State, Society, and Market: Interpreting the Norms and Dynamics of China's AI Governance

Xuechen Chen (Northeastern University London)
Lu Xu (Lancaster University), correspondence: lu.xu@lancaster.ac.uk

The authors contributed equally and are listed in alphabetical order.

Abstract

This study challenges the prevailing perception of China's AI governance as a monolithic, state-driven model and instead presents a nuanced analysis of its complex governance landscape. Utilizing governance theories, we develop an analytical framework examining key governing nodes, tools, actors, and norms. Through case studies on minor protection and content regulation, this study demonstrates that Chinese AI governance involves a diverse array of stakeholders—including the state, private sector, and society—who co-produce norms and regulatory mechanisms. Contrary to conventional narratives, China's governance approach adapts existing regulatory tools to new challenges, balancing political, social, and economic interests. This study highlights how China has rapidly formalized AI regulations, particularly in generative AI and online content, setting a precedent in global AI governance. The findings contribute to a broader understanding of AI regulation beyond ideological binaries and offer insights relevant to international AI policy discussions.

Introduction

As a newly emerging and rapidly evolving technology, the development of Artificial Intelligence (AI) has profoundly impacted the global economy and international politics, with AI governance becoming a new terrain for geostrategic and regulatory competition among major international players. Recently, in light of China’s ambition to become world-leading in AI by 2030 (State Council 2017), the advancement of AI technologies and the development of a distinctive approach to regulating AI as a policy field in China have gained increasing traction in both academic and policy circles, leading to two interrelated lines of scholarly inquiry in the existing literature.

The first scholarly camp, primarily situated within the fields of Politics and International

Relations, has examined the evolution and key drivers of China's approach to AI governance[1], as well as its potential influence on emerging global AI governance. For example, some scholars, exemplified by Zeng, have argued that China's bold AI practices should be regarded as part of its wider, though incoherent, adaptation strategy to governance by digital means. From this perspective, AI forms a crucial component of a broader digital technology package that the Chinese authoritarian regime utilizes not only to enhance public service delivery but also to consolidate its authoritarian control (Zeng 2020, 2022). Zeng further explored a range of political and security-related considerations at domestic and international levels that constitute the key drivers of China's AI governance approach (Zeng 2022). Similarly, Tuzov and Lin examined China's path to AI governance, highlighting how the country has transitioned from an early laissez-faire approach to a security-focused AI development strategy underpinned by strong government intervention (Tuzov and Lin 2024). The nature of China's AI governance approach has been described as a model of 'fragmented authoritarianism' that seeks to strike a delicate balance between central government agencies and local government stakeholders, with the ultimate objective of 'supporting innovation, responding to and utilizing populism, and further enhancing central government control' (Roberts et al 2023). These discussions on China's AI governance model resonate with a broader debate over the nature of China's overarching approach to digital governance, often labelled as 'digital authoritarianism' (see for example Taylor 2022, Lilkov 2020). The key assumption is that China's practices in digital governance are primarily driven by its objective to strengthen its authoritarian regime and advance its political ambitions at both domestic and global levels (Ming and Narisong 2020, Daniëlle 2021).

The second line of inquiry, rooted in legal studies, has focused on how China has established an array of legal and regulatory frameworks in AI governance (Filipova 2024, Roberts H et al 2021, Sheehan 2023, Dong and Cheng 2024). In comparison to the International Relations scholarly discussions, which prioritize macro-level factors such as national security strategy, political stability, and state-level policymaking, legal scholars tend to provide more detailed examinations of the legal and regulatory dimensions of China's AI governance model. For instance, adopting the concept of 'meta-regulation', Dong and Chen (2024) analysed China's approach to regulating generative AI (GAI) as a specific sub-area of AI governance and argued

[1] In this paper, we adopt a broad conception of *AI governance* that extends beyond AI technologies in the narrow sense to encompass the wider ecosystem of internet governance, online platforms, and digital applications that are increasingly shaped by AI techniques. AI governance, in our usage, refers to the constellation of legal, political, social, and commercial mechanisms through which both AI-specific systems and AI-influenced digital infrastructures are regulated, directed, and contested. This broader scope is necessary because in the Chinese context, measures initially designed for internet or platform governance (such as identity verification or content moderation) have been adapted and redeployed to address challenges raised by AI, creating hybrid governance arrangements. Accordingly, while we foreground AI as the focal point, we situate it within the wider digital governance environment in which AI logics, tools, and norms are embedded.

that China's regulatory model is based on 'primary responsibility', which emphasizes constraining GAI service providers. Other scholars, such as Sheehan (2023), have provided an overview of key Chinese AI regulations to date and illustrated the key actors and stakeholders influencing policy processes. Similarly, Wang et al. analysed China's evolving AI laws and regulations, unpacking the interplay between fragmented legislation, standards, and sectoral governance frameworks (Wang et al 2024).

Despite the growing body of scholarly debate on this topic, numerous limitations exist in the current discussions. First, the mainstream international scholarship on Chinese AI governance (and digital governance more generally) tends to follow an interesting pattern. China is recognized for its concrete achievements, even comparative strengths, in the realms of technology development and application. However, anything China does is perceived primarily as serving the interests of the authoritarian state, the ruling Communist Party, and its leaders. If Chinese AI governance policies benefit the digital economy, it is because the economy is critical to the legitimacy of the Chinese Party-state. If China develops new technology, it is because technology enhances the state's surveillance and control capabilities. If ordinary Chinese people ostensibly enjoy the benefits of digitization, it is because this aligns with the government's priority of fostering a harmonious and prosperous society—an essential condition for the Communist Party's regime survival. For some commentators, this perspective diminishes any optimism that technology could undermine authoritarianism (Creemers 2020:130). At best, the dominant international narrative concedes that China has performed well in certain areas *despite* its authoritarian nature. The Chinese government is acknowledged for its capacity to innovate and foster entrepreneurship, *despite* the traditional view that authoritarianism stifles creativity and business (Bradford 2023:104). A significant proportion of the Chinese population appears comfortable with the deployment of technology in their daily lives, *despite* its repressive applications (Impiombato et al 2023; Bradford 2023). Even beyond China, the Chinese authoritarian approach and model could have a wider appeal in other countries (Lin 2024), *despite* the belief that liberal democracy is purportedly a universal value and the ultimate pursuit of humanity (Drexel and Kelley 2023).

This dominant narrative has significant implications for the scholarly examination of Chinese AI governance. Anything that does not fit this narrative—anything that cannot be explained by the authoritarian state's ulterior motives—is marginalized or ignored. Consequently, the international discourse on China's AI governance is often devoid of nuance, reducing it to either irrelevance or 'a political prop' (Sheehan 2023). Moreover, while both International Relations and legal scholars have analysed the evolution of China's AI governance model and examined the key drivers and actors shaping its policymaking, most discussions focus on political and security factors or the development of binding legislation. There is a notable lack of discussion on how economic factors and social values have influenced China's AI governance model, as well as how actors at different levels co-produce the governance structure in the context of China's AI governance.

To address these gaps in the existing literature, this article endeavours to expound on both the substance and values behind China's AI governance, focusing on issues beyond the stereotypical narratives of state-driven authoritarianism that disregard individual rights. Specifically, it argues that important and distinctive elements of China's AI governance are driven by social and commercial factors, not solely by the state's paranoia about regime survival. Despite the popular conception of the Chinese model as state-driven—in contrast to the market-driven USA and rights-driven European Union approaches (Bradford 2023), Chinese AI governance reflects a balance of state-driven, society-driven, and market-driven elements. This combination has enabled China to accomplish several goals that the US and EU cannot currently achieve or even contemplate in AI regulation.

Meanwhile, this article does not seek to make normative judgments about whether China's governance model is 'good' or 'bad', or whether it confers any advantage over Western counterparts. Rather, the article highlights under-examined social and commercial dynamics that coexist with centralized state authority. Recognizing these dynamics is essential for an empirically grounded understanding of China's AI governance and counters the ideologically informed simplifications (Lin 2024) that exist in certain discussions (Arora et al 2025; Hine and Floridi 2024) and views such as that Chinese 'responsive authoritarianism' necessarily fails to address the needs of minority groups (Roberts et al 2023: 86).

The remaining article proceeds in four subsequent sections. The first part sets out the analytical framework that informs the empirical discussions on China's AI governance. Drawing on recent governance literature in International Relations scholarship, the analytical framework features a set of core conceptual tools which help unpack the governing sites, governing actors, norms, and governing tools in the context of Chinese AI regulation. The second part applies the analytical framework to examine two empirical cases that constitute two major governing nodes of China's AI governance, namely minor protection and content regulation. The third part discusses the key findings across both empirical cases, which is followed by a concluding section.

1. Analytical Framework and Methodology

To examine China's approach to governing AI, this article develops an analytical framework using numerous conceptual tools from the governance literature (Hufty 2011; Holley and Shearing 2017). This section presents a practical methodology for exploring China's AI governance processes, based on four conceptual tools: governing nodes, governing actors, norms, and tools/technologies of governance. The contribution of this framework lies in demonstrating that governance literature, which have frequently been applied to liberal-democratic contexts (e.g. Hufty 2011; Holley and Shearing 2017; Wood and Shearing 2007), illuminate unexpected dynamics in non-democratic regimes such as China. This theoretical transplantation highlights the contingent and adaptable nature of governance tools, expanding the comparative utility of governance literature.

To begin with, while the term 'governance' has been widely adopted in academic and policy debates, it remains a fuzzy concept that has been contested over time (Hufty 2011). Acknowledging the diverse range of definitions, this paper adopts Hufty's conceptualization of governance as 'a category of social facts, namely the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions' (Hufty 2011:405). This conceptualization aligns with the broader governance literature, which asserts that understanding governance processes requires a decentred, multidimensional, and multilevel perspective (Black 2002; Bisschop and Verhage 2012). Although state-centred forms of governance, typically involving coercion and hierarchical control, remain significant, it is essential to consider alternative forms of governance that are frequently described as decentred (Griggs et al 2014), polycentric (Ostrom 2010), multilevel (Börzel 2020), or multimodal (Gerny 2009). Within this decentred perspective, while states and public actors are acknowledged as pivotal, their roles and functions exist within a broader context involving other providers and auspices of governance (Holley and Shearing 2017).

In line with this view, and drawing on the nodal governance scholarship, we now outline the first conceptual tool in the analytical framework: governing nodes. The concept of governing nodes plays a key role in nodal governance research, which sees governance as layered (Holley and Shearing 2017). In the nodal governance literature, nodes can be understood as institutional 'sites' of governance, or 'institutional settings that bring together and harness ways of thinking and acting' (Wood and Shearing 2007:149). Braithwaite defines a node as a point in time and space where a cluster of actors collaborates to mobilize pooled resources (Braithwaite 2004). While governing nodes can be defined as both objects of governance and actors that govern either directly or indirectly (Wood and Shearing 2007), in this research, we conceptualize governing nodes as objects of governance. Specifically, in this study, we argue that AI governance in China is best understood as a polycentric network consisting of multiple major governing nodes across different but interrelated sub-issue areas (e.g., content regulation, platform governance, minor protection). These governing nodes are seen as policy terrains and organizational sites of capacity, knowledge, and resources relevant to shaping events in AI governance in China. As 'sites' of governance, governing nodes provide a useful tool for unpacking the complex landscape of AI governance in China, characterized by piecemeal legislation and the involvement of various public and private stakeholders. Empirically, this research focuses on two governing nodes in China's AI governance – namely (1) anti-addiction systems for minor protection, and (2) content regulation. These nodes are selected not only because they reflect notable differences of the Chinese approach as compared to Western countries, but also for their demonstrating the range of governing tools and the formation of norms.

The operationalization of these governing nodes in China's AI governance involves a wide array of 'actors', the second conceptual tool drawn from the governance literature. As Johnston and Shearing note, a key dimension of governance involves 'the question of who, in a particular collectivity, has the capacity and authority to make the rules that will be treated as the norms of governance' (Johnston and Shearing 2003:30). The governance literature defines actors broadly, ranging from public actors at the state level (e.g., national legislatures, executive governments), sub-state public actors (e.g., provincial authorities), private actors (e.g., enterprises, NGOs), and individuals. Although much research on AI governance in China focuses on public actors at the state level, the role of sub-state authorities and private enterprises has received limited attention. Conceptualizing actors as 'individuals or groups whose collective action leads to the formulation of the social norms that guide, prescribe, and sanction collective and individual behavior' (Hufty 2011: 407) allows for a more nuanced understanding of how various public and private stakeholders co-produce knowledge, norms, and a regulatory environment for AI governance in China.

The third conceptual tool is the nature of social norms of governance. In governance literature, norms are generally understood as shared understandings that make behavioral claims or standards of appropriate behaviour in a given society (Checkel 1999; Finnemore and Sikkink 1998). As pointed out by Hufty (2011), in any society, agreements among actors and collective decisions contribute to the creation of norms, which can be broadly defined as shared beliefs regarding appropriate behaviour within a given social context—what is considered 'normal'. Norms serve as a framework for guiding behaviour and are subject to change through collective action. At their core, norms are rooted in values or beliefs, reflecting societal perceptions of right and wrong. They encompass both prescriptive elements (what individuals should or should not do) and sanctions, which may be positive (reinforcing desired behaviours) or negative (discouraging undesirable behaviours). Norms are intricately connected to social institutions, which are recurring systems of social norms that guide and regulate the actions of individuals and groups. Over time, as norms become recurrent, they are institutionalized, meaning they are internalized by individuals and contribute to the establishment of stable social institutions. As mentioned earlier in the introduction, the existing scholarly discussions on Chinese AI governance has paid insufficient attention to the role that social norms have played in shaping the regulatory environment of AI in the context of China – a key lacuna of the literature which this research seeks to address.

The final analytical concept focuses on the tools or technologies used to achieve governance objectives and operationalize norms (Johnston and Shearing 2003). These tools may vary across policy sectors and between different types of actors. For instance, Johnston and Shearing identified several 'toolkits' for security governance, including legal, symbolic, and personal tools (Johnston and Shearing 2003). In the context of this research, tools or technologies of governance are broadly understood as formal and informal institutional settings, regulatory measures, concrete policy prescriptions, and technical solutions created by both public and private actors in AI governance. This approach allows a comprehensive examination of different legal and policy mechanisms that have been introduced by different governing actors, including not only hard and soft laws, but also informal regulatory measures such as self-imposed regulations in the industry.

Methodologically, our analysis draws on a systematic review and qualitative analysis of Chinese legal, policy, industrial, and social organization documents. Sources were collected from official government databases (e.g., National People's Congress, State Council, Cyberspace Administration of China), industry and professional associations, and corporate governance statements (e.g., ByteDance's community conventions). Materials were coded inductively along the four categories of our analytical framework—nodes, actors, norms, and tools—allowing us to trace how governance dynamics materialize in different sub-issue areas. While interpretation inevitably requires contextual legal-political expertise, this transparent sourcing and coding strategy facilitates reproducibility and minimizes selective bias. In addition, the analysis draws on various secondary sources, including media reports, academic journal articles and policy analyses in both Chinese and English, which serve as complementary tools to triangulate evidence and increase the reliability of the empirical findings.

Moreover, this research adopts a dual-case study approach, focusing on the governing nodes of minor protection and content regulation. While a case-study approach may be limited in scope, it enables a holistic investigation of a specific process and its context, thereby serving as a critical tool for conceptual validity and exploring complex mechanisms at the core of the research (George and Bennett 2005). These two cases are selected for three reasons. First, they are foundational and long-standing nodes within China's digital governance that have been reconfigured for AI-specific contexts, making them paradigmatic rather than peripheral. Second, they are data-rich domains where both public and private actors visibly interact, enabling us to demonstrate the co-production of governance tools and norms. Third, they reveal how governance instruments initially developed in relatively non-sensitive areas (e.g., gaming addiction, content vulgarity) later diffuse into more contested domains such as algorithmic surveillance or predictive policing. By choosing these two cases, we illustrate governance dynamics that are analytically generalizable beyond their immediate policy fields, while recognizing that politically sensitive domains deserve separate study.

2. Unpacking Chinese AI Governance: the Cases of Minor Protection and Content Regulation

In this part, the analytical framework outlined in the previous section will be applied to inform the analysis of two empirical cases, namely anti-addiction systems for minor protection and content regulation. These empirical cases constitute two important governing nodes in China's AI governance. As will be demonstrated in each case, instead of being regarded as a unitary and coherent governance and regulatory framework, China's AI governance can be better conceptualized as a configuration or assemblage of multiple governing nodes where various actors attempt to tackle specific economic, social, and political problems associated with the rapid development of artificial intelligence. These governing nodes are in the process of creating an increasingly multidimensional and complex AI governance network that brings together both public and private actors who co-produce social norms, institutions, and toolkits governing AI in China.

2.1 Anti-Addiction System for Minor Protection

The first governing node embedded within China's AI governance is concerned with the anti-addiction system for minor protection. The inception of China's 'anti-addiction' system in cyberspace can be traced back to 2005, specifically in the realm of online gaming (BBC Chinese 2005). Over the past two decades, the system has become a significant aspect of China's digital governance after several major changes and expansions. What was developed to regulate online gaming became the effective tool to regulate algorithm-based video recommendation applications and generative AI, thereby constituting a new 'governing node' in the sphere of AI governance. Emulating existing mechanisms in more familiar contexts and deploying such 'reusable tools' for the regulation of newer innovations and technologies is a notable feature in Chinese AI governance (Sheehan 2023).

Remarkably, this line of development, well known among Chinese netizens and tracked by several international media over the years (New York Times 2007; BBC News 2019; Sweney and Davidson 2021), has received limited traction in English-language academic literature, even in those studies that specifically examine pertinent topics such as gaming addictions in China (Hu et al 2022; Ji et al 2022; Tang et al 2017). Moreover, news reports typically make purposeful observations such as that the system required a 'government-issued ID' (The Economist 2021), or that it could be combined with 'military drills' (Reuters 2021), demonstrating how an authoritarian government is becoming ever more intrusive (Washington Post 2021). Through contesting such reductionist view, empirical findings from our research reveals a more comprehensive and nuanced image of this policy field, demonstrating that the development of China's anti-addiction system for minor protection within the context of AI governance has primarily driven by social factors as well as normative considerations embedded in China's unique perception towards minor protection, with stakeholders from both public and private sectors jointly co-producing the norms and governing tools.

Regarding the normative foundations of China's anti-addiction system for the protection of minors, at least two important social norms can be identified. The first is the norm of enhanced protection for minors and the requirement of parental consent—a widely recognized social and legal principle evident not only in the Chinese legal system but also in those of the United States and the European Union (Zheng and Shu, 2024). This norm is grounded in a universal consensus that, due to their developmental immaturity and limited awareness of their rights, potential risks, consequences, and protective measures, minors require enhanced safeguards. Consequently, legislators are obligated to ensure enhanced protection for minors, including the necessity of obtaining parental consent when collecting personal information from or providing services to them. While this norm is widely adopted across multiple legal systems, what distinguishes China is its prioritization of this principle within its legal framework, granting it a significantly greater impact on children's fundamental rights compared to the systems in the US and the EU. As noted by Zheng and Shu (2024), although the US, the EU, and China all require parental consent for processing children's personal information, the US and EU restrict this requirement to particular contexts. This targeted approach balances the protection of children's personal information with their fundamental rights, such as freedom of expression and the right to control their personal data. Additionally, it alleviates the regulatory burden on companies, exempting them from unnecessary information protection obligations when their services are not specifically aimed at children, even if minors may use them. In contrast, China applies the parental consent requirement universally across all contexts, rather than limiting it to situations involving heightened protection for children. Consequently, China's parental consent system exerts a much broader influence on children's fundamental rights compared to the frameworks in the US and the EU.

The second important norm is the adoption of a multi-stakeholder approach to minor protection in the age of AI. Interestingly, in the conventional literature of Chinese internet governance, China has long been regarded as an international actor that is opposing the norm of multi-stakeholderism when regulating the digital sphere (Chen and Gao 2024; Chen and Yang 2022). Nevertheless, in the specific context of minor protection in cyberspace, China has recently started highlighting the norm of multi-stakeholderism, explicitly calling for greater coordination among public and private stakeholders to actively engage in ensuring minor protection in the age of AI. For example, the Cyber Administration of China (CAC) published a statement in 2021 which features a 'dual-domain, full-chain, and multi-stakeholder network protection system for minors' (CAC 2021). Specifically, the dual-domain approach reflects the characteristics of a 'dual-layered society', integrating online and offline protections for minors. This means providing network protection not only in the digital space but also in real-world environments. The full-chain approach establishes comprehensive protective standards for all potential risk points in minors' online activities, aiming for complete and seamless coverage. It particularly focuses on preventing and regulating four major types of harm and risks that minors may encounter in the digital space: online violations and crimes, exposure to harmful information, personal privacy breaches, and internet addiction. Finally, the multi-stakeholder approach clarifies the roles and responsibilities of various parties involved in minors' online activities, including stakeholders, service providers, and regulatory bodies. This includes traditional actors such as the state, society, schools, and families, as well as specialized state agencies such as the Cyberspace Administration, public security authorities, cultural and tourism departments, and agencies for news, publishing, film, and broadcasting. Additionally, specific entities such as online game platforms, live-streaming services, online audio-visual platforms, social networking services, and network product providers are also included. Each party is assigned distinct responsibilities, working together to achieve the shared goal of protecting minors (CAC 2021). These principles provide a significant normative basis that informs the operationalization of a wide array of governance tools, which will be examined in detail later in this section.

A close scrutiny of Chinese official legal and policy documents as well as guidelines published by major commercial actors shows that at least four categories of governing tools can be identified in the sphere of anti-addiction in minor protection, namely laws, guidelines, standards, and self-imposed regulatory measures (see Table 1). It is noteworthy that the design of the governing tools has involved both state and non-state stakeholders. In particular, an increasing number of industrial and social organization standards with a particular focus on minor protection in the era of AI indicates the growing influence of private sector and industrial stakeholders in shaping the regulatory environment in this policy domain.

Table 1 Governing tools and actors in minor protection in the case of minors protection

Governing tools		**Governing actors**
Categories	**Documents**	
Laws and regulations	Law of the People's Republic of China on Protection of Minors (revised in 2020), Chapter 5	Legislation by the National People's Congress Standing Committee

<table>
<tr><td rowspan="2"></td><td colspan="2">Regulations on Protection of Minors in Cyberspace (State Council 2024a), Chapter 5</td><td>Issued by the State Council</td></tr>
<tr><td colspan="2">Interim Measures for the Administration of Generative Artificial Intelligence Services, Article 10 (CAC 2023)</td><td>Jointly issued by CAC, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Public Security, and National Radio and Television Administration</td></tr>
<tr><td>Guidelines</td><td colspan="2">Guideline for the development of the mode for minors on mobile internet platforms (CAC 2024)</td><td>Issued by CAC</td></tr>
<tr><td rowspan="2">Standards</td><td rowspan="2">Industry standards</td><td>Basic security requirements for generative artificial intelligence service, Article 7 (National Technical Committee 260 on Cybersecurity of Standardization Administration of China 2024)</td><td>Issued by National Technical Committee 260 on Cybersecurity of Standardization Administration</td></tr>
<tr><td>Requirement of enthrallment preventing system for online games (National Technical Committee of Press and Publication Standardization 2017)</td><td>Issued by National Technical Committee of Press and Publication Standardization</td></tr>
</table>

	Social organization standards	Mobile Smart Terminal Guide for Minors (Internet Society of China 2024)	Issued by Internet Society of China
		Technique requirement of minor protection for mobile terminal (Telecommunication Terminal Industry Forum Association 2022)	Issued by Telecommunication Terminal Industry Forum Association
		Guidelines for Building Internet Applications for Minors Based on Artificial Intelligence Technology (China Federation of Internet Societies 2022)	Issued by China Federation of Internet Societies
Self-regulation	Self-imposed restriction by private actors	e.g. Community Self-Discipline Convention adopted by ByteDance (ByteDance 2021)	Issued by private enterprises and digital platforms such as ByteDance

As demonstrated in Table 1, the first type of governing tools includes laws and regulations which have primarily been devised by state actors and public authorities. For instance, the Interim Measures for the Administration of Generative Artificial Intelligence Services (‘IMAGAIS’ hereinafter) (CAC 2023) came into force in August 2023, as the world’s first specific legislation on GAI. As administrative rules issued by the Cyberspace Administration of China (CAC) and endorsed by six other ministerial departments and state authorities, IMAGAIS form part of the formal law of China, albeit ranking below laws or regulations currently under consideration by the State Council (the State Council of PRC 2024b). It has expectedly attracted some scholarly attention in a short period of time (Migliorini 2024; Du and Kamenova 2023; Franks, Lee and Xu 2024), including the customary comment on how it empowers censorship in ‘autocracies’ (Yang and Roberts 2023). Some parts of IMAGAIS, however, were left out by all studies so far, including for example the specific requirement for minor protection imposed on GAI services.

Article 10 of IMAGAIS stipulate that GAI service providers must implement effective measures to prevent minor users from becoming over-reliant or addicted to GAI (CAC 2023).

Notably, in the original draft published for public consultation in April 2023, this requirement was not qualified with ‘minor users’ but applied to all users. This concept of ‘prevention of enthrallment’ or ‘anti-addiction’ (*fang chenmi*) in the domain of minor protection in AI governance must be understood in the wider context of almost two decades of development in Chinese digital governance, within which society-driven considerations have played a significant role in shaping the legislation processes.

Instead of being solely driven by political concerns, China’s efforts to enhance the legislation concerning internet addiction among minors have largely been driven by social concerns. As noted in numerous existing research, in the context of China, internet addiction has been perceived as a technology-driven social problem as well as a freely chosen behaviours that can potentially lead to social risks (Jiang 2022). After being formally added to the Chinese diagnostic manual in 2008, ‘internet addiction’ was then included in the Law on the Protection of Minors (2012 revised version) which for the first time specified that ‘the state encourages the research and development of online products beneficial to the healthy growth of minors and promotes the adoption of new technologies to prevent minors from becoming addicted to the internet.’[2] The Law on the Protection of Minors was further amended in 2020 by devising a brand new chapter entitled ‘Online Protection’ that consists numerous provisions specifying different stakeholders’ (e.g. state, schools, parents, tech companies and producers) responsibilities in preventing internet addiction among minors (State Council 2020).

Apart from laws and regulations with legally binding effects, the second category of governing tools is guidelines, which refers to a form of advisory document, primarily designed to provide recommendations and guidance for operations, practices, or policies in a particular field. A guideline is typically issued by administrative authorities or other authoritative bodies to guide relevant parties in specific areas. Whilst such type of governing tool may hold a degree of authority and influence, it does not directly establish legal rights or obligations and has often been considered as ‘soft law’ (Clark 2013). A telling example is the ‘Guideline for the development of the mode for minors on mobile internet platforms’ which was recently published by CAC in November 2024 which was mentioned in Table 1 (CAC 2024). With an aim of ‘guiding minors to use the internet in a scientific, safe, and reasonable manner and intervening in cases of internet addiction among minors’ (CAC 2024), this guideline establishes a set of norms and requirements seeking to encourage different stakeholders – ranging from platforms, mobile terminals, to mobile applications to jointly construct and develop minors’ mode (People’s Daily 2024). Notably, content provision – which constitutes a key aspect of AI governance – has been featured in the guideline, which creates an age-based recommendation standards to prioritize the provision of content appropriate for five age groups among minors

[2] Article 33; the 2012 revised version of the Law on the Protection of Minors is available at: https://law.pkulaw.com/falv/5b242b5a062cc53bbdfb.html (accessed 15 January 2025).

(People’s Daily 2024). The guideline also explicitly ‘encourages application providers to provide age-appropriate recommendation labels for content within the dedicated content pool for minors’ (CAC 2024).

The third category of governing tool identified in this empirical case is standards, which can be further divided into national standards, industry standards, local standards, and social organization standards. In this governing node, both industry standards formulated by the relevant administrative departments under the State Council, and social organization standards issued by non-governmental social organizations in the field of digital governance can be observed. Notably, in the past few years, there has been an increasing number of social organization standards dedicated to the issue of minor protection in cyberspace. As indicated in Table 1, between 2022 and 2024, three social organization standards have been released, including Technique Requirement of Minor Protection for Mobile Terminal, Guidelines for Building Internet Applications for Minors based on Artificial Intelligence (both published in 2022) and Mobile Smart Terminal Guide for Minors, published in 2024. The rapid development of social organization standards as a unique governing tool suggests that China's business community and civil society are playing an increasingly significant role in the standardization formulation processes, especially following the 2017 revision of the Standardisation Law, which stipulates that the state encourage civil society entities such as associations, chambers of commerce, industrial technology alliances to coordinate relevant market entities and to co-produce social organization standards that meet the demands of the market and innovation (Wu and Liu 2022). As exemplified in the Guidelines for Building Internet Applications for Minors Based on Artificial Intelligence Technology released in 2022 (China Federation of Internet Societies 2022), the drafting committee of this social organization standards primarily comprised industry leaders such as Tencent and Kuaishou Technology, and a wide range of academic and research institutions such as Peking University, Tsinghua University, and Communication University of China, along with China Federation of Internet Societies – China’s first NGO formed voluntarily by civil societies and institutions in the field of cybersecurity and informatization technology (Office of the United Nations High Commissioner for Human Rights 2022).

The fourth type of governing tools include self-imposed regulatory measures adopted by tech companies such as ByteDance and Tencent. For instance, ByteDance updated its Community Self-regulation Convention in 2021, announcing that all verified users under the age of 14 have been automatically placed in a ‘youth mode’ (ByteDance 2021). Under such model, all verified users under the age of 14 cannot opt out on their own and only can access the app for a maximum of 40 minutes per day and are restricted from using it between 10 PM and 6 AM the following day (China News 2021). In addition, the youth mode will only allow users to get access to curated content, including historical facts, exhibitions, scenic visuals, and science experiments. Douyin — TikTok's Chinese domestic counterpart — claims to be the first in the short-form video industry to implement such a restriction. To support this initiative, it also launched a bug bounty program, encouraging users to report suspicious activities like unauthorized access, hacking, and other vulnerabilities (Independent 2021).

The above discussion illustrates how the governance framework of minor protection in cyberspace in China has evolved overtime and how it has increasingly become a key governing node of digital governance in the age of AI. In line with the theoretical framework, three observations can be made with respect to actors, normative foundations, and tools of governance. First, the case of minor protection demonstrates that part of Chinese digital and AI governance is clearly driven by social factors and normative considerations rather than solely by authoritarian surveillance. It seems unnecessary in this day and age to detail the widespread concerns about the time children and young people spend on gaming, computers and mobile phones. This is certainly not a Chinese-only concern or problem. Parents, researchers and policymakers worldwide have sought to reduce the time that minors spend on online games, short videos and GAI (Brooke 2020; Brandon 2023; Bernstein 2023). Nonetheless, China has actually implemented the world's most elaborate system aimed at making a difference. This is not out of any fear of the Chinese state that not knowing how long a 12-year-old has been using GAI puts the regime at risk. China did it because many in Chinese society wanted it done. For example, existing research points out that one of the reasons behind the updated 2021 Regulations from the National Press and Publication Administration was that parents desire and welcome stricter rules on online gaming (China Daily 2024), which is a bottom-up societal demand rather than a political consideration. Similarly, ByetDance's self-imposed youth model has also gained wider societal support, especially by parents who are unable to control their children's behaviours online (Tan 2022).

Second, with regards to governing actors that have involved in the governing node of minor protection in cyberspace, our findings show that, contrary to the conventional view that China's digital governance is solely driven by state actors, there exist an increasingly dynamic public-private relationship in the sphere of AI governance. As shown in the governing node of minor protection, a diverse range of public authorities and relevant industry regulators (e.g. CAC, Ministry of Science and Technology, Ministry of Industry and Information Technology), business and private sector actors such as the tech companies and digital platforms, as well as social organizations in the domain of internet governance. Although it is well documented that Chinese social organizations have to operate under significant state control and influence (Hildebrandt 2011: 988), exclusive focus on 'state-dominant' theories risk obscuring the dynamics of change in China and the capacity of these organizations to influence the policy-making process or to pursue the interests of their members (Saich 2000: 125). Social organizations work both to assist the government in implementing its policies and to further their own goals (Hildebrandt 2013: 2). Therefore, it is important to recognize that these actors have jointly contributed to establishing a multi-faceted governance regime, within which governance should be viewed as an activity that concerns the dynamic interactions between public authorities, commercial actors, and the users' community (Tan 2022).

Third, AI governance in China involves the development of multiple governing tools co-produced by the wide array of public and private sector actors, blending the mechanisms of hard laws, soft laws, and industrial self-regulation designs. As demonstrated in Table 1, there is a trend that soft laws (e.g. industrial and social organization standards) and industrial self-regulation initiatives (e.g. ByetDance's self-imposed youth mode) have played an increasingly important role in governing internet addiction and minor protection in the age of AI.

Furthermore, it is also noteworthy that the Chinese 'anti-addiction' system is facilitated by many of the governmental and digital infrastructures, which could have been put in place by the Chinese state with political aims in mind. To begin with, a unified 'government-issued' ID for every Chinese citizen enables gaming and AI service providers to verify the age of each user instantaneously, which is essential for the operation of an effective age-restricting system. Without it, the Chinese system would fare no better than those in many other countries, where, for example, any user can simply click on a button stating 'I am over 18 years old' or provide the birth month of their favourite sports player to gain full access to online services meant only for adults. The Chinese system is far from impeccable, and many who are determined to do so can find ways to circumvent it. However, it is the most advanced system for this purpose currently in wide operation, and that alone should be reason enough for it to be properly examined rather than dismissed due to ideological biases.

2.2 Content governance

While restricting the use of certain online services to protect minors is largely acceptable in many countries, it becomes far more controversial when such restrictions are applied to the general population regardless of their age. China is arguably the most notorious practitioner of content regulation and censorship in the digital age, with its numerous measures and practices, such as the 'Great Firewall', having been subject to extensive analysis and sharp criticism (Bradford 2023: 78-9; Roberts 2018; Kim and Douai 2012; Han 2023). Similar to the node of minor protection, there are numerous governing tools from various actors within the node of content governance and only some representative examples are listed below (Table 2).

Table 2 Governing tools and actors in content governance

Governing tools		**Governing actors**
Categories	**Documents**	

Laws and regulations	Cybersecurity Law of the People's Republic of China (enacted in 2016)	Standing Committee of the National People's Congress
	Provisions on the Ecological Governance of Online Information Content (commenced 1 March 2020)	CAC
	Provisions on the Administration of Algorithm Recommendation in Internet Information Services (commenced 1 March 2022)	CAC & three other departments
	Provisions on the Administration of Deep Synthesis Internet Information Services (commenced 10 January 2023)	CAC & two other departments
	IMAGAIS (commenced 15 August 2023)	CAC & six other departments
Guidelines	Basic security requirements for generative artificial intelligence service (29 February 2024)	National Technical Committee 260 on Cybersecurity of Standardization Administration of China
Standards	Self-discipline Convention of the Chinese Internet Industry (26 March 2002)	Internet Society of China
	Self-discipline Standards of Internet Websites against the Dissemination of Obscene, Pornographic and other Undesirable Information (10 June 2004)	Internet Society of China
Self-regulation	E.g. User agreement of ERNIE Bot from Baidu	Issued by private enterprises and digital platforms

In English-language literature, anything China does in content governance seemingly fits into the aforementioned narrative of authoritarian state control. Nevertheless, what this stereotyping often overlooks, purposefully or otherwise, is aspects of Chinese digital and AI governance that address significant issues beyond the realm of politics. In other words, in line with the analytical framework, the different governing tools addresses different norms of governance consolidated on complex webs of political, social and economic considerations.

The most representative social norm in this context is that against 'undesirable' (*buliang*) content. Notably, both the Provisions on the Administration of Algorithm Recommendation in Internet Information Services ('Algorithm Provisions' hereinafter) and the Provisions on the Administration of Deep Synthesis Internet Information Services ('Deep Synthesis Provisions' hereinafter) stipulate multiple rules against 'illegal' or 'undesirable' content (Algorithm Provisions: Articles 6 and 9; Deep Synthesis Provisions: Article 10).[3] This is consistent with the Chinese system of online content governance over the past decades. Nevertheless, most studies of Chinese content governance tend to acknowledge only the first half of it while completely ignoring the other half.

The 'illegal' category encompasses or potentially encompasses most sensitive political issues, such as expressing views that call for the undermining of state structures or the socialist system, or the secession of any part of China's claimed territory. A significant addition to political content in this category is pornography, as the online dissemination of pornography or even facilitative information is also explicitly illegal.[4] Leading studies of Chinese censorship typically provide rather terse explanations for why pornography is restricted as much as, or in some cases more than, political content, stating that pornography is viewed by the Chinese leadership as 'violating public morality and damaging the health of young people' (King, Pan and Roberts 2013: 335). Without delving into a discussion regarding whether defending 'public morality' is a state-driven or society-driven imperative, what is important here is that a whole category of content regulation, namely 'undesirable' content, has largely been ignored by international scholarship.

There is now a non-exhaustive list of 'undesirable' content in the formal law of China, including eight specific categories and one generic 'other undesirables' (CAC 2019b: Article 7). It is difficult to discern 'authoritarian' motives behind most of these eight restricted categories, such as those content promoting discrimination, gore, horror, brutality, or vulgarity. The relevant authorities are making further efforts to clarify or provide examples of some of these categories, adapting to changing times and new trends in online content. For example, the scope of vulgarity (*cusu*), which initially focused on violence or sexually indicative content (Ye, Huang and Krijnen 2025: 90-1), has expanded to include various pranks or crass jokes that have

[3] Article 10. '*Buliang*' is sometimes translated into English as 'harmful' by some sources, although arguably 'undesirable' has a wider scope and is therefore more appropriate.

[4] Criminal Law of the People's Republic of China, Articles 105, 103, 287 and 363-7. Chinese law formally distinguishes between 'obscene' (*yinhui*) and 'pornographic' (*seqing*) materials but these are discussed together as pornography in this article.

become popular on various online platforms (CCTV 2009; CAC 2019a). The concept has received very little attention outside China and is generally under-studied. But the growing influence of China in AI has understandably brought these Chinese concepts and norms to the world stage. As an example, the open-source Chinese AI DeepSeek rose to international fame in early 2025, surprising many of its more established rivals. DeepSeek's terms of use not only stipulate the application of Chinese law but also explicitly prohibit users from generating, expressing or promoting content that is 'vulgar' (DeepSeek 2025: Article 3.4). With tens of millions of users having agreed to such terms when signing up for the service of DeepSeek, this distinctively Chinese norm by origin has already been shaping the international understanding of AI content governance.

Moreover, the combination of these evolving, expandable categories is arguably broadly representative of what the Chinese society at large finds distasteful. Some examples will best illustrate the scope of such content governance. For instance, GAI is seen as an important development in relation to pseudoscience and conspiracy theories as it can be used to either tackle or perpetuate the problem (Bago and Bonnefon 2024; Quintanilla 2023). Nevertheless, guidelines in China have expressed it as a basic security requirement that in this context AI should be guarded against content and information that are 'seriously inconsistent with scientific common sense and mainstream understanding' (National Technical Committee 260 on Cybersecurity of Standardization Administration of China 2024: Appendix A.5). Elsewhere, the use of hyperbole in titles that exaggerate or mismatch the actual content of a piece (*biaoti dang*), similar to 'clickbait', is specifically deemed undesirable. This is often assessed irrespective of any 'state interest' or political stance. For example, a famous new agency used the title of 'China to become a major cyber power: Unrivalled in the world by 2050' for one of its news reports in 2016. This was not only penalized by the Cyber Administration of Beijing Municipality but also bulletined as a typical example of a violation of content regulation (CCTV 2016). Another category of 'undesirable' is any material that could induce the imitation of unsafe behaviours or the development of unhealthy habits. For instance, if someone in China decides to publish a video of herself licking a toilet seat on a commercial flight as some kind of 'coronavirus challenge', this person will most likely not gain the attention of hundreds of thousands of views but will instead be banned promptly for promoting undesirable content (Toureille 2020).

Another emerging norm in Chinese content governance that comprise significant political, social and economic considerations is that against falsehood (*xujia*). In terms of formal law, both the Algorithm Provisions and the Deep Synthesis Provisions prohibits only 'fake news' (*xujia xinwen*) (Algorithm Provisions: Article 13; Deep Synthesis Provisions: Article 6). However, in many regards, some technologies such as GAI are all about creating what is not true or genuine in the real world. The change of label from internationally prevalent 'deepfake' to the more neutral 'deep synthesis' in the official discourse of Chinese AI governance is seen as a major achievement by Chinese tech giants and the commercial interests they represent

(Sheehan 2024: 29-30). Still, the norm of governance against falsehood in China are far more extensive in substance and expansive in scope than labels or narratives, and it also represents considerable social and economic concerns against the side-effects of technology.

The incident commonly referred to as ‘the lost homework of Qin Lang’ provides a vivid illustration of the strength of such norm and the consequences of violation (BBC News 2024a; Independent 2024). T was a popular video blogger across multiple major Chinese platforms with millions of followers. In February 2024, T published a short video of herself sitting inside a restaurant in Paris. She explained that a staff member of the restaurant had just handed her a piece of homework from a Chinese pupil that had been left behind in the restroom. The homework had the name of a primary school (without precise information as to the province or city it is located in), the name of pupil, and his or her year and form number. In cheerful tone, T said that she would bring the homework back to China and asked the pupil or parent to get into contact.

As unremarkable as the content of the video seems to be now with hindsight, some algorithms and AI promoted it to tens of millions of users at the time, and it became among the top trending videos across several platforms. This was to be the downfall of T. Journalists and netizens checked with every possible school with that name across different provinces in the next few days and it became clear that there was no such pupil by this name at any school by such name anywhere in China. Eventually T admitted to having staged this. The police got involved and T together with her colleague who helped were given administrative penalties for ‘spreading online rumours’. The more serious consequences for T came when all the major platforms permanently banned her account for violating their service agreements in relation to misleading or false information. With the number of followers she had, it was estimated that her accounts generated income between RMB 20 million (approximately 2.7 million in USD) to 100 million each year (Sohu 2024; Tencent 2024), which all came to nothing for making up the story about a non-existent primary school pupil’s homework.

Such consequences may seem disproportionate to any harm caused by staging the story, if any, given that there was no such school nor such pupil to be harmed in the first place. Even foreign journalists could not decipher the ‘political’ motives behind such incidents this time. BBC merely observed that ‘[w]hile a lot of online censorship focuses on dissident and political content, authorities have also started cracking down on non-political online falsehoods in recent years’, without further explanation (BBC News 2024a). Using the analytical framework, however, there is demonstrable consensus against any form of falsehood in Chinese cyberspace, representing both social and economic considerations. More specifically, as an example, T’s account typically got paid RMB 550,000 (approximately 75,000 USD) for one video of commercial advertisement (Sohu 2024). Understandably, those product manufacturers and commercial partners loathe to be associated with any entity that is not authentic or truthful, because of the strong social sentiment against falsehood. It is then in the commercial interests of digital platforms and AI service providers to take a firm stance against falsehood, often far stricter than the legal framework followed by state authorities.

Furthermore, there are other notable developments of potential new norms that are independent of formal law and state authorities, including in ostensibly 'political' context. As an example, ERNIE Bot (*wenxin yiyan*) developed by Baidu is one of the leading Large Language Model AIs in China. Its service agreement contains commonplace clauses against prompting illegal and unlawful content such as those threatening national security or promoting terrorism, pornography or violence. However, the prohibitions also encapsulate some unusual matters, such as anything that 'undermines international relations or damage international peace and stability' (Baidu 2025: Article 4.4.1.11). There seems to be no obvious source for such prohibitions within legal instruments or policy documents, and they are arguably framed too broadly to be useful. Nevertheless, one practical impact seems to be that when being asked to generate content about topics such as possible armed conflicts between the People's Liberation Army and the United States military, ERNIE Bot will often include notable 'warning' messages, such as the devastating consequences of wars, the importance of resolving international disputes through collaboration and dialogues, and the need to preserve peace and stability in the world.

Summarily, in the node of content governance, Chinese norms are formulated in very different ways and reflect complex interaction of various political, social and economic considerations. Some are clearly imposed by the state, such as illegal, politically sensitive content, or pornography. Other norms, such as those against undesirable content, may originate within formal law, but have substantially expanded their scope by incorporating input of social and economic consideration. Some norms, such as that against falsehood, had little obvious political implications but reflect the attitudes of Chinese society and businesses in general.

3. Analysis

3.1 Multi-use tools

It is important to note that both nodes of minor protection and content governance also take advantage of other governance tools, some of which were not originally designed for such purposes but have nevertheless become useful and important through expansion or adaptation. In the context of minor protection, a major practical obstacle is the identification of minors as such in the anonymous cyberspace. In November 2024, Australia attracted international attention by legislating to ban social media use of all under-16s.[5] However, although the law may come into force after at least 12 months, there are still much uncertainties as to how to

[5] Online Safety Amendment (Social Media Minimum Age) Bill 2024, amending Online Safety Act 2021.

verify the age of users and little more than ideas that may or may not work (BBC News 2024b). In contrast, the Chinese 'government-issued ID' system has been in place since 1984 well before the internet era, and has been enhanced with electronic and digital capabilities since 2004. It turns out to be an effective method for identity verification widely used in China for almost all purposes and became the logical choice when considering mechanisms for minor protection online.

Another tool that served multiple uses is the Algorithm Registry. Initially established by the Algorithm Provisions, the registration requirement is continued by both the Deep Synthesis Provisions and the IMAGAIS (Algorithm Provisions: Articles 24-26; Deep Synthesis Provisions: Article 19; IMAGAIS: Article 17), facilitating effective enforcement mechanisms, if needed, in contexts such as content governance. A wide range of algorithms have been filed for registration by companies, ranging from search-engine filtering to apps recommending parenting tips (Sheehan 2024: 31). The CAC, which manages the algorithm registry, publishes in due course a much more limited public version of each registered algorithm.

Although it is easy to label this system as part of the Chinese state's typical desire for information and control, the fact that any public version is published at all indicates there are further interests at play. There is certainly useful information in the published registrations. For example, Douyin explains in its algorithm registration how it takes active steps to overcome the so-called 'information cocoon' of users (Douyin 2024). Baidu also made public for the first time its criteria for determining the ranking of search results (Baidu 2024). Unsurprisingly, much of the information regarding hundreds of registered algorithms is highly technical and of little interest to the general public. Yet it is likely to be of use to professionals and competitors. The truncated nature of the published versions reflects commercial concerns about revealing too much rather than any obsession with secrecy by the Chinese state. The algorithm registry is, therefore, an evolving balance of state, social and commercial interests that China is experimenting with, currently with no known European or American counterparts. Chinese AI governance is notably different from those in the West, but it is naïve to presume that it is all about state interest in disregard of commercial realities.

With these nodes and tools in place, it is evident AI and tech companies operate in a very environment and cyberspace in China compared to most other countries. These stark differences are not lost on informed foreign observers and news media (Fox News 2022). According to one metaphor, China promotes the healthy, 'spinach version' of TikTok (i.e. Douyin) domestically while selling the harmful and addictive 'opium version' to overseas (CBS News 2022). This reference is particularly fascinating in view of the fact that China was probably the first to sound the alarm about 'electronic opium', in its most celebrated state media *People's Daily*, several years before such concerns arose in the West (People's Daily 2017). China has been combating the addiction or harms perceived in these technologies based on algorithms and artificial intelligence for some years, through tools of content governance, representing major society-driven and market-driven impetus. The West, on the other hand, seems to have its hands tied, as surely large-scale content regulation cannot be an option of liberal democracies, even if it turns out to be the most effective means for protecting the youth or society.

3.2 Protecting society from AI

The fact that China has little ideological struggle in this context means that China can freely choose any approach that serves the varied and often conflicting needs of the state, society and the market, depending on the scenario and competing interests at play. Borrowing the spinach and opium metaphor again, if a jurisdiction has neither rule nor norm against trading in opium, what is there to stop companies from selling opium instead of spinach? More importantly, today the decision to target any particular user with either spinach or opium may well be made by AI and algorithms, instead of by another human being.

The success of applications such as TikTok heavily relies on recommendation algorithms and machine learning (Wang 2022). The underlying commercial interests aim to exploit each user's interest as much as possible so that they spend more time consuming content. Thus, the task for AI is to identify, through each individual's usage pattern, what is most likely to capture their continued attention. Unless AI is instructed by humans, who are in turn mandated by law, it does not need to consider the negative impact of promoted content on human beings. In this context, many countries still rely on mechanisms and principles created before the digital age, such as self-regulation and civil lawsuits for liabilities (NBC News 2024). China, however, has little faith in self-regulation by commercial entities and has again taken it to formal law to target potential exploitation. The Algorithm Provisions explicitly prohibit service providers from using negative keywords to track user interests (Algorithm Provisions: Article 10).

It is also important to recognize that the regulation of AI not only protects society and individuals but also the market and commercial interests. The practice and impact of Uber illustrate what could happen otherwise. Uber is known to rely on machine learning to charge customers 'dynamically' according to their ability and willingness to pay (Forbes 2019). Although Uber started as a 'disruptive technology' purportedly seeking to empower taxi drivers and customers, once it attains its market position, it becomes more like the monopoly it initially disrupted (Spaulding 2023: 252). Chinese regulators have again taken clear and firm actions in this regard. The Algorithm Provisions prohibit the use of algorithms against other service providers and competitors in any form of monopolistic or unfair competition behaviours (Algorithm Provisions: Article 15). The Algorithm Provisions also outlaws the differential pricing based on algorithms, which has been hailed as one of the key intentions of the legislation in response to widespread societal discontent with the practice of 'exploiting returning customers' (*sha shu*) by certain dominant digital businesses (Algorithm Provisions: Article 21; Xinhua News Agency 2022).

4. Conclusion

It is evident that China today is a major cyber power across the board, from the more traditional, high-tech manufacturing and export to latest advances in AI and GAI. While its status and practical influence are recognized in international scholarship, Chinese digital and AI governance is often simplified, even dismissed, as ‘state-driven’ and primarily serving the need of the regime to maintain its draconian control over the Chinese people. This is the hypothesis, if not belief, of many. And it is notable to see confirmation bias at work, where information is searched for, interpreted and remembered in such a way that it systematically impedes the possibility that the hypothesis could be rejected (Oswald and Grosjean 2004: 79). Anything that China does which enhances state influence or control is highlighted and presented as evidence of how the hypothesis dictates that such a regime should behave. Anything that cannot be attributed to the state is left unexplained or even not mentioned at all in English-language literature.

This study aims to challenge this hypothesis and seeks to facilitate a more comprehensive understanding of Chinese digital and AI governance. On the basis of theories of governance, an analytical framework is developed to examine the governance nodes, tools, actors and norms in the Chinese context. Two particular nodes, namely minor protection and content governance, are selected as case studies. While the Chinese approach to both is notably different from other countries, particularly those in the West, they illustrate the variety of tools and actors involved beyond the state apparatus as well as the emergence and development of norms in Chinese cyberspace.

This study demonstrates that Chinese digital and AI governance represents a broad range of political, social and economic interests from various stakeholders including the state, commercial entities and, equally importantly, the Chinese people and society. China is also becoming more confident and comfortable with reconfiguring tools that were developed earlier for different purposes when faced with new challenges such as recommendation algorithms and GAI. This often enabled China to react quickly, as seen for example when China became the first country to have formal regulations in place specifically on GAI. Chinese GAI is also legally and normatively restricted from generating content that is illegal, undesirable, vulgar, false, and so on, reflecting the taste and wider concerns of contemporary Chinese society. China has also developed arguably one of the most effective and rigorous systems for minor protection in cyberspace encapsulating gaming, short-video and GAI services.

Looking past the political denomination or infrastructure, all countries in the contemporary world face great challenges on the governance of AI and cyberspace. The Chinese approach and experience entail numerous difficulties and failures but there are also notable successes and achievements. To use the metaphor for the last time, the ‘spinach-version’ of Chinese cyberspace is not singlehandedly dictated by the Communist Party; it is the accumulation of experiments and efforts of Chinese society and the largest online population in the world. There is much to be gained from rigorous examinations of the Chinese approach by moving beyond the stereotypical ‘state-driven’ or ‘authoritarian’ narratives.

REFERENCES

Alexander L. George and Andrew Bennett, *Case studies and theory development in the social sciences* (Cambridge, MA: MIT Press, 2005).

Bago B and Bonnefon J (2024) Generative AI as a tool for truth. Science 385: 1164.

Baidu (2024) 百度信息检索算法 [Baidu information search algorithm] (registration file No. 110108645502804220013). https://beian.cac.gov.cn/api/static/fileUpload/principalOrithm/additional/user_5de219cd-1f21-487f-9481-d5b521468a6f_8c6028d7-74ea-4f4e-bf73-9bf4c12aecbe.pdf. Accessed 15 February 2025.

Baidu (2025) 文心一言用户协议 [Ernie Bot User Agreement] (13 February 2025). https://yiyan.baidu.com/infoUser. Accessed 15 February 2025.

BBC Chinese (2005) China will implement an online anti-addiction system. http://news.bbc.co.uk/chinese/simp/hi/newsid_4180000/newsid_4184200/4184232.stm. Accessed 31 July 2024.

BBC News (2019) Video game addiction: China imposes gaming curfew for minors. https://www.bbc.co.uk/news/world-asia-50315960. Accessed 31 July 2024.

BBC News (2024a) China shuts down influencer’s account over fake story. https://www.bbc.co.uk/news/world-asia-china-68814849. Accessed 31 January 2025.

BBC News (2024b) Australia approves social media ban on under-16s. https://www.bbc.co.uk/news/articles/c89vjj0lxx9o. Accessed 31 January 2025.

Bernstein G (2023) ChatGPT Is the Wake-Up Call Schools Need to Limit Tech in Classrooms. Time. https://time.com/6266311/chatgpt-tech-schools/. Accessed 31 July 2024.

Bisschop L, Verhage A (2012) The complex(ity) of policing dirty crime. Politie Studies: Tides & Currents of Policing, 25, 273–90.

Black J (2002) Critical reflections on regulation. Australian Journal of Legal Philosophy 27, 1–35.

Börzel TA (2020) Multilevel governance or multilevel government?. The British Journal of Politics and International Relations 22(4), 776-783.

Bradford A (2023) Digital Empires: The Global Battle to Regulate Technology. Oxford University

Press, Oxford.

Braithwaite J (2004) Methods of power for development: Weapons of the weak, weapons of the strong. Michigan Journal of International Law 26: 297–330.

Brandon J (2023) TikTok Is Addressing Screen Time for Teens In A Very Disappoint Way Forbes. https://www.forbes.com/sites/johnbbrandon/2023/03/05/tiktok-is-addressing-screen-time-for-teens-in-a-very-disappointing-way/. Accessed 31 July 2024.

Brooke A et al (2020) Parenting Children in the Age of Screens. https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/ Accessed 31 July 2024.

ByteDance (2021) 抖音社区自律公约 [Douyin Community Self-regulation Convention]. https://www.douyin.com/rule/policy?activeId=self_decipline. Accessed 15 January 2025.

CAC (2019a) 全国“扫黄打非”办公室组织开展网上低俗信息专项整治 [Operation to tackle online vulgar information] (10 April 2019). https://www.cac.gov.cn/2019-04/10/c_1124346424.htm. Accessed 15 January 2025.

CAC (2019b) 网络信息内容生态治理规定 [Provisions on the Ecological Governance of Online Information Content] (CAC Order No.5 of 2019, 15 December 2019). https://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm. Accessed 15 January 2025.

CAC (2021) 开启未成年人网络保护新篇章[Open a new chapter in the online protection of minors]. https://www.cac.gov.cn/2021-01/08/c_1611677465664292.htm. Accessed 15 January 2025.

CAC (2023) 生成式人工智能服务管理暂行办法[Interim Measures for the Administration of Generative Artificial Intelligence Services]. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm. Accessed 15 January 2025.

CAC (2024) 移动互联网未成年人模式建设指南[Guideline for the development of the mode for minors on mobile internet platforms]. https://www.cac.gov.cn/2024-11/15/c_1733364304749288.htm. Accessed 15 January 2025.

CBS News (2022) Industry ethicist: Social media companies amplifying Americans' anger for profit (6 November 2022). https://www.cbsnews.com/news/tristan-harris-social-media-political-polarization-60-minutes-2022-11-06/. Accessed 31 July 2024.

CCTV (2009) 国新办副主任蔡名照详解何为网络低俗内容 [Deputy Director of the News Office of the State Council Cao Mingzhao explained what online vulgar contents were] (6 January 2009). https://news.cctv.com/china/20090106/105493.shtml. Accessed 15 January 2025.

CCTV (2016) 北京市网信办通报多起网络媒体“标题党”违规案例 [Beijing Cyberspace Administration bulletined multiple “clickbait” violations by online media] (5 December 2016). http://m.news.cctv.com/2016/12/05/ARTIniJaZsjmOXWYVfMWWjmD161205.shtml. Accessed 15 January 2025.

Arora AS, Saboia L, Arora A and McIntyre J (2025) Human-Centric Versus State-Driven: A Comparative Analysis of the European Union's and China's Artificial Intelligence Governance

Using Risk Management. International Journal of Intelligent Information Technologies 21.

Cerny PG (2009) Multi-nodal politics: globalisation is what actors make of it. Review of international studies 35(2), 421-449.

Checkel JT (1999) Norms, institutions, and national identity in contemporary Europe. International studies quarterly 43(1), 83-114.

Chen X, Gao X (2024) Norm diffusion in cyber governance: China as an emerging norm entrepreneur? International Affairs 100, 2419-2440.

Chen X, Yang Y (2022) Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness. The International Spectator 57(3), 1-14.

China Daily (2024) Parents help children dodge time limits on online games. https://www.chinadaily.com.cn/a/202408/20/WS66c3e9a1a31060630b923e74.html#:~:text=The%20National%20Press%20and%20Publication,and%20Sundays%20and%20public%20holidays. Accessed 15 January 2025.

China Federation of Internet Societies (2022). 《基于人工智能技术的儿童互联网应用指南》发布 [the Publication of Guidelines for Building Internet Applications for Minors Based on Artificial Intelligence Technology]. https://www.cfis.cn/2022-06/22/c_1128766328.htm. Accessed 15 January 2025.

China News (2021) 国内首家！抖音宣布 14 岁以下实名用户将直接进入青少年模式 [First in the country! Douyin announces that real-name verified users under the age of 14 will automatically be placed into Youth Mode]. https://www.sc.chinanews.com.cn/shouye/2021-05-26/149397.html. Accessed 15 January 2025.

Clark E (2013) China's 'soft law': a major factor for success in future. The China Internet Information Center. http://www.china.org.cn/opinion/2013-10/17/content_30321578.htm. Accessed 15 January 2025.

Creemers R (2020) China's Conception of Cyber Sovereignty: Rhetoric and Realization. In Dennis B, van den Berg, B (ed) Governing Cyberspace: Behavior, Power and Diplomacy. Rowman & Littlefield, London, pp 107-142.

Daniëlle F (2021) Emerging illiberal norms: Russia and China as promoters of internet content control. International Affairs 97: 6, 1925–44.

DeepSeek (2025) DeepSeek Term of Use (20 January 2025). https://chat.deepseek.com/downloads/DeepSeek%20Terms%20of%20Use.html. Accessed 31 January 2025.

Dong H, Chen J (2024) Meta-regulation: An ideal alternative to the primary responsibility as the regulatory model of generative AI in China. Computer Law & Security Review 54, 106016.

Douyin (2024) 头条热榜算法 [Toutiao Rebang algorithm] (registration file No.110108823483902220017). https://beian.cac.gov.cn/api/static/fileUpload/principalOrithm/additional/user_9b84b02a-0c7f-4bd4-81f2-5cad879ad4ab_9a1de9f4-581f-4877-bec6-acb3615085fa.pdf. Accessed 15 February

2025.

Drexel B, Kelley H (2023) Behind China's Plans to Build AI for the World. Politico. https://www.politico.com/news/magazine/2023/11/30/china-global-ai-plans-00129160. Accessed 31 July 2024.

Du L, Kamenova K (2023) China's new regulations on generative AI: implications for bioethics. The American Journal of Bioethics 23(10), 52-54.

The Economist (2021) Game Over: China's crackdown will hit foreign firms as well as domestic ones. The Economist (4 September 2021) 440 (9261): 54.

Filipova A (2024) Legal Regulation of Artificial Intelligence: Experience of China. Journal of Digital Technologies and Law 2(1), 46-73.

Finnemore M, Sikkink K (1998) International norm dynamics and political change. International organization 52(4), 887-917.

Forbes (2019) Uber Charges More If They Think You're Willing To Pay More (30 March 2019). https://www.forbes.com/sites/nicolemartin1/2019/03/30/uber-charges-more-if-they-think-youre-willing-to-pay-more/. Accessed 31 July 2024.

Fox News (2022) How is TikTok different in China versus America? (18 July 2022). https://www.foxnews.com/video/6309696840112. Accessed 31 July 2024.

Franks E, Lee B, Xu H (2024) Report: China's New AI Regulations. Global Privacy Law Review 5(1).

Griggs S et al (2014) Practices of freedom: Decentred governance, conflict and democratic participation. Cambridge University Press, Cambridge.

Han R (2023) Debating China beyond the Great Firewall: Digital Disenchantment and Authoritarian Resilience. Journal of Chinese Political Science 28: 85.

Hildebrandt T (2011) The Political Economy of Social Organization Registration in China. The China Quarterly 208, 970-989.

Hildebrandt T (2013) Social Organizations and the Authoritarian State in China. Cambridge University Press, Cambridge.

Hine E, Floridi L (2024) Artificial intelligence with American values and Chinese characteristics: a comparative analysis of American and Chinese governmental AI policies. AI & Society 39, 257-278.

Holley C, Shearing C (2017) A nodal perspective of governance: Advances in nodal governance thinking. In Drahos P (ed) Regulatory theory: foundations and applications. ANU Press, Acton, pp 163-180.

Hu H et al (2022) Online gaming addiction and depressive symptoms among game players of the glory of the king in China: the mediating role of affect balance and the moderating role of flow experience. International Journal of Mental Health and Addiction 20(5), 3191-3204.

Hufty M (2011) Investigating policy processes: the governance analytical framework (GAF). Research for sustainable development: Foundations, experiences, and perspectives 403-424.

Impiombato D, Lau Y, Gyhn L (2023)Examining Chinese citizens' views on state surveillance'. Australian Strategic Policy Institute. https://www.aspistrategist.org.au/examining-chinese-citizens-views-on-state-surveillance/. Accessed 31 July 2024.

Independent (2021) TikTok in China gets 40-minute limit for kids under new regulations. https://www.independent.co.uk/tech/tiktok-douyin-china-40-minutes-limit-b1923255.html. Accessed 15 January 2025.

Independent (2024) China kicks top influencer off social media for fabricating viral story of boy's lost homework. https://www.independent.co.uk/asia/china/china-ban-influencer-thurman-maoyibe-homework-b2528883.html. Accessed 15 January 2025.

Internet Society of China (2024) 适用于未成年人的移动智能终端指南 [Mobile Smart Terminal Guide for Minors]. https://www.isc.org.cn/profile/2024/09/03/790c2b4f-7894-4fff-8615-ff95a17ce349.pdf. Accessed 15 January 2025.

Ji Y et al (2022) Risk and protective factors of Internet gaming disorder among Chinese people: A meta-analysis. Australian & New Zealand Journal of Psychiatry 56(4), 332-346.

Jiang, Q. (2022). Development and effects of internet addiction in China. In Oxford Research Encyclopaedia of Communication. Oxford University Press, Oxford.

Johnston L and Shearing C (2003) Governing Security Explorations in Policing and Justice. Routledge, London.

Kim SW and Douai A (2012) Google vs. China's "Great Firewall": Ethical implications for free speech and sovereignty. Technology in Society 34: 174.

King G, Pan J and Robers ME (2013) How Censorship in China Allows Government Criticism but Silences Collective Expression. American Political Science Review 107: 326.

Lilkov D (2020) Made in China: Tackling digital authoritarianism. European View 19(1), 110-110.

Lin Bibo (2024) Beyond authoritarianism and liberal democracy: understanding China's artificial intelligence impact in Africa. Information, Communication & Society 27: 1126-1141.

Migliorini S (2024) China's Interim Measures on generative AI: Origin, content and significance. Computer Law & Security Review 53, 105985.

Min T and Narisong H (20200 Parsing the effect of the internet on regime support in China. Government and Opposition 55: 1, 130–46.

National Cybersecurity Standardization Technical Committee (2024) 生成式人工智能服务安全基本要[Basic security requirements for generative artificial intelligence service] (TC260-003, 29 February 2024). https://perma.cc/GU3Q-GAJ3. Accessed 15 January 2025.

National Technical Committee 260 on Cybersecurity of Standardization Administration of China 2024. 生成式人工智能服务安全基本要求 [Basic security requirements for generative artificial intelligence service].

National Technical Committee of Press and Publication Standardization (2017) 网络游戏防沉迷系统规范 [Requirement of enthrallment preventing system for online games]. https://static1.tianyancha.com/czd_file/standard/a378a77af52b8a32a41b7a854b9bb5c5.pdf. Accessed 31 January 2025).

NBC News (2024) Did TikTok videos inspire a teen's suicide? (22 April 2024). https://www.nbcnews.com/tech/social-media/tiktok-suicide-videos-lawsuit-social-media-self-harm-rcna146680. Accessed 31 July 2024.

New York Times (2007) China: Valid IDs to Limit Time Youths Play Online. https://www.nytimes.com/2007/04/10/world/asia/10briefs-online.html. Accessed 31 July 2024.

Office of the United Nations High Commissioner for Human Rights (2022) Written Statement about China Federation of Internet Societies (CFIS)' Efforts on Promotion and Protection of Human Rights and Gender Equality https://www.ohchr.org/sites/default/files/2022-01/CFIS.pdf. Accessed 15 January 2025.

Ostrom E (2010) Beyond markets and states: polycentric governance of complex economic systems. American economic review 100(3), 641-672.

Oswald ME and Grosjean S (2004) Confirmation Bias. In Pohl RF (ed) Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory. Psychology Press, London, pp 79-96.

People's Daily (2017) 网络如何祛除"电子鸦片" [How to eradicate "electronic opium" from cyberspace] (10 September 2017). http://opinion.people.com.cn/n1/2017/0910/c1003-29525576.html. Accessed 15 January 2025.

People's Daily (2024) China issue guidelines to promote juveniles mode on mobile internet (15 November 2024). http://en.people.cn/n3/2024/1115/c90000-20242726.html. Accessed 15 January 2025.

Quintanilla J (2023) Generative AI makes fraud an existential threat to science. Research Professional News (2 November 2023). https://www.researchprofessionalnews.com/rr-news-uk-views-of-the-uk-2023-11-generative-ai-makes-fraud-an-existential-threat-to-science/. Accessed 31 January 2025.

Reuters (2021) Explainer: Why and how China is drastically limiting online gaming for under 18s. https://www.reuters.com/world/china/why-how-china-is-drastically-limiting-online-gaming-under-18s-2021-08-31/ .Accessed 31 July 2024.

Roberts H et al (2021) The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. In: Floridi L (ed) Ethics, Governance, and Policies in Artificial Intelligence. Springer International Publishing, Cham, pp 47-79.

Roberts H et al (2023) Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. The Information Society 39(2), 79-97.

Roberts ME (2018) Censored: Distraction and Diversion Inside China's Great Firewall. Princeton University Press, Princeton.

Saich T (2000) Negotiating the State: The Development of Social Organizations in China. The China Quarterly 161, 124-141.

Sheehan M (2023) China’s AI regulations and how they get made. Horizons: Journal of International Relations and Sustainable Development (24), 108-125.

Sheehan M (2024) Tracing the Roots of China’s AI Governance. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/02/tracing-the-roots-of-chinas-ai-regulations. Accessed 15 January 2025.

Sohu (2024) “秦朗丢作业”1 条视频赚 55 万 [“Qinlang’s lost homework” earned RMB550,000 per video]. https://www.sohu.com/a/771768319_228864. Accessed 31 January 2025.

Spaulding NW (2023) Online Dispute Resolution and the End of Adversarial Justice?. In: Engstrom DF (ed) Legal Techn and Future of Civil Justice. Cambridge University Press, Cambridge. pp 251-285.

State Council of PRC (2017) New Generation Artificial Intelligence Development Plan. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm. Accessed 6 January 2025

State Council of PRC (2020) 中华人民共和国未成年人保护法[Law of the People's Republic of China on Protection of Minors]. https://www.gov.cn/xinwen/2020-10/18/content_5552113.htm. Accessed 15 January 2025.

State Council of PRC (2024a) 未成年人网络保护条例[China's Regulation on Protection of Minors in Cyberspace]. https://www.gov.cn/zhengce/content/202310/content_6911288.htm. Accessed 15 January 2025.

State Council of PRC (2024b) 国务院 2024 年度立法工作计划[Annual Plan for Legislative Work]. https://www.gov.cn/zhengce/content/202405/content_6950093.htm. Accessed 15 January 2025.

Sweney M, Davidson H (2021) China’s Tencent tightens games controls for children after state media attack’ The Guardian. https://www.theguardian.com/business/2021/aug/03/chinas-tencent-tightens-controls-for-children-amid-games-addiction-fears. Accessed 31 July 2024.

Tan L (2022) Douyin’s New Rules: More Control Under the Pretext of “Protecting Minors”. Bitter Winter. https://bitterwinter.org/douyins-new-rules-more-control/. Accessed 31 July 2024.

Tang C et al (2017) Addiction to internet use, online gaming, and online social networking among young adults in China, Singapore, and the United States. Asia Pacific Journal of Public Health 29(8), 673-682.

Taylor M (2022) China’s Digital Authoritarianism. Palgrave Macmillan, London.

Telecommunication Terminal Industry Forum Association (2022) 移动终端未成年保护技术要求 [Technique requirement of minor protection for mobile terminal]. https://www.taf.org.cn/upload/notice/2022-0706-085546-7389778.pdf. Accessed 15 January 2025.

Telecommunication Terminal Industry Forum Association (2022) 移动终端未成年保护技术要求 [Technique requirement of minor protection for mobile terminal].

https://www.taf.org.cn/upload/AssociationStandard/TTAF%20120-2022%20%E7%A7%BB%E5%8A%A8%E7%BB%88%E7%AB%AF%E6%9C%AA%E6%88%90%E5%B9%B4%E4%BF%9D%E6%8A%A4%E6%8A%80%E6%9C%AF%E8%A6%81%E6%B1%82.pdf. Accessed 15 January 2025.

Tencent (2024) 编个段子就要损失几个亿？[Loss of hundreds of millions just for staging a joke?]. https://news.qq.com/rain/a/20240414A076NB00. Accessed 31 January 2025.

Toureille C (2020) 'Stupidity at its best': TikTok star, 22, is slammed for LICKING an airplane toilet seat for a 'coronavirus challenge'. Daily Mail (16 March 2020). https://www.dailymail.co.uk/femail/article-8116799/Tik-Tok-star-22-slammed-licking-toilet-seat-claiming-complete-coronavirus-challenge.html. Accessed 15 January 2025.

Tuzov V, Lin F (2024) Two paths of balancing technology and ethics: A comparative study on AI governance in China and Germany. Telecommunications Policy 48(10), 102850.

Wang P (2022) Recommendation Algorithm in TikTok: Strengths, Dilemmas and Possible Directions. International Journal of Social Science Studies 10(5): 60.

Wang W et al (2024) Artificial Intelligence "Law(s)" in China: Retrospect and Prospect. http://dx.doi.org/10.2139/ssrn.5039316.

Washington Post (2021) China’s nanny state grows ever more intrusive. https://www.washingtonpost.com/opinions/2021/09/07/china-crackdown-personal-freedoms-video-games/. Accessed 31 July 2024.

Wood J, Shearing C (2007) Imagining Security. Willan, London.

Wu L, Liu P (2022) Investigation and Analysis of the Status Quo of Social Organization Standards in Chinese Civil Astronautics Field. Mathematical Problems in Engineering 2022(1), 4578080.

Xinhua News Agency (2022) 聚焦《互联网信息服务算法推荐管理规定》五大看点 [Focus on five key points of Algorithm Provisions] (6 January 2022). https://www.gov.cn/zhengce/2022-01/06/content_5666768.htm. Accessed 31 July 2024.

Yang E, Roberts ME (2023) The Authoritarian Data Problem. Journal of Democracy 34(4), 141-150.

Ye Z, Huang Q and Krijnen T (2025) Douyin’s playful platform governance: Platform’s self-regulation and content creators’ participatory surveillance. International Journal of Cultural Studies 28(1): 80.

Zeng J (2020) Artificial intelligence and China's authoritarian governance. International Affairs 96(6), 1441-1459.

Zeng J (2022) Artificial intelligence with Chinese characteristics: National strategy, security and authoritarian governance. Palgrave Macmillan, London.

Zheng G, Shu J (2024) In the name of protection—A critical analysis of China's legal framework of children's personal information protection in the digital era. Computer Law & Security Review 53, 105979.