***Review Article***

**Data Sovereignty and Digital Trade: China’s Legal Strategy under CPTPP and DEPA Frameworks**

**Abstract:** *This study employs a qualitative case study analysis approach to demonstrate how the general exception clauses have been integrated into CPTPP and DEPA frameworks in lieu of digital trade. Simultaneously, it focuses on China’ regulatory model. The study examines the legal flexibility offered by these agreements and evaluates the compatibility with China’s data governance laws such as PIPL, DSL and Cybersecurity laws with international obligations. The study finds that exception do account for public interest protections, yet China’s broad security justifications posit a serious challenge. The study concludes that strategic engagement and modular compliance are essential to balance digital sovereignty with international cooperation in an increasingly data-driven global economy.*

**Key Words:** *China, CPTPP, DEPA, DSL, PIPL, Cybersecurity Law*

1. **Introduction**

Digital trade encompasses the exchange of commodities enabled via electronic means. WTO (2023) states that digital trade provides opportunities to launch new products and contributes to increasing inclusivity in the global scenario. For instance, it enables micro, small, and medium-sized enterprises (MSMEs) and businesses in developing countries to access global markets without the need for costly physical infrastructure. It also facilitates remote work, cross-border freelancing, and digital entrepreneurship, thereby broadening participation among women, youth, and marginalized communities. It is thus a cornerstone of modern global economy. Additionally, according to the U.S. Congressional Research Service (2025), digital trade can be defined as commercial transactions and digitally enabled activities that are conducted via internet or other networked computer system. This includes trade of digital goods and services alongside infrastructure, platforms and data flows that support them. Therefore, such as expensive definition underscores the complexity of governing digital trade in a world that is increasingly interconnected. In the contemporary world, the growth in digitally delivered services over the last 2 decades has been evident. Figure-1 shows that it increased from US$6.6 trillion in 2005 to US$29.1 trillion in 2024, capturing the rising trend in digitally delivered services. Subsequently, as cross-border data flow intensified, it increased concerns around data protection, cybersecurity and state sovereignty. Thus, this has led to renewed attention on general exception clauses within trade agreements.

***Figure 1: Increase in Digital Trade Services 2005-2024***

***Data Source: WTO (2025)***

Over the last two decades, growth in digitally delivered services has been significant. This aspect has been captured in Figure1. The figure shows a consistent increase in the total value of digitally delivered services. This sharp increase from US$6.6 trillion in 2005 to US$29.1 trillion in 2024 is crucial to demonstrate the growing significance of digital trade. Note that the upward trajectory underscores rapid expansion of globalization especially in the context of services that is enables via technologies that rely on the internet. Figure 1 also shows how overall trends reflect a consistent increase in the reliance on digital channels for economic exchange, despite temporary plateaus such as that between the years 2015 and 2017. Safe to say that this surge is driven by the growing access to broadband infrastructure, cloud computing and e-commerce platforms (WTO, 2023). This in turn has made the delivery of digital services more accessible across borders. Subsequently, cross borders data flows also intensified the concerns around data protection, cybersecurity and state sovereignty. Therefore, such as exponential rise in digital services has prompted renewed scrutiny of the digital exception clauses within trade agreements. This is crucial to address the emerging challenged that pertain to governance.

Digital trade has become a central pillar of international commerce due to the exponential expansion over decades. Thus, structured governance is now imperative. In order to address this, Regional Trade Agreements (RTAs) have evolved. They now include digital trade provisions as well that regulate emerging issues such as cross-border data flows, cybersecurity, digital services and e-commerce platforms. Moreover, note that they are quite different from traditional trade agreements that focused mainly on gods and tariffs. The modern RTAs reflect the complexities of the digital economy. They serve as critical instruments that harmonize standards and reduce regulatory fragmentation across jurisdictions. This is particularly relevant in the absence of binding multilateral rules on digital trade. These RTAs vary in scope and ambitions typically. This variation depends on a number of signatories alongside the underlying political economy.

The variations have been illustrated in Figure 2, which shows that Joint Initiative (JI) participants under the WTO’s e-commerce discussions, such as members of the CPTPP and DEPA, tend to cover a broader range of digital trade issues compared to non-JI countries (The Asian Foundation, 2024). Key provisions in JI-based agreements include rules on data privacy, scams, consumer protection, cross-border data flows, and electronic authentication. In contrast, non-JI countries often omit such rules or address them less comprehensively, leading to regulatory divergence. This has resulted in two distinct approaches: plurilateral agreements aim for deeper digital integration, while others follow a sovereignty-first model. Within this divergence, general exception clauses play a critical legal role. These clauses originate from Article XX of GATT and Article XIV of GATS (WTO, n.d.a; n.d.b), and allow states to deviate from trade rules for legitimate policy goals. Legitimate exceptions include protection of public morals, national security, and data privacy. However, applying these exceptions to digital trade is legally complex and politically contested, particularly when countries enforce data sovereignty through domestic legislation.

**

***Figure 2: RTA Coverage of data privacy concerns (OECD, 2023)***

**The extent to which Joint Initiative (JI) and non-JI countries incorporate various digital trade provisions in their RTAs have been visually represented in Figure 2. In this regard, the provisions include but are not limited to those the related to privacy, cybersecurity and data governance. It is evident that JI members tend to demonstrate a more comprehensive coverage of data protection, consumer rights and cross-border data flows. This highlights their proactive stance on digital regulation. Moreover, these clauses serve as legal safeguard for sovereign policymaking that lie within the liberalized trade order. Additionally, on one hand, digital trade promotes openness and efficiency. However, on the other hand, it raises critical questions regarding privacy, regulation of content and national security. In this regard, general exceptions tend to offer governments a means via which they would be able to reconcile trade commitments with public interest. Nonetheless, their interpretation remains widely contested alongside their application in the digital domain. This is especially relevant in the cases that concern localization of data, cross-border data flows and cybersecurity regulation. Thus, it is rather imperative to understand how general exception clauses function in plurilateral agreements such as CPTPP and DEPA. This analysis in turn will reveal its significance when it comes to evaluating legal and strategic viability of national digital regimes of nations such as China.**

**The aim of this case study is to examine how general exception clauses articulate in the context of CPTPP and DEPA. For this purpose, the study will primarily demonstrate how they intersect with the legal framework on Chinese digital trade that is consistently evolving. Note that China’s approach is particularly significant especially given its dual role: one as a major global trading partner and second as an assertive regulator of digital technologies. As China is the second-largest economy in the world and also has the largest e-commerce market, it is not merely a participant in digital trade. Instead, it shaped the global scenario. The Chinese government has successfully established a sovereign regulatory model that focuses on security and emphasized state oversight over cross-border data flows. The nation has integrated policies such as the Data Security Law (DSL), the Personal Information Protection Law (PIPL) and the Cybersecurity Law, which collectively ensure its superiority in the context of digital trade. These laws are in sharp contrast with liberal rule-based frameworks such as those that are found in agreements such as CPTPP and DEPA. These agreements predominantly prioritize openness, interoperability and transparency.**

**Additionally, the digital governance strategy in China also has certain extraterritorial implications. This has been observed in Belt and Road digital infrastructure projects and efforts that were made to influence norms of global internet governance. Thus, although China currently is not a member a CPTPP or DEPA, it has applied for accession to the former and has also expressed formal interest in the latter. These moves raise critical legal concerns alongside strategic questions pertaining to whether China’s domestic regulatory regimes are in fact compatible with international digital trade commitments particularly in relation to the scope and application of general exception clauses. Therefore, this study aims to explore how this exception could enable or perhaps constrain China in aligning with CPTPP and DEPA principles and what might that mean for the future of global digital governance.**

* 1. **Research Questions**
1. How are general exception clauses related to digital trade incorporated within the legal frameworks of the CPTPP and DEPA?
2. In what ways has China’s domestic legal and data governance framework—such as the PIPL, DSL, and Cybersecurity Law—responded to or aligned with the digital trade provisions in these international agreements?
3. What legal and policy tensions, or areas of compatibility, exist between China’s digital governance model and the general exception provisions in the CPTPP and DEPA?
4. **Literature Review**

As the complexity surrounding digital trade has grown, it has brought renewed attention on the role of general exception clauses in international trade laws. These clauses are rooted in GATT Article XX and GATS Article XIV. They were originally designed to permit limited deviations from trade obligations in cases of public interest. These include but are not limited to the protection of public morals, maintenance of public order and national security, the enforcement of domestic laws, protection of plant, animal and human life or health, and the conservation of non-renewable natural resources (Bartels, 2017; Marwell, 2006). However, their extension to the context of digital trade has been rather contentious. Several scholars have debated their adequacy in addressing emerging challenges such as data privacy (Sun, 2025; Brkan, 2019; Woods, 2016), cybersecurity (Peng, 2015; Nanxiang, 2023) and cross-border data flows (Voss, 2020; Zhang, 2020). Additionally, recent research has explored how agreements such as CPTPP and DEPA structure digital trade provisions. In this regard, CPTPP and DEPA establish common standards on issues such as bans on data localization, cross-border data flows, disclosure of source codes and open access to internet (Burri, 2021). These shared norms provide grounds for a strong stance that promotes international cooperation in digital trade. Therefore, this provides a useful bases for creating a model in the realm of international participation. The shared commitments from a regulatory baseline. This is a form of threshold that enhances legal certainty, lowers cost of compliance for businesses and simultaneously promotes trust among the member nations. Thus, if national regulations are aligned with the norms of digital trade, the agreements would be able to create a more predictable and interoperable digital environment. This will provide a practical foundation for international participation as it will encourage broader cooperation and also enable smoother integration into the global digital markets.

According to Kimura (2019), chapter 14 of CPTPP mandates cross-border data flow and prohibits data localization. It encompasses the e-commerce chapter that necessitates no imposition of import duties under Article 14.3, no discriminatory treatment under Article 14.4. It also prohibits data localization under Article 14.10. and cross-border transfer of computing facilities under Article 14.13. Lastly, it inhibits forced transfer of software source codes. However, it also includes general exceptions in Chapter 29 to preserve policy space (CPTPP Portal, 2025). On the other hand, DEPA encompasses a modular framework that emphasizes regulatory cooperation and interoperability which offers flexibility while simultaneously supporting liberalization. In this regard, the US, EU and China are utilizing domestic and foreign policies to reap the benefits from data-oriented economies of scale and scope (Aaronson & Leblond, 2018). However, tensions between trade liberalization and protection of domestic regulatory autonomy, epitomize in this framework (EU Parliament, 2020). This is particularly true across digital domains. Therefore, while on hand, digital transformation and technological enhancement are crucial to achieve sustainability of resources and reduce trade costs (Yingchao & Xiang, 2024; Xiang & Zhao, 2025), on the other, trade provision and privacy protection clauses in the RTA tend to exert much stronger positive impacts on imports than provisions for data flow (Xiang & Zhao, 2025).

In the same context, China’s evolving data governance regime is rooted in the Cybersecurity Law of 2017, Data Security Law (DSL) of 2021 and Personal Information Protection Law (PIPL) of 2021 (NZFAT, 2022). These embody a strategy of data sovereignty. It emphasizes state control over data that has been generated within its territory. These policies are in sharp contrast with that of the US and EU, as the former has a market friendly data governance model whereas the latter entails the General Data Protection Regulation (GDPR) framework (Yun, 2024). Both of these models prioritize the protection of human rights. Thus, although in the context of China, data sovereignty has been framed as necessary for national security and public interest, these laws subsequently raise concerns regarding China’s compatibility with international frameworks of digital trade.

Thus, despite a rich literature that exists in this realm, there is a notable gap in examining how general exceptions operate as legal bridges or perhaps points of friction between multilateral agreements and domestic digital regimes. Therefore, the concepts of legal pluralism implying the coexistence of multiple legal system within or perhaps across countries, regulatory sovereignty which captures the state’s ability to set and enforce its own digital rules without referring to outside norms, and digital protection meaning safeguarding data privacy, cybersecurity and control over information flows, are essential to understand where China stands in this normative landscape that is so highly contested. These concepts will collectively provide useful insights into how China navigates the tension between global digital trade commitments and its domestic regulatory priorities.

* 1. **Legal Background: WTO General Exceptions and the Two-Tier test**

General exception clauses that are embedded in Article XX of GATT and Article XIV of GATS, provides member states with a legal space that is essential to adopt trade-restrictive measures. These measures pursue public policy objectives that are legitimate. These include the protection of public morals, human, animal or plant life and health, and national security (Bartels, 2017; Marwell, 2006). However, in order to prevent the misuse of such clauses, they have been subjected to strict legal scrutiny and have rarely been invoked successfully. In this regard, as per Public Citizen (2015), as of 2015, only 1 out of 44 attempts to use the general exception clauses, have succeeded. This was the EC-Asbestos case. Moreover, out of the 44 cases, the general exceptions were considered to be relevant enough across 33 cases however, 32 out of these 33 cases failed to satisfy 1 out of 3 of the threshold tests that the clauses’ application demand. These are:

***Table 1: Threshold Tests***

***Adapted from Public Citizen, 2015***

|  |  |  |
| --- | --- | --- |
| **Threshold Test** | **Definition** | **Number of cases failed** |
| Matter/Scope threshold | “Tribunal concluding that the Respondent failed to show that the measure was designed for the protection of human health or for securing compliance with laws or regulations which were not inconsistent with WTO provisions” | 5 |
| “Necessary” or ‘Related” threshold | - | 18 |
| Chapeau threshold | “Tribunal finding arbitrary or unjustifiable discrimination in the measures’ application.” | 9 |

Both GATT Article XX and GATS Article XIV adopt a two-tier structure. According to Van den Bossche & Zdouc, 2017) The first-tier mandates that a contested measure falls within one of the listed sub-paragraphs such as Article XX(b) for health protection or Article XX(a) for public morals. The second tier which is often referred to as the *chapeau,* imposes additional constraints. It demands that the measure ought to not be applied in a manner that would constitute as arbitrary or unjustifiable discrimination. Moreover, it should not be a disguised restriction on international trade. This two-step analysis has been clarified by the WTO jurisprudence repeatedly. In the US-Gambling, the Appellate Body emphasized that even when a measure serves a legitimate purpose, it must still be a “necessary” and should be applied non-discriminatorily in order to qualify under the *chapeau* (Appellate Body report, 2005). Moreover, the burden of proof lies with the party that is invoking the exception which in turn must satisfy both the necessity of the measure and its consistency with the *chapeau* (Cottier et al., 2008). The WTO Dispute settlement Body has also underscored that the general exceptions must be interpreted narrowly. This will help in preserving the liberalizing goals of the system. However, according to Appellate Body Report, 1998) and (Appellate Body Report, 2012), recent decisions such as EC – Seal Products and compliance ruling in Shrimp/Turtle and Tuna, Mexico, suggests that there is a growing willingness to balance trade and regulatory autonomy. This is particularly true in areas such as public morals and environment protection. However, the high threshold for satisfying both tiers of the tests implies that several state measures risk failing legal scrutiny especially those in the digital domain.

1. **Methodology**

This paper adopts a qualitative case study approach to examine how general exception clauses in digital trade agreements interact with China’s data sovereignty regime. A case study method is well-suited for examining complex legal-institutional dynamics, especially in contexts where rules are evolving and politically contested. While construct validity is typically associated with quantitative methods, in this study it is achieved through triangulation—by comparing legal texts, policy documents, and secondary academic sources to ensure consistency in how key legal concepts are interpreted. This method also enables historical explanation, identification of omitted variables, and exploration of institutional interactions that are not easily captured through quantitative models (Bennett, 2004). Thus, for this study, the case study method is appropriate given the complex legal, institutional and geopolitical context that surrounds China’s digital governance. It also reflects in its evolving relationship with CPTPP and DEPA. These agreements serve as contrasting yet complementary frameworks via which exception clauses and digital trade commitments are articulated. Therefore, the analysis for this study will employ a legal-interpretive method. It involves close reading and comparative interpretation of legal texts.

The study thus adopts a legal-interpretive method. This does not include mere reading of texts. Instead, it emphasizes systemic and contextual analysis as well to provide in depth insights into the scope of the study. It specifically analyzes legal provisions from CPTPP, DEPA and Chinese laws namely Cybersecurity Laws, DSL and PIPL. These legal provisions will be interpreted using doctrinal analysis. This will focus on internal logic, structure and purpose of the legal rules. Doctrinal analysis includes identification of operative clauses, qualifiers and exceptions. It also examines how they are framed in terms of their scope, their applicability and the intended policy outcomes. Additionally, the case study will also employ comparative textual analysis. This analysis will correspond to provisions across CPTPP, DEPA and China’s domestic laws which would be systematically compared. The textual analysis allows the identification of legal convergence, divergence or perhaps ambiguity. This is especially true in relation to localization of data, cross-border data flow and the invocation of general exceptions. For instance, terms such as ‘necessary’, ‘public morals’ and ‘national security’ will be examined in lieu of their use across domestic and international legal instruments. They will also be assessed for their consistency with WTO jurisprudence. To enhance interpretive depth, the study also applies contextual legal analysis, which situates legal provisions within broader institutional and political contexts. For instance, China's enforcement approach and administrative procedures will be evaluated alongside the legal text to assess their practical implications. Moreover, interpretation will be informed by international treaty law principles under the Vienna Convention on the Law of Treaties—particularly Article 31, which mandates that treaties must be interpreted in good faith, in accordance with the ordinary meaning of their terms, in their context, and in light of their object and purpose.

The goal is not just to describe legal language, but to understand how legal instruments construct regulatory authority, policy space, and compliance obligations. This interpretive framework enables the study to determine whether China’s legal framework aligns with the digital trade governance principles embedded in CPTPP and DEPA, and whether general exceptions are framed and applied in a manner consistent with international norms of necessity, proportionality, and non-discrimination. Hence, the primary sources include the full texts of CPTPP and DEPA, especially chapters on digital trade and general exceptions. Additionally, Chinese laws such as Cybersecurity, DSL and PIPL, will also be analyzed in correspondence. Furthermore, secondary sources such as academic commentary, policy papers and institutional reports has also been included. Overall, this methodology allows the study to assess how exception clauses are structured in order to accommodate state interest. However, China either aligns with or resists these provisions. They stand on an ambiguous legal space as their focus remains on legal function of exceptions as mechanisms of flexibility, contestation or normative divergence in digital trade governance.

1. **Case Analysis**
	1. **CPTPP and General Exceptions**

The CPTPP establishes a comprehensive framework for digital trade under Chapter 14 (CPTPP, n.d.). This mandates free flow of information and restricts data localization as suggested by Kimura (2019). In this context, Article 14.11.2 of CPTPP (n.d., p. 14-6) states:

“*Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person*.”

Thus, this implies that CPTPP members ought to permit data including personal data, to be transferred across borders when it is deemed essential for businesses. However, Article 14.13.2 (CPTPP, n.d., p. 14-7). states:

“*No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory*.”

This implies that members of the CPTPP cannot force businesses to store data or set up servers locally as a condition for them to operate in that country. Thus, these provisions aim to eliminate barriers to digital trade while fostering interoperability across jurisdictions.

Nonetheless, these commitments are subjected to general exception clauses included in Chapter 29 (CPTPP, n.d). It reflects the structure of GATT Article XX and GATS Article XIV. It thereby permits deviations wherein measures are crucial for the protection of public morals or public order reiterating Bartels (2017) and Marwell (2006). It also allows deviation to ensure compliance with domestic laws provided that the measures are not applied in a “*manner which would constitute a means of arbitrary or unjustifiable discrimination between Parties or between Parties and non-Parties where like conditions prevail, or a disguised restriction on investment in financial institutions or cross-border trade in financial services as covered by this Chapter*” (CPTPP, n.d., p. 11-12). Thus, this two-tier test requires a legitimate objective and necessity-based proportionality. This has been clarified in WTO jurisprudence that demands a weighing and balancing of policy goal, trade restrictiveness and existence of less intrusive alternatives (WTO, n.d.a; WTO, n.d.b).

In this regard, China’s current legal regime reveals structural incompatibilities given the aforementioned requirements. Article 38 of PIPL requires that any cross-border transfer must undergo a security assessment that has been organized by national authorities (China Briefing, 2021). Furthermore, Article 40 imposes a localization mandate on ‘critical information infrastructure operators’ (China Briefing, 2021). It requires personal data to be stored within Chinese territories regardless of case-specific risks. These provisions create a de jure localization obligation that directly contravenes CPTPP Article 14.13.2. Moreover, DSL reinforces this approach. Article 24 authorized the export of important data if such transfers could affect national security or public interest (China Law Translate, 2021). Additionally, the 2025 draft amendments to Cybersecurity Law proposes enhanced enforcement mechanisms that include administrative penalties, license revocation, and business suspension for firms failing to comply with cross-border data rules (Fan & Zhou, 2025). Thus, collectively, these laws construct a regulatory model that centered around preventive state control over digital infrastructure and outbound flows of information.

Although China may attempt to justify the restrictions under the general exceptions section of CPTPP Chapter 29, the broad and inflexible nature of the measures presents considerable legal challenges. Burri (2017) argues that exception clauses should be narrowly interpreted in order to preserve the liberalization objective of digital trade agreements. Thus, blanket mandates and risk-averse transfer bans are unlikely to satisfy CPTPP’s necessity and non-discrimination criteria especially when they are implemented without demonstrating proportionality or offering less trade-restrictive alternatives. Additionally, while applying WTO’s two-tier test, CPTPP parties ought to first assess whether China’ s data localization rules pursue a legitimate objective for instance national security or public morals. This threshold is likely to be met. However, the more difficult question arises while assessing whether China’s measures are “necessary” under Article XX(a) or (b) and whether they satisfy the *chapeau.* WTO jurisprudence such as in US-Gambling, requires the demonstration that there are no reasonable available alternatives that are less trade restrictive. Moreover, blanket localization rules are unlikely to pass this test without any risk-based differentiation. Furthermore, the chapeau prohibits measure that result in arbitrary or unjustifiable discrimination. For instance, in EC-Seal products, the Appellate body found that the legitimate moral justification was insufficient wherein inconsistent application undermined fairness. If China’s enforcement of localization disproportionately impacts foreign firms without any transparent justification, it may also face a similar failure as per chapeau standard. **According to China Briefing (2021), Article 40 of the PIPL mandates that personal information collected within China must be stored domestically, especially by ‘critical information infrastructure operators. This requirement is applied broadly and often without individual risk assessments, which raises concerns about non-discrimination.** Furthermore, the **2025 draft amendments to the Cybersecurity Law** introduce enforcement tools such as license revocation and business suspension for non-compliant firms, including foreign entities (Fan & Zhou, 2025). These mechanisms intensify compliance risks for foreign businesses without clearly articulated public justifications. Additionally, the **NZFAT (2022) report notes** that China's localization and outbound data transfer rules are often interpreted and enforced with limited transparency, creating uncertainty for foreign digital service providers. The case Russia-traffic in Transit clarifies the restrictions motivated by security must still conform to objective legal principles. Although the CPTPP adopts its own language, these WTO precedents are rather informative given the structural equivalence of chapter 29 with GATT Article XX. Therefore, CPTPP scrutiny of China’s laws would likely be shaped by the WTO’ evolving standard of necessity and non-discrimination. Overall, China’s legal framework reflects a sovereignty first model. It prioritizes national control over digital policy. This stance may fundamentally misalign CPTPP’s vision of open and rules-based digital trade even though it is anchored in legitimate regulatory concerns.

* 1. **DEPA**

DEPA represents a novel approach to digital trade governance via its modular framework. It allows economies to engage flexibly across 16 core areas. The modular framework of DEPA is captured chronologically in Table-2. These include cross-border data flows, artificial intelligence, cybersecurity, and digital inclusion. DEPA’s design supports high-standard digital commitments alongside differentiated paths of implementation. Hence, it has attracted interest from diverse economies including China.

***Table 2: DEPA Modular Framework (DEPA, n.d.)***



Table-2 shows that DEPA’s modular structure allows participatory economies to adopt digital trade rules with flexibility. The nations can do so at their own pace and as per the readiness of their domestic policies. Therefore, this approach lowers the barriers to entry for developing nations and it also simultaneously enables advanced nations to pursue higher digital standards. Additionally, modules such as Module 4 encompassing data issues and Module 15 including exceptions, are increasingly relevant for this study. This is because they engage with sensitive areas such as data governance as well as the use of public interest justifications in trade. Therefore, the inclusion of these modules facilitates DEPA to accommodate legal diversity. It also encourages regulatory alignment on foundational issues such as trust, inclusion and cross-border interoperability. Thus, China’s interest in DEPA can is interpreted through the lens of its ability to engage with modules selectively. This offers a strategic entry point into digital trade governance without any immediate full compliance. It thereby preserves space for its sovereignty-oriented model of digital regulation.

At the core of DEPA’s digital governance are commitments to **interoperability and regulatory trust.** Module 4.3. clause 2 (DEPA, n.d., p. 4-3) mandates:

“*Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.*”

This is the same as Article 14.11.2 of CPTPP. Additionally, the cross-border transfer of information under DEPA is subjected to limited exceptions for *legitimate public policy objective* that are not *applied in a manner which would constitute a means of arbitrary or unjustified discrimination*. Similarly, parties are also discouraged from imposing data localization requirements. These provisions collectively mirror the CPTPP digital norms however, they have been integrated into a more flexible and cooperative context.

China formally applied to join DEPA in November 2021 and the Accession Working Group (AWG), chaired by Chile was established in August 2022 (APEC, 2024). According to MOFCOM (2024), positive progress is being made as China actively exchanges views with DEPA members. This strategic interest reflects China’s intent to enhance participation in regional digital governance frameworks. It consequently signals regulatory openness to global investors.

However, the domestic legal regimes in China represents several frictions with DEPA’s vision. For instance, PIPL requires cross-border transfers to undergo state-organized security review and mandates data localization for critical infrastructure operators (China Briefing, 2021). Additionally, Article 24 of DSL authorized restrictions on outbound data (China Law Translate, 2021). Meanwhile, the **Cybersecurity Law Amendments (2025)** reinforce compliance mechanisms such as license revocation and business suspension for violations (Fan & Zhou, 2025). In this context, DEPA’s exception clause under Module 15 incorporates Article XX of GATT and Article XIV of GATS ‘mutatis mutandis” (DEPA, n.d., p. 14-5). These clauses allow regulatory measures that are necessary to protect public morals, privacy or national security. However, these measures should not be arbitrary or unjustifiable or perhaps disguised as restrictions on trade. The interpretive flexibility in this context offers a more diplomatic space than CPTPP. Yet it still mandates transparency, proportionality and dialogue. Moreover, the term *mutatis-mutandis* signals that although DEPA draws from the WTO’s general exception framework. Its application is adjusted to fir the digital context and cooperative spirit of the agreement. This approach arguably gives China a softer landing than CPTPP which directly transplants the stricter two-tier test. However, DEPA still expects members to uphold core principles of proportionality and non-discrimination as developed by the WTP case laws such as US-Gambling and EC- Seal Products.

To further clarify, Table-2 below compares how CPTPP, DEPA and WTO agreements respectively frame and apply general exception in digital trade. This table shows that while DEPA is more flexible procedurally, it inherits the same substantive obligations that have led to failure in 32 of 33 WTO cases attempting to invoke general exceptions (Public Citizen, 2015). Hence, legal divergence may be tolerated in form, but not in effect.

***Table 3: Comparison of General Exceptions Frameworks***

|  |  |  |
| --- | --- | --- |
| **Agreement** | **Basis for Exceptions** | **Non-Discrimination Test** |
| CPTPP Chapter 29 | Article XX GATT-style (explicit) | Yes – via chapeau |
| DEPA Module 15 | GATT/GAT’S exceptions “mutatis mutandis” | Yes – adapted, but still binding |
| WTO (GATT XX / GATS XIV) | Structured two-tier test | Strict jurisprudence (e.g., *US – Gasoline*) |

Thus, instead of a legal confrontation, DEPA’s cooperative model offers a path for gradual alignment. Aaronson and Leblond (2018) argue that such frameworks allow regulatory experimentation without forcing any binary choices. Thus, China’s success in joining DEPA will not depend on strict legal equivalence. Instead, it will be based on its willingness to engage in trust-based convergence. This will demonstrate that its data governance model can be made compatible with international interoperability norms, if not completely identical.

1. **China’s Strategic Response**

China’s model for data governance reflects a deliberate legal strategy entailing ‘controlled openness’. It balances global integration with data sovereignty. In the same context, Chinese laws such as PIPL, DSL and Cyrbersecurity laws are usually justified on the grounds of general exception clauses under CPTPP, DEPA, GATT and GATS frameworks. These account for public safety and moral concerns. These measures invoke legitimate objectives. However, they blanket application is rather contested as far as proportionality and transparency is concerned (Sun, 2025; Brkan, 2019). Thus, China should not oppose global digital rules completely. Instead, it should participate in CPTPP and DEPA accession talks in lieu of adopting pragmatic and incremental approaches to shaping its norms. In this regard, firms such as Alibaba and Tencent makes this approach rather evident. They have built compliance systems that are specific to jurisdictions (Tusikov, 2019; Cao, 2020). Hence, nations like China ought to navigate their digital rulemaking rather strategically. It will help them gain economic as well as regulatory leverage as suggested by Aaronson and Leblond (2018). Overall, it will transform compliance to a competitive advantage.

1. **Policy Implication and Future Research**

To enhance compatibility, China should adopt proportionality assessment. It should create transparency portals and pilot security review sandboxes in collaboration with partner economies. These steps would demonstrate a commitment to fair and non-discriminatory digital regulation. **In addition, establishing dedicated regulatory liaison units to coordinate with DEPA and CPTPP members could ensure real-time policy alignment and dispute prevention. Such institutional mechanisms would demonstrate China’s willingness to participate in rules-based governance and reduce legal uncertainty for digital investors.** Furthermore, the pressing need for a plurilateral digital-trade exception toolkit, that would harmonize how necessity and chapeau standards are applied across agreements, become rather evident. Thus, future WTO Joint Statement Initiative (JSI) discussions on e-commerce should consider codifying uniform general exception tests, drawing on the evolving jurisprudence from cases such as US – Gambling and EC – Seal Products.

1. **Conclusion**

The case study thus explored how CPTPP and DEPA incorporates general exception clauses in digital trade. It also examined the legal and strategic tensions posed by China’s data governance model that relied primarily on PIPL, DSL and Cybersecurity laws. Thus, while both agreements allow flexibility of policies under exceptions to incorporate public interest and national security, they simultaneously impose conditions of necessity, proportionality, and non-discrimination. These are criteria that China’s rigid localization mandates. Moreover, opaque enforcement might not consistently meet these criteria. Nonetheless, China positions itself in direct opposition to these frameworks. It pursues controlled openness while signaling interest in joining CPTPP and DEPA. It also demands to maintain its core regulatory sovereignty. Moreover, Chinese firms further reinforce this hybrid approach by adapting compliance models to international standards. **This dual-track strategy enables Beijing to assert digital sovereignty while mitigating international criticism and preserving trade ties.** Thus, China’s legal regime ought to coincide with DEPA and CPTPP in the future. This necessitates **institutional transparency, case-by-case assessments,** and the development of **interoperability mechanisms.** This will enable China to balance digital trade sovereignty with cooperations. The nation will then be able to position itself not only as a rule-taker, but as a credible participant in shaping the future of global digital trade.

Disclaimer (Artificial intelligence)

The author(s) acknowledge the use of generative AI tools, such as large language models, in a limited and supportive capacity during the preparation of this manuscript. These tools were used solely to assist with language refinement, clarity improvements, and formatting suggestions. The core ideas, analysis, and conclusions presented are entirely the work of the author(s).

Details of the AI usage are given below:

1. Tool used: ChatGPT (OpenAI), version GPT-4, accessed via <https://chat.openai.com>.
2. Purpose: Assisted with paraphrasing, grammar correction, and sentence structure refinement.
3. Input type: Draft text written by the author(s) provided for language assistance only.

**References**

Aaronson, S. A., & Leblond, P. (2018). Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. *Journal of International Economic Law*, *21*(2), 245–272. <https://doi.org/10.1093/jiel/jgy019>.

APEC. (2024). *Digital Economy Partnership Agreement.* Asia-Pacific Economic Cooperation. Available at: <https://mddb.apec.org/Documents/2024/CTI/CTI3/24_cti3_004_r.pdf>.

Appellate Body Report. (1998). *United States - Import Prohibition of Certain Shrimp and Shrimp Products - AB-1998-4 - Report of the Appellate Body*. World Trade Organization. Available at: [https://docs.wto.org/dol2fe/Pages/FE\_Search/FE\_S\_S006.aspx?Query=(@Symbol=%20wt/ds58/ab/r\*%20not%20rw\*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#](https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20wt/ds58/ab/r*%20not%20rw*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true).

Appellate Body Report. (2005). *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body – Corrigendum.* World Trade Organization. Available at: [https://docs.wto.org/dol2fe/Pages/FE\_Search/FE\_S\_S006.aspx?Query=(@Symbol=%20wt/ds285/ab/r\*%20not%20rw\*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#](https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20wt/ds285/ab/r*%20not%20rw*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true).

Appellate Body Report. (2012). *United States - Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products - AB-2012-2 - Report of the Appellate Body*. World Trade Organization. Available at: [https://docs.wto.org/dol2fe/Pages/FE\_Search/FE\_S\_S006.aspx?Query=(@Symbol=%20wt/ds381/ab/r\*%20not%20rw\*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#](https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20wt/ds381/ab/r*%20not%20rw*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true).

Bartels, L. (2017). The chapeau of the general exceptions in the WTO GATT and GATS agreements: a reconstruction. *American Journal of International Law*, *109*(1), 95–125. <https://doi.org/10.5305/amerjintelaw.109.1.0095>.

Bennett, A. (2004), Case Study Methods: Design, Use and Comparative Advantages. In Detlef, F.S., and Yaek, W.N. (eds) *Models, Numbers, and Cases: Methods for Studying International Relations.* University of Michigan Press.

Brkan, M. (2019). The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU’s constitutional reasoning. *German Law Journal*, *20*(6), 864–883. <https://doi.org/10.1017/glj.2019.66>.

Burri, M. (2017). The Regulation of Data Flows Through Trade Agreements. *Georgetown Journal of International Law*, 48(1). [https://ssrn.com/abstract=3028137.](https://ssrn.com/abstract%3D3028137)

Burri, M. (2021). Towards a New Treaty on Digital Trade. *SSRN Electronic Journal.*

Cao, Y. (2020). Regulating digital platforms in China: current practice and future developments. *Journal of European Competition Law & Practice*, *11*(3–4), 173–180. <https://doi.org/10.1093/jeclap/lpaa001>.

China Briefing. (2021). T*he PRC Personal Information Protection Law (Final): A Full Translation.* China Briefing. Available at: <https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/>.

China Law Translate. (2021). *Data Security Law of the PRC*. China Law Translate: Community-supported, Crowd-Sourced Translation and Commentary. Available at: <https://www.chinalawtranslate.com/en/datasecuritylaw/>.

Congressional Research Service. (2025). *Digital Trade and Data Policy: Key Issues Facing Congress.* Congress.Gov. Available at: <https://www.congress.gov/crs-product/IF12347#:~:text=Digital%20trade%20includes%20trade%20in,%2C%20streaming%20or%20cloud%20services)>.

Cottier, T., Delimatsis, p., Deibold, N.F. (2008). *Article XIV GATS: General Exceptions. MAX PLANCK COMMENTARIES ON WORLD TRADE LAW, WTO - TRADE* IN SERVICES, Rüdiger, W., Peter-Tobias, S. and Clemens, F., eds., volume 6, pp. 287-328, Leiden/Boston: Martinus Nijhoff Publishers, 2008.

CPTPP Portal. (2025). *Chapter 29 – Exception and General Provisions.* Asia Pacific Foundation of Canada. Available at: <https://apfccptppportal.ca/agreement/31>.

CPTPP. (n.d.). *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*. Institute of International Law and Justice. Available at: <https://www.iilj.org/wp-content/uploads/2018/03/CPTPP-consolidated.pdf>.

DEPA. (n.d.). *Digital Economy Partnership Agreement*. Ministry of Trade & Industry. Available at: <https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Digital-Economy-Partnership-Agreement/Text-of-the-DEPA.pdf>.

EU Parliament. (2020). *Legal Analysis of International Trade Law and Digital Trade.* Directorate-General for External Policies: Policy Department. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/603517/EXPO\_BRI(2020)603517\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/603517/EXPO_BRI%282020%29603517_EN.pdf).

Fan, C. & Zhou, Q. (2025). *China’s Cybersecurity Law Amendments: Key Changes in the Second Draft*. China Briefing. Available at: <https://www.china-briefing.com/news/china-cybersecurity-law-amendments-2025/>.

Kimura, F. (2019). The Importance and Implication of the e-Commerce Clause in the CPTPP. *Financial Cooperation in East Asia*, 106-113. <https://www.jstor.org/stable/resrep25423.17>.

Marwell, J. C. (2006). *Trade and Morality: The WTO Public Morals Exception after Gambling*. *New York University of Law Review, 81*, 802. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=907393>.

MOFCOM. (2022). *Report on Foreign Investment in China.* Ministry of Commerce People’s Republic of China. Available at: <https://wzs.mofcom.gov.cn/cms_files/oldfile//wzs/202301/20230104194942451.pdf>.

MOFCOM. (2024). *Ministry of Commerce Holds Regular Press Conference*. Ministry of Commerce People’s Republic of China. Available at: <https://english.mofcom.gov.cn/News/PressConference/art/2024/art_95700a953fdb4d7085628008e7a825d9.html>.

Nanxiang, S. (2023). Internet Regulation and the Invocation of Security Exceptions in the WTO Agreeement, *HeinOnline, J. WTO & China, 13.*

NZFAT. (2022). *China’s Data Governance Framework takes shape: Implications for New Zealand business*. New Zealand Foreign Affairs & Trade. Available at: <https://www.mfat.govt.nz/assets/Trade-General/Trade-Market-reports/China-data-governance-framework-takes-shape.pdf>.

OECD. (2023). *Key Issues in Digital Trade: OECD Global Forum on Trade 2023 “Making Digital Trade Work for All”.* OECD. Available at: <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/01/key-issues-in-digital-trade-review_5a91f9a0/b2a9c4b1-en.pdf>.

Peng, S. (2015). Cybersecurity threats and the WTO national security exceptions. *Journal of International Economic Law*, *18*(2), 449–478. <https://doi.org/10.1093/jiel/jgv025>.

Public Citizen. (2015). *Only One of 44 Attempts to Use the GATT Article XX/GATS Article XIV “General Exception” Has Ever Succeeded: Replicating the WTO Exception Construct Will Not Provide for an Effective TPP General Exception*. Public Citizen. Available at: <https://www.citizen.org/wp-content/uploads/general-exception_1.pdf>.

Sun, Q. (2025). The Study on Exception Clauses of Cross-Border Data Flows in International Trade Agreements. *Journal of Theory and Practice in Humanities and Social Sciences, 2*(2), 1-18.

The Asian Foundation. (2024). *Digital Trade and Digital Economy Agreements in Asia and the Pacific.* The Asian Foundation. Available at: <https://asiafoundation.org/wp-content/uploads/2024/05/Digital-Trade-Agreements-in-Asia-and-the-Pacific_Tech-Policy.pdf>.

Tusikov, N. (2019). How US-made rules shape internet governance in China. *Internet Policy Review*, *8*(2). <https://doi.org/10.14763/2019.2.1408>.

Van den Bosschem, P. & Zdouc, W. *The Law and Policy of the World Trade Organization: Text, Cases and Materials, 4th edition*. Cambridge, United Kingdom; New York, USA: Cambridge University Press, 2017.9, p.547.

Voss, W.G. (2020). Cross-Border Data Flows, the GDPR, and Data Governance. *HeinOnline: Wah, Int’l L.j., 29*, 485.

Woods, A.K. (2016). Against Data Exceptionalism. *HeinOnline: Stan. L. Rev, 68*, 729.

WTO. (2023). *Digital Trade for Development*. World Trade Organization. Available at: <https://www.wto.org/english/res_e/booksp_e/dtd2023_e.pdf>.

WTO. (2025). *Digitally delivered services trade dataset*. World Trade Organization. Available at: <https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm>.

WTO. (n.d.a). *Article XX: General Exceptions*. World Trade Organization. Available at: <https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art20_e.pdf>.

WTO. (n.d.b). *Article XIV: General Exceptions*. World Trade Organization. Available at: <https://www.wto.org/english/res_e/publications_e/ai17_e/gats_art14_jur.pdf>.

Xiang, X., & Zhao, J. (2025). Enhancing sustainable development through digital service trade liberalization: Analyzing the effects and mechanisms on bilateral imports. *Sustainability*, *17*(5), 1823. <https://doi.org/10.3390/su17051823>.

Yingchao, H., & Xiang, Y. (2024). Influence of trade liberalization and digital trade on material footprint in the BRICS region. *Resources Policy*, *88*, 104374. <https://doi.org/10.1016/j.resourpol.2023.104374>.

Yun, H. (2024). China’s Data Sovereignty and Security: Implications for Global Digital Borders and Governance. *Chinese Political Science Review.*

Zhang, S. (2020). Protection of Cross-Border Data Flows Under International Investment Law. *Handbook of International Investment Law and Policy*, 1-23.