Article

Not peer-reviewed version

The Criteria of Chinese Regulatory Framework on Artificial Intelligence: Reflections Based on Cost-Benefit Analysis

Dong Zheng *

Posted Date: 27 December 2023

doi: 10.20944/preprints202312.2082.v1

Keywords: artificial intelligence; regulation framework; legal risks; cost-benefit analysis; evolutionary game theory

Article

The Criteria of Chinese Regulatory Framework on Artificial Intelligence: Reflections Based on Cost-Benefit Analysis

Dong Zheng †,‡

School of Law, Nanjing Normal University of China; 122 Ninghai Road, Nanjing, CN, Nanjing China (Mainland)
230401014@njnu.edu.cn
† Current address: Nanjing Normal University.
‡ These authors contributed equally to this work.

Abstract: This article summarizes Chinese framework for regulating artificial intelligence and integrates evolutionary game theory with cost-benefit analysis to establish a model and simulation. This framework is employed to analyze the behavioral trends among three distinct entities: governmental bodies, third-party independent institutions, and AI companies within the context of regulatory relationship. The findings indicate that: (1) The cost-benefit dynamics within the regulatory legal nexus significantly influence the behaviors of these entities; (2) Under the condition of normalized government regulation approaching full enforcement, the behavioral choices of third-party independent institutions and AI companies exhibit cyclical fluctuations. The paper draws two principal conclusions: (1) The regulatory framework need to be tailored to the specific risks presented by AI and the relative costs and benefits of legal enforcement in different jurisdictions. (2) From a cost-benefit standpoint, government intervention in AI regulation ought to be circumscribed, with government regulation focusing on critical legal risks. Other aspects of regulatory control should be delegated to cooperative legal framework that allows the participation of the independent third-party institution, which brings a nuanced and specialized approach to the governance of AI.

Keywords: artificial intelligence; regulatory framework; legal risks; cost-benefit analysis; evolutionary game theory

1. Introduction

1.1. Background

As science moves faster than moral understanding, people even struggle to articulate their unease with the perils novel technologies introduce [1]. Just as William Gibson points that: 'The future is already here – it's just not very evenly distributed. 'Whether people are aware of it or not, Artificial intelligence (AI) is taking us into the fourth industrial revolution, known as Industry 4.0. This is likely to result in the applicability of AI-based technologies across multiple industries, particularly those involved in process or manufacturing activities. Healthcare, petroleum, power generation, automotive, and related fields are examples of industries that could potentially benefit from the implementation of AI-based technologies, including Machine Learning (ML) and Deep Learning (DL) [2]. According to the McKinsey Global Institute, AI will raise the global GDP by more than $15 trillion [3]. However, The risks of different types of privacy protection and regulation on AI cannot be overlooked as well [4]. Early this year, more than 30 thousand people, including Steve Wozniak, Elon Musk, and more, are so concerned the rapid development of powerful AI system that they call on all AI labs to immediately pause for at least 6 months [5]. As Sam Altman points that:

'Society will face major questions about what AI systems are allowed to do, how to combat bias, how to deal with job displacement, and more... A gradual transition gives people, policymakers, and institutions time to understand what's happening, personally experience the benefits and downsides of these systems, adapt our

 doi:10.20944/preprints202312.2082.v1

economy, and to put regulation in place. It also allows for society and AI to co-evolve, and for people collectively to figure out what they want while the stakes are relatively low.' [6]

Do we really have enough time to put regulation in place and catch up with the artificial intelligence?In 2021, the European Commission drafted the world's first proposal for an Act on regulating artificial intelligence aiming to create a solid European regulatory framework for trustworthy AI, which will protect all people by preventing the risk of data breaches, misinformation and non-compliance with intellectual property rights et al. However, the Act will still need to go through more negotiation before it finally come into power. Other relevant laws and regulations can be classified as these domain like Data, Electronic Communications, Cyber security, Consumer Rights Protection et al. While the chemical, food, and pharmaceutical industries established years ago use evidence based models that ensure the safety of these products EU-wide, these frameworks have yet to be see within AI regulation [7]. In the past five years, the Data Protection Commission published more than one hundred cases [8], which ranged from data breaches to privacy transparency policy. Among all the risks, the most common and most emerging privacy or security risk was difficulty maintaining compliance across various regulatory regimes with different requirements, such as data breaches during the use of AI or the data localization policy in the EU [9]. Since the *General Data Protection Regulation* (GDPR) came into force, authorities have issued a few hundred more fines [10]. Some of the fines imposed on prominent platform companies like Google, Amazon, Instagram, Equifax, and others have sparked considerable interest and stimulated thought on the connection between privacy and personal information, trade secrets and company data, and how to balance the growth of AI industry with regulation [11].

The comparable confusion regarding the equilibrium between innovation and regulation of artificial generative intelligence has emerged in China as well. With the promulgation and implementation of laws and regulations such as the Data Safety Law and the Personal Information Protection Law, China has continuously improved the working mechanism of data security. In December 2022, the central committee of the Communist Party of China and the State Council issued the policy entitled "Building the basic data system and better utilizing the role of data production factors". This policy elevated the data circulation and trading compliance to national strategic height, as well as, aiming to establish efficient compliance and inside and outside the data circulation and trading system.*Interim provisions on the management of artificial intelligence services*, jointly promulgated by the Cyberspace Administration of China and other seven departments, officially came into force on August 15,2023. This new policy centers its attention on the realm of pre-regulatory or preventive supervision. However, it remains conspicuously bereft of a definitive resolution concerning the regulatory conundrum posed by the generation of inappropriate content by generative AI services. Expedient measures have now been taken that parallel endeavors are undertaken to mitigate the risks associated with data breaches and privacy infringements arising from the utilization of artificial intelligence. In accordance with the latest report, the Nation's Internet Information System of China conducted an exhaustive examination of 8,608 websites and digital platforms over the course of the previous year. This comprehensive review yielded a cascade of regulatory actions, including formal warnings issued to 6,767 entities, the imposition of fines or punitive measures upon 512, and the suspension of functions or updates for 621 others. Additionally, a stringent response was directed towards 420 mobile applications, leading to their removal from circulation. The licenses of illicit websites were either revoked or duly recorded with the competent telecommunication authorities, leading to the cessation of operations for 25,233 unauthorized websites. Furthermore, 11,229 pertinent case leads were meticulously transferred for further inquiry and action [12]. One of the well-known cases is the cybersecurity inspection on the Chinese ride-hailing platform Didi Global. In July 2022, the State Internet Information Office (SIIO) imposed a fine of $1.19 billion on Didi Global Inc in accordance with the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and the Administrative Penalty Law of China, among other laws and regulations.

 doi:10.20944/preprints202312.2082.v1

In contrast to the European Union's proposed AI Act and China's efforts to prevent privacy risks posed by artificial intelligence, Southeast Asian countries have adopted a draft document titled "Guide to AI Ethics and Governance" that encourages companies to consider cultural differences and does not specify any unacceptable risk categories. As officials in Singapore and the Philippines have pointed out, hasty regulation could stifle their countries' AI innovation. It appears that Southeast Asian countries are taking a "business-friendly" [13] approach to AI regulation. Similarly, other Asian countries such as Japan and South Korea have also eased AI regulation.

With different AI regulatory policies taking place in different countries and regions, there is an urgent need for a scientific argumentation on the influencing factors of AI regulation and whether or not legal regulation may take place, in order to promote a virtuous circle between AI technological breakthroughs and manageable development. Given the potential upheaval that AI could bring to the productivity landscape, we are facing new puzzles about the social innovation and regulation in AI system. The challenge is adopting regulation that is flexible enough to allow Al to 'create' in the domain of intellectual property [14]. Is it possible to establish a consistent global regulatory framework?While the belief that something needs to be done is widely shared, there is far less clarity about what exactly can or should be done, or what effective regulation might look like [15].

1.2. Literature Review

This paper examines the legal frameworks pertinent to the governance of artificial intelligence (AI), concentrating on the delineation of jurisdiction and responsibilities assigned to various stakeholders within the AI milieu through the mechanisms of administrative law. Such regulatory stratagems are orchestrated to preemptively attenuate the inherent risks of AI applications, with the ultimate ambition of endorsing the beneficence of these technologies for humankind. At the heart of this legal inquiry is the imperative to precisely articulate a definition for AI, as this definition is instrumental in ascertaining the reach and intensity of regulatory oversight. Notwithstanding the ubiquity of the term "artificial intelligence" in common parlance and its extensive portrayal across diverse media platforms, the scholarly and policy-making arenas are yet to converge upon a universally endorsed explication of the term [16]. Nilsson delineates AI as the exhibition of intelligent comportment by artificial agents, encompassing attributes such as cognition, inference, learning, communication, and the capacity for feedback within intricate environments [17]. The European Commission's 2018 blueprint for AI strategy characterizes these systems as manifesting intelligent behavior through environmental analysis and executing actions with a modicum of independence to fulfill explicit objectives [18]. Presently, we find ourselves amidst the 'narrow AI' epoch, wherein AI constructs are proficient in a limited array of tasks. Prospectively, the advent of 'General AI' is anticipated, which aspires to replicate a broad spectrum of human capabilities [19]. Furthermore, AI can be construed as the capacity for adaptation in contexts marred by a paucity of knowledge and resources [20]. This conceptualization posits AI as an overarching term that encapsulates methodologies devised to synthesize intelligence artificially, thereby equipping machines with the faculty to emulate human actions [21]. While unanimity in the academic discourse concerning a definition for AI remains evasive, the definitions proffered herein can be embraced as instrumental in demystifying the technical essence of AI in an academic framework. This elucidation serves as a vital precursor, establishing an intellectual base for the ensuing formulation and enforcement of jurisprudential statutes.

The spectrum of regulatory practices is both comprehensive and exhibits significant variation across different international jurisdictions. For example, state apparatuses commonly enact oversight across various sectors to maintain economic stability. These areas include, but are not limited to, regulatory frameworks governing financial institutions, such as banks and capital markets. Additionally, state regulatory purview encompasses sectors such as education, food production and distribution, transportation, and healthcare. In the contemporary scholarly landscape, considerable attention has been allocated to the regulatory challenges posed by artificial intelligence (AI). It is vital to acknowledge the singular capabilities that AI technologies possess, which are inherently distinct

 doi:10.20944/preprints202312.2082.v1

and without historical precedent. This uniqueness provides a strong impetus for the proposition that AI requires its own bespoke and independent regulatory framework, distinct from those applied to existing technologies [22]. As AI systems gain increased autonomy and as the frequency and depth of human-AI interactions intensify, there emerges an exigent need for a careful evaluation of potential regulatory, ethical, and legal impediments. Governments are instrumental in fostering digital innovation and promoting the development of digital technologies for societal benefit [23]. Without appropriate regulatory frameworks, encompassing both soft and hard law approaches, even the most altruistically intended "Tech for Good" initiatives are susceptible to failure [24]. When it comes to global AI regulation framework, some researcher pointed that international cooperation is vital in establishing common AI governance standards and addressing cross-border AI challenges [25]. The foundational work of Pigou illuminated various socio-economic challenges, including tariff policy, unemployment, price control and public finance, positing the necessity of rigorous regulation at all levels of governance state, provincial, district, and local to ensure societal welfare [26]. Contemporary discourse suggests that AI regulation should align with the Council of Europe's standards on human rights, democracy, and the rule of law, insisting that any legal framework for AI development and deployment should embed principles that protect human dignity, uphold human rights, and respect democratic norms and the rule of law [27]. The High-Level Expert Group on Artificial Intelligence (HLEG AI) has underscored the imperative for new legal measures and governance structures to adequately shield the public from potential adverse impacts of AI, while simultaneously ensuring proper enforcement and oversight without impeding beneficial innovation [28]. Ensuring an appropriate level of technological neutrality and maintaining the proportionality of regulatory measures is paramount in mitigating the vast array of potential risks associated with AI utilization [29]. Moreover, stringent regulation of AI has been identified as a contributing factor in enhancing public willingness to engage with AI-powered robotic technologies [30]. Policy makers face a variety of regulatory strategies, the selection of which depends on numerous factors, including the degree of uncertainty, the nature of the interests involved, and the context or magnitude of AI development and usage [28]. Notably, once the need for regulation becomes evident, implementing corrective measures can be challenging due to entrenched decisions and established power dynamics [31]. Some scholars discuss the legal procedures of regulating on AI. Buiten discussed the regulatory process of AI bias in terms of data input, algorithmic structure and content models [32]. Particular consideration is given to the domain of medical treatment, where AI introduces complex ethical questions. Scholarly proposals have thus been discussed for the establishment of regulatory mechanisms to navigate these emerging challenges. Such discourse evidences the multifaceted nature of AI regulation, highlighting a clear mandate for holistic and adaptive legal responses to the evolving landscape of AI technology [33].

A body of scholarly research has levied substantial critique against existing regulatory theories, especially within the purview of AI technology legislation. Such efforts to legislate with foresight in the digital domain have been largely marked by failure [34]. Within this context, a regulatory framework for Artificial Intelligence (AI) is advocated to provide considerable latitude for technological progression [35]. Furthermore, there is a contention that the complexities introduced by AI have not been subjected to sufficient scrutiny, which suggests that the inception of a comprehensive regulatory system for AI may be premature [36]. In the scholarly critique of regulatory practices, concerns have been raised that poorly conceived regulations could potentially impede the progress and deployment of beneficial Artificial Intelligence (AI) technologies. Such regulations may fail to advance safety and control measures, thus undermining their intended purpose [37]. A strategic regulatory approach, characterized by judicious restraint—or "masterly inactivity"—is posited as a preferable pathway. This approach suggests that masterly inactivity except when prompted by law enforcement is the economically most advantageous policy open to them [38]. This principle advocates for a cautious approach that allows for the natural evolution of AI, may yield more favorable outcomes in the long term compared to precipitous regulatory actions taken without a comprehensive understanding of the AI landscape. Further, the public interest theory of regulation faces critiques primarily originating

 doi:10.20944/preprints202312.2082.v1

from the Chicago School of Law and Economics [39]. Libertarian scholars, including Nozick, have highlighted a pronounced divergence between rule enforcement as adjudicated by the judiciary compared to regulatory agencies [42]. On the one hand, Much of government regulation of industry was originated and is geared to protect the position of established firms agains competition [40]; On the other hand, regulators find themselves at a strategic disadvantage due to information asymmetries, a lack of knowledge to properly understand the implications of technologically enabled social relations as well for lack of resources and institutional mechanisms to intervene timely before technology has been developed and widely adopted [7]. Like all regulation, it can be used both to enhance public welfare and to facilitate sovereign abuse of the public. More regulated legal systems appear to cost more and to produce higher delay, without offsetting benefits in terms of perceived justice [41]. Contrast with regulation, private litigation has many advantages, which is of no special interest to the government, and hence disputes can be resolved apolitically [42].

The regulatory dialogue regarding the inherent risks of artificial intelligence (AI) necessitates an exhaustive analysis. AI, as a cornerstone of the informational technology sector and a frontier innovation, is anticipated to exert substantial impacts on economic development. In scenarios where explicit regulatory frameworks are absent, emergent AI enterprises may confront the daunting task of maneuvering through a patchwork of inconsistent regulatory demands. This complexity could exacerbate their regulatory compliance obligations and potentially impede innovation by inhibiting or completely deterring entrepreneurial risk-taking. It is, therefore, critical to articulate a foundational theoretical framework and establish supervisory structures that are integral to AI regulation. Such a framework should aim to balance the promotion of innovation with the imperative of containing the risks associated with AI. Furthermore, the prevailing system of law enforcement and judicial processes has not yet evolved to include specific provisions for administrative regulation or the assessment of corporate liability concerning AI-related offenses. This gap prompts a crucial inquiry into how law enforcement entities might adapt existing legal norms to regulate issues arising from AI. A complex aspect of this inquiry involves ascertaining the appropriate allocation of liability in situations where risk of infringement arises from AI-powered production. Moreover, the international arena displays a diversity in the maturity levels of AI technologies across different jurisdictions, with the corresponding regulatory costs and benefits of AI manifesting variably. Given these discrepancies, it is essential to consider whether these varied conditions affect the feasibility of enacting a comprehensive and consistent global regulatory regime for artificial intelligence.

2. The Chinese Legal Framework of Regulating Artificial Intelligence

While specific legislation dedicated to the regulation of artificial intelligence is presently absent in China, the discourse surrounding regulatory frameworks for artificial intelligence has garnered heightened attention in recent years.

2.1. Why Artificial Intelligence Need to be Regulated

Artificial intelligence is presently undergoing a transformative evolution, transcending its erstwhile virtual confines to manifest as a palpable reality. Formerly relegated to the confines of scientific experimentation, it has transcended the domain of pure theoretical inquiry to assume a pivotal role in our quotidian existence. Its reach extends beyond rudimentary applications typically associated with mobile devices or personal computers, maturing into sophisticated entities endowed with competencies encompassing data assimilation, information dissemination, profound machine learning, and autonomous decision-making across multifarious facets of society.

As is illustrated in Figure 1, the operation of artificial intelligence is intricately intertwined with a tripartite sequence, encompassing the phases of input, analysis, and output. In the initial input stage, the acquisition of raw data necessitates the utilization of sensors or manual data entry. These data manifest in diverse formats, including textual, auditory or visual content, and subsequently require preprocessing and parameterization to facilitate their comprehensive analysis in the subsequent phase.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2082.v1

Within the analytical stage, the AI system undertakes the emulation and training of neural networks akin to the human brain, employing an array of algorithms and models to attain advanced cognitive and decision-making proficiencies. These algorithms and models encompass machine learning, deep learning, natural language processing, computer vision, and other technological paradigms. The selection of particular algorithms dictates the domain of application for AI. For instance, the advent of large language models (LLMs) represents a transformative breakthrough in the domain of natural language processing (NLP). These models, such as ChatGPT, unveiled last year by OpenAI, are founded on a deep neural network model imbued with a Transformer architecture. These models are adept at simulating human conversation, responding to queries, and generating comprehensive written content. The final phase, the output stage, entails the amalgamation and refinement of outcomes derived from the prior analysis phase, by incorporating multimodal external environmental data, which may encompass input text or audio instructions. The ultimate result can manifest in diverse forms, such as text, auditory, visual, or videographic content, or even behavioral instructions governing the operation of machinery or systems. The overarching objective of this stage is the transformation of AI's analytical outcomes into tangible applications or decisions, thereby culminating in the realization of the objectives of intelligence and automation.

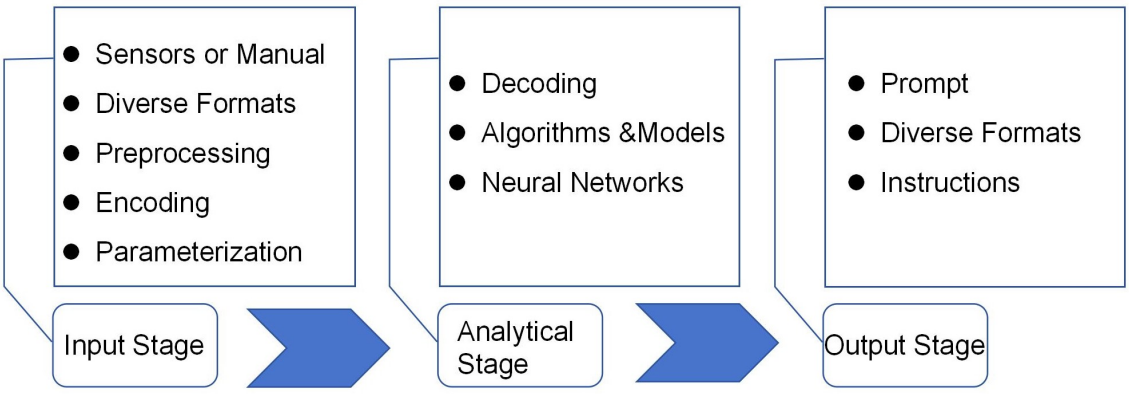

Figure 1. The Schematic Diagram of How AI Works.

The proliferation of AI-powered technologies and products, while holding the promise of substantially augmenting human convenience, has concurrently engendered apprehensions pertaining to potential issues of racial bias, breaches of data security, and the dissemination of misinformation. These concerns, in turn, bear profound ramifications for the established legal framework, warranting astute examination as we navigate the intricacies, challenges, and prospects posed by the burgeoning landscape of this transformative technology.

2.1.1. Challenges to Security

In the preceding section, it was elucidated that the optimal functioning of artificial intelligence (AI) during its initial stage hinges significantly upon an extensive data training process. This training process draws upon data acquired through a combination of sensors and human input. These advanced sensors encompass a diverse range of capabilities, allowing AI devices to capture intricate details about their immediate environment. Such information encompasses crucial parameters like geographical coordinates (latitude and longitude), altitude, velocity, heading, temperature, humidity, light intensity, and other pertinent attributes. These data streams serve as the bedrock for a multitude of applications spanning navigation, environmental monitoring, smart home automation, health tracking, and more. However, the utilization of this data for alternate objectives, such as advertising or political purposes, invariably raises concerns related to privacy and security. Within the realm of self-driving vehicles, powered by artificial intelligence, a notable array of amenities awaits the occupants of these smart cars. Such vehicles are equipped with an ensemble of technologies, including cameras, inertial navigation

 doi:10.20944/preprints202312.2082.v1

systems, and radar systems, which empower them to achieve autonomous functionality. This technological marvel has found widespread application in the vehicle fleets of numerous self-driving taxi companies operating in Beijing. In the course of their operation, these intelligent vehicles traverse a diverse range of environments, including overpasses, viaducts, tunnels, and other specialized road settings. In these unique contexts, the vehicles maintain a constant connection with the operational system, facilitating the real-time acquisition of critical data. This data encompasses a spectrum of variables, including the status of the throttle, brake pedal pressure, geographical coordinates, bridge height, tunnel specifications, and more. The generation of this data is incessant, and numerous data instances are transmitted to vehicle manufacturers through encrypted channels, often without soliciting the preferences of the vehicle owners [43]. Once the AI-captured data reaches the manufacturer's data center, it undergoes meticulous categorization, capturing detailed information pertaining to each distinct spatial coordinate. This information includes the state of the road, navigational distances, and the totality of environmental data amenable to mapping. In the public spaces traversed by autonomous vehicles, a discernible limitation exists with regard to the expectation of privacy. Moreover, the public is frequently left bereft of any explicit notice or choice regarding the collection and utilization of this data, thereby engendering substantial apprehensions concerning privacy and security [44]. This situation underscores the pressing need for rigorous examination of the privacy and security implications inherent in the operation of AI within public spaces. Such scrutiny is imperative in order to safeguard the interests and rights of individuals and the broader public while harnessing the benefits of this transformative technology.

Through the integration of data inputed by manual, the potential for bias within the data collection process emerges, subsequently leading to the risk of the trained artificial intelligence model generating inequitable outcomes for specific demographic cohorts. For instance, should gender or racial biases be ingrained within the dataset, the trained AI model is susceptible to reflecting these biases, thereby engendering disparities in its treatment of certain groups. Furthermore, as such biases proliferate throughout the broader social milieu, they become vulnerable to exploitation for political manipulation and may precipitate sundry issues in the realm of societal governance. This apprehension accentuates the paramount importance of proactively addressing bias mitigation strategies and ethical considerations in both the development and deployment phases of AI systems. These measures are indispensable to ensure that AI technologies are conducive to positive societal contributions while upholding the rights of both individuals and collectives.

The AI's aggregation of public data engenders an array of disquieting considerations. Take, for example, AI-powered vehicles, which autonomously collate and process data pertaining to road traffic flow, information readily accessible via government websites for the optimization of driving routes. This practice gives rise to apprehensions regarding the AI's capacity to harvest and scrutinize data that is in the public domain, thus unfurling a spectrum of concerns. The publicly available datasets encompass a broad spectrum of information emanating from diverse sectors, including transportation, education, commerce, administrative enforcement, community affairs, healthcare, and the justice system. When AI systems engage in the comprehensive acquisition and analysis of this multifaceted data landscape, it precipitates an inherently unpredictable milieu fraught with regulatory and governance risks. For instance, the AI might potentially exploit its analytical capabilities to circumvent government oversight in pivotal sectors such as healthcare, food production, and urban water supply. By scrutinizing the numerical count and geographical distribution of administrative lawmen, the AI may orchestrate strategies to evade or subvert regulatory frameworks, ultimately posing a substantial and consequential threat to the lives and well-being of countless individuals.

Artificial intelligence also introduces notable risks in the domain of personal data collection and management. Presently, a multitude of automobile seats are endowed with the functionality of autonomous seat adjustment. This feature entails individuals, be they drivers or passengers, preloading facial recognition imagery and subsequently configuring their preferred seat settings, encompassing parameters like seat height, tilt angle, and distance from the steering wheel. The vehicle's integrated

 doi:10.20944/preprints202312.2082.v1

system retains this data, and next times, a mere facial recognition procedure is requisite, upon which the car's operating system automatically adjusts the seat configurations in accordance with the facial recognition data. Moreover, providers of AI technology solicit substantial quantities of data and information from consumers, including voice recordings and fingerprint data, which facilitate the issuance of commands to the vehicle for functions such as air-conditioning regulation, window operation, and automated navigation, among other operations. Evidently, AI-equipped vehicles are no longer confined to their primary function as means of transportation; instead, they have evolved into complex entities featuring advanced operating systems and network communication capabilities, rendering them an extension of an individual's private space for work and relaxation. The personal data archived by these AI systems encompass an expansive spectrum of information, encompassing user emails, internet search histories, conversational interactions, and documents. This repository of data may encompass sensitive personal details, including identity particulars, online gaming profiles, philosophical outlooks, individual proclivities, sexual preferences, health records, and various other confidential information [45]. In the regrettable occurrence of data breaches or cyber attacks, which can have profound security ramifications and disrupt regular operations [46], and malicious entities may exploit the abundance of information acquired to compromise the personal safety and assets of individuals. Such incidents not only pose substantial security risks but also have the potential to significantly impact the normal functioning of various systems and processes. Therefore, it is imperative to address and mitigate these threats in order to safeguard the well-being and property of individuals.

As depicted in Figure 2, the risks inherent to artificial intelligence (AI) transcend its nascent stages and endure throughout the entirety of AI technology's lifecycle, undergoing dynamic evolution in synchrony with the progressions in AI technology A notable point of contention emerges in the arena of products liability when AI-driven products or services are introduced into practical application: Who are liable for the infringement? For instance, Tesla's Autopilot and Full Self-Driving system have encountered rigorous regulatory and legal scrutiny, precipitating a plethora of products liability lawsuits across the nation. In the context of products liability, the Third Restatement of Tort Law has introduced the concept of "rationality," which applies to producer liability. This notion carves out a legal space for the application of the development risk defense. The development risk defense posits that if a product is considered non-defective in alignment with the prevailing scientific and technological standards at the time of its introduction into the market, the producer may not be held liable, even if subsequent scientific and technological developments reveal defects after a certain duration. Traditionally, in matters of product liability, manufacturers bear strict liability for any injuries arising from defects in their products. In accordance with Article 1202 and Article 1203 of the Civil Code of China, in instances where a product defect results in harm to others, the producer is held liable for tort. It is essential to acknowledge the formidable challenge faced by plaintiffs or injured parties in substantiating claims of defective AI products. Manufacturers possess the legal recourse to assert, as a defense, that their product embodies the "state of the art," thereby necessitating a careful assessment of the technological landscape in the determination of liability. A noteworthy illustration of this principle is the case of Molander v. Tesla Inc., wherein Tesla emerged victorious in its initial trial in the United States against allegations that its Autopilot feature resulted in a fatality. The two surviving passengers, who sustained severe injuries, have filed a lawsuit seeking $400 million in compensation for their physical injuries, emotional distress, and the loss of the driver's life. The jury's determination hinged on whether the vehicle exhibited a manufacturing defect in accordance with the technological standards. This case underscores the paramount significance of the "state of the art" principle in the domain of tort liability law, particularly within the realm of AI product liability. If the question in the lawsuit was whether the vehicle was defective, then the "state of the art" defense could foreclose manufacturer liability when programming weaknesses were later identified [47]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2082.v1

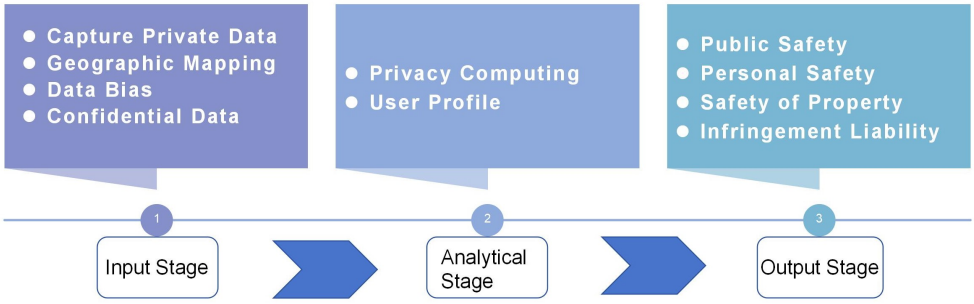

Figure 2. Schematic of Security Risks at Different Stages of AI.

2.1.2. Challenges to the protection of intellectual property

Leveraging centuries of cumulative human knowledge, artificial intelligence is steadily advancing toward surpassing human intellect. AI companies are leveraging their technological prowess in an attempt to evade accountability for the widespread misappropriation of countless copyrighted works. This conduct has given rise to legitimate concerns that the concealment of such infringement may exacerbate the challenges associated with safeguarding intellectual property rights in the context of AI-related infringement cases.

As is shown in Figure 2, the initial stage of traning AI necessitates inputing a substantial volume of data. According to article 7 of the GAISM, providers of generated AI services are obligated to conduct pre-training and optimization training in strict adherence to legal principles. In the pursuit of pre-training and optimization training, AI service providers must exclusively employ data and foundational models obtained from legitimate sources. The sourcing of information and models should conform to established legal frameworks, ensuring compliance with ethical standards and legal requirements. In instances where intellectual property rights are implicated, AI service providers are expressly enjoined from infringing upon the intellectual property rights of third parties. This mandates a scrupulous examination of the legal landscape to ascertain and respect existing intellectual property rights, safeguarding against unauthorized use or replication that may contravene legal norms and ethical standards.

However, it lacks well-defined legitimate behavioral standards for artificial intelligence training and the legal regulations governing its fair use. Moreover, there remains a conspicuous lack of transparency concerning the extent of data utilization within the "black box" analysis, the precise number of variables that are collected, and the specific algorithmic model employed. The opacity of this process complicates the substantiation of claims related to intellectual property rights. In case *Getty Images vs. Stability AI*, Stability AI has been accused of engaging in widespread infringement of Getty Images' intellectual property rights. The reputation and trademarks of Getty Images enjoy substantial recognition both within the United States and across the global landscape. A significant proportion of the visual content, encompassing images and videos, featured on Getty Images' online platforms comprises original and creative works that hold protection under the purview of United States copyright laws. In the case of numerous visual assets, including those that are at the center of copyright infringement allegations in the ongoing lawsuit, Getty Images either retains copyright ownership or holds exclusive licensing rights. For certain other assets, Getty Images assumes a role as a non-exclusive licensee. Crucially, Stability AI possesses a clear awareness that its Stable Diffusion model generates images that incorporate distorted iterations of Getty Images' watermark and various other watermarks. Nevertheless, it has not undertaken any modifications to its model to proactively prevent or rectify such occurrences, thus giving rise to the allegations of infringement. As is accused by Getty Images, Stability AI employs a multi-step process in training its model: Initially, it collects a vast dataset of text-and-image pairs, such as those found on platforms like Getty Images. This dataset is processed through encoding, which involves compressing the images and their corresponding text to optimize memory usage. These encoded versions are saved for training. To challenge the model, Stability AI introduces visual "noise" to the encoded images, intentionally degrading their quality.

 doi:10.20944/preprints202312.2082.v1

This "noise" makes it harder to visually interpret the images and serves as a training method for the model to generate images consistent with specific text descriptions. The model then decodes the altered images, learning to eliminate the added noise by comparing them to the original images and stored text descriptions. This process enables the model to generate images that closely resemble the originals, with noise removed. In case *Andersen et al v. Stability AI Ltd. et al*, Plaintiffs'Complaint alleges that Stability AI copied over five billion images from websites as training images for Stable Diffusion without the consent of the creators or the websites that hosted those images.

Both aforementioned legal actions were instigated by intellectual property rights holders, citing infringements in the sphere of pre-training data within the domain of artificial intelligence. If we persist in allowing the perpetuation of this regulatory void, it may give rise to a burgeoning legal conflict, pitting content creators against AI companies, as contentious issues surrounding data rights and intellectual property continue to mount. This vacuum in regulatory provisions presents the possibility for technology companies specializing in artificial intelligence to engage in large-scale data mining and replication of human knowledge. If the evolution of AI technology continues to erode the intellectual property rights of the majority of the population, a situation could arise where a subset of AI companies dominate the creative field, thereby exposing more people to AI and consequently replacing jobs that would otherwise require only a lower degree of innovation to perform.

2.2. How China Regulates Artificial Intelligence

Pertinent regulatory provisions are observable incorporated in the pertinent laws or policies, such as the *Data Safety Law*(DSL), the *Comprehensive Governance Regulations for Internet Information Services* (CCRIIS), the *Internet Information Service Algorithm Recommendation and Management Regulations*(IISARM)and the *Interim Measures for Generative Artificial Intelligence Service Management*(GAISM). The establishment of regulatory framework takes into full account the legal risks encountered during the AI application process, leading to the gradual formation of a collaborative AI regulatory framework.

2.2.1. Differentiated Regulation Based on the Size of the AI Company

In the era of artificial intelligence, large companies have assumed the role of an "invisible government" owing to their expansive user base, substantial repositories of user behavioral data, ample reserves of AI talent, and substantial investments in computing infrastructure. These entities possess the capacity to develop AI technologies independently or through subsidiaries, thereby exerting significant influence and mobilization capabilities within society. Chinese AI companies are categorized by their social mobilization prowess or public opinion attributes, undergo different regulatory oversight. According to article 24 of IISARM, algorithmic recommendation service providers possessing attributes of public opinion or social mobilization capabilities are obligated, within a stipulated period of ten working days from the commencement of service provision via the internet information service algorithm, to complete the record system documentation. This documentation entails furnishing details such as the service provider's name, service format, application domain, algorithm type, and the algorithm itself, along with the pertinent information derived from the evaluation report, encompassing public content. Article 24 of the IISARM stipulates that large artificial intelligence companies endowed with social mobilization capabilities are exempt from the obligation to seek government authorization for the development of AI technology. Instead, they are mandated to promptly register the AI technology within a predetermined system established by the government, within a prescribed timeframe subsequent to the development of AI products or services introduced into the societal or market domain. Government departments have the authority, as outlined in Article 28 of the IISARM, to assess and regulate archival algorithms. They are also able to organize law enforcement for the purpose of supervising and inspecting enterprises. In instances where issues are found, they can provide suggestions for correction and require companies to rectify them within a specified timeframe. Similar provisions are also present in Article 17 and Article 19 of the GAISM.

 doi:10.20944/preprints202312.2082.v1

For companies that do not have social mobilization ability or public opinion attribute, they do not have to complete the record system documentation above. In accordance with Article 8 of the *Guiding Opinions on Accelerating Scene Innovation and Promoting High-Quality Economic Development with High-Level Application of Artificial Intelligence*, AI startups ought to engage in innovation proactively, get involved in city and industrial construction, and attain business expansion through innovation. Overall, Chinese regulatory framework for AI differentiates between enterprise size. The law provides considerable support to small and medium-sized enterprises that lack societal influence to encourage active participation in AI technology development and innovation.

2.2.2. Establishing a Regulatory Framework with the Participation of Multiple Subjects

Collaborative governance involving the government, companies, and society constitutes a pivotal approach for enhancing both the efficacy and capacity of governance systems. While the government assumes a primary role in the realm of artificial intelligence, the technological advantages wielded by AI enterprises in the contemporary era pose a formidable challenge to the regulatory capabilities of governmental bodies. Consequently, in China's legislative framework, specific provisions within laws and regulations delineate the roles and responsibilities of corporations and the public in participating in regulatory processes. Particularly, for entities utilizing artificial intelligence technology for data processing or engaging in intermediary services related to data trading, legal mandates specify the obligations incumbent upon companies or intermediaries to actively engage in compliance with data integrity and safety standards. Moreover, non-governmental entities are accorded both rights and responsibilities to partake in the regulation of misinformation, thereby contributing to efforts aimed at curbing unlawful activities within the artificial intelligence domain. This multifaceted legal approach reflects a concerted effort to address the intricate dynamics between the government, companies, and the public in the regulation on artificial intelligence. According to article 29 of the DSL, AI companies engaged in data processing should enhance risk monitoring and undertake corrective actions promptly upon identifying hazards, including data security defects and vulnerabilities. In the event of a data security breach, they should take immediate measures to resolve it, inform affected users promptly and report it to the relevant government department responsible for data security. In the realm of data trading endeavors, partial regulation authority is vested in a independent third-party institution, whereby the intermediary entity undertakes a preliminary scrutiny of the identities and legal standing of the two entities engaged in the data trading. Pursuant to Article 33 of the DSL, any entity offering intermediary services for data trading is compelled to require the data provider to disclose the provenance of the data and authenticate the identities of all parties participating in the transaction. Furthermore, the said entity is obligated to meticulously record and uphold comprehensive documentation encompassing all audit and transaction particulars.

In accordance with the stipulations delineated in Articles 10-13 of Regulations on In-depth Synthesis of Internet Information Services(ISIIS), providers of artificial intelligence services engaged in activities such as speech synthesis, facial recognition, text synthesis, video clips, or similar services are mandated to augment the regulation of synthesized content. This necessitates the utilization of both technical methodologies and artificial intelligence mechanisms to govern user input data and the resultant synthesized content. The artificial intelligence entity is further obligated to institute a robust system for the identification of illegal and deleterious information. Any such identified content is to be expeditiously handled in conformity with extant legal provisions, with pertinent records meticulously maintained. Timely notifications are imperative, requiring the prompt submission of reports to the cyberspace department and pertinent regulatory authorities. The legal framework further imposes sanctions, as per statutory provisions, upon relevant users availing themselves of deep synthetic services. Such sanctions may encompass warnings, limitations on functionality, suspension of services, or the closure of user accounts. Furthermore, the legislation underscores the regulation authority vested in third-party application stores over providers of deep synthetic services. Article 13 of the ISIIS mandates that internet application stores and akin platforms assume safety

 doi:10.20944/preprints202312.2082.v1

management responsibilities, inclusive of daily operational regulation and contingency response measures. Furthermore, these entities are enjoined to ensure the conduct of safety assessments and the verification of filings for applications involving deep synthesis. In the event of violations of pertinent state regulations, measures such as withholding, issuing warnings, suspending services, or delisting from stores are prescribed.

Analogous regulatory norms are discernible in the domain of civil unmanned aircraft. The Civil Aviation Administration of China has developed the Unmanned Air-craft system traffic management information service system(UT-MISS) to regulate civil Unmanned Aerial Vehicle(UAV)flight activities. It provides services such as civil UAV flight, airspace and safety assessment, planning, and coordinated supervision with relevant regulatory authorities. In pursuit of achieving real-time monitoring of the flight dynamics of lightweight and compact civil UAV, there exists a gradual streamlining of the airspace, flight trajectories, and management of flight activities for such drones. This is accompanied by the implementation of an aerial traffic management system specific to civil drones, and to complement this, the Civil Aviation Administration has promulgated regulatory frameworks governing the Management of Real-time Flight Data for Lightweight Civil Unmanned Air-craft(MDCUAV). In accordance with Article 3.4.2 of the MDCUAV, third-party platforms that satisfy specified technical and safety criteria are permitted to interface with the Unmanned Traffic Management and Information Sharing System (UTMISS). These authorized third-party platforms assume the responsibility of receiving the flight dynamic data submitted by the unmanned aerial vehicle (UAV) systems. This provision contemplates the potential integration of numerous third-party platforms, serving as recipients and regulators of the flight data transmitted by a multitude of unmanned aerial vehicles. Simultaneously, as delineated in Article 5.6 of the MDCUAV, the Civil Aviation Administration retains the authority to regulate these third-party platforms. It is incumbent upon the Civil Aviation Administration to conduct regular and systematic regulation on these third-party platforms. Those platforms found to be non-compliant with stipulated requirements pertaining to data storage and security may face discontinuation of access to the UTMISS system.

Generally, China exhibits a proclivity for crafting a regulatory framework that integrates governmental entities, corporate entities, and the public. This cooperative regulatory framework not only affords artificial intelligence (AI) companies the opportunity to maximize their technological capabilities but also underscores the pivotal role of government regulation in providing support to those requiring assistance.

2.2.3. Decentralized Regulatory Norms Based on Differential Industry Application Scenarios

Presently, China's artificial intelligence (AI) technology and its applications in products are predominantly concentrated within sectors such as the Internet, manufacturing, transportation, finance, and healthcare. Given the diverse application scenarios across these distinct domains, the risks associated with AI technology and products exhibit considerable variability. Adopting a uniform set of criteria to regulate artificial intelligence has the potential to result in excessive regulation or deregulation within specific industries. Consequently, China has refrained from instituting a comprehensive regulatory framework encompassing uniform laws for artificial intelligence. Instead, regulatory oversight is decentralized, with government departments assuming responsibility for formulating and administering specific laws and policies pertaining to artificial intelligence within their respective domains. This decentralized approach is exemplified by Article 16 of the GAISM. As articulated therein, government departments such as those overseeing Internet and information, development and reform, education, science and technology, industry and information technology, public security, radio and television, as well as press and publication, are entrusted with the mandate to fortify the administration of generative AI services in accordance with their respective spheres of influence and regulatory responsibilities. Within the domain of medical artificial intelligence (AI) in China, a rigorous framework for comprehensive life-cycle supervision of medical AI technology has been diligently enforced. This has resulted in the gradual establishment of a regulatory framework with

 doi:10.20944/preprints202312.2082.v1

The State Council assuming a leadership role, while various ministries and commissions collaboratively contribute within their respective spheres of expertise. The application domains of medical AI in China encompass public health intelligent services, the medical device industry, clinical auxiliary diagnosis and treatment, intelligent hospital management, and the broader development of the health industry. According to the article 57 of the Regulation of Medical Devices(RMD), Both pre-market registration inspection of AI medical device products and post-marketing evaluations are conducted by qualified medical device inspection institutions. Inspection of medical devices is exclusively delegated to institutions recognized by the certification and accreditation supervision and administration department under The State Council and the drug regulatory department under The State Council.

In the autonomous driving sector, China has delegated the authority for formulating regulations governing driverless vehicles to various provinces, enabling them to tailor local regulations according to the developmental nuances of their regional automotive industries. Exemplifying this decentralized approach, the Regulations on the Intelligent Connected Vehicles in the Shenzhen Special Economic Zone(RICV) dictate that the road testing, access, registration, and operational management of intelligent connected vehicles within this jurisdiction shall adhere to locally prescribed legislation. Article 8 of the RICV delineates the supervisory obligations of distinct government departments, including the transportation department, market supervision department, traffic administrative department of the public security organ, and the network information management department. Article 14 of the RICV establishes a declaration and management system for road testing and demonstration applications. Entities seeking to conduct road tests or demonstration applications in Shenzhen must, in conformity with stipulated provisions, apply to the relevant municipal competent department. Subsequently, the commencement of road tests or demonstration applications is contingent upon confirmation by the municipal competent department and the acquisition of a temporary driving license plate for the test self-driving vehicle from the traffic administrative department of the municipal public security organ.

A comparative analysis of China's regulatory frameworks pertaining to the domain of self-driving between medical artificial intelligence reveals the absence of standardized and universally applicable regulatory norms. In the arena of autonomous driving, China has embraced a permissive stance, affording individual regions the latitude to devise regulatory policies conducive to the advancement of intelligent vehicles, contingent upon the specific developmental trajectories of the autonomous vehicle industry within those respective localities. Conversely, in the domain of AI-driven medical care, China has adopted a circumspect approach, with The State Council assuming a guiding role in regulating the application of medical artificial intelligence.

3. Regulatory Rationality in the Age of Artificial Intelligence: a Cost-Benefit Analysis in the Framework of Cooperation

The previous section analyzed China's legal framework for regulating AI, yet questions remain to be discussed: Is this cooperative framework for regulating AI really rational?what are the cost and benefit arising from China's regulatory framework?In the realm of public policy and regulatory assessment, the concept of cost-benefit analysis elicits multifaceted interpretations. When the government undertakes the task of subjecting regulatory formulation, it is imperative to engage in a comprehensive evaluation of the associated costs and benefits. Furthermore, such an analytical endeavor necessitates a consideration of both qualitative and quantitative prospective regulatory consequences [48]. The overarching objective is to ensure that regulations yield a net benefit of a positive nature, aligning with the criteria of Pareto efficiency. The judicious implementation of multiple policies and regulations, which collectively generate a positive net effect over the long term, can yield substantial societal advantages, ultimately resulting in gains for the populace as a whole, while concurrently refraining from inflicting harm upon any individual [49].

 doi:10.20944/preprints202312.2082.v1

3.1. The costs of regulating AI

In the context of regulatory analysis, the term "cost" may be aptly defined as the aggregation of all expenditures and the concomitant reduction in overall well-being resulting from either regulatory or non-regulatory policy measures. To enhance precision and conceptual clarity, it is more appropriate to employ the generic term "impacts," categorizing costs as adverse impacts and benefits as favorable ones [50]. The enactment and enforcement of legal statutes represent a substantial fiscal commitment on the part of the government, particularly when it comes to the implementation of regulatory policies pertaining to artificial intelligence, entailing considerable financial outlays. Realizing legal benefits from these endeavors necessitates significant investment; nonetheless, persistent limitations in financial resources and personnel often impede the efficacy of law enforcement. Neglecting to adequately account for the expenses associated with AI regulation, inclusive of operational budgetary allocations, can significantly impede the realization of the intended regulatory impact post-implementation. There exists a substantial likelihood that in the face of excessive regulatory costs or enforcement challenges, the enforcement of regulations may be deferred or selectively applied. In instances where the costs of compliance with regulatory statutes become unduly burdensome, innovative AI companies may seek avenues to circumvent regulatory oversight or relocate their startups to other jurisdictions, thereby undermining competitiveness and imposing societal welfare costs. In the event of a successful legal challenge against regulatory statutes, the sustainability of AI regulation may be called into question, particularly if the litigation costs outweigh the accrued benefits or if the assets subject to seizure or execution prove insufficient to cover the legal expenses incurred.

3.1.1. Regulatory Cost of the Government

When the government elects to regulate AI technology, it assumes the financial responsibility for each phase of the regulatory process, spanning from legislative formulation to enforcement. Within the legislative phase, it is imperative to substantiate the necessity of regulation, a requirement driven by the constraints inherent in legislative resources. In accordance with the Legislation Law and other pertinent legal frameworks, the National People's Congress (NPC) and its Standing Committee undertake the enactment of laws, encompassing the stages of bill initiation, deliberation, voting, and promulgation. A pivotal aspect of this process revolves around the deliberative examination of proposed bills, which must undergo three sessions of the Standing Committee before they are subjected to a decisive vote. If a bill remains unresolved beyond the third Standing Committee session and demands further scrutiny, it may be referred to the Constitution and Law Committee of the NPC, in conjunction with the relevant specialized committees, for extended examination. For a law to advance, it must successfully traverse the gauntlet of deliberation and secure the endorsement of the majority of all deputies, requiring active participation from a diverse array of legal experts, government officials, NPC representatives, and broader community members. The legislative process in China is characterized by its multi-faceted and comprehensive nature, necessitating the passage through numerous procedural stages. This extensive process inherently demands a considerable duration of time to reach its completion. The involvement of a diverse and substantial cohort of individuals in the deliberative discussions further compounds the complexity of this process. Consequently, this intricate and prolonged approach to legislation unavoidably incurs elevated costs, both in terms of resources and time. Such an in-depth mechanism, while ensuring thorough scrutiny and broad-based input, also presents challenges in terms of efficiency and expediency in the legislative domain.

As is shown in Figure 3, the implementation of the law also cost a lot. If a law is enacted successfully, it must be overseen by people's congresses at all levels and carried out by governments at all levels. The Chinese government has fully implemented three administrative law enforcement systems, namely the administrative law enforcement system, the law enforcement record system, and the major law enforcement decision legal audit system. This was articulated in *The General Office of the State Council's guidance on comprehensive implementation of administrative law enforcement system for the public law enforcement process record system*. The administrative law enforcement system

 doi:10.20944/preprints202312.2082.v1

within the public sector refers to the institutions responsible for enforcing administrative law. This includes the territorial jurisdiction of the administrative law department, the personnel involved in administrative law enforcement, their duties, the legal basis for their actions, the procedures they follow, the outcomes of their activities, and the mechanisms for oversight and redress available to the public. The fundamental concept of the administrative law enforcement transparency system is to disclose relevant administrative law enforcement information to society in a timely manner, in accordance with the law, to guarantee transparent administrative enforcement and to facilitate social oversight. The recording system for the entire process of administrative law enforcement refers to the practice of documenting and archiving administrative law enforcement actions using written, electronic, audio, and video recording techniques. This ensures a traceable and retroactive management system for the entire process, thereby standardising administrative law enforcement.

As Article 42 of the Administrative Punishment Law, administrative penalties are to be enforced solely by law-men possessing administrative law enforcement qualifications. Each enforcement must involve a minimum of two officers, thereby incurring the labor cost of two individuals as well as the operation cost for law enforcement recorders and data centres, and the commuting consumption of law enforcement vehicles. The legal audit system for significant administrative law enforcement decisions pertains to the internal framework for oversight and restriction, in which the administrative law enforcement agency assesses legality, provides written examination opinions, and refrains from making any decision without prior legal examination or approval. The fundamental objective of the legal review system concerning significant law enforcement decisions is to ensure the legality and reasonability of decisions made by administrative law enforcement institutions. According to Article 58 of the Administrative Punishment Law, inexperienced personnel in administrative organs responsible for legally examining administrative punishment decisions must obtain qualification as legal professionals through the national unified legal profession qualification examination. Therefore, the personnel conducting legal audits within internal institutions are subject to higher qualification requirements and correspondingly incur higher labor costs than other positions. On the contrary, what if the government were to relax regulations without implementing the law? This approach would also come with some costs. The government may ease regulations to promote economic benefits, which could potentially save costs from legislation to enforcement. However, from the perspective of overall social welfare, the costs may far outweigh the benefits. As for artificial intelligence technology, the preceding analysis explores the challenges that artificial intelligence poses to human safety and creativity. AI has the potential to worsen social injustice and inequality by discriminating against certain groups via automated decision-making systems. Failure to prevent this aspect could prove costly not only in financial terms, but also for society as a whole.

3.1.2. Cost of the third-party institution

As is illustrated above, china is establishing a regulatory framework with the participation of multiple subjects, such as the third-party institution(TPI). The engagement of the TPI in the governance of Artificial Intelligence (AI) pertains to the involvement of external entities entrusted or officially recognized by the government due to their professional competence and qualifications in the field of AI technology governance. These entities are delegated the responsibility of conducting regulatory functions aimed at mitigating risks associated with the application of AI technology. A third-party independent institution in this context may take the form of a corporate entity, an AI industry association, or a collaborative regulatory platform. The establishment of an impartial regulatory agency by the government serves as a mechanism to address the deficiency of public oversight within the domain of AI regulation. The cost of the TPI includes the operation cost and liability cost. On the one hand, the third-party independent institutions, equipped with comprehensive access to precise firsthand data, advanced algorithms, and robust infrastructure, are adept at swiftly identifying and verifying any illicit practices related to the utilization of artificial intelligence technologies. It has been established that third-party independent institutions possess distinct personnel, organizational

 doi:10.20944/preprints202312.2082.v1

structures, and assets that separate them from governmental entities. Consequently, these institutions maintain autonomy akin to private corporations in matters concerning the appointment of staff, the configuration of their organizational hierarchies, and the utilization of their properties. In the task of regulation, it is imperative that the TPI enlists experts with the requisite proficiency and secure the necessary supervisory technology to guarantee impartiality in both the supervisory processes and the resultant outcomes. On the other hand, as the ultimate measure of oversight concerning the governance of artificial intelligence systems, governmental agencies are vested with the capacity to oversee the activities of these independent regulators. The agency of a credit rating mechanism through independent third-party institutions, coupled with the incorporation of societal oversight, empowers the citizenry to contest and scrutinize the conclusions of third-party independent institution. In instances where a third-party independent institution engages in deregulation, it is within the purview of the government to enact punitive measures. This also stands as a testament to the liability cost associated with non-compliance by third-party independent institutions.

3.1.3. Cost of the Artificial Intelligence Company

The operationalization of regulatory policies for artificial intelligence (AI) presents a dichotomy for corporations, necessitating a choice between adherence and non-compliance, which results in compliance costs and violation costs. The compliance expenditures borne by multinational AI enterprises are not uniform but instead fluctuate across various regions. The European Union's Artificial Intelligence Act serves as a paradigm, endowing national regulatory authorities with the capacity to requisition any pertinent information, encompassing source codes, software, and datasets. Entities responsible for AI models must assure adequate standards of performance, predictability, interpretability, correctability, and safety throughout the model's lifecycle. When an enterprise's AI system is classified as high-risk, its compliance activities within the European jurisdiction require the formation of a department dedicated to Artificial Intelligence Act adherence, tasked with devising a comprehensive risk management strategy spanning the AI technology's entire lifecycle, from its development to deployment. During the development phase, the institution of compliance mechanisms for data and knowledge is essential, necessitating the organization of human resources to oversee all training, validation, and testing of datasets, as well as the verification of their authenticity and lawfulness. Should the textual, visual, or auditory content potentially transgress the intellectual property rights of others, it becomes incumbent upon the legal department to ascertain the involvement of intellectual property rights, with particular emphasis on copyrights and trade secrets. It must also evaluate the robustness and efficacy of these rights, along with the implications of any infringing behaviors. In circumstances where there is an inability to access public knowledge or alternative datasets, the enterprise may be compelled to incur the costs associated with acquiring the necessary permissions. Illustrative of the financial penalties for non-compliance, in 2019, the French national data protection authority imposed a fine of €50 million on Google for deficiencies in disclosing its data processing undertakings in alignment with the requirements set forth by the General Data Protection Regulation (GDPR). Although this fine did not constitute a substantial proportion of Google's revenues, it nonetheless exerted an impact on the firm's financial health. To adhere to the AI regulatory demands of various nations and territories, numerous companies find themselves obligated to invest substantially in the realignment of internal systems, the refinement of processes, and the management of data compliance. For instance, multinational entities may be necessitated to modify their data processing approaches and algorithm designs to conform to the disparate privacy and data protection statutes of the multiple jurisdictions in which they operate.

In the context of artificial intelligence development, it is imperative that the data and knowledge sources utilized for AI training are legally procured and should not contravene intellectual property rights, trade secrets, nor partake in any form of unfair competition. Presently, AI companies are increasingly specialized within their respective vertical fields, necessitating the acquisition of substantial amounts of specialized data. Should AI companies require authentic and specialized data,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2082.v1

they are to procure these through methods that are unique, lawful, and expedient. Pursuant to Article 55 of the Personal Information Protection Law(PIPL), AI firms are mandated to evaluate the impact of their use of personal information within the realms of automated decision-making and data training and processing, ensuring a thorough consideration of data characteristics, quality, and sensitivity. It is essential that data are classified with precision, safeguarded by appropriate security measures, and utilized in a manner that maximizes their value while concurrently safeguarding data security and privacy. Furthermore, AI-generated content must comply with legal standards. Such content must not transgress legal prohibitions or contain discriminatory material based on nationality, belief, region, gender, age, profession, or health status. Service providers who encounter unlawful content are required to take prompt actions to halt its generation and dissemination, eliminate it, engage in model optimization and training to address the issue, and report the incident to the appropriate authorities. This process mandates human oversight to preclude situations that might compromise safety or the physical and mental well-being of individuals. Noncompliance with management protocols or disregard for national and regional regulatory policies may provide artificial intelligence enterprises with short-term savings on compliance expenditures. However, there may also need to pay for the violation cost because they could risk encountering administrative sanctions, the accrual of negative credit records, trade restrictions, or diminished market influence. Consequently, these potential repercussions ought to be factored into the cost-benefit analysis of compliance the legal regulation.

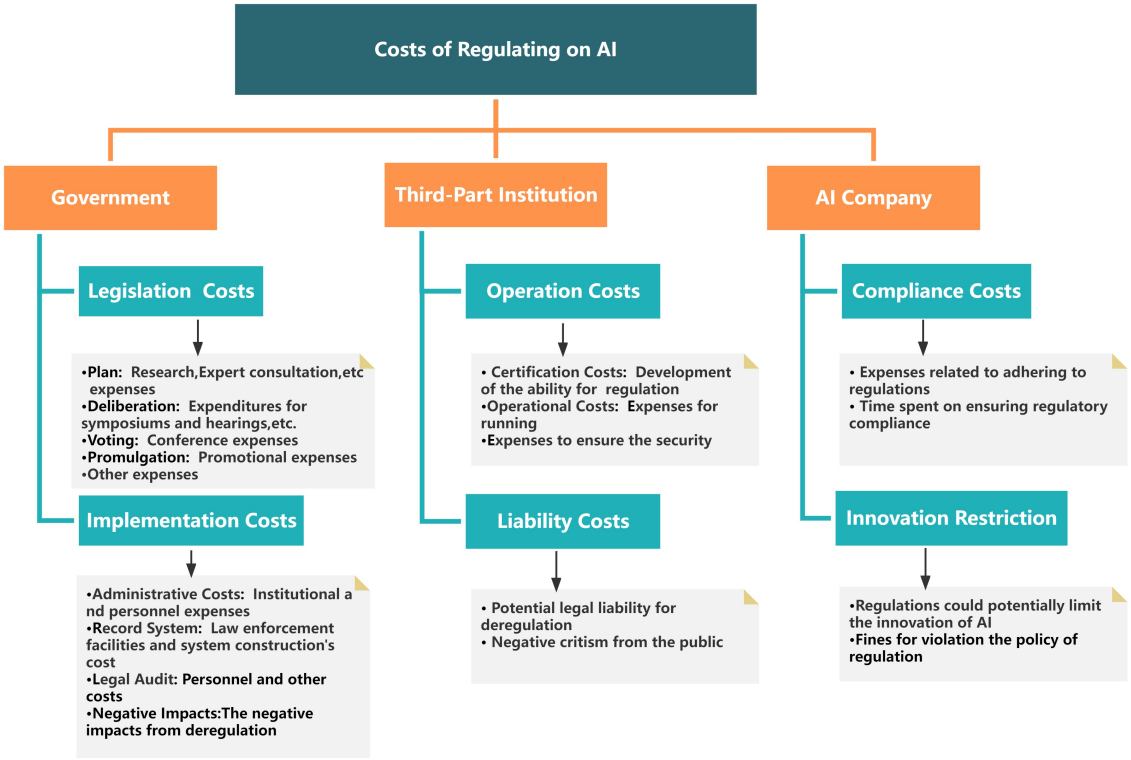

Figure 3. Costs of different subjects in the regulatory framework.

3.2. The Benefits of Regulating Artificial Intelligence

For the government or TPI, the benefit of regulation lie in the optimal allocation of resources and the controlled development of resources through the implementation of laws and regulations to maximise productivity and overall social welfare. Regulating AI is not intended to hinder its development, but to embed human production relations for improved productivity, while managing the risks associated with AI technology. Firstly, in the AI age, it is apparent that people pursue social dignity, security, order, freedom, justice, and public welfare. Through the development and

 doi:10.20944/preprints202312.2082.v1

implementation of controllable AI technology in all areas of social governance, the level of social security can be significantly enhanced while reducing the occurrence of crimes. AI can also be deployed to help people better respond to emergencies, such as natural disasters and public health events, and to improve emergency response capabilities. Regulated development of AI can reduce the threat of challenges to human dignity, security and social order, while maximizing the creation of additional wealth and promoting freedom and justice. Secondly, the public should abide by AI-related laws and regulations and use AI technology to enhance the value of the individual. Guidelines and standards must be followed by citizens when using AI technology to secure data, protect privacy, and ensure ethical behaviour. AI technology should be utilised for learning and creation in compliance with the law. In the conventional methodology of acquiring knowledge, one must read books, articles, and reports to gather pertinent information. This process is both time-consuming and inefficient. However, with the aid of Artificial Intelligence (AI) technology, we can conveniently extract knowledge and information through search engines, recommendation systems, natural language processing, and other AI-based instruments. This advanced technology eases the process of information processing and analysis. In the traditional method of processing information, a significant amount of data and information must be manually filtered, classified, and analyzed. This approach is not only prone to errors but also highly inefficient. With the aid of artificial intelligence technology, we can effectively automate the processing and analysis of vast amounts of data and information by utilizing machine learning, deep learning, and other relevant technologies. Machine learning algorithms are capable of automatically classifying, identifying and analysing vast quantities of images, audio, video and other unstructured data. With the help of deep learning technology, it can also automatically analyse, comprehend and create large quantities of textual data. Moreover, AI technology can expedite ideas and work. Creative workers and scientists alike may employ artificial intelligence to assist with early research inspiration. Thirdly, the enhancement of overall social productivity is expected as AI technology evolves. General AI-powered robots will increasingly undertake a greater proportion of work, restructuring employment and refining job requirements. Although some repetitive and perilous jobs may become automated, others that demand highly skilled professionals will become even more important. Ultimately, this shift will support economic and social development and positively transform the job-market landscape. By enhancing the structure of employment, innovative talents can invent new scientific and technological advancements, facilitate the modernization and metamorphosis of conventional industries, and boost the advancement and expansion of nascent industries. This will, in turn, bring forth opportunities and challenges to society, while furthering the sustainable development and prosperity of the economy.

AI companies' corporate gains encompass both direct and indirect benefit. Direct benefit may be reflected in the acquisition of users in the process of providing services. If an AI company were to operate in compliance, it would incur expenses to ensure the security and control of data, algorithms and services. This would attract a significant number of users and generate value by offering a tailored experience, optimizing decision support, enhancing production efficiency, innovating products and services, and refining customer services. These methods can assist enterprises in elevating their market share and profit margin, thereby augmenting their competitiveness and sustainable development ability. Indirect benefit arises from the fact that regulatory errors bring down the risk associated with AI and bolster social trust. In the AI decision-making process, the public is likely to trust the AI system more if they comprehend the algorithmic mechanism governing the AI's decision-making. Therefore, regulators may request that AI system owners or developers provide an in-depth explanation of how AI reaches its decisions. Moreover, for AI systems in sectors of high risk, such as medical diagnostic tools or self-driving cars, regulators can request that developers provide interpretable algorithms allowing for liability determination and compensation when necessary. For AI service providers or developers involved in personal information security and privacy, the development of rigorous privacy and data security systems by companies to ensure that AI systems securely and compliantly collect,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2082.v1

store and use personal data will alleviate concerns about AI system data privacy and security held by the public.

4. Behavioural Evolution in the Regulatory Framework

In the foregoing, we analyze the cost and benefit that may arise for different subjects in the legal relationship of regulating AI, including the government, Third-Party Institutions (hereinafter referred to as the TPI), and AI companies. Next, we apply evolutionary game theory to further analyze the impact of cost and benefit on the behavior of each subject. The main parameters and their implications are as shown in Table1.

Hypothesis 1. *This paper assumes that the main players in the game are the government, the TPI and the AI company. However, none of these entities has complete knowledge of the intricacies of regulating artificial intelligence or the broader socio-economic landscape. Furthermore, they lack the ability to develop the most effective oversight or business strategies, making them limited in their rationality.*

Hypothesis 2. *In the context of regulation process, the government, TPI, and AI company each have two distinct strategies. The probability of the government choosing "regulation" is denoted as* ***y1****, while the probability of selecting "no regulation" is represented as* ***(1-y1)****. Likewise, the probability of the TPI opting for "regulation" is* ***y2****, and the probability of selecting "no regulation" is* ***(1-y2)****. Similarly, the likelihood of the AI company opting for "compliant operation" is* ***y3****, while the possibility of selecting " illegal operation" is* ***(1-y3)****. The constants* y_1*,* y_2*, and* y_3 *all take values in the interval* $[0, 1]$*. We define a positive strategy as one that involves regulation or compliance, whereas a negative strategy is characterized by the absence of regulation or non-compliance.*

Hypothesis 3. *In the case that governmental regulation is opted for, resources must be allocated to enhance technology, resulting in a cost of* ***C1****. When the government implements a regulatory strategy, it stands to gain benefits denoted as* ***U1****, as long as either one of the TPI or AI company opts for a proactive approach. In the event that the government imposes regulation, and both TPI and AI company employ negative tactics, the government stands to gain an additional benefit denoted as* ***F****. If the government does not regulate, then the government's gain from either the TPI or the AI company adopting a positive strategy is* ***U2****. In the absence of government regulation, the TPI and AI company may opt for a negative strategy, which could result in a negative public perception of the government, referred to as* ***N****.*

Hypothesis 4. *In pursuit of economies of scale and to ensure the sustainable regulation, the TPI must opt for compliance regulation of both the TPI itself and AI company. To achieve this, the TPI will invest in big data, blockchain and cloud computing technologies, and employ specialised personnel to implement the regulatory strategy. The regulatory costs incurred due to investment in personnel, technology and infrastructure are denoted by* ***C2****, and the resulting operating benefit is denoted by* ***I1****. Alternatively, the TPI may choose a non-regulatory strategy, which incurs no regulatory costs, but results in an operating benefit of* ***I2*** *due to the unregulated development. However, this may lead to a decline in the social reputation of the TPI and possible punishment by the government, denoted by* ***F****. Regardless of whether the government exercises regulation or not, if the TPI fails to regulate, it may incur additional comprehensive losses which can be represented by the loss value as* ***S****.*

Hypothesis 5. *AI company face two choices: compliance operation and illegal operation. AI company utilise their professional expertise to provide AI technology for society and earn a basic income of W, while incurring an operating cost of* ***C3****(****C3*** *is not infinite and its value is less than* ***W****). If the AI company opts for compliance operation services, it gains market reputation due to its professional and compliant services, yielding additional economic benefits represented as* ***W1****. Conversely, if the AI company adopts an illegal business strategy, it generates an operating benefit of* ***W2*** *through over-the-counter transactions or illegal charges. In the event that the TPI detects illegal activities operated by the AI company, the latter incurs a punishment denoted as* ***F2*** *from the TPI.*

 doi:10.20944/preprints202312.2082.v1

Table 1. Main Parameters and their Implications.

Subject	Behavior	Parameter	Implication
Government	Regulation	y1	The probability of government regulation
		U1	Positive social benefits for government when the TPI proactively regulate
		U2	Partial social benefits for government
		C1	The regulatory cost of government
	Deregulation	1-y1	Probability that the government will not regulate
		N	The negative social impact on the government becomes apparent when the government and the TPI both deregulate
Third-Party Institution(TPI)	Regulation	C2	The comprehensive cost of the TPI's own regulatory costs
		I1	The eds from compliance operation when the TPI regulates
		y2	The probability of the TPI adopting a regulatory strategy
	Deregulation	I2	Short-term gains obtained when the TPI does not regulate
		F	The TPI 's fine by the government for AI company' violations
		S	The total loss due to the TPI's failure to fulfil its regulatory obligations
		1-y2	The probability that the TPI does not regulate on AI company
AI Company	Compliance with regulations	W	Basic income of the compliance operation of the AI company
		C3	The cost of running a compliance operation for AI company
		W1	Surplus revenue generated by AI company's compliance activities
		y3	Probability of the AI company's compliance operation
	Violate regulations	W2	The additional economic benefits of the illegal activities of the AI company
		F2	the TPI's punishment on illegal AI company
		1-y3	Possibility of the AI company violating regulations

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2082.v1

4.1. Legal Behavior and Expected Payoff

As previously mentioned, each player has two strategic options, resulting in eight possible combined legal behavior. In an effort to streamline our analysis, we will examine these three types of participants in various contexts. As shown in Table 2, through implementation of the payoff matrix [51], the expected payoff of each subject can be attained.

Table 2. Payoff Matrix

AI Company / Government / TPI	Regulation	No Regulation
Regulation, Compliance	U1-C1,I1-C2,W-C3+W1	U2,I1-C2,W-C3+W1
Regulation, Violation	U1-C1,I1-C2+F2,W-C3+W2-F2	U2,I1-C2+F2,W-C3+W2-F2
No Regulation,Compliance	U1-C1,I2,W-C3+W1	U2,I2,W-C3+W1
No Regulation, Violation	U1-C1+F,I2-F-S,W-C3+W2-F2	-N,I2-S,W-C3+W2

As evident from the payoff matrix, there exist corresponding payoffs for the stochastic behaviors exhibited by the government, the TPI, and the AI company. In the course of their interaction, the conduct of these three parties may undergo changes over time, leading to the evolution of rewards associated with their behaviors, which can be described by the the Malthusian dynamic equation [52]. Then, our dynamic equation becomes

$$F1 = \frac{dy1}{dt} = y1 \times (y1 - 1) \times (C1 - F - N - U1 + F \times y2 + F \times y3 + N \times y2 + N \times y3 + U2 \times y2 + U2 \times y3 - F \times y2 \times y3 - N \times y2 \times y3 - U2 \times y2 \times y3) \quad (1)$$

$$F2 = \frac{dy2}{dt} = y2 \times (y2 - 1) \times (C2 - F2 - I1 + I2 - S - F \times y1 + F2 \times y3 + S \times y3 + F \times y1 \times y33) \quad (2)$$

$$F3 = \frac{dy3}{dt} = y3 \times (C3 - W - W2 + F2 \times y1 + F2 \times y2 - y1 \times y2 - C3 \times y1 \times y2 - F2 \times y1 \times y2 + W \times y1 \times y2 + W1 \times y1 \times y2 + 1) \quad (3)$$

4.2. Stability of different subjects'behavior

In this section, we use matlab R2014 as a computational and simulation tool. Based on the method of Friedman [52], The Jacobi matrix of the system can be used to discuss the local stability of the equilibrium point. The Jacobi matrix of the dynamic system of equations is as follows

$$J = \begin{bmatrix} \frac{\partial F1}{\partial y1} & \frac{\partial F1}{\partial y2} & \frac{\partial F1}{\partial y3} \\ \frac{\partial F2}{\partial y1} & \frac{\partial F2}{\partial y2} & \frac{\partial F2}{\partial y3} \\ \frac{\partial F3}{\partial y1} & \frac{\partial F3}{\partial y2} & \frac{\partial F3}{\partial y3} \end{bmatrix} \quad (4)$$

Based on Taylor and Jonker's theory [53], the hybrid equilibrium point possesses a pair of eigenvalues, with negative real parts, indicating it as the steady stable equilibrium point of the system. The system's evolutionary trajectory forms a stable spiral loop, where Mixed equilibrium point serves as the stable central point. Then we can use the Lyapounov method to demonstrate that there are ten equilibrium points for the above Jacobi Matrix and these points are progressively stable point [53]. These ten equilibrium points are then substituted into the Jacobi matrix to obtain ten eigenvalues. The following, we will analyze the evolutionary trend of the system under changing initial conditions.

Example 1. *The first equilibrium point is* $[0, 0, 0]$*, where both the government, TPI and AI company take negative strategy. The matrix after substitution of the 1st equilibrium into the Jacobi matrix can be obtained as*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2082.v1

$$\begin{bmatrix} F-C1+N+U1 & 0 & 0 \\ 0 & F2-C2+I1-I2+S & 0 \\ 0 & 0 & C3-W-W2+1 \end{bmatrix} \tag{5}$$

So we can hold three eigenvalues as (F - C1 + N + U1),(F2 - C2 + I1 - I2 + S)and(C3 - W - W2 + 1). Additionally, we can simulate the interactive behaviour evolution process of the government, TPI and AI company. We assume the probability for each subject of the Government, TPI and AI company are the same. The initial time is 0, the evolution end time is 2, and the initial probability state is$(0.5, 0.5, 0.5)$. The parameter values were $U1 = 1; U2 = 5; C1 = 10; I1 = 2; C2 = 12; I2 = 6; F = 4; S = 2; W1 = 7; C3 = 2; W2 = 5; N = 1; F2 = 3; W = 4$. The simulation experiment results are shown in Figure 4.

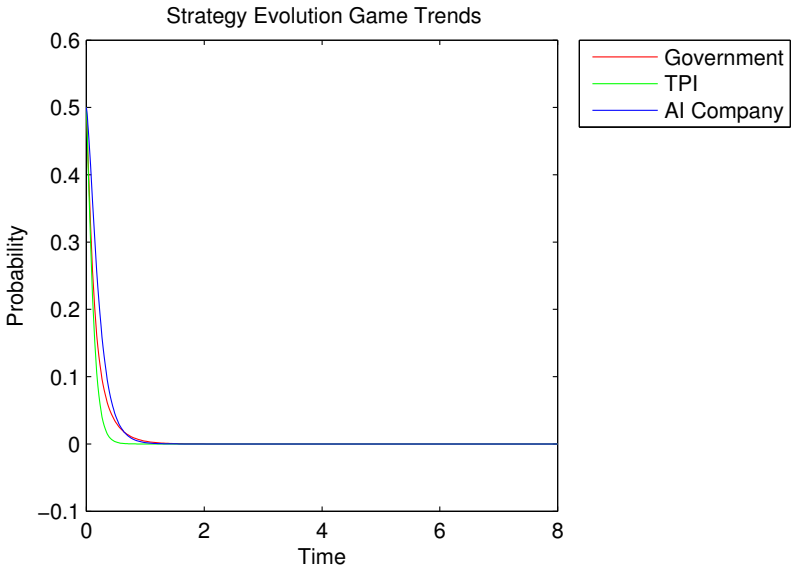

Figure 4. Simulation diagram of Example 1.

Example 2. *The second equilibrium point is* $[0, 1, 0]$*, where the government and the AI company choose negative strategy while the TPI choose positive strategy. In this situation, we can see the TPI take the main responsibility to regulate the security of AI. The matrix after substitution of the equilibrium into the Jacobi matrix can be obtained as*

$$\begin{bmatrix} U1-C1-U2 & 0 & 0 \\ 0 & C2-F2-I1+I2-S & 0 \\ 0 & 0 & C3+F2-W-W2+1 \end{bmatrix} \tag{6}$$

So we can hold three eigenvalues as (U1 - C1 - U2),(C2 - F2 - I1 + I2 - S)and(C3 + F2 - W - W2 + 1). The same method likewise, we can simulate the interactive strategy evolution process of the government, TPI and AI company and analyze the influence of each parameter change on the evolution results. We assume the probability for each subject of the Government, TPI and AI company are the same. The initial time is 0, the evolution end time is 8, and the initial probability state is$(0.5, 0.5, 0.5)$. The parameter values were $U1 = 1; U2 = 5; C1 = 10; I1 = 20; C2 = 12; I2 = 6; F = 4; S = 2; W1 = 7; C3 = 2; W2 = 5; N = 1; F2 = 3; W = 4$. The simulation experiment results are shown in Figure 5.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 December 2023 doi:10.20944/preprints202312.2082.v1

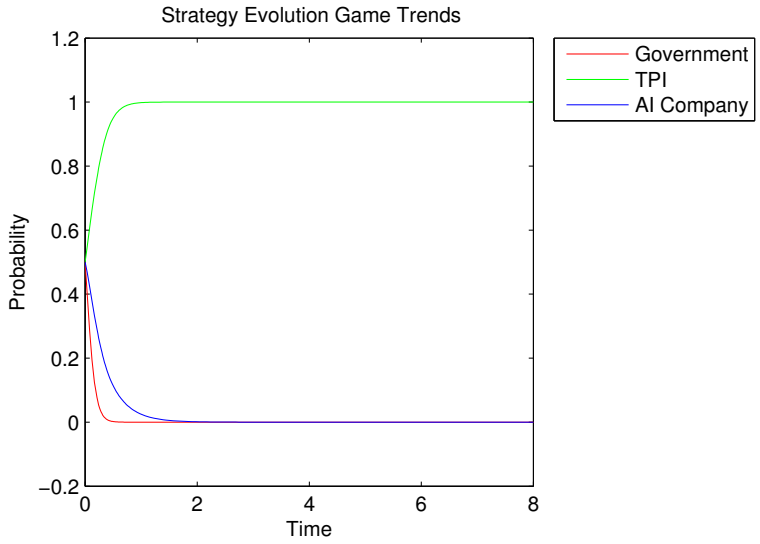

Figure 5. Simulation diagram of Example 2.

Example 3. *We will now examine a more specific example of the equilibrium point as* $[1,1,1]$*, where the government, TPI and AI company choose positive strategy. In this situation, with the regulation of government and TPI, the AI company also select a Compliance Strategy. The matrix after substitution of the equilibrium into the Jacobi matrix can be obtained as*

$$\begin{bmatrix} C2-I1+I2 & 0 & 0 \\ 0 & C1-U1+U2 & 0 \\ 0 & 0 & W2-W1-F2 \end{bmatrix} \tag{7}$$

So we can hold three eigenvalues as (C2 - I1 + I2),(C1 - U1 + U2)and(W2 - W1 - F2). The same method likewise, we can simulate the interactive strategy evolution process of the government, TPI and AI company and analyze the influence of each parameter change on the evolution results. We assume the probability for each subject of the Government, the TPI and AI company are the same. The initial time is 0, the evolution end time is 8, and the initial probability state is$(0.5, 0.5, 0.5)$. The parameter values were $U1 = 10; U2 = 5; C1 = 2; I1 = 8; C2 = 2; I2 = 5; F = 4; S = 2; W1 = 6; C3 = 2; W2 = 5; N = 1; F2 = 2; W = 4$. The simulation experiment results are shown in Figure 6.

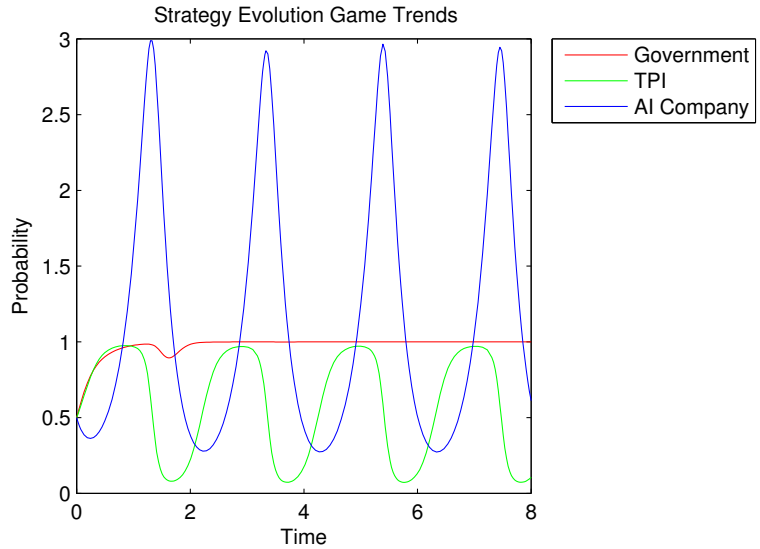

Figure 6. Simulation diagram of Example 3.

 doi:10.20944/preprints202312.2082.v1

The simulation of other cases on the evolutionary results can be tested using the methods above and are not discussed further here. Current deliberations regarding the legal framework governing artificial intelligence (AI) remain ongoing, particularly in the absence of specific legislative measures addressing the cost-benefit analysis of real case data. However, this section offers a novel approach that employing evolutionary game theory to simulate the legal behavior of different subjects in regulating AI's legal relationships. This method enables a detailed examination of the varying cost and benefit trends associated with different behavioral subjects within AI's sphere. Such an analysis could potentially offer substantial theoretical support to the development of a comprehensive legal framework for AI regulation.

4.3. Simulation Results of the Behavior of Three Subjects

In this part, we provide novel insights into the influencing factors governing the behavior of the government, TPI, and AI company, based on previous simulation results.

Figure 4 clearly illustrates that when the costs of government regulation are high enough to exceed the sum of the positive social benefits, negative social impacts and corresponding fines that it can reap, the probability of regulation falls sharply over time and eventually tends to zero. The trend in the probability of regulation for TPI follows a similar pattern to that for governments, in that if the sum of the costs of regulation and the short-term benefits of non-regulation is too high, the incentives for TPI to regulate are clearly lacking, and the probability of their regulation eventually tends to zero as well. In addition, if the benefits of breaking the law are high enough for AI companies, their probability of compliance also decreases over time. Figure 5 provides further verification of our assumes. In Figure 5, the probability of TPI engaging in regulation gradually increases and ultimately converges to 100 per cent when the sum of costs of regulation are effectively controlled and the benefits from complying with regulation outweigh the short-term benefits of non-compliance. The trends in the probability of government and AI company taking proactive measures follow a pattern similar to that seen in Figure 4, and are not repeated here for the sake of brevity. As is illustrated in Figure 6, the probability curve of government regulation demonstrates a stable trend following its peak, whereas the probability distributions of TPI and AI company regulation exhibit cyclical fluctuations. During the initial phase, both government and TPI's regulation rapidly ascend and attain a steady regulatory state, suggesting that their regulatory policies can maintain a certain level of congruity, thereby fostering a synergistic regulatory model. Nonetheless, the proportion of AI company who elect to operate in compliance experiences a slight decline in the initial stage and subsequently plummets to its lowest ebb, at which juncture only a minuscule fraction of AI company opt for compliance. Under the government's macro-regulatory policy direction, TPI are able to emulate this by investing in regulatory measures to rigorously manage any violations. This dual supervision from both the government and TPI enables AI company to align their business practices with relevant laws and policies, thus gradually promoting the normalization of the AI industry. Consequently, an increasing number of AI company elect to operate in a compliant manner, enhancing their business service capabilities, expanding their revenue, and effectively managing their costs. With the continuous enhancement of compliance constructs, AI company commonly adhere to service laws and gain substantial benefits through compliant practices. This, in turn, attracts a larger proportion of AI companies to actively embrace compliant behavior, resulting in a rapid increase in this trend and a further expansion of the industry scale. However, the trend behind the curve also reveals other disparities among different entities. In contrast, the probability of TPI choosing to regulate plummets rapidly after reaching an inflection point. As the probability of TPI choosing positive regulatory policy declines, it is clear that the probability of AI company being compliant also declines, and ultimately both sides fall to their lowest point. Upon examining the entire figure, it becomes evident that once the government's regulatory policy stabilizes, the probability of TPI electing to regulate and AI company choosing compliant behavior becomes irrespective of the government's regulatory approach.

 doi:10.20944/preprints202312.2082.v1

Combine this with the three figures above, we can clearly observe that the probability of governments and TPI taking regulatory action as well as AI company operating in a compliant manner is closely linked to the costs and benefits of the respective subjects. This finding also indicates that the promulgation and implementation of regulatory laws alone cannot guarantee the desired regulatory effects.

5. Discussion And Conclusion

This paper engages in a scholarly examination of the nascent criteria constituting the regulatory framework for artificial intelligence (AI). Our key findings have confirmed the influence of costs and benefits on the behavior of different subjects in the legal relationship of regulating artificial intelligence. Many studies has noted legal framework is necessary for regulating artificial intelligence, but most studies only focus on the discussion of legal framework at the macro level. Previous studies have analyzed policies to regulate AI from the perspective of a single discipline, such as law, management or computer science, with topics focusing on ethics, value judgements and regulatory processes [54]. However, there is still a lack of research on the the criteria of regulatory framework on artificial intelligence. Based on this, we discuss the impact of costs and benefits on the the behavior of different subjects in the legal relationship of regulation on AI. The results show that the imperative to regulate AI emerges from the inherent risks associated with safety breaches and violations of intellectual property that are concomitant with the application of such technologies. Absent regulatory oversight, these risks pose a formidable threat to human welfare and the expanse of innovative activity. In the arena of legal enactment, it is elucidated that the proportions of costs to benefits are pivotal in influencing the behavioral inclinations of governments, third-party institutions (TPIs), and AI enterprises towards legal compliance or contravention. While it is posited that cost-benefit considerations wield substantial influence over the strategic choices of entities such as governments, TPIs, and AI companies, our research uncovers a peculiar dynamic wherein the regulatory interplay between TPIs and AI companies manifests cyclical fluctuations, even as governmental regulatory efforts reach a plateau of stability. This phenomenon, resonant with the metaphor of Adam Smith's 'invisible hand' [55], intimates that government agencies need not perpetually escalate their regulatory investments in AI. Such amplifications in regulatory spending are found to be ineffectual in altering the capricious behavioral patterns of other market constituents within the AI milieu, aligning with the concept of diminishing marginal utility [56]. The discovery of this cyclicality and the associated diminishing returns on governmental regulatory investment underscore the multifaceted challenges inherent in governing burgeoning technologies like AI. Market dynamics, the impetus for innovation, and the mutable conduct of industry stakeholders collectively elude comprehensive governance through unilateral regulatory interventions. This insight suggests that efficacious regulation may necessitate auxiliary approaches, inclusive of industry self-regulation, the adoption of ethical frameworks, or the creation of market-based incentives, to fully engage with the intricacies and issues pervading the AI domain. In the endeavor to craft a regulatory framework that is consonant with the specific realities of a nation, a risk classification system should be devised with due consideration to the nation's unique context. Subsequent to this classification, it is imperative that a legislative framework be established to clearly define the rights and obligations of the implicated parties. For instance, within the domain of security or innovation, where AI poses distinct challenges, it is the government's role to assume primary responsibility, ensuring rigorous regulatory oversight. Conversely, for managing other risk types, such as those pertaining to the security of property, the participation of a third-party independent institution is advocated to develop a co-regulation model. This model would operate with market mechanisms at the forefront, underpinned by a governmental foundation, ensuring a balanced and responsive regulatory environment. This dual-structured oversight aims to facilitate both the thriving of AI technologies and the safeguarding of societal interests. In summary, artificial Intelligence (AI), much like the steam engines and generators that catalyzed the Industrial Revolution, is a tool that propels the advancement of productivity. It is incumbent upon governments to adopt an approach

that is both inclusive of technological advancements and cautious in the face of potential disruptions wrought by AI. The study posits that there may exist intrinsic limitations to the impact of escalated governmental investment in the regulatory sphere, especially with respect to mitigating volatility in legal compliance behaviors within the AI industry. The implications for policymakers and regulatory bodies are clear: there is a need for a judicious and integrated approach that accounts for the rapid evolution and inherent complexities of the technology sector. Such an approach must strike a balance between direct regulation and the facilitation of industry-led governance mechanisms to navigate the challenges presented by AI.

These insights are of great significance in guiding the optimization of regulatory framework, while also providing a solid theoretical foundation for the development of relevant policies. There are still shortcomings in the existing research:

Quantitative Data on Cost-benefit: The first limitation is the difficulty in collecting quantitative data on the cost-benefit of law implementation in different countries and regions. This limitation can restrict the extent to which our findings can be generalized. Future research should aim to gather real-world data from various countries and regions to provide a more comprehensive understanding of the impact of AI regulation.

Scope of Risks: The second limitation is this research primarily examining one aspect of the risks associated with AI. In practice, AI presents various risks, not merely legal risks, but also including ethical, privacy, security, and economic considerations. Future studies could expand to encompass a broader range of AI-related risks and how they are addressed through legal frameworks, including delving into the legal and ethical aspects of data usage in AI.

Multidisciplinary Perspectives: The third limitation is this research focuses on cost-benefit analysis. However, it's essential to acknowledge that regulatory decisions are influenced by various factors, including ethical, social, and political considerations. Future research can benefit from a multidisciplinary approach, incorporating perspectives from fields such as ethics, sociology, and political science to provide a more comprehensive understanding of AI regulation.

Legal design is indeed a complex process that extends beyond cost-benefit analysis. Researchers can explore alternative theories and approaches, such as ethical frameworks, to analyze and design regulations that are both effective and ethically sound. In conclusion, our research serves as a valuable starting point for understanding the cost-benefit analysis of AI regulation. To address the identified limitations and enhance the robustness of AI regulatory policies, future research should aim to collect real data, broaden the scope of risks, consider intellectual property implications, adopt a multidisciplinary approach, and explore various theoretical perspectives in the field of AI regulation.

References

1. S. M. J., *The Case Against Perfection: Ethics in the Age of Genetic Engineering*. Cambrige: Harvard University Press, 2007.
2. T. Kristensen, *Artificial Intelligence: Models, Algorithms and Applications*. Bentham Science Publishers, 2021. [Online]. Available: https://books.google.com.tr/books?id=DDY0EAAAQBAJ
3. Price Waterhouse Coopers (2017), 'Sizing the Prize', Available:www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf (Accessed: 13-Oct-2023).
4. A. Sarabi, P. Naghizadeh, Y. Liu, and M. Liu, "Risky business: Fine-grained data breach prediction using business profiles," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 15–28, 2016.
5. Future of Life Institute,*Pause Giant AI Experiments: An Open Letter*, Available:https://futureoflife.org/open-letter/pause-giant-ai-experiments/(Accessed: 13-Oct-2023).
6. Sam Altman,*Planning for AGI and beyond*, Available:https://openai.com/blog/planning-for-agi-and-beyond(Accessed: 13-Oct-2023).
7. C. Calleja, H. Drukarch, and E. Fosch-Villaronga, "Harnessing robot experimentation to optimize the regulatory framing of emerging robot technologies," *Data & Policy*, vol. 4, p. e20, 2022.
8. DPC,*Case Studies 2018-2013 booklet*, Available:https://www.dataprotection.ie/sites/default/files/uploads/2023-09/DPC_CS_2023_EN_Final.pdf (Accessed: 28-Sep-2023).

9. IAPP,*PRIVACY RISKS STUDY 2023: Five highest, Additional priority privacy, top-ranked compliance risks, and emerging risks*, Available:https://iapp.org/media/pdf/resource_center/privacy_risk_study_infographic_2023.pdf (Accessed: 28-Sep-2023).
10. M. Saemann, D. Theis, T. Urban, and M. Degeling, "Investigating gdpr fines in the light of data flows," *Proceedings on Privacy Enhancing Technologies*, vol. 4, pp. 314–331, 2022.
11. K. Barnett, *Google's $400m penalty and impact of the 5 heftiest data privacy fines on 2023 ad plans*, Available:https://www.thedrum.com/news/2022/11/15/googles-400m-penalty-the-impact-the-5-heftiest-data-privacy-fines-2023-ad-plans(Accessed: 28-Sep-2023).
12. Cyberspace Administraion of China, *National Cyber Enforcement Efforts Continue to Grow in Effectiveness In 2022*, Available:http://www.cac.gov.cn/2023-01/19/c_1675676681798302.htm(Accessed: 28-Sep-2023).
13. Fanny Potkin, Supantha Mukherjee,*Exclusive: Southeast Asia eyes hands-off AI rules, defying EU ambitions*, Available:https://www.reuters.com/technology/southeast-asia-eyes-hands-off-ai-rules-defying-eu-ambitions-2023-10-11/(Accessed: 13-Oct-2023).
14. J. M. Balkin, "The path of robotics law," *Calif. L. Rev. Circuit*, vol. 6, p. 45, 2015.
15. T. Wischmeyer and T. Rademacher, *Regulating artificial intelligence*. Springer, 2020, vol. 1, no. 1.
16. COE,*What's AI?*, Available:https://www.coe.int/en/web/artificial-intelligence/what-is-ai(Accessed: 15-Oct-2023).
17. N. Nilsson, *Artificial Intelligence: A New Synthesis, Elsevier Science,1998*.
18. European Commission,*A definition of AI: Main capabilities and disciplines, Independent High Level Expert Group on Artificial Intelligence set up by the European Commission, Brussels*.
19. Inga Ulnicane,*Artificial intelligence in the European Union: Policy, ethics and regulation*.
20. Pei Wang,*What do you mean by 'AI', Artificial General Intelligence 2008-Proceedings of the First AGI Conference.*Amsterdam: IOS Press, pp.362-372,2008.
21. S. Hadzovic, S. Mrdovic, and M. Radonjic, "A path towards an internet of things and artificial intelligence regulatory framework," *IEEE Communications Magazine*, 2023.
22. N. A. Manap and A. Abdullah, "Regulating artificial intelligence in malaysia: The two-tier approach," *UUM Journal of Legal Studies*, vol. 11, no. 2, pp. 183–201, 2020.
23. G.-Z. Yang, J. Bellingham, P. E. Dupont, P. Fischer, L. Floridi, R. Full, N. Jacobstein, V. Kumar, M. McNutt, R. Merrifield *et al.*, "The grand challenges of science robotics," *Science robotics*, vol. 3, no. 14, p. eaar7650, 2018.
24. M. Tschopp and H. Salam, "Spot on sdg 5: Addressing gender (in-) equality within and with ai," in *Technology and Sustainable Development*. Routledge, pp. 109–126,2023.
25. R. Rayhan and S. Rayhan, "Ai and human rights: Balancing innovation and privacy in the digital age," 2023.
26. A.C. Pigou,*The Economics of Welfare,*4th ed. (London: Macmillan, 1938).
27. CAHAI,*Ad hoc Committee on Artificial Intelligence*, Available:https://rm.coe.int/possible-elements-of-a-legal-framework-on-artificial-intelligence/1680a5ae6b (Accessed: 7-Nov-2023)
28. E. Fosch-Villaronga and M. A. Heldeweg, ""meet me halfway," said the robot to the regulation: Linking ex-ante technology impact assessments to legislative ex-post evaluations via shared data repositories for robot governance," in *Inclusive Robotics for a Better Society: Selected Papers from INBOTS Conference 2018, 16-18 October, 2018, Pisa, Italy*. Springer, pp. 113–119, 2020.
29. J. Zhao and B. Gómez Fariñas, "Artificial intelligence and sustainable decisions," *European Business Organization Law Review*, vol. 24, no. 1, pp. 1–39, 2023.
30. S. Chatterjee, "Impact of ai regulation on intention to use robots: From citizens and government perspective," *International Journal of Intelligent Unmanned Systems*, vol. 8, no. 2, pp. 97–114, 2019.
31. H. Sheikh, C. Prins, and E. Schrijvers, *Mission AI: The New System Technology*. Springer Nature, 2023.
32. M. C. Buiten, "Towards intelligent regulation of artificial intelligence," *European Journal of Risk Regulation*, vol. 10, no. 1, pp. 41–59, 2019.
33. A. Y. Lau, P. Staccini *et al.*, "Artificial intelligence in health: new opportunities, challenges, and practical implications," *Yearbook of medical informatics*, vol. 28, no. 01, pp. 174–178, 2019.
34. C. Reed, "How to make bad law: lessons from cyberspace," *The Modern Law Review*, vol. 73, no. 6, pp. 903–932, 2010.
35. A. O'Sullivan and A. Thierer, "Counterpoint: regulators should allow the greatest space for ai innovation," *Communications of the ACM*, vol. 61, no. 12, pp. 33–35, 2018.

36. C. H. Hoffmann and B. Hahn, "Decentered ethics in the machine era and guidance for ai regulation," *AI & society*, vol. 35, pp. 635–644, 2020.
37. C. Reed, "How should we regulate artificial intelligence?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 376, no. 2128, p. 20170360, 2018.
38. C. T. Marsden, *Net neutrality: Towards a co-regulatory solution*. Bloomsbury Academic, 2010.
39. A. Shleifer, "Understanding regulation," *European Financial Management*, vol. 11, no. 4, pp. 439–451, 2005.
40. R. Nozick, *Anarchy, state, and utopia*. John Wiley & Sons, 1974.
41. S. Djankov, R. La Porta, F. Lopez-de Silanes, and A. Shleifer, "Courts," *The Quarterly Journal of Economics*, vol. 118, no. 2, pp. 453–517, 2003.
42. S. Djankov, E. Glaeser, R. La Porta, F. Lopez-de Silanes, and A. Shleifer, "The new comparative economics," *Journal of comparative economics*, vol. 31, no. 4, pp. 595–619, 2003.
43. D. Zimmer, "Property rights regarding data?" p. 101, 2017.
44. C. Bloom, J. Tan, J. Ramjohn, and L. Bauer, "Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles," in *Thirteenth Symposium on Usable Privacy and Security*, pp.357–375,2017.
45. A. Winograd, "Loose-lipped large language models spill your secrets: The privacy implications of large language models," *Harvard Journal of Law & Technology*, vol. 36, no. 2, 2023.
46. R. Zahid, A. Altaf, T. Ahmad, F. Iqbal, Y. A. M. Vera, M. A. L. Flores, and I. Ashraf, "Secure data management life cycle for government big-data ecosystem: Design and development perspective," *Systems*, vol. 11, no. 8, p. 380, 2023.
47. R. S. Peck, "The coming connected-products liability revolution," *Hastings LJ*, vol. 73, p. 1305, 2022.
48. C. R. Sunstein, "The cost-benefit state: the future of regulatory protection." American Bar Association, 2002.
49. D. Baracskay, "Cost-benefit analysis: Concepts and practice," 1998.
50. A. Renda, L. Schrefler, G. Luchetta, and R. Zavatta, "Assessing the costs and benefits of regulation," *Brussels: European Commission*, 2013.
51. R. Axelrod and W. D. Hamilton, "The evolution of cooperation," *science*, vol. 211, no. 4489, pp. 1390–1396, 1981.
52. D. Friedman, "Evolutionary games in economics," *Econometrica: Journal of the Econometric Society*, pp. 637–666, 1991.
53. P. D. Taylor and L. B. Jonker, "Evolutionary stable strategies and game dynamics," *Mathematical biosciences*, vol. 40, no. 1-2, pp. 145–156, 1978.
54. A. Tallón-Ballesteros and P. Santana-Morales, "Policy regulation of artificial intelligence: A review of the literature," *Digitalization and Management Innovation: Proceedings of DMI 2022*, vol. 367, p. 407, 2023.
55. A. Smith, *The wealth of nations [1776]*. NA, vol. 11937,1937.
56. E. R. Hirt, J. J. Clarkson, and L. Jia, *Self-regulation and ego control*. Academic Press, 2016.