Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD27192

The Sovereignty Exception: China's State-Centric Approach to National Security in Cross-Border Data Flows

Jiashuo Niu

School of Criminal Law, East China University of Political Science and Law, Shanghai, China
Jiashuo_Niu@outlook.com

Abstract. This study examines China's broad application of the national security exception governing cross-border data flows. We trace the development of the exception from being the "constructive ambiguity" in the General Agreement on Tariffs and Trade (GATT) Article XXI exception, to an exception subject to limited judicial review. By examining the distinctive Chinese legal framework on data flows enforced through its Cybersecurity Law, Data Security Law and Personal Information Protection Law (PIPL), we identify a Chinese legal concept of "data sovereignty." A case study of the Didi Chuxing cybersecurity review serves to illustrate how this state-centric regulation of data flows works in practice. In light of the EU's rights-centric and US's power-centric normative approach to data flows, China's legal safeguards for cross-border data flow reveal fundamental tensions in global data governance. We argue that, while internally coherent, the Chinese approach creates serious uncertainty for multinational firms, challenges global norms of international trade law and is a leading contributor to the phenomenon of "digital decoupling".

Keywords: Cross-Border Data Flow, National Security Exception, Data Sovereignty, Cybersecurity Law

1. Introduction

The global economy in the 21st-century is characterized by a primary paradox: the economic need for free-flowing cross-border data against the sovereign need to regulate such flows for national security purposes. This paradox grows as data changes from an object of commercial value to an object of strategic value to nation-states [1]. China is drawing on this contradiction to develop a compelling, robust model of data governance that is based on "data sovereignty"—the notion of state control over data within its territory [2,3]. In contrast to the U.S. free flow model and the rights-based regional governing model of the EU, this state-centric model positions national security as a proactive regulatory tool rather than a reactive exception. This approach to data governance will not merely reflect a momentary action, but rather, it is part of China’s overall national strategy to carry out a "comprehensive national security outlook" [4].

This manuscript provides a scholarly review that advances the argument that China has developed a broad and distinct model for exercising the national security exception which, while based on its domestic theory, produces significant legal uncertainty for multinational corporations (MNCs) [5]. This paper further argues that this approach substantively challenges established norms

DOI: 10.54254/2753-7048/2025.LD27192

of international trade law and represents one of the foremost triggers for the fragmentation of global data governance, a trend that has come to be known as "digital decoupling" [6]. In order to support this argument, the manuscript will first provide an account of the international law context of the national security exception. It will then demonstrate a breakdown of China's domestic law scheme and its normative theory, followed by a practical example in the Didi Chuxing case. A comparative analysis will then be made situating China's model relative to the EU & US models. Finally, the paper will provide an analysis of the implications for the global economy and the digital world order.

2. The national security exception in international law: from ambiguity to adjudication

Historically, international trade law's national security exception has been characterized by a principle of "constructive ambiguity" [7]. Article XXI of the General Agreement on Tariffs and Trade (GATT) embodied the dilemma, with its "self-judging" nature embedded in the clause "which it considers necessary," and provided significant discretion to member countries so that core security interests would be paramount to trade rules. For many years, countries used this ambiguity to enable the resolution of diplomatically sensitive matters rather than a de jure adjudication, because they were often reluctant to have politically sensitive aspects of a matter to be judged by trade lawyers [8]. This informal agreement maintained the stability of this multilateral trading system through an especially important safety valve.

Nonetheless, the considerable reluctance of courts to intervene in state questions relating to sovereignty and trade was sharply reversed in the last couple of years when increasingly difficult geopolitical competition began to blur trade and security. The genesis was a World Trade Organization (WTO) panel report in 2019, Russia – Measures Concerning Traffic in Transit, which implemented a two-tiered standard of review with a place for state sovereignty along with legal oversight [9]. Certainly, the WTO panel stated that it had the authority to objectively review whether an "emergency in international relations" existed but also gave deference to the state regarding whether the measures were indeed necessary, provided those measures were put in place in "good faith." While these developments provide at least a possible approach, their applicability to the digital age is less clear. These standards were developed for traditional trade in goods and, therefore, are ill-suited for addressing the non-traditional and longer-term threats characteristic of the data era, such as large-scale, systematic exfiltration of sensitive data by a foreign adversary. As such, the disjoint in these processes shows that existing WTO jurisprudence will not be sufficient to sort out future disputes as a result of data security challenges, potentially leading to more fragmentation as states pursue unilateral measures in the absence of a sufficiently agreed-upon multilateral framework.

3. China's legal architecture: "data sovereignty" as the organizing principle

3.1. The "tripartite" legal framework

Beginning in 2016, China quickly completed a full data governance regime, or "tripartite legal structure," consisting of the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL). Together these laws create a regulatory structure for the entire data lifecycle.

The CSL, which came into effect in 2017, was the first statute of its kind in China. It introduced the phrase Critical Information Infrastructure (CII) into the statutory framework and mandated a

DOI: 10.54254/2753-7048/2025.LD27192

local data storage requirement for operators of CII. These operators were required to store personal information and "important data" within the borders of the PRC and to conduct a security assessment of any cross-border data transfer. The DSL, made effective in 2021, expanded the domain of regulation to all categories of data and elevated data security to the level of national security. The most significant contribution of the DSL is a tiered classification scheme for "important data" and "national core data," with national core data subject to the strictest levels of restrictions [10]. The PIPL, made effective in 2021, is China's first comprehensive law on personal information, with some influence from the European Union General Data Protection Regulation (GDPR) [11]. The PIPL establishes three primary legal mechanisms for transferring data across the border: a state-mandated security assessment for transfers of a significant scale, professional certification, or the use of standardized clauses. The three statutes referenced above are all connected and create a top-down scheme of regulation where national security is the principal concern.

3.2. "Data sovereignty" as the core principle

The salient concept that grounds the above legal architecture is the concept of “data sovereignty” [2,3], which reconstitutes China's claims to Westphalian sovereignty in cyberspace and assumes that the state has primacy of jurisdiction and sovereignty over any and all data 'acts' in relation to the state. Data sovereignty is a hybrid strategy designed to advance national security, economic development and social stability. data is framed in a dual fashion as a strategic resource with respect to security and as a new type of production input. This dual logic induces a logic of "orderly flow under the condition of security," where the exception of national security becomes a proactive and managerial tool for adjusting the geography of data flows [12].

A key feature of this framework is its "strategic ambiguity." Crucial terms like "important data" and "national security" are left broad and ill-defined. This is not a legislative oversight but a deliberate governance choice. The ambiguity grants significant discretionary power to regulators, particularly the Cyberspace Administration of China (CAC), allowing for flexible, case-by-case enforcement. For MNCs, this uncertainty generates a powerful chilling effect that encourages over-compliance and de facto data localization, as companies proactively limit data exports to mitigate unpredictable legal risks [5]. This approach effectively shifts the burden of proof onto corporations to demonstrate their data activities are harmless, rather than on the state to prove a specific threat.

4. The national security exception in practice: a case study of Didi Chuxing

The cybersecurity assessment of Didi Chuxing represents the most effective real-world example of the dominant role of national security in the regulatory calculus in China. In June 2021, Didi, who is China's leading ride-hailing platform, opened its initial public offering (IPO) on the New York Stock Exchange; some reports indicated that the IPO process was occurring against the backdrop of push-back from regulators that warned of serious data security concerns. In fact, two days after the IPO announcement the CAC issued an announcement that they were conducting a cybersecurity assessment of the company and ordered it to cease new user registration in China and to remove 25 apps from domestic app stores. A year later, after a lengthy investigation, the CAC announced a fine of RMB 8.026B (or $1.2B) for numerous violations of Data Laws including illegal collection of user data such as facial recognition and clipboard data.

Importantly, the CAC stated that Didi's actions "has severely affected national security" but offered no detail on what that meant, citing the sensitivity of this information [13]. Outside

DOI: 10.54254/2753-7048/2025.LD27192

observers have been reasonably tireless in suggesting that the most likely explanation regarded the massive cache of detailed geolocation and mobility services, which could have presented a national security risk if foreign actors were able to aggregate and analyze sufficient data to reveal traffic patterns around sensitive military or governmental sites. The Didi episode provides important lessons regarding how China views the broader tech ecosystem. First, this was a clear act of "performative enforcement" intended as a major deterrent to every tech company, and to signal to the world that the state can call the economic shots over the powerful private sector [13,14]. Beyond the clear signal to capital markets in China that national security concerns trumped shareholders' interests, this would obviously extend to other global capital markets and add to the overall chilling effect of foreign listings of Chinese tech companies. Second, it secured the cybersecurity review as an incredibly powerful state instrument that can be deployed proactively whenever commercial decisions are perceived to conflict with national security interests. Third, this represented a clear example of the "black box" nature of the review process. While the report provided ample detail about data privacy violations, it avoided any true explanation behind the justifications grounded in national security. The opaque process itself was a type of governance whereby regulation is rendered unpredictable and reinforces how the state ultimately and absolutely controls the ability to flow data.

5. A comparative analysis of global data governance models

5.1. The EU model: a rights-centric approach

The EU model of data governance is essentially "rights-based," predicated on the protection of personal data as a fundamental right as per the EU Charter of Fundamental Rights. This makes sense of the 2020 Court of Justice of the European Union (CJEU) ruling in Schrems II. The CJEU did not invalidate the EU-U.S. Privacy Shield agreement because of commercial data misuse; the invalidation was based on the finding that U.S. national security surveillance laws failed to meet the EU's standards of necessity and proportionality and did not provide effective judicial redress for EU citizens [15]. The EU model is a "negative national security exception" that limits data flows on the assessment that another country's national security practices are not consistent with the fundamental rights standards of the EU. The model itself has strong global consequences, as this so-called "Brussels effect" has produced global outcomes because firms across the world will enact practices consistent with the GDPR [16].

5.2. The U.S. model: a power-centric dual-track system

In comparison, the U.S. operates a "power-centric" dual-track system that is defensive and offensive at the same time. Defensively, the Committee on Foreign-Investment in the United States (CFIUS) investigates inward investment to limit the ability of foreign adversaries to gain access to sensitive U.S. technology or data. Offensively, in 2018 the U.S. passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, giving U.S. law enforcement the power to compel U.S.-based tech companies to provide data, regardless of where the data is kept, anywhere on earth [17]. The U.S. system protects its domestic assets while projecting U.S. power in order for U.S. agencies to gain access to data, reflecting a philosophy that prioritizes both free enterprise and national security interests.

5.3. Divergence and conflict

The comparison of the three models in Table 1 shows a fundamental clash of governing philosophies: the approach taken by China is sovereignty-centric, by the EU is rights-centric, and

DOI: 10.54254/2753-7048/2025.LD27192

the U.S. is power-centric. The differing concepts of extraterritoriality and the legal clashes they create (through claims of extraterritoriality) [16] force companies into an untenable "legal trilemma." For example, a U.S. cloud provider may be ordered by a U.S. court under the CLOUD Act to produce data from a data center in Germany. This presents an extraterritoriality problem if the data involves Chinese entities under China's DSL, while also raising GDPR concerns regarding strict controls on transfer. The legal confusion and financial exposure involved with the way that governance is exercised puts companies in an untenable position.

Table 1. Comparative analysis of data governance models

Dimension	People's Republic of China	European Union	United States
Core Principle	Data Sovereignty & State Control: Data as a strategic asset under ultimate state authority.	Fundamental Rights: Protection of personal data as a fundamental human right.	Free Flow & National Security: A dual approach promoting commerce while reserving intervention powers.
Key Legislation	CSL, DSL, PIPL.	GDPR.	No single comprehensive law; CLOUD Act, sectoral laws (e.g., HIPAA), FIRRMA.
National Security Review	Administrative-led (CAC Review): Proactive, discretionary reviews by state agencies based on a broad definition of national security.	Judicial-led (CJEU Review, e.g., Schrems II): Reactive judicial review assessing if third-country laws meet EU fundamental rights standards.	Hybrid Model (CFIUS & Law Enforcement): Administrative investment screening (CFIUS) and judicially authorized law enforcement data access (CLOUD Act).
Cross-Border Transfer	State-gated: "Important data" or large-scale personal information exports primarily require state-led security assessments.	Conditional Flow: Transfers limited to "adequate" countries or through mechanisms like SCCs with supplementary measures.	Presumed Free, with Access Rights: Generally permits free flow but asserts U.S. right to compel access to data stored abroad via legal process.
Primary Rationale for Restriction	Comprehensive National Security: Broadly includes economic security, social stability, and public interest.	Protection of Individual Rights: Restrictions are imposed to prevent the erosion of data subjects' fundamental rights.	Specific National Security Threats & Law Enforcement Needs: Targeted interventions for defined threats (CFIUS) or investigation of serious crime (CLOUD Act).

6. Implications: legal uncertainty and digital decoupling

The collision of all of these data governance regimes has tremendous implications for multinational corporations and is contributing to a more general structural change in the global digital order. MNCs face a "legal trilemma" whereby they no longer have the ability to comply with the laws of other major jurisdictions as to do so would be to violate the law of at least one alternative jurisdiction [17,16]. But beyond what is entailed in direct legal conflicts, the costs of compliance are skyrocketing beyond being inefficient, e.g., data localization; this practice creates disjointed corporate IT architectures with inefficient data silos [18]. These fragmented architectures have resulted in increased operating costs and a further impediment to firms who are eager to innovate and identify competitive advantage through interpreting global data.

On a macro level, this regulatory divergence is an important source of "digital decoupling" or the emergence of a "Splinternet" [6,19]. The universal, open Internet is increasingly being divided up along maps of geopolitics, resulting in separate and often incompatible digital systems. It is a trend that serves as a dynamic of the "weaponization of interdependence," in which states utilize the positions that they are occupying in global networks to exert influence [20]. China uses access to its

DOI: 10.54254/2753-7048/2025.LD27192

market, the U.S. uses the global footprint of its tech companies, and the EU uses regulation. In all of this, the national security exception sets up the key legal framework for states to prioritize sovereign control as opposed to free trade and the principles of open data flows.

7. Conclusion

This study has shown that China has developed and anchored a principled, expansive and sovereign state-centric approach to applying the national security exception to cross-border data flows that is based on the concept of "data sovereignty." This state-centric framework is being enacted through the legal and regulatory infrastructure that has been firmly established by data regulatory authorities and institutions. This approach presents a significant divergence from the rights-based model and power-based model adopted by the European Union and the United States respectively. The result has been diverging regulatory regimes that establish the current climate of heightened legal uncertainty for cross-border data flows by multinational businesses and create a significant push for the "digital decoupling" of the world's economies. This trend threatens to fragment the internet, raise costs for businesses, and stifle global innovation. Ultimately, this suggests a significant departure from the former ethos of a borderless digital world toward a future heavily framed by national sovereignty in cyberspace. Future research should therefore focus on the long-term economic impacts of such decoupling and explore what, if any, multilateral mechanisms could be developed to mitigate the 'legal trilemma' facing global enterprises.

References

[1] McKnight, S., Kenney, M. and Breznitz, D. (2023) Regulating the platform giants: Building and governing China's online economy. Policy & internet, 15, 243-265.
[2] Yun, H. (2025) China’s data sovereignty and security: Implications for global digital borders and governance. Chinese Political Science Review, 10, 178-203.
[3] Chen, S. (2021) Research on data sovereignty rules in cross-border data flow and Chinese solution. US-China L. Rev., 18, 261.
[4] He, A. (2023) State-centric data governance in China. CIGI Paper No. 282. Retrieved from https: //www.cigionline.org/publications/state-centric-data-governance-in-china/
[5] Akinsola, O.K. (2025) The Impact of International Trade Laws on Corporate Strategy: Navigating Cross-Border Legal Challenges for Multinational Corporations. [Publisher information not provided].
[6] Aaronson, S.A. (2021) Data is disruptive: How data sovereignty is challenging data governance. Hinrich Foundation. Retrieved from https: //www.hinrichfoundation.com/research-and-analysis/trade-policy-briefs/data-is-disruptive/
[7] Alford, R.P. (2011) The self-judging WTO security exception. Utah L. Rev., 697.
[8] Jackson, J.H. (1997) The world trading system: law and policy of international economic relations. MIT press.
[9] Davis, S. (2019) Inherent Limits to the World Trade Organization's Article XXI Self-Judging Security Exception. Md. J. Int'l L., 34, 364.
[10] National People's Congress of the People's Republic of China (2021) Data Security Law of the People's Republic of China. Retrieved from http: //en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.htm
[11] Li, W. and Chen, J. (2024) From brussels effect to gravity assists: understanding the evolution of the GDPR-inspired personal information protection law in China. Computer Law & Security Review, 54, 105994.
[12] Borgogno, O. and Savini Zangrandi, M. (2024) Chinese data governance and trade policy: from cyber sovereignty to the quest for digital hegemony?. Journal of Contemporary China, 33, 578-602.
[13] Kokas, A. (2023) Trafficking data: How China is winning the battle for digital sovereignty. Oxford University Press.
[14] Shu, C. (2016) Didi Chuxing confirms it is buying Uber’s business in China. TechCrunch. Retrieved from https: //techcrunch.com/2016/08/01/didi-chuxing-confirms-it-is-buying-ubers-business-in-china/
[15] Lancieri, F.M. (2019) Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift. Journal of Antitrust Enforcement, 7, 27-53.

DOI: 10.54254/2753-7048/2025.LD27192

[16] Pernot-Leplay, E. (2020) China's approach on data privacy law: a third way between the US and the EU?. Penn St. JL & Int'l Aff., 8, 49.
[17] Mattoo, A. and Meltzer, J.P. (2018) International data flows and privacy: The conflict and its resolution. Journal of International Economic Law, 21, 769-789.
[18] Kansara, M. (2021) Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. International Journal of Applied Machine Learning and Computational Intelligence, 11, 78-121.
[19] Broeders, D., Cristiano, F. and Kaminska, M. (2023) In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. JCMS: Journal of Common Market Studies, 61, 1261-1280.
[20] Segal, A. (2016) The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. Hachette UK.