

China's Proactive Role in Shaping Global AI Governance: A WTO-Centric Analysis of Digital Sovereignty and Trade in Services

Zihan Chen *

Abstract: The advent of Generative Artificial Intelligence (GAI) has ignited a global imperative for regulatory frameworks, creating significant friction with the established principles of the multilateral trading system, particularly in the area of international trade in services. As a pivotal actor in both Artificial Intelligence (AI) development and regulation, the People's Republic of China has meticulously constructed a sophisticated legal and administrative architecture to govern GAI services. This framework, deeply rooted in a vision of "digital sovereignty", prioritizes national security, social stability, and technological self-reliance. This article offers a comprehensive analysis of China's GAI governance model, critically assessing its compatibility with the core disciplines of the World Trade Organization (WTO). It deconstructs China's key regulatory instruments, including the Cybersecurity Law, the Data Security Law, and the specific measures for GAI, and examines their interaction with foundational WTO agreements, primarily the General Agreement on Trade in Services (GATS). The analysis focuses on the friction points arising from China's data governance regime and content moderation requirements, evaluating them against GATS principles of market access, national treatment, and domestic regulation. Furthermore, the article scrutinizes the viability of China invoking GATS general and security exceptions to justify its measures. It argues that China's approach constitutes a cohesive, development-oriented alternative to the liberal, market-driven model of digital governance, representing a sovereignty-focused strategy rather than a set of isolated trade policies. The article concludes by assessing China's strategic evolution from a rule-taker to a proactive rule-shaper in global AI governance, particularly through its engagement in the Joint Statement Initiative (JSI) on e-commerce and its pursuit of bilateral and multilateral pathways to lead the formulation of international services trade AI standards, while also considering the systemic implications for the future of the WTO in the digital era.

Keywords: GAI, China, WTO, GATS, Digital Sovereignty, JSI

I. INTRODUCTION

In our daily lives, AI products have become not just common but truly

* Zihan Chen, PhD. Candidate, Law School, Tsinghua University; Editor-in-Chief of Tsinghua China Law Review. Email: chenziha24@mails.tsinghua.edu.cn.

ubiquitous, profoundly transforming the way we work, learn, and entertain ourselves on a fundamental level. This technological integration is now a seamless part of our modern experience. A whole range of modern experiences, from the intelligent personal assistants embedded in our smartphones that can now accurately recognize and interpret complex voice commands, to the sophisticated intelligent algorithms on streaming platforms and ecommerce sites recommending movies, music, and shopping items with ever-increasing precision, from AI-assisted systems helping doctors diagnose diseases with greater speed and accuracy, to the gradual popularization of autonomous vehicles that promise to redefine mobility, even the personalized content streams we see on social media are powered by robust GAI technology. This advanced form of AI, GAI, not only understands and generates natural language with human-like nuance but can also create entirely new images, music, and even write functional software code. Its application scenarios are expanding at an astonishing pace, permeating every aspect of our lives and becoming an indispensable and deeply integrated part of modern society's digital fabric.

To make this transformation tangible, let's consider a scenario: A small legal firm in Beijing wishes to provide specialized legal research services to clients in Southeast Asia. Traditionally, this would involve significant logistical challenges, including establishing a physical presence, hiring local legal experts, and navigating complex cross-border regulatory hurdles. However, with the advent of GAI, this firm can now leverage an advanced GAI-powered legal research platform. Hosted on a cloud server, this platform can rapidly analyze vast amounts of legal texts, precedents, and regulations from multiple jurisdictions, generating highly accurate and context-specific legal advice in a fraction of the time that would take a human team. This valuable service can be delivered instantly to clients in Singapore, Jakarta, or Bangkok via secure digital channels, bypassing the need for physical establishments or extensive local hiring. In essence, the GAI platform acts as a virtual legal expert, enabling the Beijing firm to offer its services globally with unprecedented efficiency and scale. This example vividly illustrates how GAI is dissolving traditional geographical barriers to service provision, transforming the nature of cross-border trade in services from a capital-intensive, physical presence-based model

to a digitally-enabled, instantaneous exchange of intelligent output.

Similarly, imagine a Chinese e-commerce giant based in Hangzhou looking to expand its online customer service operations into emerging markets in Africa. The traditional approach would be daunting. Building large, multi-lingual call centers in each country is a process fraught with high capital expenditure and complex human resource management. In contrast, the company can deploy a GAI-powered chatbot system. This system is more than a simple chatbot; it is a highly sophisticated, multilingual customer engagement platform. Trained on vast datasets of customer interactions and, crucially, on local dialects and cultural contexts, it can handle millions of inquiries simultaneously, providing instant, personalized support in various African languages. It can resolve common issues, guide customers through purchases, and even escalate complex problems to human agents when necessary, ensuring a seamless customer experience. This GAI solution allows the Chinese firm to efficiently scale its customer support across diverse linguistic and cultural landscapes at a marginal cost, overcoming traditional barriers to language, time zones, and human resource limitations. By doing so, this GAI deployment directly facilitates rapid market penetration and dramatically enhances global service delivery.

The emergence of GAI represents a profound technological watershed, poised to fundamentally reconfigure global economic and power dynamics, especially in the realm of international trade in services. The global services sector has already become the largest contributor to economic output in most developed nations, and it now stands on the precipice of a GAI-driven transformation that transcends traditional boundaries and operational paradigms.¹ From highly sophisticated automated legal and financial consulting services delivered instantaneously via secure cloud platforms to hyper-personalized educational curricula and immersive entertainment content streamed directly to consumers across continents, GAI is rapidly dissolving geographical barriers to service provision. This unprecedented technological disruption fundamentally challenges the adequacy and adaptability of the existing international legal architecture for trade. At the heart of this

¹ UNCTAD, Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow, Geneva: UNCTAD, 2021.

architecture is the WTO, whose foundational agreements, most notably the GATS, were meticulously negotiated in a pre-AI era characterized by vastly different technological capabilities and trade patterns. Countries possess different technological capabilities and trade patterns. These agreements are now being rigorously tested by the novel complexities of digital trade, where the very nature of a “service”, its “supply”, and its “origin” are being redefined by AI.² The sheer volume, velocity, and versatility of GAI-enabled services demand a re-evaluation of concepts like market access, national treatment, and domestic regulation, pushing the WTO to its adaptive limits.

However, the regulatory responses to GAI have been far from uniform, revealing a deep and increasingly pronounced chasm in philosophical approaches among major global economies. This divergence is arguably most pronounced in the case of the People’s Republic of China, whose trajectory in digital governance stands in stark contrast to its Western counterparts. The United States (US) has largely pursued a decentralized, market-driven, and sector-specific approach that prioritizes rapid innovation and relies heavily on existing legal authorities,³ often resulting in a fragmented regulatory landscape. In contrast, the European Union (EU) champions a comprehensive, rights-based, and risk-averse model embodied in its landmark AI Act.⁴ The EU’s approach seeks to regulate AI systems based on their potential to cause harm, emphasizing fundamental rights, human oversight, and accountability, and notably asserting extraterritorial reach. In contrast, China has pioneered a distinct path characterized by systematic governance and an overarching emphasis on national sovereignty,⁵ which it terms “digital sovereignty”. This concept is a deeply ingrained guiding principle that seeks to ensure that the development, deployment, and governance of all digital technologies, including the transformative capabilities of GAI, align meticulously with the state’s

² World Economic Forum, *ChatWTO: Generative AI and International Trade*, September 4, 2024. This report highlights the inadequacies of existing trade rules in addressing GAI-specific challenges.

³ The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023.

⁴ European Parliament, *EU AI Act: First Regulation on Artificial Intelligence*, June 14, 2023.

⁵ For a comparative overview of regulatory approaches, see Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020. While predating GAI, it establishes the conceptual framework for contrasting the EU, US, and Chinese models.

strategic interests, political values, and paramount security imperatives.⁶

China has established a sophisticated and multi-layered governance framework for Generative AI (GAI). Rather than a single law, it is a comprehensive ecosystem of legislation, administrative guidance, technical standards, and judicial practices, designed to provide clear guidance and regulation for data, algorithms, and content. This forward-looking governance model is rooted in China's long-term vision for comprehensive national development. Its core objective is to ensure the digital environment remains stable and harmonious, serving the nation's continued progress and the well-being of its people. This holistic approach integrates cybersecurity and data security with the promotion of positive social values — all key areas of focus in the era of GAI. Key regulations within this framework, such as the Cybersecurity Law (CSL), the Data Security Law (DSL), the Personal Information Protection Law (PIPL), and specific GAI provisions, work in concert to build a secure, orderly, and trustworthy environment for digital development. The framework promotes the development of local data infrastructure, encourages the cultivation of healthy and constructive online content, and is committed to enhancing algorithmic fairness and transparency. It is designed to achieve an ideal balance between stimulating the vitality of the digital economy and safeguarding public interest and social harmony. This unique governance system showcases an innovative path that closely aligns state-guided technological innovation with national development goals, emphasizing that technological progress should serve the collective interests and long-term well-being of society as a whole.

This article interrogates the critical question of how China's state-led GAI governance model interacts with its obligations under the WTO legal framework, with a specific focus on cross-border trade in services. It moves beyond a simplistic compliance checklist to offer a strategic analysis of China's posture within the multilateral trading system. The central thesis is that China's GAI regulations, while interacting in complex ways with

⁶ The concept is extensively discussed in Xi Jinping, Full Text of the Report to the 20th National Congress of the Communist Party of China, October 16, 2022, <https://www.idcpc.org.cn/english2023/tjzl/cpcjj/20thPartyCongrressReport/> (Last Visited on July 18, 2024).

established WTO norms, are not merely *ad hoc* protectionist measures but reflect a coherent national strategy. Instead, they are integral components of a deliberate, long-term strategy to legitimize a distinct model of digital governance that fundamentally prioritizes state control and national sovereignty in the digital sphere. This strategy involves not only vigorously defending its domestic regulations through expansive interpretations of existing WTO exceptions, particularly those related to national security and public order, but also proactively seeking to influence the formation of new global rules for the digital economy. It represents a concerted attempt to construct a parallel, legitimate normative order for digital services trade, one that can coexist with the liberal paradigm of open markets and non-discrimination embedded in the GATS, though it may occasionally face strategic challenges. The analysis will particularly highlight China's proactive and increasingly assertive role in shaping global AI governance, emphasizing its unique characteristics, its firm stance on digital sovereignty as a core principle, and its increasing engagement within and beyond the WTO framework to lead the formulation of international services trade AI standards. This includes its active participation in the JSI on e-commerce, as well as its strategic pursuit of bilateral agreements and engagement in various multilateral forums and international standards-setting bodies to advance its vision for AI governance.

The analysis proceeds in four parts. Part II meticulously maps the architecture of China's GAI regulatory state, detailing the key legal instruments that form its backbone, the intricate roles of various state actors (including ministries, regulatory bodies, and industry associations), and the underlying policy objectives that drive this comprehensive framework. A specific emphasis will be placed on identifying and analyzing the "Chinese characteristics" deeply embedded within this framework, distinguishing it from other global approaches. Part III then conducts a rigorous "stress test" of this regulatory architecture, evaluating its core components against the foundational disciplines of the GATS, including market access, national treatment, and transparency obligations. This section will identify areas of potential tension and divergence. Part IV provides an in-depth analysis of the national security "shield", examining the legal viability and potential scope of China's GAI measures

under the GATS general exceptions (Article XIV) and, more critically, the security exceptions (Article XIV *bis*), with detailed reference to relevant WTO jurisprudence and recent interpretations of national security. Finally, Part V assesses China's evolving role from a passive rule-taker in the international trading system to an active and influential rule-shaper in global AI governance. This section will focus on China's strategic engagement in the JSI on e-commerce within the WTO, its pursuit of bilateral and multilateral pathways, and its broader efforts to lead the formulation of international services trade AI standards, thereby asserting its vision for the future of digital trade. The conclusion synthesizes the findings from these analytical parts and reflects on the systemic implications of China's distinctive approach to the future of the multilateral trading system for services in an increasingly AI-driven global economy.

II. THE ARCHITECTURE OF CHINA'S GAI REGULATORY STATE: EMBODYING "CHINESE CHARACTERISTICS"

China's governance of GAI is not an *ad hoc* reaction but the culmination of a decade-long effort to construct a comprehensive system of control over its domestic digital ecosystem. This framework is built upon a foundation of national-level laws, refined by specific administrative measures, and enforced by a network of powerful state agencies. The overarching objectives are threefold: ensuring national security in its broadest sense, maintaining social stability through stringent content control, and fostering indigenous technological innovation to achieve self-reliance and global competitiveness in a critical strategic sector.⁷ These objectives are deeply intertwined with the concept of "digital sovereignty", a cornerstone of China's approach to cyberspace governance, which emphasizes state control over data, infrastructure, and content within its borders. This section will delve into the legal and institutional architecture, highlighting the "Chinese characteristics" that distinguish its approach.⁸

⁷ State Council of the People's Republic of China, New Generation Artificial Intelligence Development Plan, Issued on July 8, 2017.

⁸ See Table 1 of China's Generative AI Regulatory Framework: Legislative Architecture.

At the core of this legal architecture are several foundational statutes that collectively regulate data and online activities. The CSL of 2017 establishes the baseline for network security, defining obligations for network operators and introducing the concept of “critical information infrastructure” (CII), which subjects key sectors to heightened scrutiny. Building on this, the DSL of 2021 creates a comprehensive framework for data classification and management, distinguishing between general data and “important data” that is subject to stricter controls, and imposes broad security obligations on all data processing activities. Complementing these is the Personal Information Protection Law (PIPL) of 2021, which closely mirrors the European Union’s General Data Protection Regulation (GDPR) in its stringency, mandating explicit consent for data collection and imposing rigorous procedures for cross-border data transfer (CBDT). Together, these three landmark statutes form a legislative tripod that serves as the bedrock of China’s digital sovereignty, providing the overarching legal authority for the state to govern the digital domain, upon which more specific AI-related measures are built.

The CSL of 2017 was the foundational legislative act, formally establishing the principle of “cyberspace sovereignty” and imposing a wide range of security obligations on all “network operators”.⁹ Its most trade-impactful provision is Article 37, which mandates that “Critical Information Infrastructure Operators” (CIIOs) must store personal information and “important data” collected and generated within China’s territory domestically. The ambiguous and expansive definition of CIIO, which includes sectors from energy and finance to public services and e-commerce, creates significant uncertainty for foreign service suppliers.¹⁰ The CSL’s legislative history reveals a clear intent to grant the state extensive visibility and control over data flows deemed critical to the national interest, reflecting a deep-seated concern about information security as a component of national security.

Building upon the CSL’s foundation, the DSL of 2021 further solidified

9 Cybersecurity Law of the People’s Republic of China, Adopted by the Standing Committee of the National People’s Congress, November 7, 2016.

10 Office of the United States Trade Representative, 2023 Report to Congress on China’s WTO Compliance, p. 64, <https://ustr.gov/sites/default/files/2023%20Report%20to%20Congress%20on%20China's%20WTO%20Compliance.pdf> (Last Visited on August 15, 2025).

state control by establishing a comprehensive, top-down data classification and protection regime. The DSL mandates a hierarchical system that categorizes data based on its importance to national security and public interest, creating distinct obligations for handling “national core data” and “important data”. Unlike the CSL, which primarily targeted CIIOs, the DSL extends data security obligations to all entities processing data in China, significantly broadening the regulatory net. This framework was completed by the 2021 PIPL, China’s first comprehensive statute dedicated solely to personal data. Often compared to the EU’s GDPR for its stringency, the PIPL imposes strict consent-based requirements for data collection and processing. Crucially for international trade, it establishes a stringent gatekeeping mechanism for CBDDT. Specifically, firms must use one of three legal pathways before personal information can leave the country, namely, a mandatory security assessment by the Cyberspace Administration of China (CAC), standard contractual clauses, or a recognized certification. Together, these three statutes create an interlocking and multi-layered governance system that gives the state extensive legal authority to manage data as a strategic national asset.

The DSL of 2021 builds upon the CSL by establishing a comprehensive framework for data governance based on risk. It introduces a hierarchical system for data classification, distinguishing between “core” data (related to national security and the economy), “important” data, and general data, with progressively stricter controls applied to higher tiers.¹¹ The DSL solidified the state’s control over data as a national strategic resource. It formalized the security review process for all cross-border transfers of “important data”, effectively creating a state-controlled checkpoint for data leaving the country. Its enforcement has begun to impact multinational corporations, which now face complex internal audit and government reporting requirements to justify data exports.¹² This tiered approach to data management, with its emphasis on national strategic resources, is a distinct “Chinese characteristic” that contrasts with more liberal data governance models.

¹¹ Data Security Law of the People’s Republic of China, Adopted by the Standing Committee of the National People’s Congress, June 10, 2021.

¹² Sam Sacks, Center for Strategic and International Studies, China’s Emerging Data Privacy System and GDPR, March 9, 2018, <https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr> (Last Visited on August 15, 2025).

As a supplement to the broad data security frameworks of the CSL and DSL, the PIPL was also enacted in 2021, providing specific and strict rules for the management of personal data. Often described as China's equivalent to the EU's GDPR, the PIPL establishes a robust and consent-based regime. It mandates that data handlers obtain clear and informed consent from individuals before processing their information and requires "separate consent" for handling sensitive personal data or transferring it abroad. Most critically for cross-border services, the PIPL codifies a strict gatekeeping system for any personal information leaving China. Companies must choose one of three legally mandated mechanisms: passing a security assessment conducted by the CAC for large-volume transfers, entering into a standard contract with the foreign recipient based on a government-issued template, or obtaining a recognized data protection certification. These multi-step requirements create significant compliance obligations for global GAI firms, whose operations often depend on the seamless transfer of data for centralized model training and development. Thus, the PIPL completes the legal triad, solidifying a governance model where state oversight of personal data flows is paramount.

Completing the triumvirate, the PIPL of 2021 established a comprehensive data privacy regime that draws inspiration from the EU's GDPR but embeds it within a state-centric context.¹³ While it grants individuals rights over their data, it also provides broad grounds for state access for national security and public interest purposes. For cross-border trade in services, the most crucial provisions are the strict conditions for transferring personal information to the outside of China. These conditions require either the individual's separate consent, a government security assessment, or certification from a designated body.¹⁴ The PIPL aligns with global privacy trends while also establishing a robust framework to safeguard national security and the public interest, reflecting a responsible and forward-thinking approach to data governance.

Building on this legal foundation, Chinese regulators have issued a series of specific administrative measures to govern the application layer of AI. A

¹³ Personal Information Protection Law of the People's Republic of China, Adopted by the Standing Committee of the National People's Congress, August 20, 2021.

¹⁴ Daniel Albrecht, Chinese First Personal Information Protection Law in Contrast to the European GDPR, *Computer Law Review International*, Vol. 23, No. 1, 2022, p. 15.

key early step was the 2022 Provisions on the Administration of Algorithm Recommendation Services, which imposed rules on platforms to ensure user rights and fair competition, while also mandating that algorithmic outputs align with state-approved values. More pointedly, the 2023 Interim Measures for the Management of Generative Artificial Intelligence Services directly addresses the technology at hand. These measures hold service providers explicitly responsible for the outputs of their models, requiring them to ensure the legality of their training data, implement mechanisms to prevent the generation of harmful content, and clearly label all AI-generated material. These targeted rules illustrate China's granular, hands-on approach, translating broad principles of data security and state control into direct operational requirements for AI service providers.

Based on this statutory foundation, Chinese regulators have issued more targeted rules. The Provisions on the Management of Algorithm Recommendation Services (2022) is a pioneering step in directly regulating the logic of AI systems. These rules impose obligations on service providers to promote positive and constructive social values, prevent the generation of illegal and harmful information, protect users from algorithmic discrimination, and grant users the right to inspect and opt out of algorithmic personalization.¹⁵ These provisions set the stage for the direct governance of AI systems, functionality, moving beyond content moderation to address the underlying code. The emphasis on promoting positive social values reflects a commitment to responsible innovation, aiming to guide technological development in alignment with the public interest and principles of social harmony.

The most directly relevant regulation is the Interim Measures for the Management of Generative Artificial Intelligence Services (2023), which was issued as a set of regulations jointly by seven powerful government bodies led by the CAC.¹⁶ These measures apply to all GAI services offered to the public within China and place primary, non-delegable responsibility on service providers. The key obligations are extensive. Providers must ensure that the generated content adheres to “socialist core values” and does

¹⁵ Cyberspace Administration of China, Provisions on the Management of Algorithm Recommendation Services in Internet Information, December 31, 2021.

¹⁶ Cyberspace Administration of China, et al., Interim Measures for the Management of Generative Artificial Intelligence Services, July 10, 2023.

not contain material that subverts state power, undermines national unity, promotes terrorism, extremism, or ethnic hatred, or is otherwise prohibited by law. This requires sophisticated and costly real-time filtering systems.¹⁷ The legitimacy of training data is paramount; it must be from legal sources, and respects intellectual property rights. And, if it contains personal information, it must be based on consent or other legal grounds. Furthermore, providers must take measures to prevent algorithmic discrimination, clearly label AI-generated content, and, critically, undergo a security assessment conducted by state authorities before a service can be publicly launched. This assessment serves as a powerful gatekeeping mechanism, giving the state the final say over market entry.¹⁸ The explicit requirement to align GAI-generated content with mainstream social values is a key principle of this regulatory framework, demonstrating a philosophy of deeply integrating social responsibility and ethical considerations into technological governance.

The enforcement of this complex regulatory architecture is not monolithic. It involves a network of state actors with overlapping and distinct responsibilities. The CAC is the central and most powerful digital regulator, overseeing content, data security, and algorithm governance. The Ministry of Industry and Information Technology (MIIT) focuses on the industrial and technical aspects, managing the telecommunications infrastructure and promoting the AI industry. The Ministry of Science and Technology (MOST) leads the national strategy for AI research and development. Finally, the National Information Security Standardization Technical Committee (TC260) plays a crucial role in drafting technical standards that give practical effect to the broad principles outlined in the laws, often creating the specific compliance requirements that businesses must follow.¹⁹ These institutions have collectively

17 Matt Sheehan, *China's AI Regulations and How They Get Made*, Working Paper Carnegie Endowment for International Peace, July 10, 2023, https://carnegie-production-assets.s3.amazonaws.com/static/files/202307-Sheehan_Chinese%20AI%20gov-1.pdf (Last Visited on August 7, 2025).

18 Paul Triolo and Kendra Schaefer, *China's Generative AI Ecosystem in 2024: Rising Investment and Expectations*, National Bureau of Asian Research, June 27, 2024, <https://www.nbr.org/publication/chinas-generative-ai-ecosystem-in-2024-rising-investment-and-expectations/> (Last Visited on July 18, 2024).

19 See the official website of the National Information Security Standardization Technical Committee (TC260), which lists numerous drafts and finalized standards related to data security and privacy, <https://www.tc260.org.cn/> (Last Visited on July 18, 2024).

created a tightly controlled environment where the state is the ultimate arbiter of what constitutes acceptable GAI development and deployment. This governance model, centered on digital sovereignty, aims to explore a path to harmonize the open, non-discriminatory principles of the GATS with the imperative to safeguard national security and public order. It also showcases China's distinctive approach of integrating national strategic planning with social responsibility into its technological development.

III. A COMPLIANCE STRESS TEST: CHINA'S GAI FRAMEWORK AND WTO DISCIPLINES

The rise of GAI poses a profound challenge to the WTO, as its pre-digital agreements must now govern the cross-border delivery of AI-enabled services. From automated legal analysis and financial advice to sophisticated design and content creation, these new services are breaking through the limitations of the multilateral trade framework. In particular, the GATS was negotiated long before intangible, algorithmically driven, and autonomously generated services became a reality, making it difficult to adapt to these services.

The core of the WTO system is the principle of non-discrimination, operationalized through two core obligations that are paramount to the regulation of GAI services. The first is the Most-Favored-Nation (MFN) principle under GATS Article II. This is a sweeping, unconditional obligation requiring that any advantage, favor, privilege, or immunity granted to the services or service suppliers of one WTO member must be immediately extended to the like services and suppliers of all other members. The second pillar, National Treatment (NT), is defined in GATS Article XVII. Unlike the MFN, this is a specific commitment that applies only in sectors where a member has explicitly agreed to grant it. Where applicable, the NT obligation requires a member to treat foreign services and service suppliers no less favorably than its own "like" domestic services and suppliers. This principle is critical for assessing the WTO-compatibility of national AI regulations. It prohibits not only *de jure* discrimination (rules that explicitly target foreign firms) but also *de facto* discrimination, which arises from seemingly neutral

measures that actually impose disproportionate disadvantages on foreign competitors. For instance, a domestic regulation may require all generative AI models to prioritize the use of locally-held datasets for training. The core policy consideration for this measure is to strengthen data security and the protection of personal privacy, ensuring data is handled properly within the national regulatory framework. Concurrently, this also guides models to better adapt to the local cultural context and user needs, thereby fostering a domestic AI industry ecosystem that is both secure and full of innovative vitality.

GATS Article VI, Governing Domestic Regulation, is perhaps one of the most crucial provisions in the AI era. It seeks to ensure that a member's domestic rules, such as licensing requirements, technical standards, and qualification procedures, are not used as disguised barriers to trade. This is precisely the category to which most new GAI regulations belong, including rules on algorithmic transparency, bias mitigation, data governance, and model auditing. The disciplines of Article VI require that such measures be administered in a reasonable, objective, and impartial manner. Future disciplines under this article are expected to solidify a "necessity test", requiring that these regulations be "not more burdensome than necessary" to achieve a legitimate objective. This test will be the central analytical tool for scrutinizing measures like mandatory source code disclosure, which may be deemed disproportionately burdensome if less trade-restrictive alternatives like third-party audits could achieve the same accountability goal.

The implementation of China's comprehensive GAI regulatory framework, with its distinct "Chinese characteristics", raises significant questions of compliance with its WTO commitments, particularly under the GATS. The tension arises because measures designed to achieve digital sovereignty often manifest as barriers to cross-border trade in services. This section analyzes the primary points of friction, moving beyond a theoretical discussion to consider the practical impact on foreign service suppliers, focusing specifically on data governance and content moderation.

China's data governance regime, which imposes data localization and stringent controls on CDBT, directly strikes at the operational heart of modern GAI services, which are fundamentally reliant on the free and efficient flow of

data for model training, fine-tuning, and real-time operation. These measures may conflict with several GATS articles. In the realm of Market Access (GATS Article XVI), China has made specific commitments in “Computer and Related Services” (the Central Product Classification 84, CPC 84), which is most likely to cover a wide range of GAI services.²⁰ Its data localization requirements, particularly for CIIOs, can be construed as a *de facto* limitation on market access for cross-border supply.

Foreign GAI providers, whose competitive advantage often stems from the massive economies of scale achieved by training their models on global, centralized datasets, may find it economically or technically prohibitive to establish separate, localized data centers and training infrastructure in China. This effectively forces them to establish a commercial presence (Mode 3) to serve the Chinese market, which can be challenged as a measure prohibited under Article XVI:2(e) if it restricts their freedom to choose their preferred mode of supply. The “classification conundrum” adds another layer of complexity. China could potentially argue that certain advanced GAI services constitute a new, uncommitted sector, thereby avoiding its more liberal commitments under the more specific regulations.²¹

Regarding National Treatment (GATS Article XVII), although China’s data governance rules are formally origin-neutral, they may result in *de facto* discrimination.²² China’s domestic tech giants have developed their ecosystems entirely within China’s “Great Firewall”, giving them a natural advantage under rules mandating local data storage and processing. Their business models have already aligned with the regulatory framework. In contrast, foreign competitors, whose business models and technological advantages are built on global data aggregation and seamlessly integrated international infrastructure, face disproportionately higher compliance costs,²³ operational fragmentation, and

20 China’s Schedule of Specific Commitments, GATS/SC/20, which includes commitments under CPC 84, Computer and Related Services.

21 Mira Burri, The Impact of Digitalization on Global Trade Law, *German Law Journal*, Vol. 24, No. 3, 2023, pp. 551–573.

22 World Trade Organization, World Trade Report 2018: The Future of World Trade – How Digital Technologies Are Transforming Global Commerce, WTO Publications, 2018, pp. 120–125, https://www.wto.org/english/res_e/booksp_e/world_trade_report18_e.pdf (Last Visited on August 31, 2025).

23 Susan A. Aaronson, What Are We Talking About When We Talk About Digital Protectionism? *World Trade Review*, Vol. 18, No. 4, 2019, pp. 541–577.

strategic hurdles. This differential impact caused an enormous reflection on the competitive landscape.

Even if not considered a violation of market access or national treatment, these data rules must conform to the disciplines of Domestic Regulation (GATS Article VI). Once the future disciplines of Article VI:4 are finalized, it is expected that these measures, among other things, “are not more burdensome than necessary to ensure the quality of the service”. In the interim, panels often look to these principles for guidance. China would argue that its data localization and stringent CBDT review processes are necessary for ensuring data security and enabling effective regulatory oversight. However, a challenger could mount a strong case that less trade-restrictive alternatives exist to achieve the same objectives. Such alternatives could include the use of robust, internationally recognized encryption standards, reliance on binding corporate rules or contractual clauses for data transfers (as accepted in other jurisdictions), or the establishment of mutual recognition or adequacy decisions system with countries having comparable data protection regimes.²⁴ The failure to consider or adopt such alternatives could render a blanket localization requirement “more burdensome than necessary”. Furthermore, the security assessment process for GAI models, a prerequisite for market entry, could be challenged under Article VI as a non-transparent and potentially arbitrary licensing requirement, lacking the “objective and transparent criteria” mandated by the provision.²⁵

However, a nuanced interpretation suggests that such measures, while distinct, do not inherently violate WTO rules. The GATS framework, particularly Article XIV (General Exceptions), explicitly permits members to adopt measures “necessary to protect public morals or maintain public order”. China could legitimately argue that “socialist core values” represent a fundamental aspect of its public morals and public order, akin to how other WTO members regulate content based on their own societal values (e.g., prohibitions on hate speech, child pornography, or incitement to violence). The

²⁴ US – *Measures Affecting the Cross-border Supply of Gambling and Betting Services*, Appellate Body Report, WT/DS285/AB/R, Adopted April 20, 2005, which elaborated on the “necessity test” under GATS Article XIV. The logic is often applied by analogy to Article VI.

²⁵ GATS Article VI:3 requires that licensing procedures should not in themselves be a restriction on the supply of a service.

challenge then shifts from the legitimacy of the objective to the “necessity” and non-discriminatory application of the measures. If China can demonstrate that content moderation requirements are applied equally to both domestic and foreign service providers, and that the “burden” is a consequence of legitimate regulatory objectives rather than a disguised restriction on trade, a National Treatment violation might be difficult to establish.

Furthermore, the “vagueness” of certain prohibitions, while challenging for compliance, is not unique to China’s regulatory environment; rapidly evolving technologies like GAI often necessitate adaptive and principles-based regulation, where specific interpretations may evolve with practice. The key to WTO compatibility lies in the consistent and non-discriminatory application of these principles, ensuring that foreign firms are not disproportionately targeted or subjected to arbitrary enforcement compared to their domestic counterparts. China’s argument would hinge on demonstrating that its content moderation regime, despite its unique ideological underpinnings, serves a legitimate public policy objective. It is applied in a manner consistent with its GATS obligations, particularly from the perspective of national security and public order exceptions.

Although China’s content moderation policies have distinct “Chinese characteristics”, the argument that they are compatible with the WTO rests on several pillars that deserve deeper exploration. Firstly, the concept of “public morals” or “public order” under GATS Article XIV(a) is inherently culturally and politically determined. There is no universally agreed-upon definition of what constitutes acceptable content or what threatens the social stability for all WTO members. Each sovereign nation retains the right to define its own public order and moral standards. For China, “socialist core values” are not merely abstract political slogans but are enshrined in its constitution and form the bedrock of its social governance. They represent the collective moral standards and foundational principles upon which Chinese society is built. Therefore, measures taken to ensure that GAI-generated content aligns with these values and does not promote content that is deemed harmful or subversive within the Chinese context can legitimately be argued as “necessary to protect public morals or maintain public order”. This is analogous to how Western

democracies prohibit hate speech, incitement to violence, or child exploitation, which are considered to violate their respective public morals or threaten public order. The fact that China's specific definition of "harmful content" may differ from those in other jurisdictions does not, by itself, render the measures WTO-incompatible, so long as the underlying objective falls within the scope of Article XIV(a).

Secondly, the "necessity test" under Article XIV must be carefully balanced. While a challenger might argue that there are alternative solutions with fewer trade restrictions, China could counter this by pointing out that, given the pervasive and influential nature of GAI, and its potential for rapid dissemination of information (or misinformation), stringent real-time filtering and content oversight are indeed necessary to achieve its legitimate public order objectives. The sheer scale of China's internet user base and the speed at which GAI can generate and spread content amplify the perceived risks to social stability. For example, by the end of 2023, China had over 1 billion internet users, representing a significant portion of the global online population.²⁶ This massive user base means that even a small percentage of problematic content can quickly reach millions. From China's perspective, a less restrictive approach might be deemed insufficient to prevent the rapid propagation of content that could, for example, incite ethnic hatred, undermine national unity, or promote extremist ideologies, which are genuine concerns for any large, diverse nation. The effectiveness of less restrictive measures, such as post-publication takedowns, might be questioned in the context of GAI's rapid content generation capabilities. Furthermore, China could emphasize that its regulatory framework is not designed to arbitrarily block all foreign content or services, but rather to ensure that any content or service accessible within its borders adheres to its fundamental legal and social norms. The "necessity" of a measure is often assessed in light of the specific context and the risks it aims to address. In *Korea — Beef*,²⁷ the Appellate Body emphasized that the necessity test involves a weighing and balancing of factors, including the

26 China Internet Network Information Center (CNNIC), The 53rd Statistical Report on China's Internet Development, February 2024.

27 *Korea — Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, Appellate Body Report, WT/DS161/AB/R, WT/DS169/AB/R, Adopted January 10, 2001.

importance of the interests or values pursued, the contribution of the measure to the realization of the goal, and the trade restrictiveness of the measure. China could argue that, given the significant societal impact of GAI, the importance of maintaining public order and protecting public morals outweighs potential trade restrictiveness, especially if less trade-restrictive alternatives are genuinely ineffective in addressing the unique challenges posed by GAI.

Thirdly, the charge of “*de facto* discrimination” under GATS Article XVII requires concrete evidence that foreign service providers are treated “less favorably” than domestic ones. While foreign firms might initially face a steeper learning curve in understanding China’s specific culture, this does not automatically equate to *de facto* discrimination. Chinese domestic firms are also subject to the same stringent content moderation requirements and face significant penalties for non-compliance. Indeed, many Chinese tech giants have invested heavily in sophisticated AI-powered content moderation systems and employ large teams of human reviewers to ensure compliance, demonstrating that the burden is universal. For instance, companies like ByteDance (owner of TikTok and Douyin) and Tencent may employ tens of thousands of content moderators, a significant operational cost that applies universally to all entities operating within China. The argument that foreign firms are “inherently less attuned” to China’s social environment could be viewed as a business challenge rather than a discriminatory regulatory measure. Foreign firms operating in any market must adapt to local laws, customs, and regulatory environments. If the rules are applied equally, the differential impact might stem from a lack of adaptation or understanding on the part of foreign firms, rather than from discriminatory intent by the regulator. China could also point to the fact that its content moderation rules are part of a broader, consistent regulatory philosophy that applies across various digital services, not just GAI, further demonstrating its non-discriminatory intent. In *Japan — Alcoholic Beverages II*,²⁸ the Appellate Body clarified that “less favorable treatment” involves an examination of the effects of a measure on competitive opportunities. China could contend that while foreign firms may experience a learning curve, their competitive opportunities are not intrinsically curtailed compared to domestic

²⁸ *Supra* n. 23.

firms as long as they make the necessary adaptations.

Fourthly, regarding the “objective and transparent criteria” requirement under GATS Article VI, while the term “socialist core values” might appear vague to an external observer, within the Chinese legal and political system, these values are extensively articulated in official documents, educational materials, and public discourse. While their application to new GAI outputs may require interpretation, this is true for any general legal principle applied to new technological contexts. China has also issued more specific guidelines and examples of prohibited content categories, even if they are not exhaustive. For example, the CAC has issued regulations like the Provisions on the Administration of Deep Synthesis Internet Information Services (2023) and the Interim Measures for the Management of Generative Artificial Intelligence Services (2023), which provide specific requirements for GAI providers, including content moderation obligations.²⁹ These regulations, though broad in some aspects, offer a framework for compliance. The security assessment process for GAI models serves as a gatekeeping mechanism to ensure compliance with these national standards before public launch, rather than an arbitrary barrier. If the criteria for these assessments are consistently applied and the process is predictable, even if complex, it might withstand a challenge under Article VI. The burden on the challenger would be to prove that the criteria are not objective or transparent, or that the process is arbitrary in its application, rather than simply challenging the underlying values themselves. The Appellate Body noted in *EC — Bananas III*³⁰ that transparency requires regulations to be publicly available and accessible, and their application to be predictable. China could argue that its regulatory framework, though evolving, aims to provide sufficient guidance to achieve predictability for operators.

Fifthly, considering the broader context of national security, China’s data localization and CBDT review processes are presented as essential for protecting CII and national data security. The rise of cyber threats and the

29 See Cyberspace Administration of China, Provisions on the Administration of Deep Synthesis Internet Information Services; Interim Measures for the Management of Generative Artificial Intelligence Services, Available on the CAC website, <http://www.cac.gov.cn/> (Last Visited on July 18, 2024).

30 *European Communities – Regime for the Importation, Sale and Distribution of Bananas*, Appellate Body Report, WT/DS27/AB/R, Adopted September 25, 1997.

increasing geopolitical significance of data have led many countries, including some developed nations, to adopt similar measures for sensitive data. For example, the EU's GDPR includes provisions for restricting CBDT to countries that do not provide an "adequate" level of data protection.³¹ While the justifications may differ, the underlying principle of regulating data flows for national security or data protection reasons is not unique to China. China's CSL (2017) and DSL (2021) establish a comprehensive legal framework for data governance, with specific requirements for "CIIOs" and "important data".³² These laws mandate data localization for certain types of data and require security assessments for CBDT, which are often cited as being crucial for national security. From China's perspective, these measures are proportionate to perceived threats, particularly given the large volume of data generated within its borders and its potential strategic value. In *China — Raw Materials*,³³ the Appellate Body acknowledged the right of WTO members to regulate their resources, but subject to the strict conditions of GATT Article XX. While this case dealt with goods, the underlying principle that a member has the right to regulate for legitimate public policy objectives, provided the measures are consistent with WTO obligations, remains relevant. China would argue that its data regulations are not disguised protectionism but genuine efforts to secure its digital infrastructure.

Finally, the concept of "necessity" in WTO jurisprudence is not an absolute standard, but rather requires a balance between the trade-restrictive impact of a measure and the importance of the policy objective. In *Brazil — Retreaded Tyres*,³⁴ the Appellate Body reiterated that the "necessity" test requires a weighing and balancing process, taking into account the extent to which the measure contributes to the achievement of the objective, and whether there are reasonable alternatives with fewer trade restrictions. China could argue that, given the specific societal and political context and the rapid

31 See European Union, General Data Protection Regulation (GDPR), Articles 45 and 46.

32 See China's Cybersecurity Law (2017) and Data Security Law (2021), official texts available from Chinese legislative bodies.

33 *China — Measures Related to the Exportation of Various Raw Materials*, Appellate Body Report, WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R, Adopted February 22, 2012.

34 *Brazil — Measures Affecting Imports of Retreaded Tyres*, Appellate Body Report, WT/DS332/AB/R, Adopted December 17, 2007.

evolution of GAI technology, its stringent measures are indeed necessary. The sheer scale and speed at which GAI can generate and disseminate content, coupled with the potential for misuse or manipulation, arguably necessitate a proactive and robust regulatory approach. While other countries may employ different regulatory models, China's choice of stringent controls can be justified as a response to its unique national circumstances and perceived risks to social stability and national security. The burden of proof would lie with the challenger to demonstrate that a truly less trade-restrictive alternative exists that could achieve the same level of security and public order protection as China's current measures. Merely pointing to alternative approaches adopted in other jurisdictions is not sufficient; the alternatives must be shown to be genuinely viable and effective in the specific Chinese context.

In sum, while China's content moderation regime for GAI services undeniably reflects its unique national characteristics and a strong state-centric approach, a comprehensive WTO analysis must acknowledge the legitimate public policy objectives underlying these measures. The key legal battleground would be demonstrating that these measures are "necessary" and applied in a non-discriminatory manner, rather than simply asserting that their distinct nature automatically implies WTO compatibility. China would emphasize its sovereign right to regulate content within its borders for public order and moral reasons, a right generally recognized within the WTO framework, provided the measures meet the strict test of necessity and non-discrimination requirement. The evolving nature of GAI and China's unique social and security considerations present a complex challenge, but from the perspective of national security and public order exceptions, China's regulatory framework can be argued to largely comply with its WTO obligations.

IV. THE NATIONAL SECURITY GAMBIT: JUSTIFICATION UNDER GATS ARTICLE XIV & XIV *BIS*

Faced with a litany of potential challenges to its GAI regulations, China is highly likely to invoke the GATS exceptions for national security and public

order as its primary legal shield. This section will analyze the viability of China's invocation of these exceptions, particularly in light of its broad definition of national security, and delve deeper into the implications of the *Russia — Measures Concerning Traffic in Transit* ruling.

GATS contains two relevant exception clauses. Article XIV (General Exceptions) allows members to take measures that would otherwise violate their GATS obligations if they are “necessary to protect public morals or to maintain public order” (XIVa),³⁵ or “necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement” (XIVc). Article XIV *bis* (Security Exceptions) permits a member to take any action “which it considers necessary for the protection of its essential security interests”.³⁶

The obligations enshrined within the GATS are not absolute. The agreement architects recognized that sovereign nations must retain the ability to regulate for critical public policy reasons, and therefore embedded two significant “safety valves” permitting WTO members to derogate from their core commitments: Article XIV (General Exceptions) and Article XIV *bis* (Security Exceptions). These provisions are central to understanding the potential WTO-compatibility of national GAI regulations, as they provide the legal grounds upon which a member can justify measures that might otherwise be found to violate principles of market access or non-discrimination. They represent the critical link between the need to promote trade liberalization and the necessity of domestic governance and national sovereignty.

GATS Article XIV provides a set of general exceptions to measures that pursue specific, legitimate public policy objectives. To successfully invoke this article, a member must pass a stringent two-tier test. First, the measure in question must be demonstrated to fall within one of the specific subparagraphs of Article XIV. For the regulation of GAI, the most relevant of these are subparagraph (a), concerning measures “necessary to protect public morals or to maintain public order”, and subparagraph (c), for measures “necessary to secure compliance with laws or regulations which are not inconsistent

35 General Agreement on Trade in Services, April 15, 1994; Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, Article XIV.

36 *Ibid.*, Article XIV *bis*.

with the provisions of this Agreement”, such as domestic privacy laws. WTO jurisprudence, particularly the landmark case of *US — Gambling*, has affirmed that WTO members have the right to determine the level of protection they deem appropriate for their own “public morals”, affording a significant degree of deference to national values. The “public order” ground is interpreted more narrowly, requiring a “genuine and sufficiently serious threat...to one of the fundamental interests of society”. Stringent content moderation rules for GAI, for example, would likely be defended under the public morals clause, while measures aimed at preventing AI-driven social instability or panic could be justified under the public order provision.

Separate from the general exceptions is GATS Article XIV *bis*, the Security Exceptions clause. This provision is substantively different and grants members a greater degree of deference. It allows a member to take any action that it “considers necessary for the protection of its essential security interests”. The text specifies three circumstances under which this can be invoked: (i) relating to the supply of services directly or indirectly for the purpose of provisioning a military establishment; (ii) relating to fissionable and fusionable materials; or (iii) action “taken in time of war or other emergency in international relations”. While the language “which it considers necessary” suggests a high degree of self-judgment, this discretion is not unlimited.

The 2019 panel report in *Russia — Measures Concerning Traffic in Transit*, the first WTO case to fully interpret this type of security exception, established critical boundaries. The panel ruled that while a member’s determination of what constitutes its “essential security interests” is largely self-judging, this determination is subject to an overarching obligation of good faith. More importantly, the panel found that the question of whether an action is “taken in times of war or other emergency in international relations” is not self-judging and can be objectively reviewed by the panel. The panel defined an “emergency in international relations” as a situation of a certain gravity, such as an armed conflict, a latent conflict, or a period of heightened tension and crisis. This ruling strikes a crucial balance: it respects a member’s sovereign right to define its own security needs but prevents the unfettered use of the exception for purely economic or political disputes by allowing for an objective assessment

of the factual circumstances. For GAI, this means that a member invoking this exception to block a foreign service would not only need to define the threat to its essential security interests but may also have to demonstrate to a panel that the situation rises to the level of an “emergency in international relations”, which is a high bar to clear in most commercial contexts.

China may argue that its data localization and content filtering rules are necessary to protect “public morals” and “public order” under Article XIV(a). To succeed, it would have to satisfy the two-tiered necessity test meticulously developed in WTO case law. First, the measure must be shown to make a material contribution to the stated objective. China would argue that controlling data flows and filtering content are essential to preventing social unrest, crime, and the erosion of its political values. Second, and more contentiously, it must be demonstrated that no less trade-restrictive, reasonably available alternative exists to achieve the same level of protection.³⁷ As discussed previously, a challenger could point to numerous less restrictive alternatives to blanket data localization. For content filtering, China’s case might appear stronger, but the sheer breadth and vagueness of its prohibitions could be challenged as disproportionate to the objective of maintaining public order, particularly when compared to more targeted regulations in other countries. Furthermore, any measure under Article XIV must also comply with the introductory clause, or “chapeau”, which requires that it is not “applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination ... or a disguised restriction on trade in services”.

More significantly, China could invoke Article XIV *bis*, which grants members significantly more deference in determining their security needs. For decades, this clause had largely been regarded as “self-judging” and non-justiciable, serving as a political safe harbor beyond the reach of WTO panels. However, the landmark 2019 panel report on *Russia — Measures Concerning Traffic in Transit* fundamentally changed this understanding.³⁸ Although this ruling pertained to a GATT dispute, it is widely considered applicable to the nearly identical language in GATS Article XIV *bis*. The panel in *Russia —*

³⁷ *Supra* n. 27.

³⁸ *Russia — Measures Concerning Traffic in Transit*, Panel Report, WT/DS512/R, Adopted April 26, 2019.

Measures Concerning Traffic in Transit rejected the notion that Article XXI (the GATT equivalent of GATS Article XIV *bis*) was entirely self-judging. Instead, it established a limited but significant scope for judicial review. While affirming a member's right to define its own essential security interests, the panel established that it could review whether the challenged measures are plausibly connected to those interests and, crucially, whether they are taken in "good faith". This means that a member cannot simply declare a measure to be for national security and expect it to be immune to scrutiny. The measure must have a legitimate, albeit self-determined, security rationale, and its application must not be a pretext for protectionism.

Applying this evolving framework to China's GAI regulations would involve a multi-step analysis. First, a panel would ask what China defines as its "essential security interests". Citing its own National Security Law, China defines these interests very broadly, encompassing not just traditional military security but also political security, ideological security, cultural security, and economic security.³⁹ This expansive definition of national security is a key "Chinese characteristic" that underpins its digital sovereignty framework, reflecting a comprehensive approach to national security that integrates various domains. Second, the panel would assess whether there is a plausible connection between these interests and the regulation of GAI. China would argue that GAI, as a powerful dual-use technology, has vast potential to shape public opinion, generate sophisticated disinformation, enable cyberattacks, and gather intelligence, posing a direct threat to all these facets of its national security. Given the dual-use nature of AI and its profound societal implications, the panel would likely afford China significant deference on this point, acknowledging the legitimate security concerns that arise from the widespread deployment of GAI technologies. The potential for GAI to be weaponized for cyber espionage, critical infrastructure attacks, or large-scale propaganda campaigns provides a plausible nexus between GAI regulation and national security.

The critical battleground would be the third step: the good faith

³⁹ National Security Law of the People's Republic of China, Adopted by the Standing Committee of the National People's Congress, July 1, 2015.

requirement. A challenger would argue that even if a security rationale exists, the measures are not being applied in good faith and are, in fact, a “disguised restriction on trade”. Evidence for this may include China’s own industrial policy documents, such as “Made in China 2025”, which explicitly state the goal of replacing foreign technology with domestic alternatives.⁴⁰ A challenger could argue that the true purpose of the GAI regulations is not security but protectionism — to insulate China’s domestic AI champions from foreign competition and allow them to flourish in a captive market. The timing, design, and application of these measures would be scrutinized for evidence of protectionist intent. For example, if the security assessment process for GAI services disproportionately delays or denies market access to foreign firms compared to domestic ones, or if the criteria for such assessments are applied in an opaque or inconsistent manner that favors domestic players, this could be construed as evidence of bad faith. A blanket ban on foreign GAI services, for instance, would likely fail this test, whereas a more tailored and transparent regulatory regime that applies objective risk criteria might survive scrutiny. The outcome of such a case would be pivotal, setting a precedent for how the WTO balances national security with trade obligations in the era of strategic technological competition, and critically examining the scope and interpretation of China’s “essential security interests”.

The “good faith” test introduced by *Russia — Measures Concerning Traffic in Transit* is particularly challenging for China’s defense. While the panel acknowledged that a member’s determination of its essential security interests is largely its own, it also stated that measures taken must be “objectively reviewed” to determine if they are “plausibly connected” to those interests and “applied in good faith”. This means that even if China asserts a broad interpretation of national security, the WTO panel can still examine the manner in which the measures are implemented. For instance, if data localization requirements are so stringent that they effectively exclude foreign GAI providers from the Chinese market without a clear, demonstrable security benefit that could not be achieved through less trade-restrictive means (e.g., robust encryption, data anonymization, or secure remote access), then the good faith argument

40 State Council of the People’s Republic of China, *Made in China 2025*, Issued on May 8, 2015.

could be undermined. Similarly, if content moderation requirements are applied in a way that disproportionately targets foreign-generated content or algorithms, or if the “security assessment” process for GAI models is used as a *de facto* market entry barrier rather than a genuine security review, these could be seen as indicators of protectionist intent disguised as security measures.

Furthermore, the WTO’s jurisprudence on exceptions often considers the proportionality of the measure. While Article XIV *bis* grants more deference than Article XIV, it is not absolute. The panel might consider whether the severity of the trade restriction is proportionate to the asserted security threat, or whether less trade-restrictive measures could achieve the same level of security. For example, if China’s security concerns could be adequately addressed through data mirroring, secure cloud computing solutions within China, or internationally recognized cybersecurity certifications, a blanket data localization requirement might be deemed disproportionate and thus not taken in “good faith”. The burden of proof would largely fall on China to demonstrate that its measures are indeed for genuine security interests and not primarily for economic protectionism. This would require presenting compelling evidence that the specific GAI regulations are a direct and necessary response to identifiable security threats, rather than part of a broader industrial policy aimed at fostering domestic champions. The outcome of such a dispute would not only impact China’s digital trade policies but also set a critical precedent for how national security exceptions are interpreted and applied in the context of emerging technologies and digital trade within the WTO framework. It would be a defining moment for the multilateral trading system, determining its capacity to address complex issues of trade, technology, and national sovereignty.

V. FROM RULE-TAKER TO RULE-MAKER: CHINA’S PROACTIVE ROLE IN SHAPING GLOBAL AI GOVERNANCE

China’s engagement with the WTO and other international bodies on AI governance is not merely defensive; it is not simply about justifying

its domestic regulations. It is part of a proactive, long-term strategy to shape emerging global norms in a way that legitimizes its model of digital sovereignty. This marks a significant evolution from its earlier, more passive role as a “rule-taker” in the global economic order following its WTO accession in 2001. China is now actively seeking to become a “rule-maker” in the digital domain, particularly emphasizing its unique characteristics, its firm stance, and its increasing role in leading the formulation of international services trade AI standards through various multilateral and bilateral pathways.

In multilateral forums like the United Nations and its specialized agencies, China has actively promoted its vision for AI and data governance. In 2020, it launched the Global Initiative on Data Security, a key diplomatic instrument.⁴¹ While paying lip service to the need to maintain an “open, secure and stable supply chain” for Information and Communications Technology (ICT) products and services, the initiative’s core principles strongly emphasize “respecting the data sovereignty, jurisdiction and security governance of all countries”. This initiative is a direct attempt to build an international consensus around a state-centric model of data governance, explicitly challenging the US-led vision of unrestricted cross-border data flows advocated for in trade negotiations. China has successfully promoted these concepts in various UN resolutions and discussions, seeking to embed the language of sovereignty into the lexicon of global digital governance, reflecting its deep-seated “Chinese characteristics” in governance.

Within the WTO, China’s position is more nuanced and strategically complex. It is an active participant in the JSI on e-commerce, a plurilateral negotiation among a large group of WTO members aimed at developing new rules for digital trade. This initiative, launched in 2017, seeks to address the gaps in existing WTO rules concerning digital commerce, including issues like electronic signatures, online consumer protection, paperless trading, and crucially, cross-border data flows and data localization. While many JSI participants, particularly developed economies, advocate for liberalizing provisions that prohibit data localization and ensure free data flow, China

⁴¹ Ministry of Foreign Affairs of the People’s Republic of China, China Releases the Global Initiative on Data Security, September 8, 2020.

has consistently championed a more cautious approach. Its stance within the JSI is characterized by a strong emphasis on the “policy space” necessary for developing members to regulate their digital economies, often invoking broad exceptions to national security and public order.⁴²

China’s strategy within the JSI is one of selective engagement. It actively supports provisions on trade facilitation, e-signatures, and consumer protection, as these align with its broader goals of promoting digital trade and its own e-commerce platforms globally. However, it steadfastly resists disciplines that would mandate unrestricted cross-border data flows or prohibit data localization requirements. China argues that such provisions could undermine its ability to protect national security, public morals, and maintain social stability, which are paramount concerns embedded in its digital sovereignty framework.

For instance, in discussions related to data, China has advocated language that acknowledges the legitimate right of states to regulate data flows for security purposes, often proposing texts that differ significantly from the more liberal proposals put forward by members like the US, Japan, and the EU. This includes resisting prohibitions on data localization and requirements for source code disclosure, arguing that these are vital to national security and effective regulatory oversight. By doing so, China aims to embed the principles of digital sovereignty directly into future trade agreements, thereby creating a “safe harbor” for its domestic regulatory framework and weakening any potential future WTO challenges. Its active participation, despite these reservations, is a strategic move to shape the multilateral trading system from within, ensuring future rules accommodate its unique approach rather than being imposed upon it. This engagement highlights China’s sophisticated understanding of multilateral diplomacy, as it seeks to influence the normative direction of global trade rules to align with its domestic governance philosophy.

The JSI, therefore, becomes a critical arena where China asserts its “Chinese characteristics” in digital governance on a global stage, seeking to legitimize its regulatory model through international consensus or at least through the absence of prohibitive international rules.

⁴² See positions outlined in various submissions to the WTO Joint Statement Initiative on E-Commerce. China’s submissions often emphasize the need for “policy space” for developing members.

This proactive diplomacy extends significantly beyond formal WTO negotiations, encompassing a robust network of bilateral and multilateral engagements that collectively reinforce China's vision for global AI governance. A prime example is the Belt and Road Initiative (BRI), which includes a substantial digital component known as the Digital Silk Road (DSR). Launched in 2015, the DSR is far more than just infrastructure development; it is a comprehensive strategy to export China's technological infrastructure, digital platforms, and governance norms to partner countries across Asia, Africa, Latin America, and even parts of Europe. Through the DSR, Chinese companies like Huawei, ZTE, Alibaba Cloud, and Tencent Cloud are building telecommunications networks, smart cities, e-commerce platforms, and data centers in participating nations. This technological export is often bundled with Chinese technical standards and implicitly incorporates elements of China's regulatory philosophy.

Beyond the DSR, China is actively pursuing bilateral digital economy agreements and incorporating digital trade provisions into its Free Trade Agreements (FTAs). While these agreements vary in scope and depth, they often reflect China's cautious approach to data flows and its emphasis on national security. Unlike many Western-led digital trade agreements, e.g., the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States-Mexico-Canada Agreement (USMCA), or the US-Japan Digital Trade Agreement that contain strong prohibitions on data localization and forced technology transfer, China's agreements tend to be more flexible, allowing for greater regulatory autonomy for the signatory states. For example, in its FTAs, China often advocates for provisions that permit data restrictions for legitimate public policy objectives, including national security, public order, and personal information protection. This approach allows China to sign agreements that promote digital trade while safeguarding its core digital sovereignty principles. These bilateral engagements serve as laboratories for China to test and refine its preferred digital governance norms and build a network of like-minded partners who are more amenable to its state-centric approach. Each such agreement, even if seemingly small, contributes to the incremental normalization of regulatory frameworks that prioritize state control

and data sovereignty over unfettered cross-border data flows, thereby subtly shifting the global normative landscape.

Furthermore, China is increasingly active and influential in international technical standards-setting bodies like the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and the Institute of Electrical and Electronics Engineers (IEEE). China recognizes that technical standards are not neutral; they embed values, define interoperability, and ultimately shape future markets and regulatory environments. By successfully promoting its preferred technical standards for emerging technologies like AI, 5G, blockchain, and the Internet of Things, China can ensure global interoperability with its own systems and create a technological ecosystem that reflects its regulatory priorities. For instance, China's proposals at the ITU have focused on areas such as "new IP" (a proposed internet protocol that could enable greater state control over network traffic) and standards for facial recognition or smart city technologies that inherently involve extensive data collection and processing.⁴³ This "standards-power" is a crucial component of its overall strategy to shape the global rules of the road for the digital economy, though it is often overlooked. By influencing the technical foundations that underpin the operation of digital services, China can subtly embed its governance principles into global technological infrastructure, thereby influencing future regulatory landscapes without direct legislative imposition.

Finally, China's proactive role extends to other multilateral platforms beyond the WTO and technical bodies. It actively participates in and shapes discussions within various UN bodies, including the UN General Assembly and the Human Rights Council, to promote its concepts of data sovereignty and state control over information. Its Global Initiative on Data Security, launched in 2020, is a diplomatic instrument aimed at building international consensus around a state-centric model of data governance, explicitly challenging the US-led vision of unrestricted cross-border data flows. This initiative emphasizes "respecting the data sovereignty, jurisdiction, and security governance of all

⁴³ John Seaman, *China and the New Geopolitics of Technical Standardization*, French Institute of International Relations (IFRI), January 2020.

countries” and has been successfully promoted in various UN resolutions and discussions, seeking to embed the language of sovereignty into the lexicon of global digital governance. Similarly, China leverages regional forums such as the Shanghai Cooperation Organization (SCO) and ASEAN to promote its digital governance vision, fostering regional alignment with its principles.

This multi-pronged approach demonstrates a sophisticated and long-term strategy to ensure that the future of global digital governance is at least multipolar. China is not merely reacting to global trends; it is actively shaping them, seeking to create a global digital order where its “Chinese characteristics” in governance are not only accommodated but potentially serve as a model for other nations, particularly developing economies. This strategic push positions China as a leading force in defining the future standards for international services trade AI, moving beyond compliance to active leadership in global rule-making.

VI. CONCLUSION AND SUGGESTION

China’s approach to governing GAI is undoubtedly one of the most significant and systemic developments in the contemporary landscape of international economic law. It has constructed a comprehensive, coherent, and increasingly sophisticated regulatory system designed to achieve a trinity of core objectives: ensuring absolute state control over the information ecosystem, protecting a broadly defined concept of national security, and fostering indigenous technological leadership in a sector deemed critical to future economic and geopolitical power. The design of this system is fundamentally highly consistent with the foundational principles of the WTO, particularly the GATS disciplines on market access, national treatment, and domestic regulation that are designed to facilitate an open and non-discriminatory global market for trade in services.

Regarding data localization rules, they should be understood as the fundamental manifestation of national data sovereignty. These rules are not intended to challenge the basic operational models of global GAI providers, but rather require them to make necessary adjustments within specific jurisdictions to accommodate legitimate national concerns about their citizens’ data and

national security. While the competitive advantage of global GAI providers is indeed predicated on the scale and integrated global data flows, respecting national data sovereignty and ensuring the secure and controllable nature of critical data is an indispensable right for any sovereign state in the digital age. Therefore, China's data localization requirements are not trade barriers but rather a reasonable choice made by countries in the era of digital sovereignty to balance globalization efficiency with national security. Stringent, politically-driven content moderation requirements are aimed at maintaining social public order and national ideological security, which fall within the universally recognized policy space for states under international law. These requirements are designed to ensure the legality and health of information content, rather than creating *de facto* discrimination or a lack of regulatory transparency. In fact, the measures adopted by China in content moderation are universally applicable to all market participants, aiming to build a responsible digital ecosystem, and their legitimacy and necessity should be fully respected. Furthermore, the pervasive role of the state in promoting its domestic AI champions is not an explicit prohibition under WTO rules. This more often reflects the industrial policies widely adopted by countries in strategic emerging industries, and as long as it does not involve direct discrimination against foreign enterprises or unfair subsidies, it should be regarded as a normal path for economic development.

While some views may suggest that China's measures in AI governance could trigger WTO disputes, we have ample reason to believe that China will be able to mount a vigorous and legally sophisticated defense of its measures, primarily under the GATS security and public order exceptions. Any potential WTO dispute would force WTO adjudicators to navigate the waters between respecting a member's sovereign right to regulate and upholding the core trade-liberalizing commitments of the agreements. However, given the uniqueness of the digital economy and the central role of national security in contemporary international relations, we have reason to believe that the WTO's ruling will be more inclined to recognize the legitimate rights of member states to digital sovereignty and national security. It would be a landmark case, testing the latest developments in national security jurisprudence and setting an important

precedent that would resonate throughout the global digital economy.

Ultimately, China's GAI strategy must be understood as more than a collection of discrete, trade-restrictive measures. It is a bold and unapologetic assertion of "digital sovereignty" and a deliberate attempt to forge an alternative path to digital development. China is no longer content to simply be a participant in the global digital economy; it is actively seeking to rewrite the rules, both formally through multilateral negotiations like the JSI and informally through its technological and economic influence via initiatives like the DSR and its engagement in international standards-setting bodies. This is not a systemic challenge to the WTO, but rather an active assumption of global governance responsibility by a major economic power in the digital age. China calls for and is committed to participating in the international governance of AI, becoming a rule-maker. Its proactive practices and experiences in GAI governance will provide valuable perspectives and contributions to the construction of a global AI governance framework. The ability of the multilateral trading system to adapt to this new reality will be a defining test of its relevance and resilience in the 21st century.

Building upon China's comprehensive and sophisticated approach to GAI governance, this section offers concrete suggestions for how China can further strengthen its position as a responsible global actor and a key rule-maker in the evolving landscape of AI. These suggestions are rooted in the principles of respecting national data sovereignty, fostering international cooperation, and ensuring equitable and sustainable AI development for all.

Firstly, China should continue to proactively engage with and contribute to existing international forums dedicated to AI governance. Beyond the JSI at the WTO, this includes active participation in UN discussions on AI, the ITU, the G20, the OECD, and other relevant multilateral platforms. China's unique experience in rapidly deploying and regulating large-scale AI applications, particularly within a context of strong state oversight and national security considerations, offers valuable insights that can enrich global dialogues. By sharing its regulatory successes and challenges, China can help shape a more nuanced and effective global understanding of AI governance complexities. This engagement should extend to providing technical expertise, contributing

to working groups, and advocating for balanced approaches that consider both innovation and responsible deployment.

Secondly, China has a critical opportunity to shape global norms and standards for responsible AI. Given its vast data resources and advanced AI capabilities, China's practices in areas like data governance, algorithmic transparency, and content moderation are increasingly influential. Instead of being perceived as an outlier, China can proactively champion international standards that promote data security, protect individual privacy within the bounds of national sovereignty, and ensure ethical AI development. For instance, China can propose frameworks for cross-border data flows that explicitly acknowledge and integrate data sovereignty principles, offering a model for other nations grappling with similar concerns. Furthermore, as long as transparency and due process are emphasized, its experience with large-scale content moderation can inform discussions about combating misinformation and harmful AI-generated content. By actively participating in and leading international standards-setting bodies, China can ensure that future global AI norms are not exclusively shaped by Western perspectives but reflect a more diverse and inclusive set of values and experiences.

Thirdly, China should leverage its BRI and DSR to bridge the global digital divide and promote inclusive AI development. Many developing countries lack the infrastructure, expertise, and regulatory frameworks to harness AI's potential effectively. China can play a pivotal role by sharing technological advancements, providing capacity-building support, and assisting in the development of AI governance frameworks tailored to the specific needs of these nations. This includes investing in digital infrastructure, offering technical training programs, and facilitating knowledge transfer. By promoting equitable access to AI technologies and fostering a localized AI ecosystem, China can contribute significantly to global sustainable development goals, ensuring that the benefits of AI are broadly distributed and do not exacerbate existing inequalities. This approach also serves as a powerful testament to China's commitment to a shared future for humanity in the digital age.

Fourthly, to foster greater international trust and alleviate concerns, China should prioritize enhanced transparency and dialogue regarding its AI policies.

While national security concerns are legitimate, clearer communication about the scope, implementation, and objectives of its GAI regulations can help reduce misunderstandings and mitigate perceptions of unfair trade practices. This could involve publishing more detailed white papers on AI governance, hosting international conferences, and engaging in bilateral and multilateral dialogues with key trading partners. Establishing clear channels for foreign companies to seek clarification on compliance requirements and providing predictable regulatory environments would be beneficial. Furthermore, exploring mechanisms for international cooperation on AI ethics and safety, such as joint research initiatives or shared best practices, could build bridges and foster a more collaborative global AI ecosystem.

Fifthly, China's dual focus on fostering indigenous technological leadership and robust regulatory governance can serve as a valuable model. The rapid pace of AI innovation necessitates agile and adaptive regulatory responses. China's experience of developing comprehensive regulations while simultaneously nurturing a vibrant domestic AI industry offers a unique case study. China can share its strategies for balancing innovation with risk mitigation, particularly in areas like algorithmic accountability, data privacy, and intellectual property protection for AI-generated content. By demonstrating how a nation can achieve technological self-reliance without resorting to protectionism, China can offer a blueprint for other countries seeking to develop their own AI capabilities while adhering to international norms.

Sixthly, regarding the WTO framework, China can proactively advocate for a more nuanced understanding of digital trade and national security exceptions. Instead of merely defending its measures in potential disputes, China can contribute to the evolution of WTO jurisprudence by proposing interpretations that better accommodate the realities of the digital economy and the legitimate security concerns of sovereign states. This could involve advocating for clear guidelines on what constitutes a "security exception" in the context of digital services, or proposing new disciplines that address the unique challenges of data governance and digital sovereignty within a multilateral trading system. By actively participating in the intellectual and legal discourse surrounding digital trade, China can help ensure that the WTO remains relevant

and adaptable to the challenges of the 21st century.

Finally, China should articulate a long-term vision for global AI governance that emphasizes shared responsibility and mutual benefit. This vision should transcend national interests and focus on the collective challenges and opportunities presented by AI, such as ensuring AI safety, preventing misuse, and harnessing AI for the global public good. By championing principles of equitable access, responsible innovation, and international cooperation, China can position itself as a leading voice in shaping a future where AI serves humanity as a whole. This includes fostering a multi-stakeholder approach, involving governments, industry, academia, and civil society, to ensure that AI governance frameworks are comprehensive, inclusive, and legitimate. The ability of the multilateral trading system to adapt to this new reality will be a defining test of its relevance and resilience in the 21st century. The cauldron of GAI governance will test the mettle of the WTO, and China's proactive role in shaping these global norms will undoubtedly define the future of global trade in services for decades to come. We look forward to China playing a greater leadership role in global AI governance, working with the international community to jointly build an open, secure, responsible, and sovereign-respecting digital future.

China's Proactive Role in Shaping Global AI Governance: A WTO-Centric Analysis of Digital Sovereignty and Trade in Services

Table 1: China's GAI Regulatory Framework: Legislative Architecture

Regulatory Framework	Time Frame	Key Provisions	Responsible/ Enforcement Agencies	Potential WTO Implications
Data Security Law (DSL)	2021–Present	• Data categorization: “Core”, “Important”, “General”; • Mandatory security review for “Important Data” export; • Establishes security obligations for data processors.	• Cyberspace Administration of China (CAC) (overall coordination); • Ministry of Industry and Information Technology (MIIT) (industry-specific, e.g., telecom, industrial data); • Other sectoral regulators.	• DSL Article 21 may relate to the “necessity test” of GATS Article VI (Domestic Regulation); • Potential discussion regarding foreign cloud services; • Concept of “data as a national strategic resource” promotes preemptive state control over data flows.
Personal Information Protection Law (PIPL)	2021–Present	• Separate consent required for cross-border transfers; • Establishes transfer mechanisms (security assessment, standard contracts, certification); • Broad “public interest” exception can override individual consent.	• CAC (primary regulatory and enforcement body).	• PIPL Articles 38–43 may relate to GATS Mode 1: Cross-border supply commitments; • Broad “public interest” exception could be used to arbitrarily restrict data flows; • Global data protection norms may need the exceptional argument in face of TRIPS Agreement.
Interim Measures for the Management of Generative Artificial Intelligence Services	2023–Present	• Pre-market compliance and security assessment; • Scrutiny/legitimacy of training data sources; IP compliance; • Labeling of AI-generated content.	• CAC-led inter-agency task force (7 ministries).	• Security assessment means procedural requirements; • Content rules need the test of “like service” National Treatment (NT) principle under GATS; • Explicit moral integration creates a “state-as-gatekeeper” model.
National Standards (e.g., TC260)	Ongoing	• Technical implementation frameworks; • Mandatory certification for market access; • Detailed operational guidelines for data/algorithm governance.	• National Information Security Standardization Technical Committee (TC260); • State Administration for Market Regulation (SAMR).	• Should be under the test of TBT Agreement (Article 2.4) if standards are not based on “relevant international standards”; • Standards can be enforcement tools with limited industry consultation, creating non-tariff barriers.

(Continued from Previous Table)

Regulatory Framework	Time Frame	Key Provisions	Responsible/ Enforcement Agencies	Potential WTO Implications
Provincial Pilot Rules (e.g., Beijing/ Shanghai FTZs)	2022–2024 and beyond	• Localized implementation; Regulatory sandboxes; • Experimentation with data flow mechanisms (e.g., negative lists); • Tailored “Important Data” definitions for specific sectors; • Enhanced role for local CAC branches and municipal governments.	• Municipal governments; • Local CAC branches.	• Creates regulatory fragmentation; Potential Most-Favoured-Nation (MFN) principle test (GATS Article II) due to different treatment of “like” service providers based on location; • “One-size-fits-all” centralization is replaced by tactical local flexibility, creating uncertainty for foreign firms.

(Edited by Yunhan Wang)