Beijing Law Review, 2025, 16(1), 501-540
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Contrasting Approaches to AI Regulation

—A Comparative Analysis of the EU AI Act and China's Cyberspace Administration Decrees

Roberto Vasconcelos Novaes, Bruno Wanderley Júnior

Faculdade de Direito, Universidade Federal de Minas Gerais, Belo Horizonte, Minas Gerais, Brazil
Email: rnovaes@ufmg.br, brunowanderley@ufmg.br

How to cite this paper: Novaes, R. V., & Wanderley Jr., B. (2025). Contrasting Approaches to AI Regulation. *Beijing Law Review, 16,* 501-540.
https://doi.org/10.4236/blr.2025.161025

Received: February 20, 2025
Accepted: March 24, 2025
Published: March 27, 2025

Abstract

The regulation of artificial intelligence (AI) presents a fundamental challenge: how can legal frameworks govern a technology whose definition remains fluid and historically contingent? This paper begins by examining the conceptual ambiguity surrounding AI, arguing that the term does not denote a singular, clearly defined entity but rather an evolving collection of techniques, with machine learning and deep learning currently at the forefront. Recognizing this conceptual uncertainty is essential for understanding the divergent regulatory approaches adopted by the European Union and China. The EU AI Act embraces a comprehensive and definition-based framework, characteristic of the continental European tradition of legal codification. By establishing a broad legal definition of AI, it seeks to create a unified regulatory structure applicable across a wide range of applications. In contrast, the Cyberspace Administration of China (CAC) has adopted a more incremental and adaptive approach, regulating AI through a series of targeted decrees. This model aligns with China's paradigm of experimental governance, which prioritizes flexibility, localized pilot programs, and iterative regulatory development. Through a comparative analysis of these regulatory paradigms, this paper highlights the trade-offs between legal certainty and adaptability in AI governance. While the EU aims for harmonization and predictability, China's approach emphasizes responsiveness to technological advancements. This study contributes to the broader discourse on AI regulation by demonstrating how distinct legal traditions shape the governance of emerging technologies, offering insights into the challenges and implications of regulating AI in an evolving global landscape.

Keywords

Artificial Intelligence, EU AI Act, Cyberspace Administration of China, AI Regulation, Experimental Governance

1. Introduction

The label "artificial intelligence" (AI) does not have a singular or unequivocal meaning. It is not a term technically or scientifically defined based on a solid system of concepts, but rather a loosely applied expression that has been used over the years to designate various techniques, mathematical models, algorithms, and computational systems. The wording is also anthropomorphically misleading, as it suggests that computers could emulate or behave similarly to human beings (Novaes & Ferraz, 2025). Notably, Alan Turing avoided providing definitions when discussing computers and intelligence. Ironically, he asserted that the terminology is so vague that a Gallup survey would be required to clarify the understanding of the words "intelligence" and "thinking", an absurd procedure. Instead, he proposed a simulation, the well-known, although today somewhat obsolete, "imitation game", also known as "Turing test" (Turing, 1950).

We must point out from the beginning of our argument that some extremely broad or ambiguous concepts do not aid in the task of comprehending AI regulation. For instance, the Electropedia (*IEV Online*), curated by the International Electrotechnical Commission, defines AI as a discipline "devoted to developing data processing systems" (IEV ref. 171-09-16) or as a capability of a functional unit (IEV ref. 171-09-17), whether hardware or software, "that performs functions normally associated with human intelligence, such as reasoning and learning" (International Electrotechnical Commission, n.d.). This definition defers addressing the core issue. While it provides some clarification by distinguishing between *discipline* and *capability* and by circumscribing AI to data processing systems, it remains tautological when considering the essence of the concept—intelligence, reasoning, and learning.

Definitions, such as the one presented by the International Organization for Standardization, which outlines AI as "research and development of mechanisms and applications of AI systems", and AI systems as "engineered systems that generate outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives", provide a more precise outline for understanding the issue. However, adhering strictly to these definitions may obscure the meaning-related complexity inherent in the development and use of the term. They do not, on their own, clarify their origin. While these definitions may serve as operative tools for various contexts, what is sought in this discussion is, if possible, a comprehensive explanation capable of encompassing the semantic diversity of the term and illuminating the subject of AI regulation.

To debate AI regulations effectively, it's important to understand what the term encompasses. Let us engage in a "Socratic doubt", through a process of rigorous inquiry, much like the dialectical method exemplified in Plato's dialogues. In these works, the character of Socrates probes fundamental questions like, "what is justice?", "what is virtue?", "what is beauty?" or "what is love?" Similarly, we must ask: "what is artificial intelligence?" By drawing in this exploration, we can better grasp the complexities and nuances that underpin the regulation of AI. However, we will refrain from attempting to replicate the Athenians' intricate argumentation model, which frequently concluded in an impasse (*aporia*). Although motivated by Socratic doubt, our perspective is radically different. Our approach will be straightforward and consist of two parts. It will explain the historical origin of the term and the range of technologies currently associated with it. The goal is to demonstrate that there is not a precise concept nor an entity that could be designated by the expression "artificial intelligence" and that we should not naively speak of the term as if its meaning is precise. Even the above definitions of the IEC and ISO are, thus, historically situated. The logical corollary is that many different techniques are contemporarily called such, with special importance given to the fields of machine learning and deep learning nowadays in this ever-evolving field.

Our specific topic, which concerns the regulation of artificial intelligence in comparative law, calls for such a prologue. How can we address such a subject if we do not know what we are talking about or if we take the meaning of the expression for granted?

Upon delineating the historical trajectory of artificial intelligence (AI) and listing, although not exhaustively, many of the current applications referred to as such, this paper will examine two divergent frameworks for state regulation of the subject: the approach articulated in the European Union's AI Act and the model implemented by the Cyberspace Administration of China (CAC) (国家互联网信息办公室, *Guójiā Hùliánwǎng Xìnxī Bàngōngshì,* literally the National Internet Information Office). The EU's regulatory structure adopts a comprehensive and expansive characterization of AI, reflecting the continental European tradition of legal codification. In this approach, a definition of a fact or scenario is formulated, and a corresponding set of legal consequences is applied whenever a specific instance aligns with the expressed hypothesis. In contrast, the Chinese regulatory strategy diverges significantly. Rather than pursuing a broad, codified frame, it employs a legal technique characterized by the incremental development of concise, targeted regulations tailored to the specific technologies in question. This method aligns with the paradigm of experimental governance, emphasizing adaptability and iterative refinement in response to technological evolution. China's use of experimental governance—characterized by iterative, localized, and flexible regulations—contrasts sharply with the EU's preference for comprehensive, principle-based legislation. This comparison highlights the trade-offs between adaptability and legal certainty, providing a nuanced perspective on the challenges of regulating a rapidly evolving technology like AI.

2. Two Standpoints to Define Artificial Intelligence

2.1. A Brief Historical Overview

Historically, the possibility of intelligent human-built devices could be traced to myth, literature, and legend[1]. This retrospective is well beyond the scope of this text. In a sense closer to the modern one, i.e., intelligent digital computers, Alan Turing could be considered one of the pioneers, and the field was active in Britain under the name of *machine intelligence* since the end of WWII (Copeland, 2000). The earliest record we have of the expression *artificial intelligence* itself is the title of a conference held at Dartmouth College in the United States. This name was deliberately proposed in a broad and intentionally vague manner by John McCarthy, "to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it" (Dartmouth University, n.d.). As anyone who has organized academic conferences knows, this strategy is often employed—rather than narrowing the scope of the event, a broad title is chosen to encourage the participation of researchers and scholars from diverse fields, without favoring or excluding any particular line of inquiry or school of thought.

At the time of its proposal, the conference aimed to encompass thinkers concerned with mathematics, logical problems, cybernetics, and automata theory, specifically trying to delineate a distinction from the latter (McCorduck, 2004). Throughout the years, the term gained significant traction, becoming a commonplace reference and a catch-all phrase to describe what is a highly heterogeneous set of technologies.

Nevertheless, the conference marked the "formal" emergence of artificial intelligence as an academic discipline, rooted in the ambition to replicate human reasoning through computational systems. During the 1950s and 1960s, early AI research coalesced into two distinct intellectual camps: one centered on emulating the computational principles underlying the human brain and another one concerned with logical and formal reasoning processes (Samuel, 1962). The first approach has its roots in the initial conceptualization of artificial neurons in logical and mathematical terms. It dates to 1943, credited to neuroscientists Warren McCulloch and Walter Pitts. In their groundbreaking work, they illustrated how interconnected neurons could be used to model logical propositions and carry out

[1]One of the first registered examples can be found on Homer's Iliad, where the blacksmith god Hephaestus creates wheeled tripods thar could automatically serve the banquets of the Gods: "[370] […] Him [Hepahestus] she [Tetis] found sweating with toil as he moved to and fro about his bellows in eager haste; for he was fashioning tripods [τρίποδας (*tripodas*) three-legged cauldrons or stands, often sacred in Greek mythology, used for offerings or rituals], twenty in all, to stand around the wall of his well-builded hall, [375] and golden wheels had he set beneath the base of each that of themselves they might enter the gathering of the gods at his wish [αὐτόματοι (*automatōi*) self-moving or autonomous] and again return to his house, a wonder to behold." (Homer, n.d. *Iliad*, 18, 371-375). A thorough historical account of intelligent machines and robots can be found on Cohen (1967). The reader can also find a similar and more contemporary summary of automata and philosophical inquiries on the subject in MacCorduck's work (2004).

computational tasks. By drawing on mathematical abstractions inspired by biological neurons, the authors introduced anthropomorphic elements into scientific terminology, including ideas like neurons, activation thresholds, and learning processes (McCulloch & Pitts, 1943). Future developments such as Perceptrons (Rosenblatt, 1957; Widrow & Hoff, 1960; Minsky & Papert, 1969) and the first neural networks can be considered the ancestors of contemporary deep learning models[2]. The second trend prioritized logical languages and symbolic reasoning, inspired by mathematical logic and cognitive science. For example, pioneers like Allen Newell and Herbert Simon sought to formalize human thought developing systems such as the *Logic Theorist*, "an information process system that is able to discover, using heuristic methods, proofs of theorems in symbolic logic" (Newell & Simon, 1956). John McCarthy developed *LISP* programming language, designed for "artificial intelligence work on the IBM 704 computer" (Wexelblat, 1978). These efforts were aimed at modeling intelligence through rule-based algorithms and deductive reasoning.

However, the limitations of symbolic approaches soon became apparent: rigid logical frameworks struggled with ambiguity, real-world complexity, and the need for vast contextual knowledge. By the 1970s, enthusiasm waned as early promises of human-level intelligence remained unfulfilled, contributing to the first *AI winter*—a period of reduced funding and skepticism about the field's viability (Russel & Norvig, 2021).

The 1980s saw a resurgence of interest with the rise of *expert systems*, which applied AI to specialized domains by encoding human expertise into rule-based programs. Systems like MYCIN (Buchanan & Shortliffe, 1984), used for medical diagnosis, and XCON (McDermott, 1980), deployed for configuring computer hardware, demonstrated practical value in narrow contexts. These systems relied on knowledge engineering, where domain-specific rules were manually curated into if-then structures (and more complex ones, of course) stored in knowledge bases. While expert systems revitalized commercial investment and temporarily countered critiques of AI's impracticality, they faced scalability challenges. The labor-intensive process of knowledge acquisition, coupled with brittle reasoning methods in the face of uncertainty and the fact that expert systems could not learn from experience, triggered a second AI winter, underscoring the gap between theoretical ambition and real-world application (Russel & Norvig, 2021).

The cyclical narrative of AI, alternating between optimism and disillusionment, reflects broader tensions in defining and achieving machine intelligence. The limitations of logical languages and expert systems highlighted the inadequacy of

[2]"Two undergraduate students at Harvard, Marvin Minsky (1927-2016) and Dean Edmonds, built the first neural network computer in 1950. The SNARC, as it was called, used 3000 vacuum tubes and a surplus automatic pilot mechanism from a B-24 bomber to simulate a network of 40 neurons. Later, at Princeton, Minsky studied universal computation in neural networks. His Ph.D. committee was skeptical about whether this kind of work should be considered mathematics, but von Neumann reportedly said, 'If it isn't now, it will be someday.'" (Russel & Norvig, 2021)

purely symbolic methods, prompting a paradigm shift toward statistical and data-driven approaches in the 1990s-2000s (Crevier, 1993). Meanwhile, the AI winters served as cautionary milestones, reshaping research priorities toward incremental progress and hybrid methodologies.

Contemporary AI, fueled by machine learning and neural networks, owes its success to lessons learned from these historical phases: the necessity of adaptable learning systems, the value of scalable data processing, and the importance of tempering expectations with pragmatic benchmarks. Thus, the trajectory of AI technologies reveals not only technical evolution but also the enduring interplay between ambition, limitation, and societal context.

The availability of powerful hardware, particularly graphics processing units (GPUs), has been a game-changer. Originally developed to enhance real-time 3D graphics for gaming and image processing, GPUs now play a critical role in deep learning by performing massive parallel computations, which are essential for training complex neural networks (Merrit, 2023). At the same time, the explosion of large-scale datasets built upon the availability of internet data has been equally transformative. These vast collections of data allow deep learning models to uncover intricate patterns and representations, making them more effective and versatile.

Together, these advancements have turned deep learning from a theoretical idea into practical technology. Researchers and engineers can now deploy sophisticated algorithms at scale, driving breakthroughs in fields like computer vision and natural language processing. Today, the domain continues to evolve, with datasets and models growing larger while achieving greater accuracy, complexity, and real-world relevance. These trends show no signs of slowing, solidifying deep learning's impact across industries (Goodfellow, Bengio, & Courville, 2016).

2.2. Technical Frameworks and Applications

We have approached the concise history of AI above mainly from a technical development standpoint. If we envisage the subject from another perspective, we find an even richer scope of the developments that fall under the umbrella term.

Nevertheless, we could create an illustrative inventory, simply to fulfill the present purpose of demonstrating the breadth of the expression. The small list in **Table 1** is divided into what we like to call a technical framework—a broad and loose aggregation of computer techniques—with some commercial examples extant at the time of writing[3].

If we create a list according to the application domain, the collection is even

[3]The use of the term "technical framework" in this context is deliberate, as it avoids the potential for misinterpretation associated with terms such as "algorithms", "systems", or "models" which may not accurately capture the breadth and diversity of the technologies being regulated. Instead, "technical frameworks" serves as a more inclusive and flexible categorization, encompassing various related technologies that share similar characteristics and potential risks.

Table 1. Exemplificative inventory of technical frameworks of Artificial Intelligence.

Technical Framework	Applications (exemplificative)
Natural Language Processing (NLP)	**Chatbots and Virtual Assistants**: AI-powered chatbots for customer service and personal assistance. E.g.: Amazon Alexa: https://alexa.amazon.com, Apple Siri: https://www.apple.com/br/siri, Google Assistant: https://assistant.google.com. **Language Translation**: Various translation services. E.g.: Deepl: https://www.deepl.com, Yandex Translate: https://translate.yandex.com, Bing Translator: https://www.bing.com/translator. **Sentiment Analysis**: Analyzing customer feedback, social media, and reviews to gauge public opinion. E.g.: Lexalitics: https://www.lexalytics.com, Chattermill: https://chattermill.com. **Text Summarization**: Automatically generating summaries of long documents or articles E.g.: Coral AI: https://www.getcoralai.com, Quill Bot: https://quillbot.com. **Speech Recognition**: Converting spoken language into text (Cockatoo: https://www.cockatoo.com, Transkriptor: https://transkriptor.com). **Text Generation**: Creating new text samples from command prompts (ChatGPT: https://chatgpt.com, DeepSeek: https://www.deepseek.com).
Computer Vision	**Image and Video Recognition:** Identifying objects, faces, and scenes in images and videos. E.g.: Google Lens: https://lens.google, Amazon Rekognition: https://aws.amazon.com/pt/rekognition, Gryfo: https://gryfo.com.br. **Medical Imaging:** Assisting in diagnosing diseases from X-rays, Microscope Images, MRIs, and CT scans. E.g.: AIforia: https://www.aiforia.com, CT Read: https://ctread.com. **Autonomous Vehicles:** Enabling self-driving cars to perceive and navigate their environment E.g.: Westwell Qomolo: https://en.westwell-lab.com/qomolo.html, Imagination: https://www.imaginationtech.com/products/automotive. **Augmented Reality (AR):** Enhancing real-world environments with digital overlays. E.g.: Banuba: https://www.banuba.com, Snap Ar: https://ar.snap.com. **Quality Control:** Inspecting products in manufacturing for defects. E.g.: Siemens Inspekto: https://www.siemens.com/global/en/products/automation/topic-areas/artificial-intelligence-in-industry/ai-on-shopfloor/ai-based-machine-vision/inspekto.html
Machine Learning and Predictive Analytics	**Fraud Detection:** Identifying fraudulent transactions in banking and finance. E.g.: Feedzai: https://www.feedzai.com, Fraud.net: https://fraud.net. **Predictive Maintenance:** Forecasting equipment failures in industrial settings. E.g.: Uptake: https://www.uptake.com, Siemens MindSphere: https://siemens.com/mindsphere. **Recommendation Systems:** Personalizing content and product recommendations. E.g.: Netflix: https://www.netflix.com, Amazon: https://www.amazon.com.br. **Risk Assessment:** Evaluating credit risk, insurance claims, and investment opportunities. E.g.: Darktrace: https://darktrace.com, Quantexa: https://www.quantexa.com. **Demand Forecasting**: Predicting future demand for products and services. E.g.: Blue Yonder: https://www.blueyonder.com, ToolsGroup: https://www.toolsgroup.com.

more diversified[4]. A comprehensive catalog is thus impossible to make, especially

[4]We could keep account for products that are identified or claim to be using artificial intelligence in domains such as *Robotics*: Industrial Automation: Robots performing repetitive tasks in manufacturing and assembly lines. Service Robots: Robots used in healthcare, hospitality, and domestic settings (e.g., robotic surgery, cleaning robots). Autonomous Drones: Drones used for delivery, surveillance, and agriculture. *Healthcare*: Diagnosis and Treatment: AI systems assisting doctors in diagnosing diseases and recommending treatments. Drug Discovery: Accelerating the process of discovering new drugs and therapies. Personalized Medicine: Tailoring medical treatments to individual patients based on their genetic makeup. Health Monitoring: Wearable devices that monitor vital signs and alert users to potential health issues. *Finance*: Algorithmic Trading: Using AI to execute trades at high speeds and volumes based on market conditions. Credit Scoring: Assessing the creditworthiness of individuals and businesses. Portfolio Management: AI-driven investment strategies and portfolio optimization. Regulatory Compliance: Automating compliance processes and detecting anomalies. *Cybersecurity*: Threat Detection: Identifying and mitigating cyber threats in real-time. Anomaly Detection: Detecting unusual patterns in network traffic that may indicate a security breach. Phishing Detection: Identifying and blocking phishing attempts. Automated Response: Automating responses to security incidents to minimize damage. *Retail and E-commerce*: Inventory Management: Optimizing stock levels and supply chain operations. Customer Insights: Analyzing customer behavior to improve marketing strategies. Visual Search: Allowing customers to search for products using images. Dynamic Pricing: Adjusting prices in real-time based on demand, competition, and other factors. *Transportation and Logistics*: Route Optimization: Finding the most efficient routes for delivery and transportation. Fleet Management: Monitoring and managing fleets of vehicles. Traffic Management: Using AI to optimize traffic flow and reduce congestion. Autonomous Delivery: Drones and robots for last-mile delivery. *Education*: Personalized Learning: Adapting educational content to the needs of individual students. Automated Grading: Grading assignments and exams automatically. Intelligent Tutoring Systems: Providing personalized tutoring and feedback to students. Administrative Automation: Automating administrative tasks such as scheduling and record-keeping. *Entertainment and Media*: Content Creation: Generating music, art, and written content using AI. Video Game AI: Creating intelligent NPCs (non-player characters) and adaptive game environments. Content Recommendation: Suggesting movies, shows, and music based on user preferences. Deepfake Technology: Creating realistic but fake audio and video content. *Agriculture*: Precision Farming: Using AI to optimize planting, watering, and harvesting. Crop Monitoring: Analyzing satellite and drone imagery to monitor crop health. Pest Control: Identifying and targeting pests with precision. Yield Prediction: Predicting crop yields based on environmental and historical data. *Energy and Utilities*: Smart Grids: Optimizing the distribution and consumption of electricity. Energy Forecasting: Predicting energy demand and supply. Fault Detection: Identifying faults in power lines and equipment. Renewable Energy Optimization: Maximizing the efficiency of solar and wind energy systems. *Legal and Compliance*: Document Review: Automating the review of legal documents and contracts. Legal Research: Assisting lawyers in finding relevant legal rules, case law and precedents. Compliance Monitoring: Ensuring that organizations adhere to regulatory requirements. Predictive Analytics: Forecasting legal outcomes based on historical data. *Human Resources*: Recruitment: Automating the screening and shortlisting of job candidates. Employee Engagement: Analyzing employee feedback and sentiment. Performance Management: Providing insights into employee performance and productivity. Workforce Planning: Predicting future workforce needs and skill gaps. *Environmental Monitoring*: Climate Modeling: Predicting climate change and its impacts. Wildlife Conservation: Monitoring endangered species and their habitats. Pollution Detection: Identifying sources of pollution and monitoring air and water quality. Disaster Prediction: Forecasting natural disasters such as earthquakes, floods, and hurricanes. *Gaming*: Procedural Content Generation: Creating game levels, maps, and environments automatically. Player Behavior Analysis: Understanding and predicting player behavior to improve game design. AI Opponents: Creating challenging and adaptive AI opponents in games. Realistic Simulations: Enhancing the realism of game physics and environments. *Telecommunications*: Network Optimization: Improving the performance and efficiency of telecommunications networks. Customer Support: Automating customer service through AI-powered chatbots. Predictive Maintenance: Identifying potential issues in network infrastructure before they occur. Traffic Analysis: Monitoring and managing network traffic to prevent congestion. *Real Estate Property Valuation*: Estimating the value of properties using AI algorithms. Market Analysis: Analyzing real estate market trends and predicting future prices. Virtual Tours: Creating virtual reality tours of properties. Customer Insights: Understanding buyer preferences and behavior.

if we consider that the field is rapidly expanding, and it is not an exaggeration to state that we are continuously being presented with novel developments.

Finally, a critical factor in discussing AI meaning today is the significant growth of machine learning technologies over the past few years, as evidenced, for instance, by research paper data[5]. Additionally, we should note the exponential growth in computing power, data availability, hardware performance, and the efficiency gains achieved through algorithmic innovations. Some even suggest that the availability of human-generated text for training models may become a limiting factor by the late 2020s (Epoch AI, 2023).

By crossing the two semantic digressions—the historical technical recapitulation and the technical framework/applications standpoint—it cannot be asserted that a clear, well-defined, and circumscribed concept fully corresponds to the term "artificial intelligence". No one is the owner of any word, not even the established institutions we have mentioned in the beginning of the text.

So far, we have dealt with the expansion of the meaning of artificial intelligence. On many occasions, the broadness of the expression is reduced. McCorduck introduces a noteworthy concept, designated the "Strange Paradox", which posits that the perception of intelligence is inversely correlated with familiarity (McCorduck, 2004). Specifically, as a given technology transitions from a state of novelty and relative incomprehensibility to one of widespread adoption and integration into daily routines, its perceived "intelligence" diminishes. This paradox implies that the attribution of intelligence is often contingent upon a sense of mystery or a lack of complete understanding. Once the underlying principles and operational mechanisms of a technology become commonplace, it is no longer perceived as possessing the same degree of cognitive complexity, thereby losing its association with intelligence.

A contemporary illustration of this paradox can be observed in the current fascination with generative AI technologies, such as those capable of generating text, images, and video content. However, as these technologies become increasingly pervasive and integrated into everyday applications, the initial awe and perception of intelligence may subside, potentially leading to a normalization of their capabilities[6].

Rather, artificial intelligence ought to be conceptualized as an abstract hypernym,

[5]"Machine learning publications have seen the most rapid growth over the past decade, increasing nearly sevenfold since 2015. Following machine learning, the most published AI fields in 2022 were computer vision (21,309 publications), pattern recognition (19,841), and process management (12,052)." (Stanford University, 2024)

[6]McCorduck (*op. cit.*) effectively illustrates this point with the historical trajectory of computer chess. In the nascent stages of AI research, the prospect of a machine capable of playing chess at a competitive level was considered a formidable challenge, often framed as a uniquely human cognitive endeavor and, consequently, a hallmark of intelligence. Today, however, the ability of computers to play chess at a grandmaster level is no longer perceived as remarkable or indicative of intelligence, having become a routine computational task. It is crucial to recall the watershed moment when Garry Kasparov's defeat by the Deep Blue computer marked a pivotal point in the evolution of computer science, demonstrating the potential of AI to surpass human capabilities in specific cognitive domains. This landmark event, once a source of intense debate and speculation, is now largely relegated to historical accounts.

gaining content only when enriched by its historical trajectory and diverse contemporary applications. It is a dynamic construct, perpetually evolving—shedding certain meanings over time while assimilating emerging technologies, novel applications, and evolving commercial and academic practices.

3. Two Contrasting Regulatory Approaches

The rapid development of machine learning technologies has garnered widespread attention due to its considerable economic, social, geopolitical, and ethical motivations and implications. Consequently, legislators from various political entities have been prompted to address this issue with increasing urgency.

We will examine two quite different legal paradigms that are being established: the all-encompassing EU AI Act and the experimental approach adopted by the People's Republic of China. The reader should keep in mind the background we have delineated so far—namely, how to regulate such a complex and varied landscape of a subject that lacks a single, simple definition but contains a broad variety of elements discussed above.

3.1. The All-Encompassing EU AI Act

The analysis of the full text of the EU AI Act (Regulation (EU) 2024/1689) falls outside the scope of this work. As previously outlined, the objective is to compare two distinct regulatory paradigms, specifically examining how each model defines and governs the factual domain of reality subject to its legal influence and consequences.

The European Union has established a comprehensive definition of artificial intelligence. Whether this model will exert a significant influence on global regulatory discourse and legislative initiatives—given its status as one of the first comprehensive AI regulatory frameworks—remains to be seen[7].

The definition has departed and is currently aligned with the revised definition agreed upon by the OECD (European Parliamentary Research Service, 2024). It is useful to read them side by side, as shown in **Table 2**, to demonstrate that the EU definition practically transcribes word for word the OECD concept.

Table 2. OECD and EU AI Act definition of artificial intelligence.

OECD Revised Definition[a]	EU AI Act[b]
An AI system is a machine-based system that 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.	Article 3 (1) 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, 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.

a. Russel, Perset & Grobelnik, 2023. b. European Union, 2024.

[7]This phenomenon of regulatory diffusion, wherein European regulations influence global standards, has been termed the "Brussels Effect" (Bradford, 2020). A notable precedent for this effect is the influence of the European Union's General Data Protection Regulation (GDPR) worldwide.

From the texts above, we should highlight some crucial topics. We will mainly use the more detailed explanation contained in the OECD web document and in Recital 12[8] of the EU AI Act to clarify the concepts as needed[9]. Nevertheless, as is usual in legal text hermeneutics, the explanations below are tentative, and the full content of meaning will be progressively established in the following years through the conjunct effort of legal scholars, regulators and jurisdictions across the EU[10].

First, the Act states that an AI system is fundamentally a *machine-based* system.

[8]Recital 12: "The notion of 'AI system' in this Regulation should be clearly defined and should be closely aligned with the work of international organisations working on AI to ensure legal certainty, facilitate international convergence and wide acceptance, while providing the flexibility to accommodate the rapid technological developments in this field. Moreover, the definition should be based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations. A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling. The term 'machine-based' refers to the fact that AI systems run on machines. The reference to explicit or implicit objectives underscores that AI systems can operate according to explicit defined objectives or to implicit objectives. The objectives of the AI system may be different from the intended purpose of the AI system in a specific context. For the purposes of this Regulation, environments should be understood to be the contexts in which the AI systems operate, whereas outputs generated by the AI system reflect different functions performed by AI systems and include predictions, content, recommendations or decisions. AI systems are designed to operate with varying levels of autonomy, meaning that they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention. The adaptiveness that an AI system could exhibit after deployment, refers to self-learning capabilities, allowing the system to change while in use. AI systems can be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serves the functionality of the product without being integrated therein (non-embedded)." (European Union, 2024)

[9]European legislative practice frequently employs these detailed preambles to articulate the rationale, objectives, and underlying principles of the legislation. In the context of the EU AI Act, these recitals play a crucial role in interpreting the legal text itself. The Recital 12, dedicated to defining AI provides a broader conceptual framework and contextual background for the definition. A key distinction lies in the level of detail provided: Recital 12 offers a more comprehensive and nuanced explanation of the concept of AI than the concise legal definition presented in Article 3. This practice allows for a more flexible and contextualized interpretation of the law, considering the broader objectives and considerations that motivated its enactment. "In EU law the recitals can provide additional interpretative context in case of ambiguity in the operative provisions, but are not binding as such." (Fernández-Llorca, Gómez, Sánchez, & Mazzini, 2024). The mentioned authors opted in the referenced work not to analyze the recitals or OECD documentation, nevertheless recognizing the interpretative value of the recitals and other sources.

[10]The AI Act prescribes in Article 96(f) that guidelines further elaborating on the definition provided in Article 3 should be developed. At the time of our writing, this document had not yet been made public. Nevertheless, our objective here is not to engage in a thorough discussion of the European definition and the criticism already found on literature, but rather to compare the different strategies adopted by the European Union and the Chinese government. The clarifications that the future guidelines will provide will not diminish the distinction between the legislative models but will probably amplify the contrast of our comparison.

Recital 12 does not provide much clarification on this point and simply states tautologically that "The term 'machine-based' refers to the fact that AI systems run on machines" (European Union, 2024). However, considering the context, "machine" refers to computational infrastructure such as computers, servers, or specialized hardware like GPUs and TPUs. These systems rely on software algorithms and data to function, enabling them to perform tasks that traditionally require human intelligence.

Second, AI systems have the ability to operate with *varying levels of autonomy*. From Recital 12, we read that "they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention" (European Union, 2024). This means they can function with different degrees of human involvement, ranging from systems that require significant oversight—such as recommendation engines that suggest products but leave the final decision to humans—to highly autonomous systems like self-driving cars or drones that operate with minimal human intervention.

Third, AI systems exhibit *adaptiveness* after deployment. We can find in Recital 12 that it "refers to self-learning capabilities, allowing the system to change while in use" (European Union, 2024). Unlike traditional software, which operates based on fixed rules, AI systems can improve or adjust their behavior over time. This adaptiveness can manifest in several ways, such as through online learning, where the system continuously updates itself with new data, or through reinforcement learning, where it learns from feedback or rewards. For example, a chatbot might refine its responses based on user interactions, becoming more accurate and context-aware over time. The OECD document also exemplifies this characterization, stating that "for example, recommender systems that adapt to individual preferences or voice recognition systems that adapt to user's voice" (Russel, Perset, & Grobelnik, 2023).

Fourth, the European definition asserts that AI systems are designed to achieve *explicit or implicit objectives*. Explicit objectives are those clearly defined by developers, such as maximizing accuracy in predictions or optimizing resource allocation. Implicit objectives, on the other hand, are learned from data or inferred during operation. For instance, an AI system analyzing customer behavior might identify patterns and preferences that were not explicitly programmed, allowing it to make more nuanced recommendations. We might also add clarifications from OECD experts, who state that implicit objectives

> "include self-driving systems that are programmed to comply with traffic rules (but do not 'know' their implicit objective of protecting lives), or a large language model like ChatGPT where the objectives of the system are not explicitly programmed but acquired in part through the process of imitation learning from human-generated text and partly from the process of reinforcement learning from human feedback (RLHF)" (Russel, Perset, & Grobelnik, 2023).

Fifth, at the core of an AI system's European definition is its ability to *infer* outputs from inputs. This means the system processes input data—whether text, images, sensor readings, or other forms of information—and uses it to generate outputs such as predictions, content, recommendations, or decisions. For example, an AI system might analyze medical images to predict the likelihood of a disease, generate written content based on a user's prompt, recommend products based on past purchases, or make decisions like approving a loan application. The inclusion of content as a form of inference is a significant departure from many prior definitions discussed by the European Commission, the European Council, and the European Parliament (Fernández-Llorca, Gómez, Sánchez, & Mazzini, 2024). The explicit mention of "content" clearly alludes to the rise of generative AI models, which can produce novel text, images, audio, and other forms of media.

The term "infer", originating from the field of logic, denotes the process of deriving conclusions from premises (Ferrater Mora, 2001). While this concept has a long history in various logical traditions, including Aristotelian logic, symbolic logic, and formal logic, its application to AI systems in the European regulation is more specific. The regulation effectively operationalizes "inference" within the context of AI by defining it as the generation of outputs categorized as decisions, recommendations, predictions, and content. This operationalization is crucial for establishing the scope of the regulation and determining which systems fall under its purview. The inclusion of "content" expands this scope considerably, encompassing a broad range of AI applications that were not explicitly addressed in earlier definitions. This expansion reflects the growing recognition of the transformative potential and associated risks of generative AI.

Finally, AI systems have the capacity to *influence physical or virtual environments*. In physical environments, this might involve controlling machinery, driving vehicles, or managing energy grids. In virtual environments, AI systems can alter digital spaces, such as curating social media feeds, optimizing online marketplaces, or powering virtual assistants. This dual capability underscores the transformative potential of AI, as it can impact both the tangible world around us and the digital ecosystems we interact with daily.

The European model's impetus stems from a set of key exigencies. For the purposes of this text, we should deal with two of them.

First, there is the need for alignment with established international standards and internal harmonization. This commitment to international harmonization is explicitly articulated within the AI Act itself (see, for example, Recitals 1, 7, 8, and 9) and is reflected in broader European standardization efforts, as outlined in Article 114 ("Approximation of Laws") of the Treaty on the Functioning of the European Union (European Union, 2016). The pursuit of international compatibility serves several key objectives. First, it facilitates interoperability and reduces trade barriers between jurisdictions. Second, it aims to promote a consistent understanding of AI and its associated risks, fostering international collaboration on research, development, and ethical considerations. Finally, adherence to international standards enhances the legitimacy and global acceptance of the European regulatory framework[11].

A second key objective within the European model is the establishment of a clear demarcation between traditional software systems and those employing artificial intelligence. This distinction is crucial for effective regulation. The European approach elucidates this difference by defining traditional systems as those whose functionalities are entirely determined by human programming. This definition refers, in technical terms, to conventional software development methodologies, wherein all program logic, governing the relationship between input and output data, is explicitly defined *a priori* by human programmers. In such traditional programming paradigms—exemplified by management information systems, conventional e-commerce platforms, invoicing systems, or airline reservation systems—all operational rules are meticulously stipulated during the software requirements specification phase and subsequently translated into executable code by human developers. This contrasts sharply with AI systems, where algorithms can learn and adapt their behavior based on data, often without explicit pre-programming of every possible scenario.

To illustrate this distinction, consider the example of an autonomous vehicle navigating an urban environment. A traditional software system designed for navigation would rely on explicitly coded rules for identifying pedestrians, vehicles, and other obstacles. We could also envisage a scenario where the complete trajectory, speed, and functioning of the vehicle would be defined beforehand. The number of rules would be astronomical, evidently, if not impossible. However, an AI-driven system, particularly one employing machine learning techniques, learns to identify these objects from vast amounts of training data, or to modify its trajectory dynamically in real-time. Consequently, if the AI system encounters a novel or unusual scenario—for instance, a person pushing a popcorn cart holding an umbrella in a dark street against a blue light background, an event not adequately represented in its training data—it may fail to correctly classify this as a pedestrian. In such a case, the autonomous vehicle might not respond appropriately, potentially leading to an undesirable outcome. This example highlights a crucial difference: the output of an AI system is not entirely predetermined by human programmers but is contingent on the characteristics and comprehensiveness of the training data. The system's behavior emerges from its learned patterns

[11]"The AI Act is part of the 'New Legislative Framework' introduced in the EU in 2008. Thus, the AI Act is a product safety law. The New Legislative Framework is the EU's approach to harmonising product safety rules. Building on Regulation No. 765/2008/EC (on the accreditation of conformity assessment bodies) and Decision No. 768/2008/EC (on a common framework for the marketing of products), the EU has harmonised the structure of numerous regulations and directives of product safety. The underlying concept of the New Legislative Framework is a uniform approach to risk for the health and safety of natural persons. Thus, different safety aspects of the same product by various specific laws can be harmonised. As a key characteristic, the EU legal acts define requirements for market access and stipulate measures to ensure compliance with these requirements." (Voigt & Hullen, 2024).

and generalizations, rather than solely from explicit instructions. This dependence on training data and the emergent nature of AI behavior constitute a significant differentiating factor between AI systems and traditional software, where the output is entirely predictable based on the pre-programmed logic. This distinction is paramount for regulatory purposes, as it necessitates distinct approaches to validation, verification, and risk assessment.

The EU AI Act establishes a transitional period between its publication and the full enforcement of all its provisions on 2 August 2026[12]. Given its recent publication and the ongoing adaptation interval, it is premature to assess its effectiveness. What we can attest so far is that the EU has been actively organizing the regulatory infrastructure and promoting awareness of the provision of the new legislation.

For example, we can mention one of the activities of the European AI Office[13], that "plays a key role in implementing the AI Act […] fostering the development and use of trustworthy AI, and international cooperation" (European Commission, 2025a). To support these objectives, the Office oversees the AI Pact, a project specifically designed "to help stakeholders prepare for the implementation of the AI Act" (European Commission, 2025b).

The AI Pact is structured around two key pillars: first, knowledge-sharing among stakeholders, which involves organizing webinars and collaborative platforms to disseminate best practices and facilitate dialogue. Second, encouraging voluntary compliance pledges, where companies are stimulated to proactively adopt measures to align with the AI Act, such as implementing governance strategies, identifying high-risk AI systems, and promoting AI literacy (European Commission, 2025b)[14]. As of the latest update, the initiative has gained significant traction, with 190 companies from diverse sectors already participating in it (European Commission, 2025b). This could reflect the growing commitment of industry participants to comply with the Act's requirements. Furthermore, the European AI Office has compiled a substantial inventory of AI literacy initiatives, underscoring ongoing efforts to enhance awareness and understanding of AI-related issues (European Artificial Intelligence Office, 2024).

While the Act's comprehensive effectiveness remains contingent upon the completion of its transitional period, the EU has demonstrated a commitment to fostering a well-coordinated regulatory bureaucratic infrastructure. Through the establishment of dedicated governance bodies, advisory mechanisms, and stakeholder engagement initiatives like the AI Pact, the EU is laying the groundwork

[12]Article 113 states that the AI literacy obligations (Article 4) and prohibited AI practices (Article 5) entered into application on 2 February 2025. The governance rules and obligations for general-purpose AI models (Chapter III, Section 4—Notifying Authorities and Notified Bodies; Chapter V—General-Purpose AI Models; Chapter VII—Governance; Chapter XII—Penalties; and Article 78—Confidentiality) will become applicable on 2 August 2025. Additionally, the rules for high-risk AI systems (Article 6(1)) have an extended transition period until 2 August 2027.

[13]The European AI Office is established under Article 65 of the AI Act and is formalized by a European Commission (2024).

[14]The events organized so far under the AI Pact objectives can be found at https://digital-strategy.ec.europa.eu/en/policies/ai-pact-events.

for the enforcement of the new legislation.

3.2. China and Europe: The Crossroads So Far

Europe and China have had commercial relations since ancient times. The Western empires never encountered the Chinese Empire directly, but they were connected through the trade in spices and especially silk, one of the most valuable commodities for Western markets. Its importance was so great that the route used to transport these goods became known in history as the "Silk Road". For centuries, merchants traveled by land and sea, keeping the trade routes alive until the capture of Constantinople by the Ottomans in the 15th century, when the Silk Road was interrupted. As a result, the Europeans began a process of maritime expansion, aiming to open new trade routes with the East. The great Portuguese navigators, followed by the Spanish, English, French, and Dutch, conquered the seas and implemented a mercantile system that would define European hegemony throughout the world, solidifying the colonialist and imperialist model that would last until the 20th century.

China, once the world's largest empire and economy, was subjugated by European economic and military power and forced to surrender its most valuable products under Western rule. The Chinese Empire was dismantled and subjected to abuses by European powers and the United States, which emerged as an economic and military power in the 20th century. However, after a series of revolts, civil wars, and revolutions, China regained its independence and began a slow but steady journey of economic recovery, especially after adopting the reform program called "Four Modernizations" in 1978, under the leadership of Deng Xiaoping, becoming once again a world power in the late 20th and early 21st centuries.

In this context, China established new partnerships with both Eastern and Western nations, being one of the founding countries of BRICS in 2006, under the presidency of Hu Jintao. BRICS is a cooperation agreement established between Brazil, Russia, India, China, and later South Africa, which is still in full operation. It is currently in the process of expansion, with the entry of new members. China's progress did not stop there, and the country continued its process of economic development, mainly under the government of Xi Jinping, who assumed the presidency of China in 2013 and implemented a new series of reforms and projects, most notably the "New Silk Road" project (Cai & Nolan, 2019).

The New Silk Road aims to revitalize ancient trade routes and promote China's connectivity on a global level. On September 7, 2013, Chinese President Xi Jinping announced the construction of the Silk Road Economic Belt and the 21st Century Maritime Silk Road, laying the foundations for a new phase of the project, called the "Belt and Road Initiative" (Carvalho, 2023).

Although the Belt and Road Initiative began with a focus on physical infrastructure, such as the construction of highways and new railways, modernization of ports and expansion of energy sources, the rapid evolution of technology and the growing global digital interdependence led China to include a new scope in the project, with investments also in digital technology. This new phase became known as the "Digital Silk Road" and is considered a natural extension of the New Silk Road.

The Digital Silk Road refers to the construction of technological infrastructures such as telecommunications networks, submarine internet cables, data centers, cloud computing platforms, digital payment systems, 5G networks, and, more recently, the expansion of the use of artificial intelligence (AI) and other emerging technologies such as the Internet of Things (IoT) and Big Data. The central idea is to promote digital connectivity between BRI participating countries, creating a global network of digital infrastructure that facilitates trade, information flow and technological cooperation between nations.

However, the Digital Silk Road goes beyond building physical infrastructure, as it involves integrating digital technologies into the economies of the countries involved, with China providing both the financing and the technological expertise needed for this development. Chinese companies such as Huawei, Alibaba and Tencent are at the forefront of this effort, offering everything from telecommunications equipment to e-commerce solutions, developing digital payment tools, data networks and cloud computing, and digital banking (Dollar & Huang, 2023).

The main motivation behind the Digital Silk Road is to strengthen China's position as a global technological powerhouse. China aims not only to expand its economic influence, but also to shape the global digital architecture, creating technological norms and standards aligned with its priorities and governance models. By exporting its technology and building digital infrastructures abroad, China not only contributes to the growth of other economies but also increases its geopolitical and strategic presence.

The advancement of digital connectivity in developing regions, for example, can be considered a major achievement, as it provides access to modern technologies and digital infrastructure that some countries may not be able to develop on their own. This access to high-speed networks and digital platforms allows emerging economies to take advantage of technological advances without the barriers associated with the cost of developing their own infrastructure. The ability to access emerging technologies such as AI, the Internet of Things (IoT) and Big Data enables these economies to modernize rapidly, creating new opportunities for growth.

In this scenario, China can contribute to the technological development of countries in the so-called "Global South", establishing a balance in the face of the alleged technological hegemony of the United States and its Big Techs, responsible for the computers, operating systems, and social networks that dominate the Western market.

Another challenge for China in developing this program is the regulation of digital operations. To this end, China created the beforementioned Cyberspace Administration of China (CAC), which plays a key role in regulating the internet and digital technologies in the country[15]. The CAC is responsible for implementing the policies and regulations that govern cybersecurity, privacy, internet governance, and control over digital content, and is one of the main institutions when it comes to China's digital sovereignty. Below, we will discuss some of the most important decrees of the CAC, focusing on the implications for companies, governments, and citizens, as well as their global impact, especially in the context of digital governance and cybersecurity (Sharma, 2024).

Laws have been enacted to regulate the use of the internet, such as the *Cybersecurity Law of the People's Republic of Chin*a, enacted in 2016 with effects from 20217, which is one of the key regulatory frameworks of the CAC (Cyberspace Administration of China, 2016). The law seeks to ensure national security, citizens' privacy, and data protection in a digital environment. This enactment was an important step in creating a legal framework for internet governance in China that aligns with the government's concerns about cybersecurity and digital sovereignty.

The *Online Content Regulation Law*, enacted in 2020, complements the Cybersecurity Law and data protection regulation, focusing on controlling content on the internet. The law requires online platforms, including social media, search engines, and news sites, to monitor and filter harmful or illegal content, such as false information, hate speech, and subversive activities (Cyberspace Administration of China, 2020).

Another significant decree that composes the Chinese digital regulation is the *China Personal Information Protection Regulation* (PIPL), which came into effect in November 2021 (National People's Congress, 2021). This regulation is often compared to the European Union's General Data Protection Regulation (GDPR), as both address issues of digital privacy and data protection. The PIPL seeks to protect the personal information of Chinese citizens and ensure that companies handle data transparently, responsibly, and in accordance with the rights of the individual.

3.3. The Regulation of AI and Experimental Model of the Cyberspace Administration of China

The methodology adopted by the Chinese government differs starkly from the

[15]The CAC has known a process of evolution of former state and party organizations and should not be confused with a western style regulatory agency. Its responsibilities and areas of activity range from regulation, international relations, administrative activities to the direct investment on the IT sector: "no enumerated list of CAC competences currently exists, and thus its powers and responsibilities need to be inferred from broad legislative and policy frameworks, media reports, and its own statements and issued documents. Here, a measure of fuzziness is inevitable: CAC might formulate a document because it has responsibility in a certain policy area, or, sometimes, because it claims it. Furthermore, CAC is more than purely a regulator. It not only sets, implements, and enforces rules for the conduct of businesses and individuals in digital processes but also plays important roles in supporting the work of the CCIC to realise China's ambitious 'informatisation agenda'. It holds authority over specialised technical bodies as well as the sector-specific business associations that form the interface between the state and private industry. It engages in international outreach and is even a shareholder in several Chinese tech firms through the CIIF. In short, CAC's mission concerns, on its own or in coordination with other bodies, the overall governance of the Chinese digital realm in line with overall national policy goals." (Horsley & Creemers, 2024).

model espoused by the European Union. We may even say that it is the opposite.

First, we should consider that while the EU has attempted to provide a comprehensive definition of Artificial Intelligence, China has focused on specific algorithms—a distinction referred to as "horizontal" and "vertical" approaches, respectively (Sheehan, 2023).

While the European model is deductive, China's approach to policy and governance is characterized by an inductive methodology, emphasizing practical experimentation over theoretical deduction. The process begins with small-scale pilot projects and trials, which, if successful, are gradually expanded, a methodology that has been called "Experimental Governance".[16]

The well-known special economic zones initially established by Deng Xiaoping's government, the organization of the healthcare sector (NCMS, New Community Medical System), and the corporate tax reform from 2012 to 2016 (YGZ Reform) can all be considered examples of this procedure (Li, 2023).

The empirical foundation thus constructed leads to subsequent adjustments in policies, laws, and regulations. The Chinese perspective prioritizes the accumulation of practical experience as the basis for theoretical development, rather than imposing preconceived theories onto practice. This pragmatic and incremental orientation underscores a belief in the gradual discovery of rules through sustained experimentation and adaptation (Zhang, 2012)[17].

To implement experimental governance, three types of tools are currently utilized, as identified by Heilman (2008):

1. Experimental points: Small-scale experiments limited to specific economic sectors or policy areas.

2. Experimental zones: Geographic regions granted broad discretionary powers to test new approaches.

3. Experimental regulations or interim laws (暂行法—zàn xíng fǎ): Temporary legal frameworks designed to guide and evaluate experimental initiatives.

This classification highlights the diverse methods used to test and refine governance strategies in a controlled and adaptive manner.

The experimental regulations are documents typically issued by administrative bodies of the state, such as the State Council, its subordinate agencies, or even

[16]"Experimentation in a stricter definition, as used in here, implies a policy process in which experimenting units try out a variety of methods and processes to find imaginative solutions to predefined tasks or to new challenges that emerge during experimental activity. Policy experimentation is not equivalent to freewheeling trial and error or spontaneous policy diffusion. It is a purposeful and coordinated activity geared to producing novel policy options that are injected into official policymaking and then replicated on a larger scale, or even formally incorporated into national law." (Heilman, 2008).

[17]According to the same author, this procedure is rooted in a long cultural tradition, a core characteristic of the so called "civilizational state". This mindset is labeled as "practice-based reasoning". In his own words: "The philosophical outlook of the China model is based on practice. Guided by the motto of 'seeking truth from facts', China proceeds from reality, rather than textbooks, and rejects any dogmatism. Drawing on its own as well as others' experiences, China has initiated bold yet prudent institutional reforms. This philosophical outlook is a product of the Chinese civilization, which possesses a strong this-worldly culture. Concerns about life, reality and society are always paramount in the Chinese world outlook." (Zhang, 2012).

local governments. They serve as a mechanism to test the effects of legal provisions in practice, allowing for adjustments based on real-world outcomes. Interim laws are particularly useful when novel social situations arise—such as challenges posed by emerging technologies—for which there is little or no prior legal precedent. By providing a flexible framework, they enable regulators to address new issues while gaining valuable experience. According to Sun Guohua (1997), interim laws carry the same legal weight as ordinary legislation, ensuring their enforceability during the experimental period.

As of the time of writing, the Cyberspace Administration of China has issued three major decrees concerning AI regulation. The regulatory approach primarily focuses on addressing specific issues categorized within a broad, though not all-encompassing, technical framework. Instead of engaging in debates over a comprehensive definition of artificial intelligence, the decrees narrow their scope to specific technological groups: algorithmic recommendation systems, deep synthesis technologies, and generative artificial intelligence. Let us rapidly dwell on the definition of the technological families each one covers.

The 9th Decree, *Provisions on the Administration of Algorithmic Recommendations for Internet Information Services* (Cyberspace Administration of China, 2021), concerns 算法推荐 (suànfǎ tuījiàn), algorithmic recommendation. It refers to the use of algorithms to recommend content, products, or services to users based on their preferences, behavior, or other data[18]. This is commonly used on platforms like social media, news outlets, e-commerce, and streaming services. The definition of algorithmic recommendation is provided in Article 2, second paragraph: "Application of algorithmic recommendation technology […] refers to the use of algorithmic technologies such as generation and synthesis, personalized push, sorting and selection, retrieval and filtering, and scheduling decision-making to provide information to users." (Cyberspace Administration of China, 2021).

The 12th Decree, *Provisions on the Management of Deep Synthesis of Internet Information Services* (Cyberspace Administration of China, 2022) concerns 深度合成 (shēndù héchéng), deep synthesis, referring to AI-driven content creation or manipulation, encompassing different media forms. In Article 23, the *caput* presents a definition of the technologies comprehended by the regulation: "Deep synthesis technology refers to the technology that uses deep learning, virtual

[18]The need for regulation can be historically determined on a concrete situation, which further demonstrates the experimental governance approach: "Tracing the origin of the term 'algorithmic recommendation' (算法推荐) backward in Chinese state media shows that it first emerged during a 2017 CCP backlash against ByteDance's news and media apps, in which user feeds were dictated by algorithms. The party viewed this as threatening its ability to set the agenda of public discourse and began looking for ways to rein in algorithms used for information dissemination. Much of the final regulation is dedicated to these concerns, requiring that algorithmic recommendation service providers 'uphold mainstream value orientations' and 'actively transmit positive energy'. The regulation included some more concrete measures for online content control, such as requiring that platforms manually intervene in lists of hot topics on social media to ensure they reflect government priorities." (Sheehan, 2023).

reality, and other generative synthesis algorithms to produce text, images, audio, video, virtual scenes, and other network information." (Cyberspace Administration of China, 2022). The following paragraphs of the article provide a non-exhaustive list of applications or uses that can be characterized as deep synthesis, outlining various technologies used to generate or edit digital content, categorized by type:

1. Text Content: Techniques for creating or modifying text, including text generation, style conversion, and interactive dialogues.

2. Speech Content: Technologies for generating or editing speech, such as text-to-speech, speech-to-speech, and speech attribute editing.

3. Non-Speech Audio: Methods for producing or altering non-speech sounds, like music generation and scene sound editing.

4. Biological Features in Visual Content: Tools for manipulating human-like features in images or videos, such as face generation, replacement, attribute editing, and gesture manipulation.

5. Non-Biological Features in Visual Content: Techniques for generating or enhancing non-human elements in images or videos, such as image generation, enhancement, and restoration.

6. Digital Characters and Virtual Scenes: Technologies for creating or editing 3D models, simulations, and virtual environments (Cyberspace Administration of China, 2022).

This summary highlights the broad scope of deep synthesis technologies and their applications across text, audio, visual, and virtual content. One expression that is repeated in every paragraph is 生成或者编辑 (shēngchéng huòzhě biānjí), meaning "generate or edit". We can assume that this provision includes a way of using deep synthesis in what is commonly known as the creation of deepfakes— fabricated audio and video content designed to deceive.

The 15th Decree, *Interim Measures for the Management of Generative AI Services* (Cyberspace Administration of China, 2023), concerns generative artificial intelligence (生成式人工智能 (shēngchéng shì réngōng zhìnéng)). It encompasses "models and related technologies that have the ability to generate content such as text, images, audio, and video" (Cyberspace Administration of China, 2023). This last document is the only one of the briefly analyzed rules that displays in its title the adjective interim. This explicitly illustrates its provisional character but does not imply that the other rules are not subject to expedite change and review.

This focused approach does not preclude the future expansion of the regulatory scope to encompass other families of AI technologies as they mature, and their societal impact becomes more pronounced. The selective regulatory strategy suggests a pragmatic approach focused on addressing immediate concerns related to specific applications of AI, while maintaining flexibility to adapt to future technological developments. It can also be seen as a preparation for a more thorough legislative corpus, even a "Chinese AI Act", as national regulators are still "building up their bureaucratic know-how and regulatory capacity" (Sheehan, 2023).

This attitude, while potentially more agile in addressing specific issues, may also present challenges in ensuring comprehensive coverage of the rapidly evolving AI landscape. For instance, all the three regulations, although providing different scopes and definitions, make reference to generative ai. The difference between the definition provided on the decree that regulates deep synthesis (12th Decree) and generative ai services (15th Decree) is not completely clear. We can imagine many situations on which both of them would apply simultaneously, such as the generation of images using services such as DeepSeek's Janus Pro (https://janus-deepseek.com) or Alibaba's Qwen (http://chat.qwenlm.ai). In fact, the two decrees appear to be complementary in nature. The first decree demonstrates a primary focus on regulating the use of generative AI to produce false information, disseminate illegal content and propagate rumors, as outlined in Articles 6, 10, and 11. However, it does not explicitly address issues related to training data or copyright concerns. In contrast, the second decree specifically targets these aspects, as evidenced by its provisions in Articles 4 and 7. This distinction highlights the somewhat overlapping, somewhat complementary roles of the two decrees in addressing different dimensions of AI governance.

China has shaped its technology and artificial intelligence (AI) policies in a flexible and dynamic manner, according to the country's needs. China's regulatory approach is unique due to its centralized nature and the strong influence of the Chinese Communist Party (CCP), which allows for rapid policy implementation, often in contrast to the more deliberative and dogmatic approach of the European Union (EU). This flexibility and centralization provide an advantage when it comes to addressing urgent and adaptive technology issues such as AI.

China has a centralized governance structure that allows the Party leadership to quickly implement and adjust policies to meet emerging challenges. This includes technology and the Internet, where regulations can be swiftly adapted to ensure the country remains globally competitive while ensuring national security and social harmony. A key aspect of Chinese regulation is its capacity for rapid intervention, both to protect society and to drive economic development. In many cases, this results in a more flexible regulatory approach compared to the EU, which tends to prioritize transparency, democratic processes, and deliberative decision-making.

The adaptability of Chinese regulations has been crucial in several areas, including artificial intelligence and information control, allowing the government to react quickly to new issues that arise with technological development.

One of the clearest examples of how China's regulatory flexibility has been effective in addressing emerging AI issues more quickly than the European Union involves the use of facial recognition technologies.

China has implemented a mass surveillance system based on facial recognition, something that has sparked major debates about privacy and human rights in other parts of the world, including the European Union. The Chinese government's ability to adapt its AI and privacy regulations quickly in response to growing demands for public security and social control has been a hallmark of its policy (Ye, 2023).

Starting in 2015, the Chinese government began deploying facial recognition systems on a large scale with the Smart Public Security Program. Cities such as Shenzhen, Beijing, and Shanghai began using these technologies to monitor traffic, identify criminals, and even monitor social behavior. However, regulations on the use of these technologies have also evolved rapidly. In 2017, the Cybernetic Administration of China (CAC) issued a law regulating the use of big data and AI to ensure that these surveillance systems are used within legal limits and to ensure public safety.

In 2019, the Chinese government took a more formal step toward regulating the use of facial recognition by issuing new regulations requiring explicit consent from citizens for the use of these technologies in private settings and requiring registration in public spaces. Despite strong privacy concerns, the Chinese government has managed to regulate the use of these technologies in a way that balances its security needs with changing social norms.

China's regulatory flexibility is reflected in its ability to make rapid adjustments as new issues arise. The use of facial recognition in China has accelerated in part because the government has the authoritative stewardship to implement regulations directly and immediately, without having to go through a lengthy legislative process or rely on broad public consensus. This has allowed China to adapt its approach over time, adjusting regulations in response to social concerns and evolving technology.

In contrast, in the European Union, the regulatory process for AI, especially with regard to privacy, security, and civil rights issues, has been more protracted and cautious. The EU's General Data Protection Regulation (GDPR), for example, came into force in 2018 and was the fruit of years of discussion and compromise with a range of stakeholders, including technology companies, lawyers, civil rights advocates, and the general public (Hoofnagle, van der Sloot, & Zuiderveen Borgesius, 2019).

The GDPR is an innovative and important regulation to ensure the protection of personal data and also illustrates the more deliberative and complex approach of the EU, which can often be slower to react to emerging AI issues compared to China.

While the EU has developed an AI strategy and implemented regulations such as the GDPR, the issue of facial recognition is still in its early stages in terms of regulation. In 2020, the European Commission discussed a regulation on AI, which addressed ethical and safety issues related to AI, including the use of facial recognition. However, discussions were still in the early stages, with various interest groups still debating how to balance the use of technology with the protection of fundamental rights.

The AI Act, proposed by the European Commission in 2021, suggests a strict approach to the use of facial recognition, classifying it as a high-risk technology and severely limiting its use in public spaces, with very limited exceptions. This more complex and lengthy regulatory process, while robust, takes longer to implement, which could make the EU less agile than China in responding to emerging threats or deploying new technologies.

The adaptability of Chinese regulations also has important economic implications. The government has been able to rapidly develop new technologies and enable Chinese companies to become global leaders in AI, especially in sectors such as e-commerce, fintech, and surveillance technology. Government impetus has enabled companies such as Alibaba and Tencent to become global giants in their respective industries. On the other hand, the EU, with its more structured regulatory model and more focused on the protection of civil rights, may find it difficult to compete in a global technology race where innovation occurs at a rapid pace (Friedlander, 2024).

Thus, China's regulatory flexibility regarding AI and the use of facial recognition technologies stands out when compared to the European Union's more deliberative and multifaceted approach. China's ability to react quickly to new demands, including adapting regulations to emerging technology, has given it an advantage in areas such as public security, social monitoring and ideological control.

China's ability to quickly adapt its regulations therefore allows it to effectively tackle issues such as the use of AI in public surveillance, but it also raises debates about the ethical implications and civil rights, in contrast to the more meticulous and deliberate model of the European Union.

Finally, we must consider that absence of a comprehensive definition of AI, as the one observed in the EU model, may result in regulatory gaps and lack of legal certainty[19], particularly if new AI technologies emerge that do not align neatly with the existing categories of regulated technologies. This potential shortcoming, however, could be mitigated by the system's agility in formulating new rules or amending existing ones, a capability facilitated by the administrative characteristics previously discussed at the outset of this section. If such flexibility will allow for a more adaptive legal framework, capable of responding to the rapid evolution of AI technologies, or result in a chaotic regulatory landscape, remains an open question, due to the novelty of those legal rules and fast-changing landscape of the

[19]"In general, legal certainty is taken to express a fundamental principle according to which the addressees of laws must know the law in order to be able to plan their actions in accordance with it". (Raitio, 2021)

[20]"The Chinese legal system is thus, in essence, as fluid and changeable as the economy and society which it is supposed to regulate. Laws were, through administrative influence and general inadequate levels of drafting skills, made ambiguous to enable flexibility in interpretation and implementation. Consequently, the informal aspects of regulatory rules have tended to change as rapidly as the government's economic policy. Few obstacles impede such practices there is as yet simply no concept, as exists in some Western legal systems, that law or delegated legislation can be struck down on the basis of uncertainty. This indicates a fundamental difference in legal philosophy, and starkly illustrates that a concept that may be antithetical to one legal order may in another be considered beneficial." (Corne, 2002).

AI technology[20].

3.4. Initial impacts of EU and China's AI Policies on Technological Advancement

The regulatory frameworks of both polities are still in their early stages. It is too soon to definitively assess their long-term impact on AI innovation and development. Nevertheless, some estimates of the impacts of the regulatory initiatives are worth mentioning.

At this stage we can indicate the European Commission (2021) study evaluating the potential impact of various AI regulatory options, ranging from a minimal voluntary method to the currently adopted regulation of all AI applications[21]. Various impacts were taken into consideration, including the effects on AI adoption, compliance costs, financial burdens for SMEs, implications for competitiveness and innovation, costs incurred by public authorities, as well as social, fundamental rights, and environmental impacts. Let us briefly summarize compliance costs.

The preferred regulatory model in the study—regulating high-risk AI systems[22] while establishing voluntary codes of conduct for non-risk AI applications (Option 3+)[23]—indicated that the total aggregate cost of compliance and administrative expenses would range between €100 million and €500 million, with verification costs[24] slightly exceeding €100 million. Under the horizontal regulation approach adopted by the AI Act, aggregate compliance costs were projected to increase to approximately €3 billion by 2025, while verification costs were expected to range between €1 billion and €3 billion (European Commission, 2021)[25].

The significant compliance expenses and bureaucratic hurdles outlined above could deter businesses and investors. On the other hand, the stability provided by a regulated environment could stimulate market demand, enhancing the

[21]The policy options considered at the time were as follows: 1) a voluntary labelling scheme, 2) an ad hoc sectorial approach, 3) a horizontal risk-based act, 3+) a horizontal risk-based act alongside the enactment of codes of conduct, and 4) a horizontal act for all AI (European Commission, 2021).

[22]The EU AI Act classifies AI systems into four categories based on their risk levels: unacceptable risk—prohibited AI applications and uses; high risk; limited risk (subject to transparency requirements) and minimal risk. For instance, AI systems that use subliminal techniques to manipulate behavior, exploit vulnerabilities related to age, disability, or social conditions, or involve social scoring are explicitly forbidden under Article 5. Meanwhile, applications classified under Article 6 or listed in Annex III are considered high risk. These include remote biometric identification systems, safety components of critical infrastructure and AI systems used to determine access to education or recruitment.

[23]"As a result from the comparison of the options, the preferred option is option 3+, a regulatory framework for high-risk AI applications with the possibility for all non-high-risk AI applications to follow a code of conduct. This option would: 1) provide a legal definition of AI, 2) establish a definition of a high-risk AI system, and 3) set up the system of minimum requirements that high-risk AI systems must meet in order to be placed on or used on the EU market." (European Commission, 2021)

[24]"In addition to meeting the requirements, costs may accrue due to the need to demonstrate that the requirements have been met." (European Commission, 2021)

[25]The report's data was derived using the Standard Cost Model methodology and was based on standardized tables provided by the German Federal Government. A comprehensive description of the methodology and the values applied can be found in the Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe (Renda, Arroyo, Fanni, Laurer, Sipiczki, Yeung et al., 2021).

attractiveness of investing in such ventures. For example, when considering AI uptake, the report stresses a general positive impact, mentioning effects such as users trust and legal certainty (European Commission, 2021)[26].

The report further examines the specific impacts of the new regulatory framework on small and medium-sized enterprises (SMEs). While it acknowledges the varying capacities of large corporations and SMEs to absorb compliance costs, its overall prognosis remains positive. This optimism stems from the emphasis on the benefits of a regulated environment that fosters enhanced trust and stability. Additionally, the report highlights that targeted cost-mitigation measures could effectively address challenges posed by regulatory requirements. Examples include the implementation of regulatory sandboxes (Article 57), the support for digital innovation hubs[27], and knowledge sharing activities, such as the AI on Demand platform[28]. All those initiatives are supposed to alleviate bureaucratic burdens and support compliance efforts.

Finally, it is essential to recognize that the EU AI Act was designed to strike a balance between fostering innovation and safeguarding fundamental EU values, including democracy, fundamental rights, and the rule of law. This equilibrium is explicitly outlined in Article 1(1) of the AI Act, reflecting the principles established in foundational documents such as the EU AI Strategy (European Commission, 2018). While the preceding analysis has primarily highlighted the challenges posed by a regulated market, the report also addresses broader societal costs, including impacts on employment, recruitment practices, discrimination, and education. Additionally, it underscores potential safety enhancements related to product security and health protection.

A significant portion of the discussion centers on fundamental rights. For instance, Annex 5.5 of the report examines critical issues such as human dignity, privacy and data protection, equality and non-discrimination, freedom of expression, right to an effective remedy and fair trial and the right to good administration, rights of special groups, freedom to conduct a business and the freedom of science and intellectual property rights. A comprehensive evaluation of these implications exceeds the scope of this paper, as each topic warrants dedicated scholarly attention.

Nevertheless, we emphasize the Act's overarching aim: to harmonize innovation and investment with the protection of the EU's foundational values. This balance remains central to the legislation's framework and its broader societal aspirations.

This contrasts with the vision outlined by the People's Republic of China

[26]The report's data was derived using the Standard Cost Model methodology and was based on standardized tables provided by the German Federal Government. A comprehensive description of the methodology and the values applied can be found in the Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe (Renda, Arroyo, Fanni, Laurer, Sipiczki, Yeung et al., 2021).

[27]https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue

[28]https://www.ai4europe.eu

standpoint.

As one of the most rigorous and comprehensive digital regulatory frameworks in the world, the Chinese system intensively controls data and information flows on the Internet, applying various standards and adopting effective data control policies.

The Internet became widely available in the late 1980s. At the same time, China launched a series of structural projects called "Golden Projects", which were applied to a variety of areas, including agriculture, water conservation, credit, finance, taxation, and security, among others. One of the most notable projects was the "Golden Shield Project", developed in 1998 and in operation since 2003 (Walton, 2016).

Aimed at regulating the digital system in China, this project applies to all digital information and security networks, particularly aimed at crime prevention and police use. Evolving from this program, the so-called "Great Firewall of China" (GFC) was developed. Although this program should not be confused with the "Golden Shield Project", it has come to encompass internet monitoring and control policies, in which the National Computer Network Emergency Response Technical Team Coordination Center of China (CNCERT/CC) operates (Shen, 2014).

The GFC is a set of technologies and policies implemented to block access to certain international websites and services, such as Google, Facebook, X, Instagram, and YouTube, and is highly effective in restricting access to unfiltered information and regulating the dissemination of content that could potentially challenge established norms or authority. The blocking is largely invisible to users, who may not realize that their connections are being monitored.

The idea behind the Great Firewall is to protect Chinese citizens from external influences and ensure that the Internet in the country is controlled by the Chinese government, in defense of national interests. The main monitoring and control measures are blocking foreign websites, real-time monitoring, imposing limits on the activities of Chinese Big Techs, regulation through the Cybersecurity Law of 2017 and the Personal Data Protection Law of 2021.

Another effective measure is to impose content limits on Chinese platforms such as WeChat, Weibo and Douyin, which are subject to strict regulations on what can be displayed and shared on their networks. The companies operating these platforms need to ensure that content complies with local laws, which involves overseeing content and, at times, restricting material perceived as potentially destabilizing or inconsistent with the national sovereignty and objectives, adopting automated moderation systems, and using teams of human moderators to detect and remove unwanted or harmful content (Wang, 2022).

China's Cybersecurity Law, enacted in 2017, imposes a comprehensive set of rules for protecting data, monitoring online activity, and defending against cyber threats. The law requires technology companies to store user data within China and cooperate with authorities when necessary. A new personal data protection law was also implemented in 2021, modeled in part on the European Union's General Data Protection Regulation (GDPR). The law requires companies to obtain clear consent to collect personal data and imposes strict rules on how the data can be used and shared (DLA Piper, 2025).

These laws are examples of efforts to improve data security and privacy in China, but their effectiveness is ensured by constant government vigilance. Thus, China's internet regulatory framework has been extremely effective in maintaining control over information and limiting access to content that does not comply with government standards. Monitoring is robust and well implemented, and companies operating in China must follow strict protocols to operate within the law.

3.5. Stakeholder Dynamics in AI Regulation

In the formulation of regulations on Artificial Intelligence (AI) in the European Union (EU) and China, considering the social, political, economic and cultural aspects, the role of all stakeholders in the regulation of AI can be highlighted, such as technology companies, civil society, universities and the government itself.

In the European Union, digital regulation is shaped by a robust legal framework, such as the General Data Protection Regulation (GDPR) and the AI Act (Artificial Intelligence Regulation), which are directly linked to citizens' rights and transparency in the use of AI.

In this scenario, technology companies operating in the EU, such as Google, Microsoft and Meta, play an important role in shaping these regulations. However, EU AI regulation places strict restrictions on how these companies operate, especially with regard to the use of personal data and algorithmic transparency (Koene, 2019).

As Shoshana Zuboff argues, large tech companies, especially those outside Europe, face significant challenges due to stringent European legislation such as GDPR. Zuboff points out that Europe has been more aggressive in regulating tech companies to ensure that individuals' rights are protected, which is reflected in restrictions on mass data collection practices. However, tech companies are trying to influence public policy to reduce regulation, which has been a constant concern in the relationship between companies and European governments (Zuboff, 2019).

Civil society plays an active role in shaping AI regulations in the EU. Organizations such as European Digital Rights (EDRi) and Access Now lobby regulators to ensure that AI technologies do not infringe on human rights, such as privacy and freedom of expression. These organizations often act as ethical standards in AI development, especially in the area of transparency and accountability. EDRi, for example, abandoned Social Network X in February 2025 because it disagreed with new guidelines implemented by Elon Musk, X's current owner, which it considered to violate human rights (Belu, 2025).

Mireille Hildebrandt, a digital law expert, argues that algorithmic governance should be approached with a combination of legal principles and social values, which is reflected in the work of civil society in the EU (Hildebrandt, 2016).

Civil society thus acts to ensure that algorithms are not used for mass surveillance or discrimination, and to promote ethical and social norms around AI.

In turn, universities and researchers also play a crucial role in shaping AI policy in the EU. Academic institutions such as the University of Oxford and the University of Tartu have been instrumental in creating ethical frameworks for AI. In the context of the AI Act, experts in AI, ethics and philosophy have collaborated directly with policymakers.

Luciano Floridi, professor of Philosophy and Information Ethics at the University of Oxford, proposes a set of ethical principles for the use of AI, highlighting that it is essential to protect human dignity, as well as to ensure that the regulation of the use of Artificial Intelligence is approached in an interdisciplinary and transparent way, promoting social inclusion and development for the whole society and is not focused solely on technological or market issues (Floridi, 2023).

As for governments, the European Commission has been involved collaboratively in regulating AI. The AI Act, a regulation proposed by the European Commission, aims to create a balanced approach between technological innovation and the protection of human rights. The European Parliament also plays a significant role in assessing the social and economic implications of new technologies. For Judy Wajcman, the EU seeks a form of regulation that balances innovation and social justice (Wajcman, 2004).

China, on the other hand, adopts a centralized governance model, with the government playing a dominant role in formulating AI policies. The central idea is to align technological innovation with the strategic interests of the state, especially regarding social harmony and national security.

Chinese technology companies such as Baidu, Alibaba, and Tencent are important drivers of AI innovation. However, their involvement in policymaking is subordinate to the oversight of the Chinese Communist Party (CCP). Large companies do not operate independently. They must align their innovations with the CCP's strategic goals (Windsor, 2017).

Civil society in China plays a limited role in shaping decisions regarding AI regulation. Non-governmental organizations (NGOs), civil society groups, and individual citizens face challenges in exercising significant influence over or openly questioning the government's technology policies. This is due in part to the emphasis on maintaining ideological alignment and social stability, which involves measures to guide public discourse and prevent actions or expressions that could undermine national unity or provoke unrest. The Chinese government exercises surveillance over civil organizations and closely controls debates about technology (Zheng, 2013).

In China, universities play an essential role in AI research, but their activities must be aligned with government guidelines. Chinese universities, such as Tsinghua University, are key players in the execution of the state's technology strategy, contributing to social surveillance and control. However, as Lin Zou and Yi-Wen Zhu point out:

> Although Chinese universities produce a large number of scientific research papers or publications every year, the issue is whether these research achievements can be effectively transformed into market value. It has been pointed out by some researchers that the university transformation rate of S&T research achievements in China is still far behind that of western developed countries (Zou & Zhu, 2021).

In recent years, however, Chinese universities have been expanding their participation not only in the development of new technologies, but in the debate on the regulation of the virtual environment, contributing to the Chinese government in identifying internet problems, which helps in the production of regulatory standards.

The EU and China's approaches to AI regulation reflect very different political, social and cultural views. While the EU adopts a more dialogic regulatory model with strong multi-stakeholder engagement, China adopts a centralized, state-driven model where the government exercises greater control over emerging technologies. Civil society, technology companies and academia play different roles in each context, shaping governance models according to the political and ideological priorities of each region.

These differences reflect not only political systems, but also the cultures and values that each region attributes to technological innovation, social control, and the protection of individual rights. The debate on AI governance will continue to evolve as technologies advance and regulatory models adapt to new social and economic realities.

3.6. Exploring the Deeper Cultural and Political Drivers of EU and Chinese Regulatory Philosophies

The analysis of the regulatory philosophies of the internet and the use of artificial intelligence (AI) in the European Union (EU) and China reveals profound influences from their respective cultural, political, social, economic, legal and behavioral contexts (Krönke, Müller, Tian, & Yu, 2018).

From the perspective of the Chinese government, primary regulatory concerns revolve around the prevention of social disorder and the mitigation of risks associated with the dissemination of false or misleading information. The overarching objective is to maintain social stability and harmony, which are regarded as essential for national development and societal well-being. This emphasis on social order contrasts sharply with the individual rights-centric approach that characterizes Western regulatory frameworks, such as those of the European Union (Bell, 2015).

In the political and cultural context, the EU is characterized by a diversity of member states with consolidated democratic systems, emphasizing individual rights and civil liberties. This political and cultural plurality leads to a regulatory approach that prioritizes the protection of personal data and privacy, seeking to balance technological innovation with the fundamental rights of citizens. The EU Artificial Intelligence Act, for example, establishes strict guidelines for the development and use of AI, aiming to ensure that these technologies are used in an ethical and transparent manner.

In China, the Chinese Communist Party (CCP) exercises centralized control over governance, promoting policies that reflect collectivist values and the primacy of the state. China's approach to regulating the internet and AI emphasizes maintaining social order and national security, often prioritizing control over western-style individual freedom. The government implements policies that strictly regulate online content and encourage the development of AI that aligns with state interests, aiming to reinforce China's position as a global technology leader.

In China, rapid urbanization and economic growth have driven the massive adoption of digital technologies. Socially, there is widespread acceptance of digital monitoring for the sake of stability and economic progress, reflecting a culture that values collectivity and social stability. Economically, China is investing heavily in AI, which is seen as an engine for economic growth and a platform for global competitiveness. To this end, China is advancing policies that encourage collaboration between government, industry, and academia to accelerate technological innovation, industrial production, and national development.

From a legal perspective, the EU implements rules such as the General Data Protection Regulation (GDPR), which sets strict standards for the processing of personal data, reflecting a cautious and Western-oriented approach to human rights.

This fundamental difference in regulatory philosophy gives rise to distinct priorities and approaches to AI governance. While Western frameworks tend to prioritize individual autonomy, data privacy, and accountability, Chinese regulations emphasize the collective good, social stability, and the prevention of disruptions to social order. This focus on maintaining stability translates into heightened vigilance regarding the potential misuse of AI technologies for disseminating disinformation, propaganda, or content that could incite social unrest. Consequently, Chinese regulatory measures often emphasize content moderation, censorship, and the control of information flows.

This divergence in priorities reflects deeper cultural and political differences concerning the relationship between the individual and the state. In Western liberal democracies, individual rights are typically upheld as paramount, whereas in China, the collective good and social harmony are often prioritized over individual liberties. This fundamental distinction shapes the regulatory landscape for AI, leading to markedly different approaches to issues such as data governance, algorithmic transparency, and the role of the state in overseeing technological development.

The distinction in regulatory focus is not merely a technical or procedural variation but rather a reflection of fundamentally distinct conceptions of the role of technology in society and the interplay between the individual, the state, and society as a whole. These contrasting perspectives underscore the broader implications of AI governance, highlighting how cultural, political, and philosophical contexts influence the design and implementation of regulatory frameworks.

While both regulatory models aim to address the challenges posed by AI, the long-term effects of these divergent approaches remain uncertain. It is yet to be seen whether the emphasis on individual rights in Western frameworks or the focus on collective stability in Chinese regulations will prove more effective in balancing innovation with societal well-being. Only time will reveal the full impact of these strategies on global AI governance and their implications for humanity.

4. Conclusion

A quantitative distinction between Chinese and European regulatory activity lies in the scale and scope of the resulting legal instruments. The current Chinese AI regulations are considerably more concise and focused compared to their European counterpart. In contrast, EU regulations, such as the proposed AI Act, are often extensive and complex documents, encompassing numerous articles, annexes, and recitals. The sheer volume and detail of EU legislation reflect the Union's emphasis on comprehensive legal frameworks and detailed provisions. This difference in regulatory style has significant implications for implementation and interpretation. The conciseness of Chinese regulations may facilitate faster implementation and enforcement, but it may also lead to ambiguities and require further interpretation by implementing agencies. Conversely, the detailed nature of EU regulations aims to provide greater legal certainty and predictability but can also make them more cumbersome to navigate and implement. The disparity in length and complexity is readily apparent even when considering the introductory recitals of the respective regulatory instruments, with EU regulations often containing extensive preambles explaining the rationale and objectives of the legislation of the various technical frameworks under consideration, machine learning (technology we could consider a sort of super-framework) stands out as arguably the most transformative and impactful contemporary technological development. Indeed, we might assert, perhaps somewhat provocatively, that without the advent and proliferation of machine learning, the present discourse on AI regulation would likely not occur. To illustrate this point, one might consider the relative lack of academic or professional discourse dedicated to less sophisticated computational tools, such as word processing spell checkers. While such tools are undoubtedly useful, they have not generated the same level of intellectual and societal engagement. It is crucial to acknowledge that machine learning is not the sole driver of the current interest in AI regulation. However, it serves as a potent catalyst, significantly amplifying the urgency and scope of these discussions. The primary impetus for the present analysis stems from the increasing prevalence and often indiscriminate deployment of machine learning technologies. This widespread adoption is frequently accompanied by a limited understanding of the underlying mechanisms, processes, and potential outputs of these systems.

Furthermore, a significant discursive challenge surrounding artificial intelligence is the pervasive tendency towards anthropomorphism. This inclination to ascribe human-like qualities and intentions to AI systems can lead to misinterpretations and flawed assumptions about their capabilities and limitations. The expressions intelligence, learning, training and so forth exemplifies this tendency, implicitly suggesting that the AI system possesses a subjective human-like experience. This anthropomorphic projection extends to the perception that AI systems are capable of deception or are themselves susceptible to being deceived, mirroring human social interactions. This projection of human attributes onto non-human entities can distort our understanding of how these systems operate. Instead of recognizing AI as a complex computational process, we may erroneously attribute agency, consciousness, or intentionality to it. This can lead to an overestimation of the system's capabilities, as well as a failure to recognize its inherent limitations. It is crucial to maintain a clear distinction between the technical functionalities of AI and the cognitive and emotional attributes of human beings. This cautionary note serves to emphasize the importance of adopting a rigorous and objective approach to the study and analysis of AI, avoiding the pitfalls of anthropomorphic bias when dealing with regulations.

In concluding this comparative analysis, it is pertinent to stress some challenges in the regulatory angles adopted by the European Union and China. Our Socratic Doubt moment in the beginning was a somewhat western-minded instant. Even though we recognize the importance of skepticism, if we had started with a Chinese minded concern, we would probably not ask this sort of question, but we would interrogate what the main current problems our societies aim to solve and try to experiment with different solutions.

The EU method, while aiming for comprehensiveness, raises a concern around the definition's capacity to remain relevant and inclusive in the face of rapid technological advancements. Specifically, the question arises whether this general definition will adequately encompass future AI technologies that may diverge from current paradigms. Furthermore, it raises the possibility of excluding certain systems that, while not employing established AI techniques such as machine learning, logical languages, or knowledge-based systems, may nonetheless pose comparable risks. For instance, systems that generate decisions, recommendations, or content through alternative computational methods, not explicitly captured by the current definition, may still present ethical, societal, or economic risks that warrant regulatory oversight. The European Union has developed a risk-based framework for AI regulation, which categorizes AI systems based on their potential impact. However, the breadth and potential ambiguity of the general definition develops apprehensions about whether it effectively captures the full spectrum of potentially risky AI applications. A more granular and nuanced definition might be necessary to ensure that all systems posing significant risks are adequately addressed within the regulatory framework.

A consideration pertains to the inherent complexity of the European Union's legal production system. The EU operates as a supranational entity composed of member states, resulting in a multilayered legal framework characterized by diverse types of legal instruments with varying degrees of legal force. Furthermore, the EU legislative process is structured around a tripartite institutional dynamic, often referred to as "trilogues", involving negotiations and consensus-building among the European Parliament, the Council of the European Union, and the European Commission. This complex interinstitutional process, while designed to ensure democratic legitimacy and representation of diverse interests, inherently leads to a protracted and often cumbersome legislative procedure. This characteristic is further compounded by the European continental legal tradition, which emphasizes the primacy of codified law and precise legal definitions. In this tradition, legal norms are formulated as abstract definitions, and their application depends on the factual circumstances aligning precisely with those pre-defined categories. This deductive approach to legal reasoning, while promoting legal certainty and predictability, can create challenges when dealing with rapidly evolving technological domains. The EU's decision to adopt a regulatory framework based on general definitions, therefore, must be understood within the context of this established legal tradition. This line, while consistent with instituted legal practice, raises concerns about the adaptability and futureproofing of the regulation in the face of continuous technological advancement and the emergence of unforeseen AI applications. The choice reflects a balance between the desire for legal clarity and the recognition of the need for a framework that can accommodate future developments, even if it introduces some degree of interpretative flexibility.

On the other hand, the Chinese system demonstrates a significantly expedited process of rule production. This allows for a much more rapid response to emerging technological developments, a characteristic that distinguishes it sharply from the EU's more deliberative and lengthy legislative procedures. This pragmatic attitude facilitates a more agile regulatory response, but it also raises questions about the comprehensiveness and long-term coherence of the regulatory framework. By focusing on specific technologies, there is a potential risk of overlooking emerging AI applications that do not neatly fit within the pre-defined categories. Furthermore, this methodology may lead to regulatory fragmentation, with different sets of rules applying to different AI technologies, potentially creating inconsistencies and complexities for businesses operating in this space.

A comparative analysis of these two distinct regulatory models provides valuable insights into the diverse strategies employed to address the challenges posed by advancing AI technologies. This study has focused exclusively on the distinction between broad and specific approaches in legal definitions and regulatory documents. However, a comprehensive comparison of these legal frameworks must also take into account various other factors, including substantive content, risk assessment, the protection of individual rights, democratic principles, and regulatory authority. Despite the inherent limitations of this narrower focus, this foundational distinction nonetheless offers meaningful reflections on the broader question of how AI should be regulated.

The European Union has adopted a comprehensive, definition-based approach to AI regulation, seeking to establish a broad legal framework applicable to a wide range of AI applications. This approach is grounded in an overarching definition of artificial intelligence, encompassing diverse technical families while attempting to distinguish AI from traditional software. By adopting this broad characterization, the EU aims to ensure legal certainty and promote harmonized regulatory standards across its member states. However, given the inherent complexity and evolving nature of AI, any regulatory framework must be approached with a critical perspective—continuously questioning and reassessing the definition of AI and its constituent technologies.

In contrast, China's regulatory strategy categorizes AI technologies into distinct technical frameworks, offering a more nuanced and targeted approach to regulation. This methodology allows for a focused examination of specific regulatory challenges, enabling a granular and adaptable legislative style that accounts for the unique characteristics and risks associated with different AI technologies. Rather than establishing an all-encompassing regulatory framework, China has opted for a selective, incremental approach, addressing immediate concerns while laying the groundwork for future comprehensive legislation and enhancing regulatory enforcement capabilities.

Ultimately, the EU's broad approach prioritizes comprehensiveness and legal harmonization, whereas China's targeted strategy emphasizes agility and adaptability. These divergent regulatory paradigms reflect distinct legal traditions and governance philosophies, each with their own advantages and limitations. As AI continues to evolve, the interplay between these models will likely shape the future of global AI governance.

When comparing the European and Chinese legal systems, it is crucial to consider the unique philosophies that underpin each legal culture. In the West, legal certainty is highly valued as a core objective of the legal system, emphasizing clarity, predictability, and stability. In contrast, in the East, adaptability is often prioritized, reflecting a more flexible and context-sensitive approach to governance and regulation.

We must avoid the common mistake made by many scholars and policy makers of evaluating one legal system through the lens of another. Instead, we should aim to understand the distinct characteristics of each legal framework on its own terms, steering clear of superficial judgments or uninformed critiques. This approach fosters a deeper appreciation of the values and principles that shape each tradition. Such an understanding is particularly important in comparative law, as it can inform the development of new AI regulations both at the national level and internationally. By respecting the unique features of each legal practice, we can create more effective and harmonious regulatory frameworks that align with diverse cultural and legal contexts.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Bell, D. A. (2015). *The China Model: Political Meritocracy and the Limits of Democracy*. Princeton University Press. https://doi.org/10.1515/9781400865505

Belu, A. (2025). *Why EDRi Is Leaving X and Where to Find Us*. https://edri.org/our-work/why-edri-is-leaving-x-and-where-to-find-us

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

Buchanan, B., & Shortliffe, E. (1984). *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*. Addison Wesley.

Cai, F., & Nolan, P. (2019). *The Handbook of the Belt and Road*. China Social Sciences Press.

Carvalho, E. M. (2023). Renascimento da Rota da Seda e sua Extensão até a América Latina. In E. M. Carvalho, P. Steenhagen, & D. Veras (Eds.), *China e a Iniciativa Cinturão e Rota: Percepções do Brasil* (pp. 17-56). FGV Direito Rio. https://repositorio.fgv.br/items/3b18f6b5-63ea-4d41-92be-0fade88ed641

Cohen, J. (1967). *Human Robots in Myth and Science* (1st American ed.). A.S. Barnes and Company.

Copeland, B. J. (2000). The Turing Test. *Minds and Machines, 10,* 519-539. https://doi.org/10.1023/a:1011285919106

Corne, P. H. (2002). Creation and Application of Law in the PRC. *The American Journal of Comparative Law, 50,* 369-443. https://doi.org/10.2307/840825

Crevier, D. (1993). *AI: The Tumultuous History of the Search for Artificial Intelligence*. Basic Books.

Cyberspace Administration of China (2016). *Cybersecurity Law of the People's Republic of China*. https://www.cac.gov.cn/2016-11/07/c_1119867116.htm

Cyberspace Administration of China (2020). *Provisions on the Governance of the Online Information Content Ecosystem*. https://www.gov.cn/zhengce/zhengceku/2020-11/25/content_5564110.htm

Cyberspace Administration of China (2021). *Provisions on the Administration of Algorithmic Recommendations for Internet Information Services. 9th Decree.* https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm

Cyberspace Administration of China (2022). *Provisions on the Management of Deep Synthesis of Internet Information Services. 12th Decree*. https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm

Cyberspace Administration of China (2023). *Interim Measures for the Management of Generative AI Services. 15th Decree*. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

Dartmouth University (n.d.). *Artificial Intelligence (AI) Coined at Dartmouth*. https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth

DLA Piper (2025). *Data Protection Laws in China*. DLA Piper. https://www.dlapiperdataprotection.com/index.html?c=CN&t=law

Dollar, D., & Huang, Y. P. (2023). *The Digital Financial Revolution in China*. Brookings Institution Press.

Epoch AI (2023). *Key Trends and Figures in Machine Learning*. https://epoch.ai/trends

European Artificial Intelligence Office (2024). *Living Repository to Foster Learning and Exchange on AI Literacy*. https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy

European Commission (2018). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe. Document 52018DC0237. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0237

European Commission (2021). *Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Document 52021SC0084*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0084

European Commission (2024). *Commission Decision of 24.1.2024 Establishing the European Artificial Intelligence Office*. https://ec.europa.eu/newsroom/dae/redirection/document/101625

European Commission (2025a). *European AI Office*. https://digital-strategy.ec.europa.eu/en/policies/ai-office

European Commission (2025b). *AI Pact*. https://digital-strategy.ec.europa.eu/en/policies/ai-pact

European Parliamentary Research Service (2024). *Legislation in Progress: Artificial Intelligence Act. PE 698.792. European Parliament*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

European Union (2016). *Consolidated Version of the Treaty on the Functioning of the European Union. Document 12016ME/TXT*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

European Union (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Document 32024R1689*. http://data.europa.eu/eli/reg/2024/1689/oj

Fernández-Llorca, D., Gómez, E., Sánchez, I., & Mazzini, G. (2024). An Interdisciplinary Account of the Terminological Choices by EU Policymakers Ahead of the Final Agreement on the AI Act: AI System, General Purpose AI System, Foundation Model, and Generative AI. *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-024-09412-y

Ferrater Mora, J. (2001). *Dicionário de Filosofia*. Edições Loyola.

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

Friedlander, D. (2024). *EU's Digital Competitiveness Suffers from Regulatory Burden and*

Lack of Capital, Research Finds. Computer & Communications Industry Association. https://ccianet.org/news/2024/05/eu-digital-competitiveness-suffers-from-regulatory-burden-and-lack-of-capital-research-finds

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. The MIT Press.

Heilmann, S. (2008). Policy Experimentation in China's Economic Rise. *Studies in Comparative International Development, 43,* 1-26. https://doi.org/10.1007/s12116-007-9014-4

Hildebrandt, M. (2016). *Smart Technologies and the End(s) of Law*. Edward Elgar Publishing. https://doi.org/10.4337/9781849808774

Homer (n.d.). *The Iliad* (A.T. Murray, Trans.; G.R. Crane, Ed.). Perseus Digital Library. https://www.perseus.tufts.edu

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. *Information & Communications Technology Law, 28,* 65-98. https://doi.org/10.1080/13600834.2019.1573501

Horsley, J., & Creemers. (2024). The Cyberspace Administration of China: A Portrait. In R. Creemers, S. Papagianneas, & A. Knight (Eds.), *The Emergence of China's Smart State* (pp. 9-33). The Rowman & Littlefield Publishing Group.

International Electrotechnical Commission (n.d.). *Artificial Intelligence (AI). IEC Electropedia*. https://www.electropedia.org/iev/iev.nsf

Koene, A. (2019). *A Governance Framework for Algorithmic Accountability and Transparency*. European Parliament Scientific Foresight Unit (STOA).

Krönke, C., Müller, M., Tian, W., & Yu, W. (2018). *Paradigms of Internet Regulation in the European Union and China*. Nomos.

Li, E. (2023). *Party Life: Chinese Governance and the World beyond Liberalism*. Palgrave MacMillan.

McCorduck, P. (2004). *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence* (2nd ed.). A K Peters.

McCulloch, W. S., & Pitts, W. (1943). A Logical Calculus of the Ideas Immanent in Nervous Activity. *The Bulletin of Mathematical Biophysics, 5,* 115-133. https://doi.org/10.1007/bf02478259

McDermott, J. (1980). R1: An Expert in the Computer Systems Domain. In *Proceedings of the First AAAI Conference on Artificial Intelligence. AAAI'80* (pp. 269-271). AAAI Press.

Merrit, R. (2023). *Why GPUs Are Great for AI*. http://blogs.nvidia.com/blog/why-gpus-are-great-for-ai

Minsky, M., & Papert, S. (1969). *Perceptrons: An Introduction to Computational Geometry*. MIT Press.

National People's Congress (2021). *Personal Information Protection Law of the People's Republic of China*. https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

Newell, A., & Simon, H. (1956). The Logic Theory Machine: A Complex Information Processing System. *IEEE Transactions on Information Theory, 2,* 61-79. https://doi.org/10.1109/tit.1956.1056797

Novaes, R. V., & Ferraz, F. F. (2025). Protection of Copyrights in the Era of Generative Artificial Intelligence. In M. N. Santos, J. Machado, P. Novais, P. Cortez, & P. M. Moreira (Eds.), *Lecture Notes in Computer Science* (pp. 332-343). Springer. https://doi.org/10.1007/978-3-031-73497-7_27

Raitio, J. (2021). Legal Certainty. In M. Sellers, & S. Kirste (Eds.), *Encyclopedia of the*

Philosophy of Law and Social Philosophy (pp. 1-6). Springer. https://doi.org/10.1007/978-94-007-6730-0_136-2

Renda, A., Arroyo, J., Fanni, R., Laurer, M., Sipiczki, A., Yeung, T. et al. (2021). *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*. Publications Office of the European Union.

Rosenblatt, F. (1957). *The Perceptron: A Perceiving and Recognizing Automaton*. Cornell Aeronautical Laboratory, Inc.

Russel, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

Russel, S., Perset, K., & Grobelnik, M. (2023). *Updates to the OECD's Definition of an AI System Explained*. OECD AI Policy Observatory. https://oecd.ai/en/wonk/ai-system-definition-update

Samuel, A. L. (1962). Artificial Intelligence: A Frontier of Automation. *The Annals of the American Academy of Political and Social Science, 340,* 10-20. https://doi.org/10.1177/000271626234000103

Sharma, M. (2024). *Building China into a Cyber Superpower*. Routledge. https://doi.org/10.4324/9781003473510

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

Shen, F. (2014). Great Firewall of China. In K. Harvey (Ed.), *Encyclopedia of Social Media and Politics* (Volume 2, pp. 599-602). Sage Publications.

Stanford University (2024). *Artificial Intelligence Index Report 2024*. Stanford Institute for Human-Centered Artificial Intelligence (HAI). https://aiindex.stanford.edu/report

Sun, G. H. (1997). *Chinese Law Dictionary—Jurisprudence Volume*. China Procuratorial Press.

Turing, A. M. (1950). I.—Computing Machinery and Intelligence. *Mind, 59,* 433-460. https://doi.org/10.1093/mind/lix.236.433

Voigt, P., & Hullen, Nils. (2024). *The EU AI Act: Answers to Frequently Asked Questions*. Springer Nature.

Wajcman, J. (2004). *Technofeminism*. Polity Press.

Walton, G. (2016). *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Rights and Democracy, International Center for Human Rights and Democratic Development. https://ora.ox.ac.uk/objects/uuid:084840ac-b192-407b-ab6c-f8f810310369/files/m288240d9de06449ce5eb98e7ad3d0edc

Wang, J. (2022). *Platform Responsibility with Chinese Characteristics*. Digital Planet, Center for International Law and Governance, The Fletcher School at Tufts University. https://digitalplanet.tufts.edu/wp-content/uploads/2023/02/DD-Report_1-Jufang-Wang-11.30.22.pdf

Wexelblat, R. (1978). *History of Programming Languages*. Academic Press.

Widrow, B., & Hoff, M. E. (1960). Adaptive Switching Circuits. In *IRE WESCON Convention Record* (pp. 96-104). Institute of Radio Engineers. https://isl.stanford.edu/~widrow/papers/c1960adaptiveswitching.pdf

Windsor, D. (2017). Interpreting China's Model for Business. In E. Paulet, & C. Rowley (Eds.), *The China Business Model* (pp. 41-69). Elsevier. https://doi.org/10.1016/b978-0-08-100750-1.00003-6

Ye, J. (2023). *China Drafts Rules for Using Facial Recognition Technology*. Reuters.

https://www.reuters.com/technology/china-drafts-rules-using-facial-recognition-technology-2023-08-08

Zhang, W. (2012). *The China Wave: Rise of a Civilizational State*. World Century Publishing Corporation. https://doi.org/10.1142/9781938134029

Zheng, H. (2013). Regulating the Internet: China's Law and Practice. *Beijing Law Review, 4,* 37-41. https://doi.org/10.4236/blr.2013.41005

Zou, L., & Zhu, Y. (2021). Universities' Scientific and Technological Transformation in China: Its Efficiency and Influencing Factors in the Yangtze River Economic Belt. *PLOS ONE, 16,* e0261343. https://doi.org/10.1371/journal.pone.0261343

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.