sectoral regulation contains equivalent requirements, it applies instead of the horizontal rule. The mechanism for limiting the application of the AI Act through implementing acts introduced by Regulation (EU) 2026/1744 is a first step in this direction (Orrick, 2026).

The fifth layer is ex post enforcement and accountability. Following the model of the American FTC, existing legislation on consumer protection and on combating unfair practices also applies to artificial intelligence systems, making it possible to address harms that had not been foreseen ex ante (Holland & Knight, 2023). Ex post enforcement is supplemented by a clear civil liability regime and by direct judicial remedies for victims, such as the civil claims provided for by the Singaporean Online Safety Act (Ministry of Law Singapore, 2026). Strengthening this layer allows a proportionate easing of ex ante obligations for lower risk systems, since protection does not depend exclusively on certification before placing on the market. The escalation of intervention, from supervisory assessment to sanction, follows the logic of the regulatory pyramid, as applied by the MAS through the fit and proper criteria (Ayres & Braithwaite, 1992, MAS, 2025b).

Finally, the model as a whole is underpinned by the principle of international interoperability. The mapping of AI Verify to the NIST AI RMF and to the ISO/IEC 42001 standard shows that the mutual recognition of tools reduces compliance costs for organisations operating in multiple jurisdictions (Global Legal Insights, 2026), while the obligation to develop unified technical standards covering several pieces of legislation simultaneously moves in the same direction at Union level (Orrick, 2026). Interoperability does not, however, imply the acceptance of every foreign standard, since, as highlighted in section 6.2.3, recognition presupposes compatibility with the values of the binding core.

7.2.3 Characteristics Deliberately Excluded

Just as important as the selection of positive characteristics is the explicit exclusion of those elements that the analysis identified as weaknesses. From the Chinese model, the use of artificial intelligence as an instrument of state control and social surveillance is excluded, as is the requirement of ideological conformity of generated content, elements incompatible with the protection of fundamental rights (Roberts et al., 2021, Mazzini & Simonelli, 2024). The ideal model borrows from China only the regulatory technique and not the purposes it serves. From the American model, the dependence of regulatory policy on executive acts that are overturned with every change of administration is excluded, as is the fragmentation between levels of governance, which in 2026 led to judicial conflicts between the federal government and the states (Federal Register, 2025, U.S. Department of Justice, 2026).

From the European model, the concentration of all critical implementation parameters in a legislative text is excluded, since it makes every substantial adjustment dependent on a new legislative procedure, as shown by the need to postpone the deadlines in 2026 (European Union, 2026), as is the absence of a harmonised liability regime (Bird & Bird, 2025a). Finally, from the Singaporean model, exclusive reliance on voluntary instruments without external verification for high risk systems is excluded, a weakness that is also highlighted in the literature (Allen et al., 2025).

7.2.4 Preconditions for Implementation

The implementation of such a model presupposes that certain requirements are met, without which the combination of the individual elements would not function as it does in their jurisdictions of origin.

The first precondition is adequate institutional capacity and expertise on the part of the regulatory authorities. Both the flexibility of quasi regulation and rapid technical updating presuppose authorities capable of developing, monitoring and revising technical instruments. The Singaporean experience rests precisely on an effective public administration enjoying a high degree of trust (Minshawi, 2025), while the delayed

establishment of national competent authorities is expressly cited as one of the reasons for the postponement of the European deadlines (European Union, 2026, recital 40).

The second precondition is the availability of technical standards before the obligations begin to apply. The European experience shows that binding obligations without standards available in time lead to uncertainty and ultimately to postponements (European Journal of Risk Regulation, 2025, European Union, 2026). In the ideal model the sequence is reversed, since the tools and standards of the third layer are developed and tested first, and the binding obligations are activated once these become available.

The third precondition is a stable legislative basis. The flexibility of the lower layers is acceptable only if the core is established by law and not by executive acts, so that it is not overturned by political changes, as happened in the US with the revocation of Executive Order 14110 in 2025 (Federal Register, 2025).

The fourth precondition is the democratic legitimacy of rapid regulation. Delegation to administrative authorities must be accompanied by transparent consultation procedures, parliamentary scrutiny and judicial protection, so that the speed borrowed from the Chinese model does not entail the price of the lower legitimacy described in section 7.1.3.

The fifth precondition is trust and cooperation between the state and industry. The effectiveness of quasi regulation instruments in Singapore is due not only to their design, but also to the participation of industry in their development, as in the case of the AI Verify Foundation and the Veritas Initiative (Engler & Doyle, 2024, MAS, 2023). This trust cannot be legislated, but it can be cultivated through transparent and participatory procedures.

The sixth precondition is adequate staffing and funding of ex post supervision. The easing of ex ante obligations is legitimate only if market surveillance authorities have the resources and powers for effective controls; otherwise the easing turns into a regulatory gap.

The seventh precondition is international coordination. Given that artificial intelligence systems circulate across borders, the effectiveness of any national or regional model depends on the mutual recognition of tools and standards, to which arrangements such as the Seoul Declaration and the Global Partnership on Artificial Intelligence contribute (Saif et al., 2025, OECD.AI, 2024).

7.2.5 Inherent Tensions and Limits of the Ideal Model

Even under the above preconditions, certain tensions cannot be fully eliminated, but only mitigated. The first concerns the relationship between speed and legitimacy, since every mechanism of democratic control slows down updating, and therefore the ideal model cannot achieve the speed of a centralised system without also adopting its characteristics. The second concerns the relationship between flexibility and legal certainty, since the more obligations are specified through non binding instruments, the greater the interpretative uncertainty becomes, as shown by the fact that even the Commission's guidelines on high risk classification are not legally binding (European Commission, 2026a). The third concerns scale, since characteristics that work in a small state with centralised decision making do not automatically transfer to heterogeneous large scale systems (Allen et al., 2025). The fourth concerns values, since regulatory technique is not value neutral and the speed of the Chinese model is linked to its institutional structure, which cannot be reproduced in a democratic framework (Sheehan, 2023).

The conclusion of this section is that a model possessing all the positive and none of the negative characteristics of the four jurisdictions is not feasible, since certain strengths and weaknesses are aspects of the same institutional feature. What is feasible, however, is a hybrid model that significantly reduces the trade offs, combining a stable binding core with flexible, institutionally linked implementation instruments. The partial convergence observed in 2026, with the EU making use of voluntary codes within a binding framework and Singapore giving greater weight to its supervisory expectations, suggests that the jurisdictions themselves are already moving, albeit in a fragmented way, in this direction.

8 Chapter 8: Conclusions

8.1 Answers to the Research Questions

This section synthesises the findings of chapters two to seven, answering in turn the research questions posed in the first chapter.

Research question 1: What are the fundamental differences in regulatory philosophy, governance structure, legal instruments and policy priorities among the four jurisdictions?

The examination confirmed that there is no single, globally accepted model of artificial intelligence governance, but rather four substantially different regulatory philosophies, each of which stems from the particular political traditions, institutional capacities and social values of the respective jurisdiction.

The European Union, through the AI Act, created the first comprehensive, legally binding and horizontal regulatory framework for artificial intelligence worldwide, placing the protection of fundamental rights as a non negotiable priority. This model, as analysed in the second and sixth chapters, offers legal certainty and harmonisation across the internal market, but is burdened by structural challenges: the high cost of compliance for small and medium sized enterprises, the risk of delayed adaptation to rapidly evolving technologies, the overlap between sectoral and horizontal legislation, and the incompletely regulated issue of civil liability following the withdrawal of the relevant dedicated directive in 2025. The adjustments of 2026 through Regulation (EU) 2026/1744, with the postponement of the obligations for high risk systems to 2027 and 2028, the extension of the simplification measures and the partial treatment of overlaps, show that the model is adapting to these challenges without abandoning its binding character.

The United States followed the opposite course, opting for a decentralised, sectoral and largely voluntary model, which prioritises innovation and economic competitiveness. As highlighted in the third chapter, this model is characterised by notable political instability, with the complete overturning of the 2022 approach by that of 2025 demonstrating how closely American regulatory policy is tied to the presidential administration in office, while also intensifying the tension between federal and state competence. In 2026 this tension turned into a judicial confrontation, with the federal

government intervening against state laws and promoting a single national standard through non binding legislative recommendations.

China presented a third, substantially different model, in which regulation is built up gradually through successive, vertical regulations under a single state authority, achieving remarkable speed of regulatory response, as documented in the comparison of the sixth chapter. At the same time, however, the Chinese model highlights most clearly the fundamental tension between regulatory effectiveness and the protection of individual rights, since artificial intelligence there also functions as an instrument of state control, in a manner incompatible with the values governing the European, Singaporean or American frameworks. In 2026 this model was extended with specific texts on ethics review, anthropomorphic services and intelligent agents, as well as with a general provision on artificial intelligence in the Cybersecurity Law.

Finally, Singapore presented a fourth model, which, as analysed extensively in the fifth chapter, combines flexibility, voluntary governance and practical implementation tools, such as AI Verify, with a binding data protection basis through the PDPA and targeted legislation for specific harms. This model succeeded in combining speed of adaptation, particularly in the regulation of generative and autonomous artificial intelligence, with the preservation of international interoperability. In 2026 the model was strengthened by the final MAS Guidelines, the PDPC Guidelines on generative artificial intelligence and the start of operations of the Online Safety Commission, without a horizontal law being adopted.

These differences were summarised in the four way comparison of section 6.4 along three axes of divergence: the degree of bindingness, regulatory philosophy and the relationship between artificial intelligence and the state.

Research question 2: How does the apparent non binding nature of voluntary and quasi regulatory frameworks operate in practice, and what consequences are faced by those actors who choose not to comply?

The analysis in section 5.2.7 showed in detail that in Singapore non bindingness does not mean an absence of consequences, but a shift of compliance pressure towards market reputation, institutional fitness assessment and the lingering threat of future binding legislation. The finalisation of the MAS Guidelines in October 2026, with specific implementation timelines, further reinforces this character (MAS, 2026). This extensive analysis corresponds to the stated emphasis of this thesis on the Singaporean model. A

similar mechanism operates, though analysed to a lesser extent here, in the United States as well, where the substantive weight of a formally voluntary standard, such as the NIST AI Risk Management Framework, arises ex post through judicial practice, since American courts already use it as a reference point for the standard of care in negligence claims, and through state legislation that incorporates it as a condition for a legal defence (Future of Privacy Forum, 2026). This picture is, however, fluid, since the body of relevant state laws is changing, as shown by the repeal and replacement of the Colorado law in 2026 (section 3.4). A third form is now also emerging in the EU, where voluntary codes of practice, such as the Code on content labelling, function as a means of demonstrating compliance with binding obligations (European Commission, 2026b). The comparison, even in this brief form, shows that non bindingness is not a uniform category, but takes a different form depending on whether compliance pressure comes from administrative assessment, as in Singapore, or from the common law, as in the US, or from an institutional link to a binding framework, as in the EU.

Research question 3: Which factors explain the differences in the speed of regulatory response to rapidly evolving technologies, such as generative artificial intelligence?

The comparison of sections 6.2.2 and 6.3.5 showed that the speed of regulatory response is closely linked to whether regulation requires a full legislative process. China issues binding regulations administratively, through the CAC, while Singapore updates non binding frameworks without the need for broad consultation and legislation for each change. By contrast, the EU, whose legislative process requires the consensus of twenty seven Member States and the European Parliament, regulated general purpose models with a delay of approximately two years compared with China. The same difference was confirmed in 2026, when China issued specific texts on anthropomorphic services and intelligent agents, while the EU postponed the obligations for high risk systems owing to a lack of standards and institutional readiness. It is worth noting, however, that the amendment itself was completed in approximately eight months, which shows that the European process can be accelerated when there is political will. The price of speed differs from case to case: lower democratic legitimacy and ambiguities between successive regulations in China, as analysed in section 7.1.3, and limited external verifiability in Singapore.

Research question 4: How does the historical and institutional legacy of a country influence its regulatory philosophy towards artificial intelligence?

The historical examination in section 5.1 showed how the absence of natural resources and the need to survive through institutional excellence led Singapore to a regulatory ethos of speed and of trust between the state, industry and citizens. The country's history, from a small colonial trading post to a global innovation hub within a few decades, largely explains why technology governance is treated there as a matter of almost existential importance. A comparable explicit historical analysis was not carried out for the other three jurisdictions, given the deliberate emphasis of the thesis on the EU and Singapore. There are, however, indications of a similar dynamic, such as the institutional tradition of rights protection in the EU and the political tradition of limited state intervention in the US, which could be the subject of future research.

Research question 5: Which regulatory model most effectively manages the tension between the protection of fundamental rights and economic or technological competitiveness?

The thesis does not arrive at a single optimal model. Effective regulation of artificial intelligence is a matter of balancing competing objectives, namely the protection of rights, speed of adaptation, economic competitiveness and institutional legitimacy, in a manner that corresponds to the particular conditions of each jurisdiction. None of the four models manages this tension without cost: the EU sacrifices speed for rights, Singapore sacrifices external verifiability for flexibility, the US sacrifices stability for innovation, and China sacrifices individual rights for speed and national strategic coherence. The EU has a clear comparative advantage in the protection of fundamental rights, but the experience of Singapore demonstrates that speed and flexibility are not necessarily incompatible with responsible governance.

The developments of 2026 indeed show that the jurisdictions are constantly readjusting their position in this tension, with the EU seeking greater flexibility and Singapore giving greater weight to its supervisory expectations in the most sensitive sectors, an issue examined in the eighth research question.

Research question 6: To what extent is the regulatory model of Singapore transferable to jurisdictions of much larger scale and institutional heterogeneity, such as the European Union?

The answer deliberately remains open, as already noted in sections 5.2.6 and 7.1.4. The transferability of a model that rests on high institutional trust and centralised decision making in a small state to a heterogeneous system of twenty seven Member States cannot be empirically substantiated at this stage, beyond the partial influence that the Singaporean model already exerts on the ASEAN Guide. For this reason, the ideal model

of section 7.2 incorporates the instruments inspired by Singapore as an implementation layer linked to a binding core and not as a substitute for it.

Research question 7: How does the treatment of artificial intelligence as an instrument of state power affect the possibility of international harmonisation of standards and cross border trust in imported systems?

The analysis in section 6.2.3 and the future developments in section 7.1.5 showed that the use of artificial intelligence as an instrument of state control in China creates a structural obstacle to international harmonisation. The EU is already called upon to decide under what conditions it will allow Chinese artificial intelligence systems to enter its internal market. This issue is not limited to technical interoperability standards, but touches on fundamental choices of values.

Research question 8: To what extent is it feasible to design an ideal regulatory model that combines the positive characteristics of the four jurisdictions without their weaknesses, and what preconditions would its implementation require?

The analysis in section 7.2 leads to a twofold answer. On the one hand, a model possessing all the positive and no negative characteristics is not feasible, because certain strengths and weaknesses are aspects of the same institutional feature: China's speed is inseparable from the concentration of power, Singapore's flexibility is linked to limited external verifiability, and the EU's legal certainty to slowness of adaptation. On the other hand, a hybrid five layer model is feasible, with a binding horizontal core, proportionate escalation with rapid technical updating under democratic control, institutionally linked quasi regulation instruments, sectoral specialisation with a priority rule and strengthened ex post enforcement, which significantly reduces the trade offs.

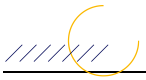
The implementation of this model presupposes institutional capacity on the part of regulatory authorities, timely availability of technical standards, a stable legislative basis, democratic legitimacy of rapid regulation, trust between the state and industry, adequate resources for ex post supervision and international coordination. The developments of 2026 show that individual elements of the model are already appearing in a fragmented way in the jurisdictions under examination, without, however, having been brought together into a single architecture in any of them.

8.2 Conclusions, Ideal Model and Limitations

The comparative analysis led to the outline of an ideal regulatory model, as analysed in section 7.2. This model draws from the EU the binding core of rights protection and risk based categorisation, from Singapore the quasi regulation instruments and sectoral specialisation, from China the regulatory technique of rapid and targeted updating, detached from the concentration of power, and from the US ex post enforcement and the use of technical standards. The model was explicitly formulated as an analytical and normative construct, with awareness of the inherent tensions that cannot be fully eliminated, such as the relationship between speed and legitimacy and the relationship between flexibility and legal certainty.

The broader conclusion that emerges from the thesis as a whole is that, as artificial intelligence continues to evolve at a pace that tests the limits of every legislative process, the ability of a regulatory system to learn from comparable international examples, without abandoning the fundamental values that govern it, emerges as a decisive factor for its long term effectiveness. The experience of China and the US highlights, each in a different way, the dangers of both excessive concentration of state power and excessive regulatory instability, while the experience of Singapore shows that there are intermediate paths that deserve to be studied as building blocks of a hybrid regulatory model.

This thesis has certain limitations. First, the deliberate emphasis on the EU and Singapore means that the US and China were examined complementarily, and that their historical and institutional legacy was not analysed in the depth in which the Singaporean one was. Second, the transferability of the Singaporean model to the EU could not be empirically substantiated. Third, the regulatory landscape is evolving very rapidly. Although Regulation (EU) 2026/1744 and the MAS Guidelines were finalised in 2026, their application begins between 2027 and 2028, the guidelines on high risk classification remain in draft form and the confrontation between the federal and state levels in the US has not been resolved, so the findings reflect the situation as of October 2026 and may need to be updated. Fourth, the ideal regulatory model of section 7.2 is an analytical and normative construct that has not been empirically tested. These limitations also point to directions for future research: a comparative historical analysis of the



institutional traditions of the four jurisdictions and an empirical assessment of the application of AI Verify type tools in larger scale regulatory environments, as well as an empirical investigation of the functioning of individual elements of the ideal model, such as the institutional link between voluntary codes and compliance.

9 Bibliography

Allen, F., et al. (2025). Cambridge Forum on AI: Law and Governance.

Allen & Gledhill. (2025). MAS Consultation on Guidelines on AI Risk Management.

Allen & Gledhill. (2026a). PDPC issues Advisory Guidelines on Use of Personal Data in Generative AI.

Allen & Gledhill. (2026b). MAS publishes AI risk management guidelines setting out supervisory expectations on responsible AI adoption.

ANZ. (2015). The man who defined Singapore. ANZ BlueNotes.

Arnold & Porter. (2026). FTC's Proposed Policy Statement on AI Accuracy and Preemption of State AI Laws.

Australian Law Reform Commission. (2019). Codes and Co-regulation, in Serious Invasions of Privacy in the Digital Era.

Ayres, I., & Braithwaite, J. (1992). Responsive Regulation: Transcending the Deregulation Debate. Oxford University Press.

Baker McKenzie. (2026a). Singapore: IMDA updates Model AI Governance Framework for Agentic AI.

Baker McKenzie. (2026b). Singapore: MAS issues Guidelines on Artificial Intelligence Risk Management.

Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding Regulation: Theory, Strategy, and Practice. Oxford University Press.

Bird & Bird. (2024). Singapore's Advisory Guidelines on AI Recommendation and Decision Systems.

Bird & Bird. (2025a). Proposed EU AI Liability Rules Withdrawn.

Bird & Bird. (2025b). New AI Content Labelling Rules in China: What are they and how do they compare to the EU AI Act.

Bird & Bird. (2026a). China’s New Regulations on AI Anthropomorphic Interactive Services.

Bird & Bird. (2026b). Singapore Introduces New Model AI Governance Framework for Agentic AI.

Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Britannica. (2024). Singapore. Encyclopaedia Britannica.

CAC, Cyberspace Administration of China. (2022). Administrative Provisions on Recommendation Algorithms· Deep Synthesis Provisions.

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

CAC, Cyberspace Administration of China. (2025). Measures for Labeling AI-Generated Synthetic Content.

CAC, NDRC & MIIT, Cyberspace Administration of China, National Development and Reform Commission & Ministry of Industry and Information Technology. (2026).

Implementation Opinions on the Standardized Application and Innovative Development of Intelligent Agents.

Calo, R. (2017). Artificial Intelligence Policy: A Primer and Roadmap. University of California Davis Law Review.

Cath, C. (2018). Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges. Philosophical Transactions of the Royal Society A.

Chambers and Partners. (2026). Artificial Intelligence 2026: Singapore, Trends and Developments. Chambers Global Practice Guides.

Clark, T. (2026). Data Minimisation versus Model Accuracy under the EU AI Act.

Cooley. (2026). New York's Frontier AI Law Gets a California Makeover, With Some Key Differences.

Crawford, K. (2021). Atlas of AI. Yale University Press.

Das & Kwek. (2024). AI and data-driven urbanism: The Singapore experience.

Data Protection Report. (2020). Singapore's Second Edition Model AI Governance Framework.

Data Protection Report. (2024). MAIGF for Generative AI and the PDPC Advisory Guidelines.

Delvaux, M. (2017). Report with Recommendations to the Commission on Civil Law Rules on Robotics. European Parliament.

Ding, J. (2018). Deciphering China's AI Dream. Oxford Internet Institute, Future of Humanity Institute.

Doshi-Velez, F., & Kim, B. (2017). Towards a Rigorous Science of Interpretable Machine Learning. arXiv preprint.

Duane Morris & Selvam. (2026). Singapore's AI Governance Landscape.

Eckert Seamans. (2026). Colorado Repeals and Replaces Its Landmark AI Statute: What Businesses Need to Know.

Engler & Doyle. (2024). AI Verify Foundation and Open-Source Governance Tools.

European Commission. (2020). White Paper on Artificial Intelligence: A European approach to excellence and trust.

European Commission. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

European Commission. (2025). Regulation (EU) 2024/2853 on liability for defective products.

European Commission. (2026a). Draft Commission guidelines on the classification of high-risk AI systems (19 May 2026).

European Commission. (2026b). Commission publishes Code of Practice on marking and labelling AI-generated content, IP/26/1328 (10 June 2026).

European Journal of Risk Regulation. (2025). Technical Standards and the AI Act Implementation Timeline.

European Union. (2026). Regulation (EU) 2026/1744 (Digital Omnibus on AI) amending Regulation (EU) 2024/1689. Official Journal of the European Union, 24 July 2026.

Federal Register. (2025). Executive Order 14179, Removing Barriers to American Leadership in Artificial Intelligence.

Floridi, L., et al. (2018). AI4People: An Ethical Framework for a Good AI Society. Minds and Machines.

Food and Drug Administration. (2021). Artificial Intelligence and Machine Learning in Medical Devices.

Future of Privacy Forum. (2025). Regulatory Sandboxes under the EU AI Act and Comparative Practice.

Future of Privacy Forum. (2026). Incentives or Obligations? The U.S. Regulatory Approach to Voluntary AI Governance Standards.

General Data Protection Regulation, Regulation (EU) 2016/679.

GovTech Singapore. (2024). Smart Nation 2.0: Initiatives in Singapore. Government Technology Agency of Singapore.

Gutierez, C., et al. (2026). SME Compliance Burden under the EU AI Act.

Hacker, P., et al. (2025). Simplifying the AI Act: Omnibus Proposals and Fundamental Rights.

Haynes Boone. (2026). Strictest Amendment to China's Cybersecurity Law In Effect.

High-Level Expert Group on Artificial Intelligence. (2019). Ethics Guidelines for Trustworthy AI. European Commission.

Holland & Knight. (2023). The FTC Is Regulating AI: A Comprehensive Analysis.

IAPP, International Association of Privacy Professionals. (2025). Global AI Governance Law and Policy: China.

IEREK. (2025). Singapore Smart City Transformation: From Old to Bold.

IMDA/PDPC. (2019). National AI Strategy. Info communications Media Development Authority of Singapore.

IMDA/PDPC. (2022). AI Verify Minimum Viable Product Pilot.

Jenner & Block. (2026). DOJ Joins xAI in Lawsuit Challenging Colorado AI Act.

Keith, B. E. (2024). China's Approach to Multilateral AI Governance.

Kuner, C., Bygrave, L., & Docksey, C. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

Lee Kuan Yew. (2000). From Third World to First: The Singapore Story 1965 to 2000. HarperCollins.

Lexology. (2024). Singapore's Implementation and Self-Assessment Guide for Organisations.

Luna, D., et al. (2024). Governance Gaps in Generative AI Frameworks: A Six Jurisdiction Comparison.

MAS. (2018). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of AI and Data Analytics.

MAS. (2023). Veritas Initiative: Toolkit 2.0.

MAS. (2025a). Consultation Paper on Guidelines on AI Risk Management.

MAS. (2025b). Guidelines on Fit and Proper Criteria, FSG-G01, revised on 30 May 2025.

MAS. (2026). Guidelines on Artificial Intelligence Risk Management for Financial Institutions (7 October 2026).

Maslej, N., et al. (2025). The AI Index 2025 Annual Report. Stanford University Human-Centered Artificial Intelligence.

Mazzini, G. & Simonelli, F. (2024). China's Interim Measures on generative AI: Origin, content and significance. Computer Law & Security Review, 53.

MDDI. (2026). Singapore Invests Over S$1 billion in National AI Research and Development Plan.

MIIT, Ministry of Industry and Information Technology of China, et al. (2026). Measures for Artificial Intelligence Science and Technology Ethics Review and Services (Trial).

Ministry of Law Singapore. (2026). The Online Safety Commission Begins Operations on 29 June 2026.

Minshawi, S. A. (2025). Singapore's Transformation from Developing Nation to Global Economic Success. Medium.

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

Nobile, C. G. (2023). Regulating smart robots and artificial intelligence in the European Union. Journal of Digital Technologies and Law, 1(1), 33 to 61.

OECD.AI. (2024). Global Partnership on Artificial Intelligence.

O'Neil, C. (2016). Weapons of Math Destruction. Crown Publishers.

Orrick. (2026). EU AI Act Update: Digital Omnibus Finalizes 8 Compliance Changes.

PDPA. (2022). Personal Data Protection Act, Amendment.

PDPC. (2026). Advisory Guidelines on Use of Personal Data in Generative AI (20 July 2026).

PDPC/IMDA. (2020). Model AI Governance Framework, Second Edition.

Regulation (EU) 2023/1230 on machinery.

Roberts, H., et al. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI & Society, 36(1), 59 to 77.

Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

Saif, I., et al. (2025). Interoperability in AI Safety Governance: Ethics, Regulations, and Standards.

Segate, R. V., & Daly, A. (2024). Encoding the enforcement of safety standards into smart robots to harness their computing sophistication and collaborative potential: A legal risk assessment for European Union policymakers. European Journal of Risk Regulation, 15(3), 665 to 704.

Seyfarth Shaw. (2025). Trump Administration Releases AI Action Plan and Three Executive Orders on AI.

SG101. (2024). 1959 to 1965: Early Economic Strategies. Singapore Government.

Sheehan, M. (2023). China's AI Regulations and How They Get Made. Carnegie Endowment for International Peace.

Siciliano, B., & Khatib, O. (Eds.). (2016). Springer Handbook of Robotics. Springer.

State Council of China. (2017). New Generation Artificial Intelligence Development Plan.

State Council of China. (2025). Opinions on Deeply Implementing the AI Plus Action.

Sunstein, C. R. (2005). Laws of Fear: Beyond the Precautionary Principle. Cambridge University Press.

U.S. Department of Justice. (2026). Justice Department Intervenes in xAI Lawsuit Challenging Colorado's 'Algorithmic Discrimination' Law (24 April 2026).

White House. (2019). Executive Order on Maintaining American Leadership in Artificial Intelligence.

White House. (2025). Ensuring a National Policy Framework for Artificial Intelligence.

White House. (2026). National Policy Framework for Artificial Intelligence: Legislative Recommendations (20 March 2026).

White House Office of Science and Technology Policy. (2022). Blueprint for an AI Bill of Rights.

Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.