Proceedings of the International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/44/20230095

Balancing Data Protection and Data Utilization: Global Perspectives and Trends

Yishi Wu[1,a,*]

[1]*Department of Law, Shantou University, Shantou, 515063, China*
a. 20yswu1@stu.edu.cn
**corresponding author*

Abstract: The exponential growth of personal data in the digital era has raised significant concerns regarding data protection and privacy. This work delves into the global perspectives and trends surrounding data protection laws, data security, cross-border data transfers, and data subjects' rights. It emphasizes the importance of balancing data utilization for economic benefits with safeguarding individuals' personal data. As the risks revealed by high-profile incidents, such as the Cambridge Analytica/Facebook scandal, Equifax data breach, and Yahoo data breaches, the hazards associated with unauthorized data exploitation have been underscored. The work examines the impact of the EU's General Data Protection Regulation (GDPR) and the proliferation of data protection legislation worldwide. It explores three international trends in data protection and utilization, including balancing personal data protection and data value utilization, promoting the sharing and utilization of public data, and establishing jurisdictional control over overseas data. However, providing an extraterritorial effect in data protection regulation faces challenges rooted in state sovereignty and non-interference. Evaluating the legitimacy of such claims requires consideration of international law sources, international conventions, customs, and general legal principles. Moreover, the benefit orientation of enterprises and technological progress limits the effectiveness of the "Brussels Effect," leading to jurisdiction-specific differentiation and fragmenting the global market.

Keywords: Data protection laws, Data security, Cross-border data transfers, Data subjects' rights

1. Introduction

The increasing reliance on digital technologies and the exponential growth of personal data have brought forth significant concerns regarding data protection and privacy. In today's data-driven economy, personal data has become a valuable asset, generated by individuals' identities and behaviors, and often traded in exchange for enhanced services and products [1]. Data can bring huge economic benefits, but the proliferation of personal data has also raised questions about the potential abuse and unauthorized use of such information at the same time [2].

DOI: 10.54254/2753-7048/44/20230095

1.1. Risk of Abuse from Data Explosion Revealed by Extensive Cases

Numerous high-profile incidents serve as stark reminders of the perils linked to data acquisition and misuse. For example, in the Cambridge Analytica/Facebook scandal, personal data from millions of Facebook users was collected without users' authorized and was subsequently used for targeted political messaging [3]. This incident brought to the forefront the pivotal role data gathering plays for online platforms and the potential ramifications of unregulated data exploitation.

Moreover, the Equifax data breach 2017 exposed the personal information of nearly 147 million consumers, including highly important details like Social Security numbers and credit card information [4,5]. The Yahoo data breaches in 2013 and 2014, affecting billions of user accounts, revealed personal information such as their real names, email addresses, and phone numbers [6,7]. Similarly, we can see that the 2018 Marriott International data breach compromised approximately 500 million guest records, divulging personal information like names, addresses, passport numbers, and payment card details [8,9]. These terrible security breaches instilled concerns about the potential for identity theft and financial fraud, highlighting the risks associated with unauthorized access to individuals' personal data.

These instances serve as concrete illustrations of data breaches, illicit data collection, and privacy controversies, effectively highlighting the hazards connected to data misuse and underscoring the imperative for robust data protection measures.

1.2. Global Shift Towards Data Protection and Privacy Legislation

In response to these growing concerns, there has been a global shift towards enacting data protection and privacy legislation. Recognizing the need to seek a balance between the benefits of data-driven economies and the protection of individual privacy, many countries have started to regulate the handling and management of personal data.

Until 2021, the data compiled by the United Nations Conference on Trade and Development (UNCTAD) reveals that data protection and privacy legislation has been implemented to varying extents in around 80% of countries worldwide [10]. These legislative endeavors seek to bolster individuals' authority over their personal data and set forth frameworks for organizations to manage such data. Notable instances of such legislation encompass the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the United States, and Brazil's General Data Protection Law (LGPD).

Even in China, the world's most populous nation, significant strides have been made in data privacy legislation. In August, China passed its first substantial data privacy law, known as the Personal Information Protection Law (PIPL). The enactment of this law has far-reaching implications, as any global business or aspiring startup engaged in online trade or service provision may be affected when interacting with Chinese residents covered by the PIPL.

The legislative frameworks implemented by various countries emphasize the importance of individuals' consent and understanding of how their data is processed. User consent has become a pillar of data protection measures, ensuring that individuals are informed participants in the data-driven ecosystem. This principle finds manifestation not just within the European Union and the United States but also in the newly adopted Directive 2019/770, which pertains to specific aspects of contracts for providing digital content. This directive recognizes the utilization of personal data as a reciprocal element in exchange for "free" digital services or discounts on online products and services.

1.3. Global Impact and Diversification of Data Governance Models

The traditional notion of territorial jurisdiction in judicial matters is ill-suited to address the complexities of data regulation in an interconnected world [6]. Recognizing this challenge, the

DOI: 10.54254/2753-7048/44/20230095

European Union (EU) has taken a “leading role” in updating its legislation to adapt to the digital age. The EU has introduced iterative updates to its regulations, encompassing digital content, digital services, digital markets, data flow, and artificial intelligence. These comprehensive measures have positioned the EU as a major influencer in global data regulation.

The impact of the EU's data rules and standards extends beyond its borders [11]. Approximately 67 countries outside the EU have embraced the GDPR framework. The EU's approach has been emulated to varying degrees by governments worldwide, ranging from East Asian nations like Japan and South Korea to Latin American countries such as Brazil, Argentina, and Uruguay. However, it is crucial to acknowledge that the expansion of a single data governance model has its limits. Factors such as the rapid advancement of digital technology, diverse legislative landscapes across different countries, and industry pressures to minimize compliance costs have led to a trend of diversification and competitiveness in global data legislation [8].

2. International Consensus on Data Protection in the Digital Era.

In the rapidly evolving digital landscape, there are three discernible international trends in data protection and utilization. This section explores these trends and provides comprehensive examples of legislation and practices that epitomize them.

2.1. Balancing Personal Data Protection and Data Value Utilization

The dynamic interplay between data value optimization and personal data preservation underscores the multifaceted nature of data governance in the digital era. The advent of the digital economy has rendered data a valuable asset, fueling economic growth and innovation. However, the ubiquity of personal data usage has engendered concerns about privacy and data protection. Achieving a delicate equilibrium between data value utilization and safeguarding personal data has emerged as a pressing challenge for policymakers worldwide.

The General Data Protection Regulation (GDPR) enacted by the European Union serves as an exemplary legal instrument in striking this balance. This landmark legislation, characterized by its stringent provisions, ensures transparency, consent, and accountability in the management of personal data. By instilling confidence in individuals that their personal data is gathered, stored, and utilized securely and legitimately, the GDPR has set a benchmark for data protection regulations globally.

Concurrently, the United States has witnessed the evolution of privacy legislation that endeavors to reconcile the interests of diverse stakeholders. Legislative initiatives in the U.S. have sought to accommodate the concerns of individuals, commercial entities, governmental agencies, law enforcement authorities, and national security services, orchestrating a delicate balancing act. This dynamic process reflects the intricate data protection landscape within an evolving digital ecosystem.

2.2. Promoting the Sharing and Utilization of Public Data

The sharing and utilizing of public data hold immense potential in informing evidence-based policymaking, optimizing resource allocation, and fostering societal advancement. Encouraging the widespread dissemination and effective exploitation of public data has become a global imperative to drive innovation and facilitate informed decision-making.

An illuminating example arises from the city of Cascais in Portugal, where the integration of data from diverse municipal agencies into a centralized command center has revolutionized urban operations. This innovative approach has bolstered the efficiency of mobility management, construction projects, waste management systems, law enforcement strategies, and emergency response mechanisms.

DOI: 10.54254/2753-7048/44/20230095

Moreover, initiatives such as Finland's Carbon Neutral Tourism project underscore the pivotal role of data collaboration within specific industries. By leveraging the synergistic potential of data sharing and analysis, this project strives to enhance energy efficiency in the tourism sector and expedite the transition toward carbon neutrality [12].

To effectively promote the sharing and utilization of public data, paramount importance must be accorded to the public welfare of data. Augmenting data mobility, fostering transparency in data acquisition and use, and cultivating user trust are pivotal steps in nurturing a virtuous cycle of data utilization, ultimately culminating in tangible societal benefits.

2.3. Data Localization and Establishing Jurisdictional Control over Overseas Data

The intricate complexities surrounding data governance in an increasingly interconnected world have instigated explorations into two key mechanisms: data localization and jurisdictional control over overseas data. These measures aim to address the challenges inherent in cross-border data flows while ensuring compliance with robust data protection regulations.

Countries like China and Russia have enacted legislation mandating data localization to safeguard their citizens' data and fortify cybersecurity measures. For instance, the Chinese Cyber Security Law mandates that operators of critical information infrastructure store personal information and crucial data within the borders of China, subject to security evaluations conducted by the government [13]. Similarly, Russia's law No. 242FZ mandates the physical localization of data pertaining to Russian citizens within the country when conducting business.

Furthermore, mechanisms for establishing jurisdictional control over overseas data have emerged, as demonstrated by the extraterritorial reach of the GDPR. The GDPR asserts jurisdiction over entities that handle the personal data of EU residents, regardless of their physical location. This extension of jurisdiction aims to ensure consistent protection of personal data, even when it is transferred to jurisdictions outside the EU.

There are also other factors that contribute to the implicit export of law. The "Brussels effect," a concept encompassing the indirect influence of EU data protection standards on global legislation, plays a significant role in shaping implicit legal outputs [14,15]. Additionally, private legal transplantation, wherein multinational enterprises act as conduits for legal homogenization, further contributes to disseminating data protection principles across borders [14].

3. Global Challenges to Regulation of Data Flows and PrESERVATION of Personal Data

The increasing globalization of data flows, and the need to protect personal data present significant challenges for regulators worldwide. In this section, we will explore the obstacles encountered in providing extraterritorial effects in data protection regulation and gain a deeper understanding of the legitimacy of extraterritorial claims and the complexities involved in regulating data flows and protecting personal data.

3.1. Challenges to the Provision of Extraterritorial Effect

The provision of extraterritorial effects in data protection regulation encounters significant challenges rooted in the limitations of state sovereignty and non-interference [16]. When assessing the legitimacy of claims related to the extraterritorial reach of data protection regulations, it becomes essential to consider the most authoritative sources of international law outlined in Article 38 of the Statute of the International Court of Justice (ICJ). These sources include "international conventions ... establishing rules expressly recognized by the contesting states; international custom, as evidence of a general practice accepted as law; (and) the general principles of law recognized by civilized nations" [16].

DOI: 10.54254/2753-7048/44/20230095

In the case of Eva Glawischnig-Piesczek v Facebook, the Court emphasized that EU law did not preclude injunctions with worldwide effects (Case C-18/18, EU:C:2019:821). However, it also referred to the need to consider "rules applicable at the international level" when imposing such global injunctions. These international rules, which Member States' courts must take into account, provide additional context for evaluating the legitimacy of extraterritorial claims in data protection regulation.

The Data Protection Directive (DPD) and the General Data Protection Regulation (GDPR) were introduced to establish a dedicated regime for the change of personal data from the EU to third countries, as well as to international organizations (DPD, GDPR). These regulations refined and extended the framework for protecting personal data beyond the EU borders. However, questions have been raised regarding the logic and rationale of the DPD and GDPR since their inception [17,18]. The primary motivation behind these regulations appears to be anti-circumvention, aiming to prevent the change of personal data from the EU to other countries without adequate safeguards [6,17].

When examining the legitimacy of extraterritorial claims, it is vital to consider international conventions that establish rules explicitly recognized by the contesting states. These conventions form the foundation for evaluating the legality and enforceability of extraterritorial measures. Furthermore, international customs provide evidence of widely accepted practices that are considered legally binding. Taking these factors into account, the legitimacy of extraterritorial claims in data protection regulation can be evaluated by thoroughly examining provisions within international conventions, established customary practices, and the acknowledgment of general principles of law by civilized nations. Policymakers should carefully assess these elements to strike a nuanced balance between the imperative of safeguarding personal data and upholding the principles of national sovereignty and non-interference.

3.2. The Benefit Orientation of Enterprises Makes the Brussels Effect Limited

The Brussels Effect posits that adopting globally unified standards is more advantageous than complying with multiple regulatory frameworks. Enterprises, driven by profit-oriented motives, often seek to minimize compliance costs and maximize their global market reach. However, the effectiveness of the Brussels Effect, which refers to the extraterritorial impact of EU regulations, is based on the concept of unilateral regulatory globalization [19] and is actually influenced by various factors, including international policies and technological progress.

International policies play a significant role in shaping the practical impact of the Brussels Effect on enterprises operating in multiple jurisdictions. While the EU's regulatory approach aims to set high standards for data protection, other countries may adopt different approaches based on their unique legal frameworks, cultural values, and geopolitical considerations. This divergence in regulatory approaches creates challenges for multinational enterprises seeking to comply simultaneously with European data laws and the data laws of other jurisdictions.

Moreover, Technological progress further complicates the reach and effectiveness of the Brussels Effect. The internet and digital infrastructure enable global interconnection, facilitating the seamless flow of information across borders. However, this interconnectedness also raises concerns regarding data preservation and privacy. The advent of emerging technologies, including artificial intelligence, big data analytics, and blockchain, presents novel challenges in ensuring the preservation of personal data and upholding privacy rights. These technologies introduce unprecedented complexities that require careful attention to mitigate potential risks and maintain a robust framework for safeguarding personal information [6,16].

In Practice, although the European Union (EU) enjoys the legitimacy of its extraterritorial claims and possesses enforcement tools for global implementation [16], concerns arise regarding the compliance records of EU data protection laws, especially when compliance is voluntary. Multinational corporations can exploit jurisdictional limitations, as exemplified by Facebook's

DOI: 10.54254/2753-7048/44/20230095

strategic relocation of users from Facebook Ireland to Facebook Inc, effectively evading the jurisdiction of the GDPR [20].

3.3. It is Difficult to Find a Perfect Solution

The provision of extraterritorial effects in data protection regulation faces challenges rooted in state sovereignty and non-interference. Assessing the legitimacy of such claims requires consideration of international law sources, including international conventions, customs, and general legal principles which are recognized by civilized nations. The Eva Glawischnig-Piesczek v Facebook case highlights the need to account for international rules when imposing global injunctions. The DPD and the GDPR aim to prevent circumvention but have faced scrutiny regarding their logic and rationale.

The benefit orientation of enterprises, influenced by international policies and technological progress, introduces limitations to the Brussels Effect. The varying regulatory approaches across jurisdictions, coupled with the rapid evolution of digital technologies, complicate compliance efforts and necessitate jurisdiction-specific differentiation. While the EU possesses tools for enforcement abroad, concerns regarding compliance records and jurisdictional limitations raise questions about the effectiveness of the Brussels Effect. Multinational corporations may strategically exploit these limitations to evade regulatory reach.

The global interconnection enabled by internet infrastructure coexists with diverse norms, laws, and values worldwide, posing challenges to establishing harmonized regulations. The possibility of using virtual private networks (VPNs) to mask one's location challenges rules based on geographic boundaries, complicating the enforcement of data protection regulations. Moreover, the rapid advancements and innovations in digital technology, such as artificial intelligence and big data analytics, bring forth new data protection and privacy challenges.

4. Conclusion

The global transition towards data protection and privacy legislation signifies a growing acknowledgment of the risks and obstacles presented by the widespread collection of personal data in the digital era [10]. Nations across the globe have acknowledged the necessity of striking a harmonious equilibrium between the advantages of data-driven economies and the safeguarding of individuals' privacy. This acknowledgment has resulted in adopting diverse legislative frameworks to address these concerns.

The GDPR in the EU, the CCPA in the US, and the LGPD are prominent examples of comprehensive data protection legislation. These regulations emphasize individuals' consent, control, and understanding of how their data is processed, setting a benchmark for global data protection standards.

However, the regulation of data flows and the preservation of personal data present significant challenges. The handling and management of personal data have become central to the functioning of digital platforms, raising concerns about data exploitation and misuse [3]. The concept of "surveillance capitalism" has gained attention, highlighting the secret extraction and manipulation of human data for economic gain. Achieving a delicate equilibrium between data value utilization and safeguarding personal data has emerged as a pressing challenge for policymakers worldwide [21].

The governance of data in an interconnected world requires international cooperation and the development of common frameworks and standards [6]. Continuous evaluation and updates of regulatory frameworks, enhanced enforcement mechanisms, public awareness and education, and multistakeholder collaboration are recommended to address the evolving landscape of data protection and privacy.

DOI: 10.54254/2753-7048/44/20230095

In conclusion, addressing the complexities of data protection in the digital era requires ongoing efforts to strike a balance between data value utilization and privacy protection. By implementing international cooperation, regular evaluation and updates, enhanced enforcement mechanisms, public awareness and education, and multistakeholder collaboration, policymakers can navigate the challenges and foster a global environment that upholds individuals' rights while enabling responsible data-driven innovation.

References

[1] *Statista, 'Google's annualized advertising ARPU from the 1st quarter of 2012 to the 1st quarter of 2014 (in US dollars)', 2015. http://www.statista.com/statistics/306570/google-annualized-advertising-arpu/.*

[2] *S. Zuboff, The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019[M]. Profile books, 2019.*

[3] *C. Cadwalladr, & E. Graham-Harrison, Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach, The Guardian, 2018.*

[4] *M. Anna et al., Global Public Perceptions of Genomic Data Sharing: What Shapes the Willingness to Donate DNA and Health Data? The American Journal of Human Genetics, vol. 107, Issue 4, 2020, pp 743-752. DOI: https://doi.org/10.1016/j.ajhg.2020.08.023.*

[5] *Federal Trade Commission v. Equifax, Inc., 1:19-cv-03297-TWT. 2019. https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc*

[6] *P. Craig and Gráinne de Búrca (eds), The Evolution of European Data Law, The Evolution of EU Law (OUP, 3rd edn), 2021, pp. 902-936. SSRN: https://ssrn.com/abstract=3762971 or http://dx.doi.org/10.2139/ssrn.3762971*

[7] *N. Perlroth, All 3 Billion Yahoo Accounts Were Affected by 2013 Attack, The New York Times, 2017. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html*

[8] *Art 3(1), GDPR: the various prongs of the GDPR's scope of application all require some connection to the EU: when firms are established in the EU, they have to comply with the GDPR anywhere.*

[9] *N. Perlroth et al., Marriott Hacking Exposes Data of Up to 500 Million Guests, The New York Times, 2018. https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html*

[10] *UNCTAD, Data Protection and Privacy Legislation Worldwide, 2021, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*

[11] *Facebook Ireland and Schrems, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, C-311/18, 16. 07. 2020.*

[12] *6Aika, Results: Carbon Neutral Tourism, 2022, https://6aika.fi/en/project/results-carbon-neutral-tourism/*

[13] *E. W. Huang, China: An Overview Of China's New Cybersecurity Law, Mondaq, 2019. https://www.mondaq.com/china/privacy-protection/714616/an-overview-of-china39s-new-cybersecurity-law*

[14] *F. Tomaso, Private Legal Transplant: Multinational Enterprises as Proxies of Legal Homogenisation, Transnational Legal Theory, Vol. 5, No. 1, 2014, p. 21.*

[15] *A. Bradford, The Brussels Effect - How the European Union Rules the World, Oxford University Press, 2020. ISBN: 9780-1-900 88583*

[16] *Adèle Azzi, The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation, JIPITEC, vol. 9, 2018, pp. 126-137. URL: http://nbn-resolving.de/urn:nbn:de:0009-29-47231*

[17] *C. Kuner, Transborder Data Flows and Data Privacy Law, Oxford University Press, vol. xix, 2013. p. 285.*

[18] *W. K. Hon, Data Localization Laws and Policy, Edward Elgar Publishing, 2017.*

[19] *B. Anu, Exporting Standards: The Externalization of the EU's Regulatory Power via Markets, International Review of Law & Economics, Vol. 42, 2015, p. 158.*

[20] *A Hern, Facebook moves 1.5bn users out of reach of new European privacy law, The Guardian, 2018. https://perma.cc/5MKD-LA6C*

[21] *S Quach et al., Digital technologies: tensions in privacy and data, 2022, J Acad Mark Sci, vol. 50, pp. 1299-1323. DOI: 10.1007/s11747-022-00845-y.*