Proceedings of the 2nd International Conference on Social Psychology and Humanity Studies
DOI: 10.54254/2753-7048/36/20240458

The Game Process and Achievement of EU and US Cross Border Data Flow Rules

Yinuo Yang[1,a], Yanya Zhao[2,b,*]

[1]*Department of English, China University of Mining and Technology, Jiangsu, 221000, China*
[2]*Department of Business Management, SKEMA Business School, Paris, 92150, France*
a. 12223882@cumt.edu.cn, b. yanya.zhao@skema.edu
**corresponding author*

Abstract: In today's data-driven era, the governance of data rules has become a focal point for countries worldwide. This paper elucidates the significant differences between the United States and Europe, both major players in this domain, in terms of legislation and value positions. They also operate within distinct social data environments and possess varying national interest needs. These influence the direction and results of the game between the two sides in the data privacy framework. The paper also encompasses many far-reaching factors involved in this process, such as the political relationships between the United States and Europe, and the economic conditions on both sides. In the contest for dominance in data governance rules, the United States and Europe have been constantly interacting, refining regulations through ongoing friction, and to some extent, driving the development of the data industry. Meanwhile, the world still needs a more mature and stable regulatory framework for data governance rules, indicating the necessity for further significant progress in this area.

Keywords: Data Flow Rules, Digital governance, EU, the United States, International Politics

1. Introduction

With the global digital wave sweeping through, data has become the lifeline of today's digital society and an important driving force for economic growth and technological innovation. As two independent entities of the United States and the European Union, which are pioneers in the construction of global cross-border data governance rule systems, there are significant differences between them. It is precisely this difference that hinders the cross-border flow of data between the European Union and the United States, which has been constrained by many laws and concepts, triggering a transatlantic game. This report will delve into the game process between the European Union and the United States on cross-border data flow rules and focus on foreseeable paths for future development.

The focus on data privacy legislation in the United States is scattered and lacks a unified national framework. But there are many state-level regulations, such as California's Consumer Privacy Act (CCPA), one of the many state-level privacy laws in the United States. In addition, many federal regulations, such as the Children's Online Privacy Protection Act and the Electronic Communications Privacy Act, involve data privacy [1]. In Europe, data protection is a fundamental constitutional right, and a comprehensive legislative system has been established to coordinate member states' regulation of personal data processing [2]. Several judicial issues arising under data protection directives have

DOI: 10.54254/2753-7048/36/20240458

been resolved through the emergence of the General Data Protection Regulation (GDPR). GDPR legal requirements immediately bind all EU member states. Although the EU has a consistent GDPR, there may still be some institutional differences within the EU. Different member states can develop national laws based on GDPR to supplement regulations and adapt them to their situations. This may lead to some differences and subtle changes in implementation and execution.

In the United States, data sovereignty focuses more on market freedom, commercial competition, and technological innovation. The United States emphasizes the free flow of data and encourages companies to use data to create business opportunities and innovation [3]. Data sovereignty is more closely related to corporate and market equity in the United States [3]. The EU places greater emphasis on protecting individual privacy rights and data sovereignty. Europe regards personal data as a fundamental right and protects the security and privacy of personal data through regulations such as GDPR. The EU places greater emphasis on individual control and autonomy over data sovereignty.

In both the United States and the European Union, there is a certain degree of data nationalism tendency, and the United States' performance in data nationalism mainly focuses on national security and economic aspects. The EU's performance in data nationalism primarily focuses on privacy protection and data sovereignty.

The international community has not reached a consensus on cross-border data flow rules. The United States and the European Union have a leading advantage in formulating relevant rules. However, the United States and Europe hope to take the lead around the determination of cross-border data flow standards, which has led to multiple rounds of intense games between the two sides [4]. A thorough examination of the debate over data protection regulations between the US and Europe can clarify the global governance framework for cross-border data flows and offer helpful resources for pursuing rule formation rights in this area.

2. The Reasons for the Game of Cross border Data Flow Rules between the United States and Europe

The evolution of cross-border data flow rules between the United States and Europe has been ongoing for over 20 years. The United States and Europe are two significant players in cross-border data flow governance actively engaged in rule coordination and cross-border data flow governance. However, due to fundamental differences in values and regulatory models between the United States and Europe, competition among digital enterprises, and significant differences in issues such as privacy protection, overseas jurisdiction, and digital service tax, the formation of a cross-border data transmission cooperation mechanism between the two is fraught with difficulties.

The divergent views on data flow held by the US and Europe reflect the disparities in cross-border data flow regulations between the two regions [4]. As early as the 1970s, The United States and Europe enacted data privacy and security regulations nearly simultaneously, realizing the value of safeguarding personal information and the risks associated with its improper use. In data privacy, two distinct enforcement methods have surfaced, nevertheless. Europe has always regarded respect for privacy and personal data protection as fundamental rights [5]. Data protection and privacy rights were incorporated in the EU Charter of Fundamental Rights in 2000. These rights were explicitly mentioned in two distinct articles, Articles 7 and 8. This charter is recognized as having the primary legal status within the hierarchical structure of EU legal sources at the same level as the founding treaty of the EU [6]. The United States Constitution is credited as being the birthplace of privacy. However, it was written in 1787, and the Bill of Rights wasn't added until three years later, long before privacy became a concern.

The conceptual distinctions between the two sides' approaches to data and privacy protection are reflected in the disparities in cross-border flow regulations for data between the United States and Europe but also directly relate to the competition between the United States and Europe around

DOI: 10.54254/2753-7048/36/20240458

technology and industry dominance. As both developed economies, the United States and the European Union significantly differ in information and communication technology and industrial development. The United States is a global leader in the digital information and communication technology industry. In contrast, the European Union's digital technology development lags far behind the United States, relying heavily on external cloud service providers and lacking the ability to process and analyze big data. Throughout the past 15 years, Europe's proportion of the worldwide R&D expenditure in technology has rapidly declined. France has decreased from 6% to 2% and Germany from 8% to 2% [7]. Therefore, in the process of cross-border data transmission between the United States and Europe, due to the technological advantages of the United States, a large amount of EU data flows to the United States. This pattern also shows that the we and the EU have implemented distinct regulatory approaches and standards for privacy protection in cross-border data transfers.

In 2018, the European Commission launched a legislative proposal on a digital service tax to adjust the taxation rules for large internet companies. EU member states such as Spain, Austria, and France have also carried out legislative work on digital service taxes. The United States is deeply unhappy about some EU member states' unilateral decision to tax internet services. As it believes it exclusively levies digital service taxes on digital advertising and cross-border data flows for trade protection, the United States is against European nations' tax policies and reach. In the view of EU countries, digital enterprises represented by American technology giants are constantly encroaching on startups, affecting a fair competitive environment in Europe. At the same time, the large amount of valuable data and information held by American technology giants has gradually formed a benign model of mutual promotion between data acquisition and economic development. The soft development model of American enterprises will squeeze the development space of digital enterprises in the European Union, and imposing a digital service tax can somewhat reduce this situation.

The relationship between the United States and Europe also has far-reaching implications for adopting measures in both regions concerning data governance. The United States, as the world's economic powerhouse, holds sway over the global economic discourse. It boasts a plethora of tech giants in various domains, such as Google, Apple, Amazon, Facebook, and more. America’s tech oligopoly Meta, Alphabet, Microsoft, Amazon, and Apple has outpaced even the breakneck growth by 10%, a third of the American GDP [8]. These companies dominate the international digital market and can collect and process digital data globally, thus affording the United States access to vast amounts of digital data. The United States has a leading technological advantage and abundant innovative research and development resources regarding internet infrastructure. This places the United States in a dominant position in science and technology, enabling it to wield considerable influence in shaping and leading international data governance rules. As the world's largest financial center and the most significant holder of global currency, the United States is instrumental in facilitating cross-border capital flows and digital payments.

There is a noticeable power asymmetry between the United States and Europe. The United States possesses superior scientific and technological capabilities and more potent economic might and wields more significant political influence. This phenomenon resulted in more rule control for the United States in negotiations between the US and Europe. As a result, the United States can advocate for establishing rules more favorable to its interests in the pursuit of data dominance. In relative terms, Europe has fewer chips during these negotiations.

3. Key Points and Trends of Three Games

The data privacy framework in Europe and America is a product of the game and a compromise between market demand and national security interests in Europe and America. Realism dictates that

DOI: 10.54254/2753-7048/36/20240458

controlling cross-border data flows is fundamentally a competition between nations. Three games have been played in cross-border data flow between the US and Europe.

Both before and after the Safe Harbor Agreement was signed in 2000. The competition mirrored the first round of the game. The Safe Harbor Agreement has formulated seven privacy principles based on the Personal Data Protection Directive. American companies that voluntarily choose to join the Safe Harbor Agreement must comply with these principles and propose specific implementation plans. At the same time, the European Union has adopted a strict attitude towards government agency regulation, and according to the privacy protection policy of the United States, American enterprises (such as telecommunications, banking, etc.) that government agencies do not regulate are not allowed to join the agreement [9]. It can be said that the Safe Harbor Agreement is the first concession made by the United States to the EU's privacy protection system.

After the Snowden incident, the European Union comprehensively accelerated the cybersecurity governance process; as a result, differences and conflicts between Europe and the United States gradually intensified. The European Union began to evaluate the security of network cooperation between Europe and the United States. The second round of game between the two sides has also started.

The large-scale online surveillance and severe infringement of citizens' privacy rights in the United States have received widespread condemnation from the international community. The European Commission has also claimed that the large-scale surveillance behavior in the United States is "unacceptable" and demanded that the United States take immediate remedial measures, renegotiate and improve the content of the Safe Harbor Agreement, and restore the EU's trust in the US government. In the same year, Austrian citizen Maximilian Schrems filed a complaint with the Irish data protection regulatory agency, claiming that EU personal data could not be fully protected due to surveillance actions by the US government and requesting a ban on Facebook Ireland from transmitting relevant personal data to the US headquarters. The US-Europe Safe Harbor Agreement was declared void in 2015 when the European Court of Justice overturned the Safe Harbor Agreement's conclusion that the US can guarantee adequate protection for EU personal data. Subsequently, after ongoing negotiations between the two parties, the US government issued a written commitment to the European Commission, pledging to restrict and provide relief measures for their "access to and use of personal data in the public interest", including the establishment of a new national security intervention supervision mechanism, which is an independent "privacy shield inspector" from the US intelligence agency.

On this basis, the United States and Europe reached the second cross-border data transmission agreement in 2016: the Privacy Shield Agreement. The Privacy Shield Agreement has stricter personal data privacy protection standards than the Safe Harbor Agreement. It stipulates that US intelligence agencies must be constrained and restricted when collecting personal data from the European Union on national security grounds [10]. It also adds an annual joint review mechanism to prevent the US government and enterprises from failing to comply with the agreement's content (enforcement issues). The signing of the Privacy Shield Agreement is the second concession by the United States to the EU's privacy protection system. In addition to failing to provide "effective administrative and judicial remedies" for EU data subjects whose rights may have been violated, the United States was found by the European Court of Justice to have violated the principle of proportionality by failing to clearly define the scope of large-scale intelligence information or data collection. A subsequent ruling declared the privacy shield agreement unenforceable.

The privacy shield invalidation ruling is not only a reiteration of the Safe Harbor Agreement invalidation ruling. The Safe Harbor Agreement did not conduct a detailed review of the relevant monitoring legislation in the United States, nor did it explain or apply the principle of proportionality. Instead, it was mainly determined to be invalid based on the agreement's flaws. In the invalidation

DOI: 10.54254/2753-7048/36/20240458

judgment of the Privacy Shield Agreement, the European Court conducted a detailed review and questioning of domestic legislation and policies related to surveillance in the United States.

In response, since 2010, the EU has wielded regulatory sticks such as antitrust, privacy protection, and platform content and repeatedly issued fines to Silicon Valley oligarchs. In July 2019, France decided to take the lead. It passed its version of the digital tax bill, taxing technology companies with global revenue of 750 million euros and French revenue of more than 25 million euros—Google, Facebook, Amazon, Apple, etc. [11] Silicon Valley oligarchs are bearing the brunt.

With the continuous awakening of the awareness of "digital sovereignty", the European Union has introduced several data security protection laws and digital service taxes, hoping to increase the protection barrier for the growth of local digital enterprises. In May 2018, the General Data Protection Regulation (GDPR) launch was an important milestone for the EU to demonstrate its "digital sovereignty." In addition to the GDPR, the European Commission is drafting other internet-related bills to assert intra-continental “digital sovereignty.” As the main subject of supervision, the United States is naturally quite dissatisfied with the above-mentioned bills. The United States believes introducing GDPR is a measure to protect the local market based on geopolitical purposes rather than genuinely safeguard user privacy. It is the latest means for European political forces to fight against the digital power of the United States [12].

In 2022, the United States and Europe issued a joint statement promising to establish a new transatlantic data privacy framework and address concerns the European Court of Justice raised in its invalid decision on the Privacy Shield in 2020. According to the Transatlantic Data Privacy Framework (2022), the US commitment includes strengthening the protection of citizens' privacy and freedom in US signal intelligence activities, establishing independent and binding new relief mechanisms, and strengthening layered supervision of signal intelligence activities [13]. The official website of the White House in the United States clearly states that to ensure the so-called "common value", the US government is in close consultation with the European Commission on the redrafting of relevant agreements for the cross-border transmission of personal information [14]. Interestingly, though, "common values" are not mentioned at all on the official website of the European Commission; instead, it solely emphasizes the protection of personal information and the promotion of open data flow.

The cross-border flow of personal information involves three intertwined interests: personal information protection, free data flow, and data, but ultimately, it is a matter of trust. However, in the current constant conflicts in the world, whether the United States can rebuild the confidence of the European Union, especially those of the 'old European' countries, may still have a long way to go.

4. Policies to Promote the Development of Digital Economy Industries

4.1. The United States

In the National Network Strategy released in 2018, the United States pointed out that it should expand government purchases, increase investment in research and development, reduce taxes on the private sector, and accelerate the growth of new-generation communication technologies such as 5G. The U.S. National Defense Authorization Act of 2020 approved special funds of US$275 million to fund the research and development of 5G network technology and the construction of test sites for domestic military facilities [15]. The large-scale expansion of digital infrastructure in the United States focuses on the role of private enterprises. In 2018, the "Legislative Outline for Reconstructing Infrastructure," launched by the United States, proposed developing digital infrastructure such as autonomous driving, new rail transportation technology, and drones. Most of the investment came from private enterprise investment and bonds. Through infrastructure construction, the manufacturing industry will return to China and promote the development of emerging industries.

DOI: 10.54254/2753-7048/36/20240458

While actively exploring the international market, the United States hopes to lead the formulation of trade-related rules. The United States regards digital trade rules as a potentially important tool for promoting its digital leadership and actively explores foreign cooperation. The current digital trade agreement in the United States mainly relies on implementing the United States–Mexico–Canada Agreement and the US-Japan Digital Trade Agreement. These agreements have become templates for the United States export rules, leading to the developing of a new generation of trade rules and an effective tool for expanding its digital globalization benefits. Under the influence of the US Indo-Pacific economic framework, countries such as South Korea, Australia, India, Malaysia, and Singapore may become new partners for the US in digital trade. At the same time, the United States also attaches great importance to its top advantage in the high-tech industry.

4.2. EU

The International Digital Ecology Index quantifies the overall status of digital ecological development in various countries in four dimensions: digital foundation, digital capabilities, digital applications, and digital regulation. The digital regulatory system of the European Union has high completeness, with scores significantly higher than those of the United States in this dimension. The "European Data Strategy" states that between 2021 and 2027, investments of between 4 and 6 billion euros would be made in cloud infrastructure and shared data space [16], including developing data-sharing platforms that scientific research institutions and government departments can use.

The European Union lags behind the United States in the three indicators of digital foundation, digital capability, and digital application in the international digital ecosystem index mentioned earlier. The European Union has muscular technological strength and a high-level manufacturing industry but has not nurtured digital technology giants, which is caused by multiple factors. The main element is that Europe's multilingual environment, small population, and relatively fragmented market make it challenging to form economies of scale, which is not conducive to the birth of digital technology giants. To support local internet and digital enterprises, traditional technology powers represented by Germany and France in the European Union have attempted to awaken the EU's "digital sovereignty consciousness" through various methods, protect digital security through legislation, and impose a "digital tax" to limit the excessive market share of American digital technology giants in the European market. The European Parliament has passed regulations such as the Digital Services Act, the Digital Markets Act, and the General Data Protection Regulations, laying a policy combination punch on the "digital hegemony" of the United States to increase protective barriers for the growth of local digital enterprises.

5. Conclusions

Since the 20th century, Silicon Valley in the United States has almost monopolized Europe's major markets, such as e-commerce, search, and social networking. It has also restricted the development of local European start-ups. At the same time, through transfer pricing and other methods, profits earned from Internet giants such as the United Kingdom, France, and Germany are transferred to "low-tax countries" such as Ireland and Luxembourg. Some central European member states have levied digital taxes to eliminate tax avoidance by multinational Internet giants.

As one of the new production factors, data has become the third largest strategic resource after materials and energy and is called the "oil of the digital economy." Global attention to international digital governance issues is consistent. How to effectively manage massive data, fully protect data, and tap the value of data has become a significant issue facing all countries. Both the United States and the European Union have launched a series of top-level designs and specific measures in infrastructure, innovative technology, human capital, etc., to support the development of the digital

DOI: 10.54254/2753-7048/36/20240458

economy. Methods include supporting and guiding government procurement and private investment and strengthening the construction of digital economic infrastructure. The EU's traditional technology powers, represented by Germany and France, are trying to awaken the EU's "digital sovereignty consciousness" through various means, protect digital security through legislation, and limit the excessive market share of US digital technology giants in the European market. The United States will also make corresponding policy adjustments to respond to the EU's policy regulations, further emphasizing the development of market-driven global market infrastructure based on an open and inclusive framework and the principles of transparency, sustainability, and responsibility.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] *Tao Jun, Qi Tianyi, and Zhu Yuehao. (2022). Regulatory Policies and Specific Case Studies of Large-Scale Internet Platforms in Mainstream Countries and Regions: The United States, Europe, and Russia. Industry Information Security, 2022(07):14-20.*

[2] *Huang Zhixiong and Wei Xinyu. (2021). The Rule Games between the US and EU on Transborder Data Flows and China's Response: From the Perspective of Invalidation Judgment of the Privacy Shield Framework. Journal of Tongji University (Social Science Section), 32(02):31-43.*

[3] *Zhang Kun.(2020). Trends, differences and cooperation prospects of digital trade rules between the US and Europe. China Journal of Commerce, 15:89-91.*

[4] *Liu Jinhe and Cheng Haiye. (2020). Global Governance of Transborder Data Flow: Progress, Trends, and China's Path. Global Review,12(06):78.*

[5] *Mariusz Maciejewski. (2023). Facts sheets on the European Union: Personal Data Protection. Retrieved from https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection#:~:text=Protection%20of%20personal%20data%20and%20respect%20for%20private,safeguarding%20human%20rights%2C%20including%20data%20protection%20and%20privacy.*

[6] *Europe Commission. (2000). EU Charter of Fundamental Rights. Available at https://www.europarl.europa.eu/charter/pdf/text_en.pdf*

[7] *Babinet, G., Coste, O. (2022). Digital Tech: Europe's Growing Gap in Eight Charts. Retrieved from https://institutmontaigne.org/en/expressions/digital-tech-europes-growing-gap-eight-charts*

[8] *The Economist. (2022). The era of big-tech exceptionalism may be over. Retrieved from https://www.economist.com/leaders/2022/07/27/the-era-of-big-tech-exceptionalism-may-be-over*

[9] *United States Department of Commerce and European Union. (2000). Safe Harbor Agreement. Available at https://sgp.fas.org/crs/misc/R44257.pdf*

[10] *Government of U.S and EU(2016). Privacy Shield Agreement. Available at https://www.myrasecurity.com/en/knowledge-hub/privacy-shield/#:~:text=Privacy%20Shield%20was%20an%20informal%20agreement%20between%20the,by%20the%20EU%20Commission%20on%20July%2012%2C%202016.*

[11] *Zhang Chunyan. (2020). Analysis of the background and impact of the French Digital Services Tax Act. Foreign Affairs College.*

[12] *Europe Commission. (2018). General Data Protection Regulation. Available at https://gdpr-info.eu*

[13] *The White House. (2022). United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework. Available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/#:~:text=Under%20the%20Trans-Atlantic%20Data%20Privacy%20Framework%2C%20the%20United,to%20ensure%20compliance%20with%20limitations%20on%20surveillance%20activities.*

[14] *U.S and EU (2022).Transatlantic Data Privacy Framework (2022). Available at https://crsreports.congress.gov/product/pdf/IF/IF11613*

[15] *Authenticated U.S. Government Information. (2020). National Defense Authorization Act for Fiscal Year 2020. Available at https://congress.gov/116/plaws/publ92/PLAW-116publ92.pdf*

[16] *European Commission. (2022). European data strategy: Making the EU a role model, a society empowered by data. Available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en*