

Balancing Data Security and Trade Secrets: A Comparative View on Multinationals

Yige Yuan

*School of Law, Nankai University, Tianjin, China
xy15076461828@163.com*

Abstract. The internet multinational corporations constitute both beneficiaries and engines of economic globalization. In the digital era, however, their dependence on cross-border data flows increasingly confronts constraints arising from divergent national and regional regulatory regimes. This paper investigates how multinationals may comply with heterogeneous data security laws while simultaneously safeguarding trade secrets, thereby preserving competitive advantage. It examines the legal risks inherent in international data flows by drawing on case-law experiences and analyzes prospective strategies for reconciling regulatory compliance with the sustainable use of cross-border data in corporate practice. The findings suggest that a balanced approach, which integrates regulatory compliance and sustainable data use, is essential for mitigating legal risks and promoting the effective utilization of cross-border data. Ultimately, the paper seeks to contribute to a deeper understanding of how MNCs can maintain stable operations under fragmented legal systems, while advancing openness, predictability, and mutual trust in international trade.

Keywords: multinationals, cross-border data protection, trade secret, digital trade

1. Introduction

In the contemporary digital era, data has emerged as the new oil [1]. For multinational corporations that heavily depend on cross-border data flows, the capacity to collect, analyze, and leverage vast quantities of information is pivotal in delivering personalized products and services and in enhancing customer satisfaction. This fast-growing business model is fundamentally built on the integration of consumers' personal data with companies' proprietary knowledge, where analytics and algorithms transform raw information into valuable commercial insights [2]. A prime example of this is the rise of cloud computing, which enables businesses to store and process data remotely through the Internet. By leveraging this technology, firms can achieve lower operational costs while improving efficiency and productivity [3].

Yet, the same reliance on data also exposes corporations to significant regulatory and legal challenges. Databases often contain sensitive personal information and may implicate broader concerns of national sovereignty over data security. As a result, the free flow of data is increasingly constrained by heterogeneous regulatory regimes across jurisdictions, ranging from data localization requirements to mandatory security reviews. These divergences create potential conflicts between

compliance obligations in host countries and the protection of trade secrets that form the foundation of a firm's competitive advantage.

As pointed out by scholars, divergences in legal frameworks profoundly affect the practice of cross-border data governance. Against this backdrop, this paper examines the discrepancies among leading regulatory regimes governing personal data and data security. Furthermore, it explores the strategies that global corporations may adopt to navigate the dilemma of balancing compliance with the imperative to safeguard their proprietary interests. This study offers practical insights into how these companies can effectively manage the complex interplay between compliance and innovation in the digital age.

2. Legal system differences in data security protection

As cross-border data transfer is a complex process, encompassing various sectors, such as data security and sovereignty, regulatory frameworks differ between countries. While each region may develop its own distinct approach to data governance, there are several advanced and recognizable frameworks that have been implemented, including the European Union's General Data Protection Regulation (GDPR) and the United States' California Consumer Privacy Act (CCPA) [4]. As Chinese big tech firms account for a larger proportion of global trade, the legal system of China's data protection is also of crucial importance for global trade. In this section, the fundamental structure and characteristics of each major legal framework are analyzed.

2.1. European Union: GDPR

The European Union (EU)'s General Data Protection Regulation (GDPR), which is set to come into force on 25 May 2018, is widely regarded as the most advanced model for data security. In accordance with Article 4 of the GDPR, which provides the regulatory framework for this particular subject, internet global companies may be considered as data controllers or processors.

In addition, the principles outlined in Article 5 of the GDPR are indicative of the fundamental regulations governing cross-border data flows. These principles encompass: the tenets of lawfulness, fairness, and transparency; the limitation of data processing to legitimate and specified purposes; the principle of data minimization, which stipulates the necessity; accuracy; storage limitation; integrity; confidentiality and accountability.

With regard to the transmission of data to external locations, if the level of protection of personal data is evaluated as being comparable to that of the EU, the transfer can be permitted. One of the primary mechanisms for achieving this is a set of authorized standard contractual clauses, another is the implementation of binding corporate rules that must be recognized by each of the EU's member states. In summary, This is illustrated by the example of the EU-U.S. Data Privacy Framework reached on 10 July 2023, in which the European Commission ensured that the U.S. offered an adequate level of protection.

In the cases where companies have previously infringed the regulations, they are subject to a two-tier penalty leading to substantial fines. For instance, in September 2023, Ireland's Data Protection Commission (DPC) imposed a fine of €345 million on TikTok for violating the core principles of the General Data Protection Regulation (GDPR) concerning the protection of children's data [5]. However, the GDPR does provide for a number of exceptions to this general rule, including the explicit consent of the subject and the considerations of public interest.

2.2. The US legal system

Similar to the EU, the US is likewise a member of the Organization for Economic Cooperation and Development (OECD). However, in contrast to the EU's General Data Protection Regulation (GDPR), the United States utilizes sectoral federal legislation. In the absence of a holistic or uniform legal framework, the protection of data is enshrined in federal statutes with limited scope, as well as in various state statutes. The most notable state statute in this regard is the California Consumer Privacy Act (CaCPA) of 2018, which sets out three thresholds ranging from penalties to clear evaluation standards for violations.

In addition, the inconsistency between statutes has been noted to present challenges for cross-border corporations in ensuring compliance. Furthermore, the restricted interpretations of statutes and the ambiguous definition of the protected object in court cases are similarly circumscribed. To illustrate this point, consider the cases of *Spokeo, Inc. v. Robins* and *Gubala v. Time Warner Cable*. In such cases, the evaluation of the concrete harm was different in the Supreme Court and the U.S. Court of Appeals for the Seventh Circuit [6].

In terms of policy preferences, the United States is in favor of the liberalization of data flows and is against the restriction narratives in the European Union's regulations. Nevertheless, there are several cases which serve as the archetypal exceptions to this rule, in that the US government has imposed limitations on the free flow of information on the grounds of national security. One such example is the prohibition of the use of TikTok.

2.3. China – legal system for data protection

The legal framework of data protection in China is closely associated with the concept of cyber sovereignty, resulting in the implementation of more stringent regulations governing cross-border data flows. The three core legislations are the Cybersecurity Law (CSL), the recently enacted Data Security Law (DSL) and the Personal Information Protection Law (PIPL). In order to ensure the effective implementation of these core legal documents, detailed regulations were established. These state council regulations and departmental rules serve to facilitate the practical application of the aforementioned regulations [7-8].

To elaborate further, the narratives and structure of the Chinese legal system bear a resemblance to those of the GDPR. However, there is a notable distinction in that the primary protected object emphasized in China's legal system is national security rather than personal information.

Nonetheless, multinational corporations conducting business in China have encountered difficulties in adhering to regulatory frameworks due to the ambiguity of certain provisions and the lack of clarity in assessment criteria. In order to ensure the effective implementation of the regulations, as well as the continued expansion of China's cross-border digital trade market, the "Provisions on Promoting and Regulating Cross-Border Data Flow" (new CBDF Provisions) were published in 2024, with a clear relaxation of the CBDF regulations. The recent CBDF Provisions have established a novel set of conditions and thresholds, denoting a shift towards a more liberalized CBDF framework. For instance, the subject to security assessment is detailed and narrower than the previous ones, and the limitation of data flows adopts a negative list approach.

3. Comparative analysis

3.1. The data protection perspective

As the EU, the US, and China represent the largest markets for digital cross-border data trade, by identifying discrepancies among their standards, multinational corporations can better understand fundamental compliance requirements and expand their business. This section compares the three legal systems from three dimensions:

First, the origin of data protection differs. The EU's GDPR prioritizes privacy and individual rights [9]. Despite structural similarities to the GDPR, China emphasizes national security under cyber sovereignty. Different to the former ones, the US sectoral approach stresses global trade liberalization, with consumer and market protection as its main objective.

Second, the scope of object varies. The EU adopts a broad approach and distinguishes categories of information, with "sensitive personal information" subject to stricter rules. For instance, the category of "sensitive personal information" receives the stricter regulations. By contrast, The US patchwork system defines protected data differently in each statute but typically covers key areas such as children's information [10]. As the tendency to free data flows, the US does not regulate certain strictions of data flows except several cases claiming to the big tech like TIKTOK of China. By comparison, China's definitions are less explicit, combining personal and "important data." However, the 2024 CBDF Provisions improve clarity by adopting a negative list approach.

Third, enforcement mechanisms differ. The EU's GDPR primarily relies on administrative fines enforced by decentralized regulators across Member States. In the US, enforcement primarily occurs through litigation and judicial interpretation, involving multiple layers of government and courts. In contrast, China's enforcement model is centralized, relying on administrative oversight—such as mandatory security assessments—and even extending to potential criminal liability for severe violations.

3.2. The trade secret protection perspective

In the TikTok case, US regulators demanded disclosure of the app's algorithm on the grounds that its data collection and flows posed a threat to national security. This controversy highlights not only the issue of data protection but also the challenge of trade secret protection from the perspective of multinational enterprises. Encountering this dilemma, cross-border companies such as TikTok's parent company face a dilemma between complying with host state data protection requirements and safeguarding their fundamental right to protect trade secrets.

The definition of trade secret in the EU, the US and China is similar, encompassing three criteria: confidentiality, commercial value, and reasonable protective measures. The distinction lies in the underlying policy rationale. The EU emphasizes market fairness and harmonization, the US framework prioritizes litigation efficiency, while China extends protection to include criminal remedies in cases of severe violations.

The data secret always integrate with sensitive data collecting in operations. This creates a persistent tension between the data protection and the trade secret: data protection frameworks determine the legal risks of cross-border operations, whereas trade secrets represent a company's core competitive advantage. In the EU, the GDPR and Trade Secrets Directive between the data protection and the trade secret: data protection frameworks determine the legal risks of cross-border operations, whereas trade secrets represent a company's core competitive advantage. In the US, disclosure of trade secrets can be compelled when an event is deemed to implicate national security

or law enforcement interests. For example, between 2017 and 2025, TikTok has faced continuous investigations by US authorities into its databases and cross-border data flows. In China, the risk of trade secret exposure primarily arises during mandatory security assessments prior to operation. Although the Anti-Unfair Competition Law provides trade secret protection within the trade market, the overarching priority remains national sovereignty.

As demonstrated above, the EU prefer to striking a balance between privacy rights and trade secrets, albeit with uncertain enforcement; the US favors free data flows but subjective companies to disclosure obligations under administrative or security concerns; and China stipulates stricter assessments of data flows, consistently prioritizing national sovereignty above commercial secrecy [9].

4. Legal and institutional strategies

How to address the dilemma between data compliance and trade secret protection is a critical challenge for multinational corporations, particularly given the sustained global expansion of the digital market. As noted in earlier chapters, cross-border data flows often implicate sensitive domains, including individual privacy rights and public interests such as national security. Accordingly, the establishment of a universal standard of data protection remains unrealistic due to divergent policy preferences. Moreover, although digital trade has expanded rapidly, gaps in the legal framework and enforcement inevitably persist. As a result, multinationals must adopt flexible strategies that combine external legal tools with internal governance adjustments.

First, the most effective external tool is legal defense. Article 39 of TRIPs incorporates trade secret protection within the scope of intellectual property rights, equating trade secrets with other forms of intellectual property, with the clear objective of prohibiting unlawful misappropriation. As data and algorithms constitute the core assets of global digital enterprises, host countries' trade secret laws—such as the UK's Trade Secrets Regulations—can be invoked as a practical defense against unreasonable disclosure demands.

Second, companies must undertake internal reforms to ensure trade secret preservation in the face of regulatory obligations. This includes segregating collected and transferred data into clear categories, such as “sensitive personal information” under Chinese law. It also requires establishing precise audit trails of databases and algorithms to simulate investigative processes. Such evidentiary records are often sufficient to satisfy the GDPR's standards of adequacy or to rebut claims of concrete harm under US law. Importantly, companies must maintain transparency with data providers by disclosing data processing practices in a manner consistent with privacy rights.

In summary, multinationals can seeks to the balance between data protection and trade secret protection by adopting record-keeping and evidentiary measures that reinforce compliance. In addition, despite the current uncertainty of data flow regulation, the shared objectives of promoting digital trade and safeguarding national interests provide the basis for emerging consensus among trade partners.

5. Conclusion

This paper examines the dilemma faced by multinational corporations, particularly those whose operations rely heavily on cross-border data flows, through a comparative analysis of the three major legal frameworks of data protection. Central to this analysis lies on the question of whether trade secrets can be sufficiently safeguarded under existing exceptions or intellectual property laws meanwhile keeping data compliance. As digital trade remains an emerging phenomenon within

global commerce, the legal frameworks governing data protection are themselves still evolving, marked by regional discrepancies and considerable uncertainty. Above all, for multinationals, the regulatory environment is undeniably complex and, at times, opaque. Nevertheless, strategies to mitigate risks are available, including strengthening legal teams to effectively invoke trade secret protection clauses, and undertaking internal governance reforms to refine the operation of cross-border databases.

In summary, balancing data protection with trade secret protection remains a formidable challenge. However, as digital trade increasingly becomes a central component of global commerce, practical strategies are emerging, and the gradual convergence of exceptions across jurisdictions indicates the possibility of broader international consensus in the future.

References

- [1] Noto La Diega, G., & Sappa, C. (2020). The Internet of Things at the intersection of data protection and trade secrets: Non-conventional paths to counter data appropriation and empower consumers. *Revue européenne de droit de la consommation / European Journal of Consumer Law*, 3, 419-458. Available at SSRN: <https://ssrn.com/abstract=3772700>
- [2] Guo, S., & Li, X. (n.d.). Cross-border data flow in China: Shifting from restriction to relaxation? Available at SSRN: <https://ssrn.com/abstract=4806703> or <http://dx.doi.org/10.2139/ssrn.4806703>
- [3] Banterle, F. (2016). The interface between data protection and IP law: The case of trade secrets and database sui generis right in marketing operations, and the ownership of raw data in big data analysis. In M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, & S. Surblytė-Namavičienė (Eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?* Available at SSRN: <https://ssrn.com/abstract=3276710>
- [4] Christakis, T. (2019). Transfer of EU personal data to U.S. law enforcement authorities after the CLOUD Act: Is there a conflict with the GDPR? In R. Milch & S. Benthall (Eds.), *Cybersecurity and Privacy in a Globalized World - Building Common Approaches* (forthcoming). Available at SSRN: <https://ssrn.com/abstract=3397047>
- [5] Voss, W. G., & Houser, K. (2019). Personal data and the GDPR: Providing a competitive advantage for U.S. companies. *American Business Law Journal*, 56, 287-344. Available at SSRN: <https://ssrn.com/abstract=3389515>
- [6] Khan, M. N. I. (2025). Cross-border data privacy and legal support: A systematic review of international compliance standards and cyber law practices. *American Journal of Scholarly Research and Innovation*, 4(01), 138-174. <https://doi.org/10.63125/a4gbeb22>
- [7] Malgieri, G. (2015). Decontextualized data sharing at the borderlines between trade secrets and data protection rules. Available at SSRN: <https://ssrn.com/abstract=2600880> or <http://dx.doi.org/10.2139/ssrn.2600880>
- [8] Sandeen, S. K. (2014). Lost in the cloud: Information flows and the implications of cloud computing for trade secret protection. *Virginia Journal of Law and Technology*, 19. Available at SSRN: <https://ssrn.com/abstract=2490671>
- [9] Wodi, A. (2023). The EU General Data Protection Regulation (GDPR): Five years after and the future of data privacy protection in review. Available at SSRN: <https://ssrn.com/abstract=4601142>
- [10] Voss, W. G., & Pernot-Leplay, E. (2024). China data flows and power in the era of Chinese big tech. *Northwestern Journal of International Law & Business*, 44, 1-68. Available at SSRN: <https://ssrn.com/abstract=4393008>